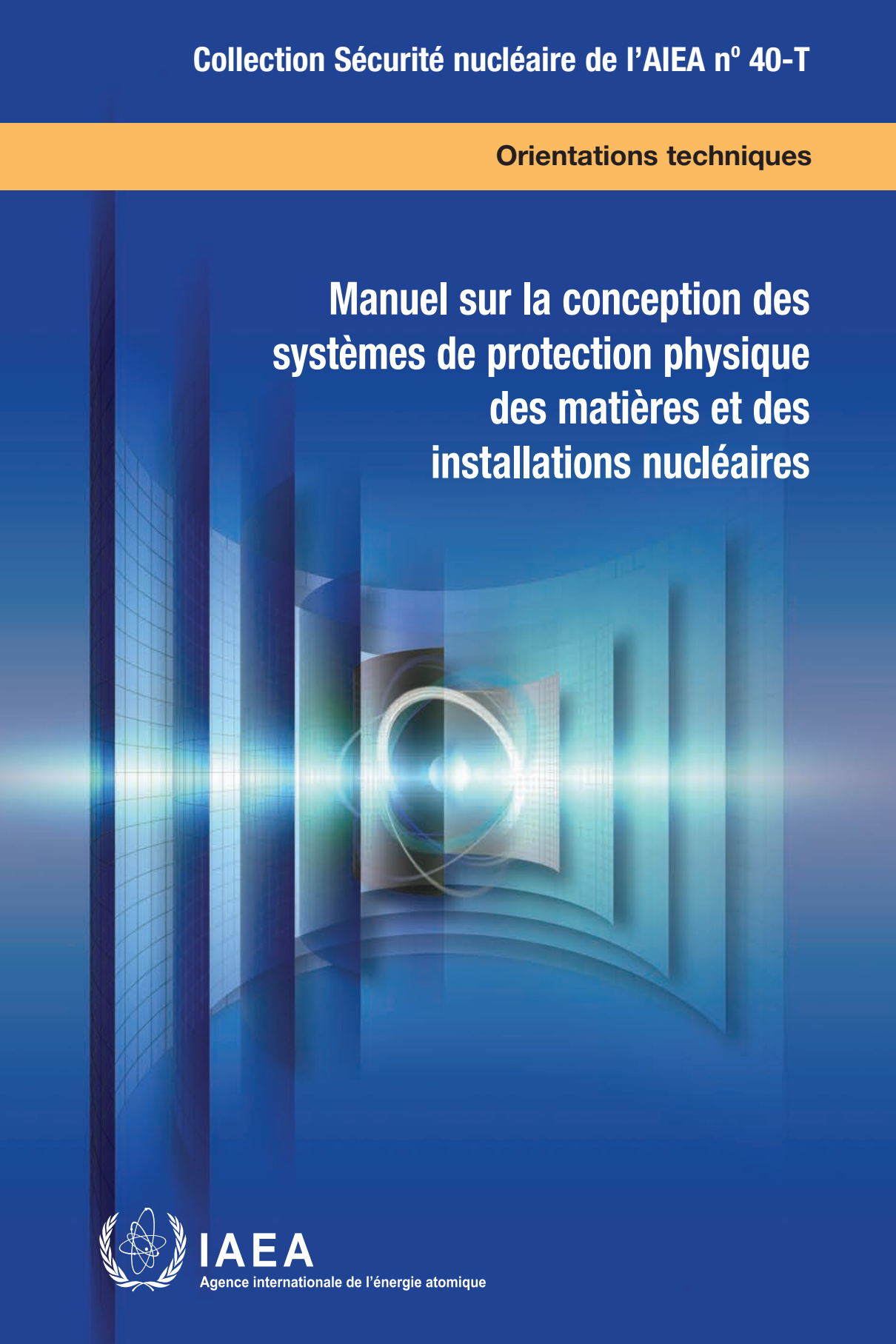
Collection Sécurité nucléaire de l'AIEA n° 40-T

Orientations techniques

Manuel sur la conception des systèmes de protection physique des matières et des installations nucléaires



IAEA
Agence internationale de l'énergie atomique

COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA

Les questions de sécurité nucléaire liées à la prévention, la détection et l'intervention en cas d'actes criminels ou d'actes non autorisés délibérés, mettant en jeu ou visant des matières nucléaires, d'autres matières radioactives, des installations associées ou des activités associées, sont traitées dans la **collection Sécurité nucléaire de l'AIEA**. Ces publications sont conformes aux instruments internationaux relatifs à la sécurité nucléaire, notamment à la Convention sur la protection physique des matières nucléaires telle qu'amendée, à la Convention internationale pour la répression des actes de terrorisme nucléaire, aux résolutions 1373 et 1540 du Conseil de sécurité des Nations Unies et au Code de conduite sur la sûreté et la sécurité des sources radioactives, et elles les complètent.

CATÉGORIES DANS LA COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA

Les publications de la collection Sécurité nucléaire de l'AIEA se répartissent entre les catégories suivantes :

- Les **Fondements de la sécurité nucléaire**, qui portent sur les objectifs et les éléments essentiels d'un régime national de sécurité nucléaire. Ils servent de base à l'élaboration des recommandations en matière de sécurité nucléaire.
- Les **Recommandations en matière de sécurité nucléaire**, qui prévoient des mesures que les États devraient prendre pour établir et maintenir un régime national de sécurité nucléaire efficace conforme aux Fondements de la sécurité nucléaire.
- Les **Guides d'application**, qui fournissent des orientations sur les moyens dont disposent les États Membres pour appliquer les mesures prévues dans les Recommandations en matière de sécurité nucléaire. À ce titre, ils s'intéressent à la mise en application des recommandations relatives à de grands domaines de la sécurité nucléaire.
- Les **Orientations techniques**, qui fournissent des orientations sur des sujets techniques particuliers et complètent les orientations figurant dans les Guides d'application. Elles exposent de manière détaillée comment mettre en œuvre les mesures nécessaires.

RÉDACTION ET EXAMEN

Le Secrétariat de l'AIEA, des experts d'États Membres (qui aident le Secrétariat à rédiger les publications) et le Comité des orientations sur la sécurité nucléaire (NSGC), qui examine et approuve les projets de publications, participent à l'élaboration et à l'examen des publications de la collection Sécurité nucléaire. Selon qu'il convient, des réunions techniques à participation non limitée sont organisées pendant la rédaction afin que des spécialistes d'États Membres et d'organisations internationales concernées puissent examiner le projet de texte et en discuter. En outre, pour faire en sorte que ces projets soient examinés de façon approfondie et largement acceptés au niveau international, le Secrétariat les soumet à tous les États Membres, qui disposent de 120 jours pour les examiner officiellement.

Pour chaque publication, le Secrétariat prépare, et le NSGC approuve, à des étapes successives du processus de préparation et d'examen, ce qui suit :

- un aperçu et un plan de travail décrivant la publication nouvelle ou révisée prévue, son objectif prévu, sa portée et son contenu ;
- un projet de publication à soumettre aux États Membres pour observations pendant la période de consultation de 120 jours ;
- un projet de publication définitif prenant en compte les observations faites par les États Membres.

Le processus d'élaboration et d'examen des publications de la collection Sécurité nucléaire de l'AIEA tient compte des considérations de confidentialité et du fait que la sécurité nucléaire est indissociable des problèmes généraux et particuliers concernant la sécurité nationale.

La prise en compte, dans le contenu technique des publications, des normes de sûreté et des activités de garanties de l'AIEA se rapportant à la sécurité constitue une préoccupation sous-jacente. En particulier, les publications de la collection Sécurité nucléaire qui traitent de domaines dans lesquels il existe des interfaces avec la sûreté, appelées documents d'interface, sont examinées à chaque étape susmentionnée par les Comités des normes de sûreté nucléaire compétents et par le NSGC.

MANUEL SUR LA CONCEPTION DES SYSTÈMES DE PROTECTION PHYSIQUE DES MATIÈRES ET DES INSTALLATIONS NUCLÉAIRES

Les États ci-après sont Membres de l'Agence internationale de l'énergie atomique :

AFGHANISTAN
AFRIQUE DU SUD
ALBANIE
ALGÉRIE
ALLEMAGNE
ANGOLA
ANTIGUA-ET-BARBUDA
ARABIE SAOUDITE
ARGENTINE
ARMÉNIE
AUSTRALIE
AUTRICHE
AZERBAÏDJAN
BAHAMAS
BAHREÏN
BANGLADESH
BARBADE
BÉLARUS
BELGIQUE
BELIZE
BÉNIN
BOLIVIE, ÉTAT PLURINATIONAL DE
BOSNIE-HERZÉGOVINE
BOTSWANA
BRÉSIL
BRUNÉI DARUSSALAM
BULGARIE
BURKINA FASO
BURUNDI
CABO VERDE
CAMBODGE
CAMEROUN
CANADA
CHILI
CHINE
CHYPRE
COLOMBIE
COMORES
CONGO
CORÉE, RÉPUBLIQUE DE
COSTA RICA
CÔTE D'IVOIRE
CROATIE
CUBA
DANEMARK
DJIBOUTI
DOMINIQUE
ÉGYPTE
EL SALVADOR
ÉMIRATS ARABES UNIS
ÉQUATEUR
ÉRYTHRÉE
ESPAGNE
ESTONIE
ESWATINI
ÉTATS-UNIS D'AMÉRIQUE
ÉTHIOPIE
FÉDÉRATION DE RUSSIE
FIDJI
FINLANDE
FRANCE
GABON
GAMBIE
GÉORGIE
GHANA
GRÈCE
GRENADE
GUATEMALA
GUINÉE
GUYANA
HAÏTI
HONDURAS
HONGRIE
ÎLES COOK
ÎLES MARSHALL
INDE
INDONÉSIE
IRAN, RÉP. ISLAMIQUE D'
IRAQ
IRLANDE
ISLANDE
ISRAËL
ITALIE
JAMAÏQUE
JAPON
JORDANIE
KAZAKHSTAN
KENYA
KIRGHIZISTAN
KOWEÏT
LESOTHO
LETTONIE
LIBAN
LIBÉRIA
LIBYE
LIECHTENSTEIN
LITUANIE
LUXEMBOURG
MACÉDOINE DU NORD
MADAGASCAR
MALAISIE
MALAWI
MALI
MALTE
MAROC
MAURICE
MAURITANIE
MEXIQUE
MONACO
MONGOLIE
MONTÉNÉGRO
MOZAMBIQUE
MYANMAR
NAMIBIE
NÉPAL
NICARAGUA
NIGER
NIGÉRIA
NORVÈGE
NOUVELLE-ZÉLANDE
OMAN
OUGANDA
OUZBÉKISTAN
PAKISTAN
PALAOS
PANAMA
PAPOUASIE-NOUVELLE-GUINÉE
PARAGUAY
PAYS-BAS, ROYAUME DES
PÉROU
PHILIPPINES
POLOGNE
PORTUGAL
QATAR
RÉPUBLIQUE ARABE SYRIENNE
RÉPUBLIQUE CENTRAFRICAINE
RÉPUBLIQUE DE MOLDOVA
RÉPUBLIQUE DÉMOCRATIQUE DU CONGO
RÉPUBLIQUE DÉMOCRATIQUE POPULAIRE LAO
RÉPUBLIQUE DOMINICAINE
RÉPUBLIQUE TCHÈQUE
RÉPUBLIQUE-UNIE DE TANZANIE
ROUMANIE
ROYAUME-UNI DE GRANDE-BRETAGNE ET D'IRLANDE DU NORD
RWANDA
SAINTE-LUCIE
SAINT-KITTS-ET-NEVIS
SAINT-MARIN
SAINT-SIÈGE
SAINT-VINCENT-ET-LES GRENADINES
SAMOA
SÉNÉGAL
SERBIE
SEYCHELLES
SIERRA LEONE
SINGAPOUR
SLOVAQUIE
SLOVÉNIE
SOMALIE
SOUDAN
SRI LANKA
SUÈDE
SUISSE
TADJIKISTAN
TCHAD
THAÏLANDE
TOGO
TONGA
TRINITÉ-ET-TOBAGO
TUNISIE
TÜRKİYE
TURKMÉNISTAN
UKRAINE
URUGUAY
VANUATU
VENEZUELA, RÉP. BOLIVARIENNE DU
VIET NAM
YÉMEN
ZAMBIE
ZIMBABWE

Le Statut de l'Agence a été approuvé le 23 octobre 1956 par la Conférence sur le Statut de l'AIEA, tenue au Siège de l'Organisation des Nations Unies, à New York ; il est entré en vigueur le 29 juillet 1957. L'Agence a son siège à Vienne. Son principal objectif est « de hâter et d'accroître la contribution de l'énergie atomique à la paix, la santé et la prospérité dans le monde entier ».

COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA Nº 40-T

MANUEL SUR LA CONCEPTION DES SYSTÈMES DE PROTECTION PHYSIQUE DES MATIÈRES ET DES INSTALLATIONS NUCLÉAIRES

ORIENTATIONS TECHNIQUES

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE, 2025

DROIT D'AUTEUR

Section d'édition
Agence internationale de l'énergie atomique
Centre international de Vienne
B.P. 100
1400 Vienne (Autriche)
Téléphone : +43 1 2600 22529 ou 22530
Courriel : sales.publications@iaea.org
www.iaea.org/fr/publications

Imprimé par l'AIEA en Autriche
Janvier 2025
STI/PUB/1875

MANUEL SUR LA CONCEPTION DES SYSTÈMES DE PROTECTION PHYSIQUE DES MATIÈRES ET DES INSTALLATIONS NUCLÉAIRES
AIEA, VIENNE, 2025
STI/PUB/1875
ISBN 978-92-0-210923-0 (imprimé) | ISBN 978-92-0-210423-5 (pdf) | ISBN 978-92-0-210523-2 (ePub)
ISSN 2520-6931

AVANT-PROPOS

de Rafael Mariano Grossi
Directeur général

La collection Sécurité nucléaire de l'AIEA fournit des orientations faisant l'objet d'un consensus international sur tous les aspects de la sécurité nucléaire afin d'aider les États à honorer leurs responsabilités en la matière. L'AIEA établit et tient à jour ces orientations dans le cadre de sa mission centrale d'assistance et de coordination internationales concernant la sécurité nucléaire.

Lancée en 2006, la collection Sécurité nucléaire est actualisée en permanence par l'AIEA, en coopération avec des experts des États Membres. En tant que Directeur général, j'entends veiller à ce que l'AIEA entretienne et améliore cet ensemble intégré, complet et cohérent de publications de qualité adaptées à l'utilisateur, aux réalités de l'époque et aux besoins en matière de sécurité. L'utilisation adéquate de ces orientations dans le cadre des applications de la science et de la technologie nucléaires devrait permettre d'atteindre un niveau élevé de sécurité nucléaire et établir la confiance nécessaire à l'utilisation continue de la technologie nucléaire pour le bien de tous.

C'est aux pays qu'il appartient de garantir la sécurité nucléaire. Les publications de la collection Sécurité nucléaire de l'AIEA complètent les instruments juridiques internationaux en la matière et servent de référence mondiale pour aider les parties à honorer leurs obligations. Bien qu'elles ne soient pas juridiquement contraignantes pour les États Membres, les orientations qu'elles contiennent sont largement appliquées. Elles sont devenues une référence indispensable et un dénominateur commun pour la grande majorité des États Membres qui les appliquent dans leur réglementation nationale pour améliorer la sécurité nucléaire des centrales nucléaires, des réacteurs de recherche et des installations du cycle du combustible ainsi que des applications nucléaires en médecine, dans l'industrie, dans l'agriculture et dans la recherche.

Les orientations de la collection Sécurité nucléaire de l'AIEA se basent sur l'expérience pratique des États Membres et font l'objet d'un consensus international. La participation des membres du Comité des orientations sur la sécurité nucléaire et d'autres personnes est particulièrement importante, et je suis reconnaissant à tous ceux qui, par leurs connaissances et leurs compétences, contribuent à l'élaboration de ces orientations.

L'AIEA utilise également les orientations de la collection Sécurité nucléaire lorsqu'elle apporte une assistance aux États Membres dans le cadre de missions d'examen et de services consultatifs, aidant ainsi ces États Membres à les appliquer et facilitant l'échange de données d'expérience et d'idées

utiles. Les informations en retour sur ces missions et services, de même que les enseignements tirés des événements et l'expérience relative à l'utilisation et à l'application des orientations sur la sécurité, sont pris en compte lors de la révision périodique de ces dernières.

Je suis convaincu que les orientations de la collection Sécurité nucléaire de l'AIEA et leur application contribuent de manière inestimable à assurer un niveau élevé de sécurité nucléaire dans le cadre de l'utilisation de la technologie nucléaire. J'encourage tous les États Membres à les promouvoir et à les appliquer et à collaborer avec l'AIEA pour en maintenir la qualité, aujourd'hui comme demain.

NOTE DE L'ÉDITEUR

Les États ne sont pas tenus d'appliquer les orientations publiées dans la collection Sécurité nucléaire de l'AIEA, mais elles peuvent les aider à s'acquitter de leurs obligations en vertu d'instruments juridiques internationaux et assumer leurs responsabilités en matière de sécurité nucléaire au sein de l'État. Les orientations énoncées au conditionnel ont pour but de présenter des bonnes pratiques internationales et de manifester un consensus international selon lequel il est nécessaire pour les États de prendre les mesures recommandées ou des mesures équivalentes.

Les termes relatifs à la sécurité ont le sens donné dans la publication où ils figurent, ou dans les orientations de niveau supérieur que la publication soutient. Autrement, les termes ont le sens qui leur est communément donné.

Un appendice est réputé faire partie intégrante de la publication. Les informations données dans un appendice ont le même statut que le corps du texte. Les annexes ont pour objet de donner des exemples concrets ou des précisions ou explications. Elles ne sont pas considérées comme faisant partie intégrante du texte principal.

Bien que l'exactitude des informations contenues dans la présente publication ait fait l'objet d'un soin particulier, ni l'AIEA ni ses États Membres n'assument une quelconque responsabilité pour les conséquences éventuelles de leur utilisation.

L'emploi d'appellations particulières pour désigner des pays ou des territoires n'implique de la part de l'éditeur, l'AIEA, aucune prise de position quant au statut juridique de ces pays ou territoires, ou de leurs autorités et institutions, ni quant au tracé de leurs frontières.

La mention de noms de sociétés ou de produits particuliers (qu'ils soient ou non signalés comme marques déposées) n'implique aucune intention d'empiéter sur des droits de propriété et ne doit pas être considérée non plus comme valant approbation ou recommandation de la part de l'AIEA.

TABLE DES MATIÈRES

1. INTRODUCTION

CONTEXTE

1.1. La protection physique des matières nucléaires et des installations nucléaires est une composante importante du régime de sécurité nucléaire des États qui possèdent des matières et des installations de ce type. La publication n° 13 de la collection Sécurité nucléaire de l'AIEA, intitulée *Recommandations de sécurité nucléaire sur la protection physique des matières nucléaires et des installations nucléaires* (INFCIRC/225/Révision 5) [1], fournit aux États des recommandations devant leur permettre d'instituer ou de renforcer, de mettre en œuvre et de maintenir une protection physique efficace. La publication n° 27-G de la collection Sécurité nucléaire de l'AIEA, intitulée *Protection physique des matières nucléaires et des installations nucléaires (Guide d'application de la publication INFCIRC/225/Révision 5)* [2], donne des orientations sur la manière d'appliquer ces recommandations.

1.2. La Convention sur la protection physique des matières nucléaires [3] propose un cadre visant à assurer la protection physique des matières nucléaires employées à des fins pacifiques pendant leur transport international. Entré en vigueur le 8 mai 2016, l'amendement de 2005 à la Convention sur la protection physique des matières nucléaires [4] étend le champ d'application de celle-ci [3] aux installations nucléaires, aux matières nucléaires utilisées à des fins pacifiques en cours d'utilisation, en entreposage et en cours de transport sur le territoire national, et à leur protection contre les actes de sabotage. La référence [1] donne aux États parties des orientations sur le respect de leurs obligations au titre de la Convention [3] et de son amendement [4].

1.3. La présente publication met à jour le contenu d'un manuel sur la protection physique des matières et des installations nucléaires qui a été publié en distribution restreinte[1]. Elle contient des informations dérivées du cours international sur la protection physique des installations et matières nucléaires, préparé et dispensé par les Laboratoires nationaux Sandia.

---

[1] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, *Manuel sur la protection physique des matières et des installations nucléaires*, IAEA-TECDOC-1276, AIEA, Vienne (2002).

OBJECTIF

1.4. La présente publication vise à donner des orientations complètes et détaillées aux États, aux autorités compétentes et aux exploitants pour les aider à appliquer les recommandations faites dans la référence [1] et les orientations fournies dans la référence [2] aux fins de la mise en place d'un système efficace de protection physique des matières nucléaires en cours d'utilisation et en entreposage et des installations nucléaires. Elle fournit de plus amples précisions techniques sur la manière de concevoir et d'évaluer un système de protection physique (SPP), en ce qui concerne le choix et l'intégration des mesures (y compris des équipements) de protection physique appropriées et efficaces. Elle est destinée à servir de document de référence général aux utilisateurs, tout en leur donnant accès à des orientations complémentaires portant sur des sujets précis.

CHAMP D'APPLICATION

1.5. La présente publication porte sur les systèmes de protection physique des matières nucléaires en cours d'utilisation et en entreposage et des installations nucléaires contre l'enlèvement non autorisé de matières nucléaires et le sabotage de matières et d'installations nucléaires. Les présentes orientations techniques ne traitent pas des aspects infrastructurels d'un régime national de sécurité nucléaire liés à la protection physique, tels que le cadre législatif et réglementaire ou les institutions et organismes chargés dans l'État de mettre ce cadre en œuvre. Ces aspects sont abordés dans les publications de la collection Sécurité nucléaire de l'AIEA n° 19, intitulée *Établissement de l'infrastructure de sécurité nucléaire pour un programme électronucléaire* [5], et n° 29-G, intitulée *Developing Regulations and Associated Administrative Measures for Nuclear Security* (Élaboration d'une réglementation et de mesures administratives associées en matière de sécurité nucléaire) [6]. Ces orientations techniques ne traitent pas non plus en détail des mesures de sécurité qui complètent les systèmes de protection physique, telles que les mesures de sécurité informatique ou la comptabilité et le contrôle des matières nucléaires. Ces mesures font l'objet d'autres orientations, telles que celles dont rendent compte les publications de la collection Sécurité nucléaire de l'AIEA n° 17, *La sécurité informatique dans les installations nucléaires* [7] ; n° 25-G, *Utilisation de la comptabilité et du contrôle des matières nucléaires à des fins de sécurité nucléaire dans les installations* [8], et n° 32-T, *Mise en place d'un système de contrôle des matières nucléaires, à des fins de sécurité nucléaire, encadrant leur utilisation, leur entreposage et leur déplacement dans les installations* [9].

1.6. Les orientations techniques figurant dans la présente publication sont applicables à tous les stades de la durée de vie d'une installation nucléaire, mais portent principalement sur la conception d'un SPP et la sélection de ses équipements, ainsi que sur les stades opérationnels de la conception, de la mise en œuvre et du maintien d'un tel système. Elles décrivent les équipements et les fonctions d'un SPP destinés à prévenir les événements de sécurité nucléaire, à les détecter et à intervenir face à ces derniers. Lorsque cela est nécessaire, elles renvoient à d'autres orientations portant sur des sujets précis. Par ailleurs, elles donnent des orientations générales sur l'évaluation d'un SPP, dans l'attente de la mise au point d'orientations spécifiques.

1.7. Bien que mis au point pour des matières et des installations nucléaires, les concepts et orientations présentés ici sont également applicables aux matières radioactives et aux installations et activités associées.

1.8. L'un des objectifs des mesures de comptabilité et de contrôle des matières nucléaires consiste à prévenir les menaces que peuvent représenter des agresseurs d'origine interne susceptibles de tenter un enlèvement non autorisé de matières nucléaires ou un acte de sabotage contre des matières et installations nucléaires, comme indiqué dans les références [8, 9] et dans la publication n° 8-G (Rev. 1) de la collection Sécurité nucléaire de l'AIEA, intitulée *Preventive and Protective Measures against Insider Threats* (Mesures de prévention et de protection contre les menaces internes) [10]. La comptabilité et le contrôle des matières nucléaires comportent des mesures de contrôle administratif et technique. Les mesures techniques relèvent notamment des technologies destinées à assurer une protection physique, telles que les systèmes de surveillance vidéo et les alarmes de détection de rayonnements. La présente publication décrit les technologies, mais ne fournit pas d'informations concernant les technologies utilisées uniquement à des fins de comptabilité et de contrôle des matières nucléaires, telles que les dispositifs d'indication de fraude (pour des orientations plus détaillées, voir la référence [9]).

1.9. La présente publication ne donne pas d'orientations détaillées sur :

a) une intervention menée dans une situation d'urgence nucléaire ou radiologique pouvant résulter d'un événement de sécurité nucléaire ;
b) l'atténuation ou la réduction maximale des conséquences radiologiques d'un sabotage dans une installation nucléaire (excepté lorsque des barrières physiques sont utilisées pour atténuer les conséquences d'une attaque) ;
c) la localisation et la récupération de matières nucléaires non soumises à un contrôle réglementaire ;

d) les considérations liées à la protection physique dans le choix du site d'une installation nucléaire.

1.10. En outre, la présente publication ne traite pas de la sécurité des matières durant le transport, question qui fait l'objet des publications de la collection Sécurité nucléaire de l'AIEA n° 26-G, *Sécurité des matières nucléaires en cours de transport* [11], et n° 9-G (Rev.1), *Sécurité des matières radioactives en cours de transport* [12].

STRUCTURE

1.11. La section 2 de la présente publication donne des orientations sur les principales fonctions et mesures de protection qui constituent normalement un SPP. La section 3 décrit le processus de conception, d'élaboration et de mise en œuvre d'un SPP. La section 4 donne des orientations détaillées sur les mesures de protection physique, notamment les diverses technologies, les divers équipements et les diverses procédures d'appui utilisés en matière de prévention, de détection, de retardement et d'intervention. La section 5 porte sur l'intervention du SPP, tandis que la section 6 est consacrée aux réseaux et aux systèmes d'appui, et la section 7 à l'adoption de technologies nouvelles et émergentes. La section 8 décrit les essais périodiques des équipements et les différents types d'essais, tels que les essais de réception et d'opérabilité, les essais fonctionnels et les essais de maintenance et d'étalonnage. La section 9 examine l'évaluation d'un SPP, la section 10 présente une vue d'ensemble de l'analyse d'un SPP et la section 11 donne des orientations sur les systèmes de gestion pour la sécurité nucléaire. L'appendice donne un exemple d'évaluation des besoins et d'analyse des prescriptions aux fins de l'adoption d'une technologie nouvelle.

2. FONCTIONS PRINCIPALES D'UN SYSTÈME DE PROTECTION PHYSIQUE

2.1. La présente section décrit les fonctions principales d'un SPP et la manière dont les diverses mesures et les divers sous-systèmes de protection physique (décrits dans les sections 4 à 6) s'articulent entre eux pour créer un SPP complet qui soit dissuasif et capable de remplir les fonctions principales de détection, de retardement et d'intervention afin d'offrir une protection contre les tentatives

d'enlèvement non autorisé ou de sabotage de la part d'agresseurs. La référence [2] présente des orientations sur les fonctions principales du SPP.

2.2. Un SPP est un système intégré de mesures de détection, de retardement et d'intervention qui devrait être efficace contre l'enlèvement non autorisé et le sabotage [1]. Il devrait comprendre des personnes, des procédures et des équipements pour fournir une défense en profondeur, selon une approche graduée, faire face aux menaces répertoriées dans l'énoncé de la menace applicable et offrir une protection contre l'enlèvement non autorisé et le sabotage. La publication nº 10-G (Rev. 1) de la collection Sécurité nucléaire de l'AIEA intitulée *Évaluation de la menace contre la sécurité nucléaire nationale, menaces de référence et énoncés de la menace représentative* [13] donne des orientations sur l'évaluation de la menace et la menace de référence.

2.3. Un SPP comprend des capteurs de détection d'intrusions intérieurs et extérieurs, des caméras pour l'évaluation, des mesures de retardement, des dispositifs de contrôle de l'accès et des mesures d'intervention. Un SPP dispose habituellement de plusieurs sous-systèmes automatisés conçus pour transmettre des informations et des images vidéo à un poste central de sécurité (PCS), où elles peuvent être utilisées par les opérateurs pour mettre en place une intervention appropriée. Le SPP devrait également prévoir un moyen sécurisé par lequel les opérateurs du PCS puissent communiquer avec les forces d'intervention sur site et hors site et les gardes puissent communiquer les uns avec les autres et avec le PCS. Le SPP intègre toutes les mesures et tous les sous-systèmes de protection physique, mais les sous-systèmes peuvent être intégrés les uns avec les autres dans le SPP ; par exemple, le système de détection d'intrusions peut être intégré avec le système de contrôle de l'accès.

DISSUASION

2.4. La dissuasion opère lorsque des agresseurs potentiels considèrent qu'une installation ne constitue pas une cible attractive et décident de ne pas l'attaquer parce qu'ils jugent la probabilité de réussite trop faible ou les risques pour eux-mêmes trop élevés.

2.5. Le cadre législatif ou réglementaire national [1] devrait prévoir des sanctions en cas d'enlèvement non autorisé ou de sabotage afin de dissuader un agresseur de tenter de commettre un tel acte.

2.6. Le maintien de la confidentialité des informations sensibles concernant le SPP pourrait dissuader des agresseurs en leur refusant l'accès à des informations clés susceptibles de les aider à tenter un enlèvement non autorisé ou un acte de sabotage. Un agresseur d'origine interne pourrait, volontairement ou non, compromettre la confidentialité de ces informations, éventuellement à l'insu de l'exploitant. Un programme d'habilitation pourrait atténuer les risques associés aux menaces d'origine interne. Le fait d'appliquer la règle des deux personnes pour l'entrée dans une zone intérieure ou une zone vitale peut être dissuasif ou faciliter la détection d'un enlèvement non autorisé ou d'un acte de sabotage.

2.7. Les autres mesures susceptibles de renforcer l'effet de dissuasion dans une installation sont notamment les suivantes :

a) Une zone de sécurité bien éclairée dotée d'un SPP pourrait donner l'impression que l'installation bénéficie d'un niveau de sécurité élevé et avoir un effet dissuasif sur un agresseur potentiel. Les concepteurs de SPP peuvent également réfléchir à la méthodologie sur laquelle repose la « prévention du crime par l'aménagement du milieu » (PCAM)[2].
b) L'utilisation stratégique des gardiens et des forces d'intervention pourrait également contribuer à la dissuasion. Par exemple, les responsables d'une installation nucléaire pourraient apprendre qu'une manifestation pacifique doit se dérouler à telle ou telle date. Étant donné que des agresseurs pourraient exploiter des manifestations pacifiques pour dissimuler un acte malveillant ou détourner l'attention de sa commission, l'exploitant peut déployer des gardiens ou des forces d'intervention supplémentaires pour créer un effet dissuasif et fournir des capacités supplémentaires de détection, de retardement et d'intervention.
c) L'organisation aléatoire de patrouilles de gardiens et de forces d'intervention, à l'intérieur comme à l'extérieur des zones d'accès limité d'une installation nucléaire, peut renforcer la dissuasion. En outre, les fouilles aléatoires, les postes de garde durcis, les tours de garde et les véhicules blindés d'intervention sur site peuvent également contribuer à la dissuasion.

2.8. Il est difficile de mesurer la dissuasion, mais l'utilisation rationnelle des mesures de protection physique pour accroître la visibilité des gardiens et des forces d'intervention tout en appliquant à leurs actions des éléments de caractère aléatoire (notamment les patrouilles) pourrait dissuader un agresseur. Toutefois, le fait qu'un SPP n'ait pas été défié par un agresseur ne devrait pas être considéré comme prouvant qu'il a eu un effet dissuasif sur ce dernier.

---

[2] Voir www.cpted.net.

DÉTECTION

2.9. La détection est un processus lié au SPP qui s'ouvre sur la perception d'un acte potentiellement malveillant ou d'un autre acte non autorisé et qui s'achève avec l'évaluation de la cause de l'alarme [1]. L'objectif est de faire en sorte que la détection intervienne aussitôt que possible.

2.10. La détection s'ouvre sur la sollicitation de capteurs, l'identification de personnes non autorisées ou d'articles interdits grâce à des mesures de contrôle de l'accès ou le signalement d'incidents suspects par les gardiens ou d'autres agents. Elle s'achève lorsque les informations initiales ont été évaluées et qu'il a été déterminé qu'elles dénotent véritablement l'existence d'une activité malveillante. La section 4 donne des orientations détaillées sur les mesures de détection, notamment les alarmes anti-intrusion, les technologies d'évaluation, les postes de sécurité, les systèmes de fouille et le contrôle de l'accès.

RETARDEMENT

2.11. Le retardement est la fonction du SPP qui vise à ralentir la progression d'un agresseur vers la cible, ce qui permet de gagner du temps pour intervenir efficacement [2]. Le retardement peut se produire avant la détection, mais seul le retardement qui a lieu après la première détection de l'acte d'un agresseur peut favoriser l'intervention. Le retardement est en principe assuré par des barrières physiques, mais il peut aussi être assuré ou augmenté par des gardiens ou des forces d'intervention. Au bout du compte, on peut venir à bout de toutes les barrières, mais la fonction de retardement est destinée à donner le temps nécessaire pour engager des mesures d'intervention avant que l'agresseur ne mène à son terme l'acte malveillant. La section 4 donne des orientations détaillées sur les barrières physiques.

INTERVENTION

2.12. L'intervention est la fonction du SPP qui vise à intercepter et à neutraliser un agresseur avant l'accomplissement d'un acte malveillant [2]. On trouvera des orientations détaillées sur l'intervention dans la section 5.

3. CONCEPTION ET ÉVALUATION D'UN SYSTÈME DE PROTECTION PHYSIQUE

3.1. Le processus de conception et d'évaluation d'un SPP devrait être systématique et, de préférence, suivre une approche basée sur l'ingénierie des systèmes. Celle-ci, qui sert à concevoir et à construire des systèmes complexes, met en jeu des processus de définition de prescriptions[3], de conception de systèmes et d'évaluation de conceptions.

3.2. L'approche basée sur l'ingénierie des systèmes repose sur des équipes de projet intégrées se composant de groupes pluridisciplinaires chargés de mettre au point et en œuvre une conception à partir des processus d'ingénierie système pertinents.

3.3. Ces processus sont décrits en détail dans des normes internationales (voir les références [14, 15]). Pour un SPP donné, il pourra être nécessaire d'utiliser une norme internationale spécifique pour le processus d'ingénierie système, des normes adoptées dans le cadre de l'industrie nucléaire nationale ou une réglementation spécifiée par l'autorité compétente, ou l'entreprise construisant ou exploitant le système pourra être autorisée à adopter sa propre variante.

3.4. La présente section décrit une proposition de méthodologie en trois phases qui utilise une approche basée sur l'ingénierie des systèmes :

a) Phase 1 : Fixer les objectifs, les prescriptions et les spécifications concernant le SPP.
b) Phase 2 : Concevoir le SPP d'une façon qui satisfasse aux objectifs, prescriptions et spécifications fixés pendant la phase 1.
c) Phase 3 : Analyser et évaluer l'efficacité du SPP conçu pendant la phase 2 au regard des objectifs, prescriptions et spécifications fixés à l'issue de la phase 1.

3.5. Ces trois phases et les principales activités menées pendant chacune d'entre elles sont présentées sur la figure 1. Celle-ci est conforme à la figure 2 de la référence [2], tout en allant un peu plus loin en incluant la vérification des prescriptions normatives.

---

[3] Dans la présente publication, les « prescriptions » peuvent comprendre les prescriptions écrites spécifiques imposées par l'autorité compétente concernée ou par l'exploitant pour se conformer aux prescriptions réglementaires.

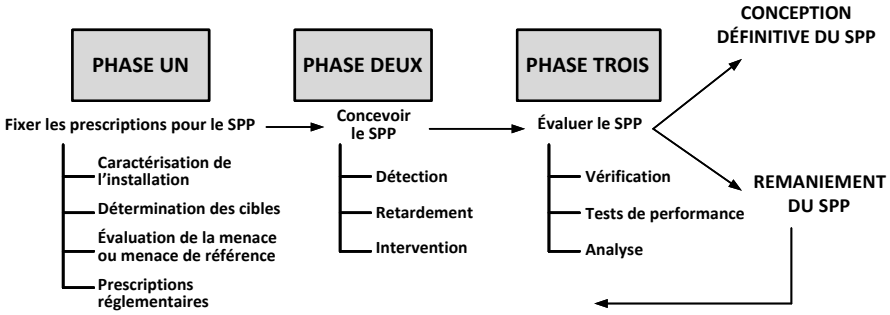


FIG. 1. Processus de conception et d'évaluation du système de protection physique

3.6. La figure 1 présente un exemple de processus d'ingénierie système qui a été adapté pour s'appliquer à la conception et à l'évaluation d'un SPP. Toutes les phases du processus peuvent s'appliquer à un nouveau système, à un système existant ou aux modifications d'un système existant. Les trois phases devraient être répétées selon que de besoin de façon à aboutir à la conception d'un SPP efficace.

FIXATION DES PRESCRIPTIONS RELATIVES AU SYSTÈME DE PROTECTION PHYSIQUE (PHASE 1)

3.7. Pour commencer la phase 1 du processus de conception et d'évaluation d'un SPP, le concepteur devrait tout d'abord recenser les prescriptions législatives et réglementaires nationales en matière de protection physique. La détermination des modalités d'application de ces prescriptions dans une installation nucléaire ou à des matières nucléaires prévoit l'utilisation de l'évaluation de la menace ou de la menace de référence, le recensement des cibles et la caractérisation de l'installation.

3.8. On trouvera dans la référence [1] des recommandations concernant les prescriptions relatives aux mesures mises en œuvre dans le cadre du SPP contre l'enlèvement non autorisé de matières nucléaires et le sabotage de matières nucléaires et d'installations nucléaires. Ces prescriptions recommandées prévoient une approche graduée qui est basée, pour l'enlèvement non autorisé, sur la catégorisation des matières nucléaires et, pour le sabotage, sur les conséquences potentielles et la définition nationale des conséquences radiologiques inacceptables et des graves conséquences radiologiques.

3.9. Les États peuvent également fixer d'autres objectifs que ceux qui sont liés à la prévention de l'enlèvement non autorisé et du sabotage, définis dans la Convention sur la protection physique des matières nucléaires [3] et l'amendement à cette convention [4]. Il peut s'agir d'objectifs en rapport avec la sûreté, les aspects économiques, la sécurité de l'alimentation électrique ou la notoriété, qui n'entrent pas dans le cadre de la présente publication.

Utilisation des informations sur la menace

3.10. La conception et l'évaluation du SPP devraient s'appuyer sur un énoncé de la menace [1, 2, 13].

Détermination des cibles

3.11. La détermination des cibles sert à répertorier les matières et équipements qui, dans une installation, doivent être protégés et à préciser le niveau de protection requis [2]. Il s'agit de déterminer la catégorie appropriée de matières nucléaires nécessitant une protection contre un enlèvement non autorisé et les matières et équipements ayant besoin d'être protégés contre le sabotage.

3.12. Les niveaux de seuil nationaux concernant les conséquences radiologiques inacceptables et les graves conséquences radiologiques devraient être utilisés pour déterminer les prescriptions de protection physique applicables aux installations nucléaires où des cibles de sabotage ont été répertoriées [1]. Les orientations données dans la publication n° 16 de la collection Sécurité nucléaire de l'AIEA, intitulée *Identification des zones vitales des installations nucléaires* [16], peuvent servir à répertorier les zones vitales d'une installation nucléaire.

3.13. Selon une approche graduée, il importe de prévoir pour chaque cible un niveau de protection approprié, défini par l'État sous la forme d'objectifs de performance, de prescriptions normatives ou d'une combinaison de ces moyens. Lorsque des cibles potentielles sont coïmplantées dans une zone ou un espace défini, cette zone ou cet espace doit être protégé conformément aux prescriptions de protection physique plus rigoureuses, fixées contre l'enlèvement non autorisé ou contre le sabotage [1]. Des mesures de détection ou de retardement importantes peuvent ainsi être appliquées à des cibles moins attractives coïmplantées dans cette zone ou ce bâtiment. Toutefois, la protection de chaque cible n'en doit pas moins être envisagée individuellement, compte tenu en particulier de la menace d'origine interne.

Caractérisation de l'installation

3.14. Le SPP devrait être conçu de manière à prendre en compte les types d'opérations qui se dérouleront dans l'installation ainsi que les diverses conditions susceptibles de l'affecter dans celle-ci (p. ex., les conditions ambiantes ou les conditions de fonctionnement).

3.15. Un ou plusieurs processus opérationnels sont généralement menés dans une installation nucléaire et chacun d'eux peut comprendre une ou plusieurs activités. Les processus menés dans des centrales nucléaires étant différents de ceux qui le sont dans des installations du cycle du combustible nucléaire, les activités opérationnelles sont également différentes. Les paragraphes 3.16 à 3.19 décrivent les types d'information à recueillir sur les activités et processus menés dans l'installation [2].

3.16. Il importe de recenser et de comprendre les conditions de fonctionnement escomptées dans l'installation (p. ex., le fonctionnement normal, la maintenance, la mise à l'arrêt et les situations d'urgence). Le calendrier d'opérations définit les activités à effectuer à différents moments de la journée et à des jours différents. Il faut également disposer d'informations sur les mouvements de matières nucléaires, notamment sur les processus d'expédition et de réception en ce qui concerne les mouvements sur site et hors site. Par ailleurs, les processus et activités liés à la sûreté et à la comptabilité et au contrôle des matières nucléaires doivent être bien compris. Les interfaces entre ces différentes fonctions, par exemple entre la sûreté et la protection physique, devraient être bien comprises et caractérisées.

3.17. Les conditions physiques et ambiantes dans l'installation peuvent affecter la performance des mesures de protection physique, en particulier celles qui sont mises en place à l'extérieur ou dans des zones sous rayonnement intense. Ces conditions sont les suivantes : topographie, végétation et vie sauvage, sources de rayonnement électromagnétique qui peuvent créer des interférences dans les systèmes de communication (p. ex., les émetteurs radio ou les microphones téléphoniques), perturbations sismiques naturelles, gammes de températures, précipitations (p. ex., pluie et neige) et vent (vent moyen et rafales). Ces facteurs pourraient avoir des incidences sur les taux d'alarmes intempestives, la capacité des sous-systèmes de capter et d'évaluer les alarmes et/ou la capacité des gardiens et des forces d'intervention de se déplacer et d'accomplir leurs tâches.

3.18. La caractérisation de l'installation implique une description complète de celle-ci, incluant notamment son périmètre, les bâtiments qui s'y trouvent, les plans de niveau, les élévations de la structure et les points d'accès en situation

normale et en situation d'urgence. Il faudrait également repérer les passages, souterrains ou non, entre les bâtiments. Les détails de construction des murs, plafonds, planchers, portes et fenêtres à la limite de l'installation nucléaire et dans les emplacements cibles devraient être bien caractérisés. Des informations analogues devraient également être obtenues sur l'infrastructure, notamment les systèmes de chauffage, de ventilation, de climatisation et de distribution d'électricité, et sur les schémas des systèmes, tels que les systèmes de sûreté redondants et dépendants dans un réacteur nucléaire.

3.19. Les informations sur l'installation peuvent provenir de sources pertinentes, comme les plans de l'installation et des descriptions des processus, les rapports d'analyse de la sûreté, les plans de sécurité et de sûreté, les diagrammes de construction, les rapports d'examen de l'installation et les observations des activités et les entretiens avec le personnel. Lors de la mise en place d'un SPP dans une installation existante, les informations devraient également inclure les dossiers de récolement[4], qui peuvent être obtenus et validés dans le cadre de visites d'inspection de l'installation. Les concepteurs de SPP ont besoin de ces informations pour comprendre ce qui doit être protégé et les contraintes propres à l'installation (comme les prescriptions de sûreté) qu'il leur faudra prendre en considération pendant la conception.

CONCEPTION D'UN SYSTÈME DE PROTECTION PHYSIQUE (PHASE 2)

3.20. Le SPP doit être conçu de manière à assurer le respect de toutes les prescriptions en matière de sécurité et de sûreté. Au cours de la phase 2, le concepteur détermine le meilleur moyen d'associer des mesures de protection physique telles que les barrières physiques, les détecteurs, les procédures, la surveillance vidéo, les appareils de télécommunication et les forces d'intervention afin de constituer un SPP qui puisse satisfaire aux prescriptions en matière de protection, compte tenu d'autres considérations telles que les coûts initiaux et le coût du cycle de vie du SPP et les incidences potentielles de la conception sur la comptabilité et le contrôle des matières nucléaires, la sûreté et l'exploitation. L'objectif général est de vérifier que le SPP répond bien aux prescriptions

[4] Les dossiers de récolement sont l'ensemble définitif de schémas qui rendent compte de l'installation telle que construite, en incluant toutes les modifications apportées aux spécifications et aux schémas d'exécution au cours du processus de construction, et montrent les dimensions exactes, la géométrie et l'emplacement de tous les éléments du travail achevé pendant la construction.

relatives à la protection en assurant un équilibre satisfaisant entre les fonctions de détection, de retardement et d'intervention, tout en permettant à l'installation de fonctionner de manière efficace. Le plan de sécurité de l'installation nucléaire devrait tenir compte de la conception définitive du SPP [2].

Considérations générales relatives à la conception

3.21. La conception du SPP devrait assurer une protection adéquate sans gaspiller des ressources en mesures de protection inutiles. En cas de risque de conflit entre les prescriptions de sûreté, d'exploitation et de sécurité, il faudrait suivre une approche équilibrée de la gestion du risque.

3.22. Les caractéristiques fondamentales de la conception d'un SPP à prévoir sont les suivantes :

a) La défense en profondeur, de sorte que l'agresseur est obligé, pour réussir, de neutraliser ou contourner successivement plusieurs mesures de protection, impliquant en principe différentes tactiques de neutralisation. La défense en profondeur est généralement mise en œuvre en plaçant une série de niveaux de protection autour des cibles. Ces niveaux de protection peuvent comprendre une combinaison de mesures physiques (comme des contrôles de l'accès aux zones permettant d'atteindre la cible) et de mesures administratives (protection des informations sensibles et application d'une politique d'habilitation, par exemple). On peut par exemple profiter des points forts de chaque élément de la protection physique et utiliser le matériel dans des combinaisons qui complètent les points forts ou compensent les limites de chaque élément.
b) L'approche graduée, qui consiste à appliquer les prescriptions de protection physique de façon proportionnelle aux conséquences potentielles de l'acte malveillant, compte tenu de l'évaluation actuelle de la menace et de l'attractivité relative de la cible. En ce qui concerne l'enlèvement non autorisé de matières nucléaires, l'application de cette approche dépendra de la nature des matières ; pour ce qui est du sabotage de matières nucléaires ou d'installations nucléaires, elle dépendra des conséquences que pourrait avoir la réussite de ce sabotage.
c) Une protection équilibrée, de sorte que l'agresseur se heurte à des mesures du SPP d'efficacité comparable de quelque façon que l'enlèvement non autorisé ou l'acte de sabotage soit tenté.
d) La robustesse, au sens où il est très probable que le SPP fonctionnera efficacement pendant des types très divers d'agressions. Cette caractéristique

est habituellement obtenue en incorporant dans la conception une série de mesures de protection redondantes et diverses.

3.23. Outre les caractéristiques énumérées ci-dessus, il est souhaitable que le concepteur du SPP réfléchisse à des conceptions qui puissent être facilement adaptées aux menaces nouvelles et émergentes, aux modifications apportées à l'installation ou aux cibles, ou aux modifications des prescriptions juridiques et réglementaires. Pendant la conception, peut également entrer en ligne de compte la capacité du SPP de protéger temporairement, à un niveau approprié, une cible qui ne soit pas habituellement utilisée ou entreposée dans un lieu particulier. C'est par exemple le cas lorsqu'une situation d'urgence, une défaillance du système ou une autre situation exige d'utiliser des mesures de remplacement ou compensatoires. Cela pourrait impliquer d'installer temporairement les types de systèmes décrits dans la section 4.

3.24. Pour réduire la menace d'origine interne d'enlèvement non autorisé de matières nucléaires et de sabotage, une approche globale devrait prévoir des mesures de prévention et de protection, notamment celles fournies par la comptabilité et le contrôle des matières nucléaires [8]. Des orientations plus détaillées sur la protection contre les menaces internes sont fournies dans la référence [10].

Sécurité intrinsèque

3.25. L'intégration des caractéristiques définies aux paragraphes 3.22 à 3.24 aussitôt que possible dans la durée de vie d'une installation nucléaire est au cœur de la « sécurité intrinsèque » telle que décrite dans la publication nº 35-G de la collection Sécurité nucléaire de l'AIEA, intitulée *La sécurité tout au long de la durée de vie d'une installation nucléaire* [17], et est susceptible de déboucher sur des mesures de sécurité qui soient plus facilement pérennisées ou adaptées. Le fait d'ajouter des mesures de sécurité à une installation une fois qu'elle a été conçue et construite peut entraîner une dépendance à long terme à l'égard de mesures de protection moins efficientes.

3.26. La sécurité intrinsèque consiste notamment à se préoccuper à un stade précoce de l'adaptabilité d'une conception (p. ex., en achetant un terrain plus étendu que celui qui est actuellement nécessaire, pour avoir à l'avenir des prescriptions plus strictes en matière de protection à distance) et à prendre en compte les compromis entre les prescriptions en matière de sûreté, de sécurité, de fonctionnement et d'autres facteurs pertinents pendant l'étude de conception, afin de choisir une conception qui tienne le mieux compte des prescriptions dans

tous ces domaines. La sécurité intrinsèque peut également être appliquée pendant que des modifications sont apportées à une installation existante, encore que les options puissent être plus limitées que pour une nouvelle installation. L'application de prescriptions de sécurité dès le début d'une reconfiguration partielle et d'une modification peut accroître l'efficience et l'efficacité de la sécurité contre les menaces définies.

ÉVALUATION DU SYSTÈME DE PROTECTION PHYSIQUE (PHASE 3)

3.27. Pendant la phase 3, la conception du SPP élaborée en phase 2 pour un nouveau système ou un système existant est évaluée afin de déterminer si elle répond aux prescriptions fixées durant la phase 1. L'évaluation du SPP comprend les trois activités visées dans la figure 1 :

a) évaluations destinées à vérifier que le SPP satisfait aux prescriptions normatives ;
b) essais de fonctionnement destinés à déterminer si le SPP satisfait aux impératifs de performance ;
c) analyse des données issues des évaluations, des essais de fonctionnement et, pour un SPP existant, des résultats des essais périodiques des équipements afin de déterminer si le SPP peut protéger efficacement l'installation contre l'enlèvement non autorisé de matières nucléaires ou un acte de sabotage.

3.28. L'évaluation d'un SPP devrait porter notamment sur les essais de fonctionnement [1, 2]. Dans la présente publication, les essais comprennent les essais périodiques des équipements et les essais de fonctionnement. Il est procédé aux essais périodiques des équipements pour appliquer les recommandations en matière de durabilité pour un SPP, tandis que les essais de fonctionnement réalisés dans le cadre des évaluations d'un SPP visent à s'assurer qu'il satisfait aux exigences fixées en matière de performance.

3.29. Les essais périodiques des équipements comprennent les essais de réception et les essais de durabilité. Les essais de réception consistent en essais des équipements et des systèmes nouvellement installés, modifiés ou récemment réparés avant leur mise en service. Ces essais permettent de déterminer si les équipements et les systèmes ont été installés et fonctionnent correctement avant d'autoriser leur utilisation. Les essais de durabilité consistent à effectuer périodiquement des essais de maintenance, d'étalonnage et d'opérabilité et des essais fonctionnels des équipements pendant le fonctionnement du SPP. Les essais périodiques des équipements font l'objet de la section 8.

3.30. Les essais de fonctionnement consistent en essais de performance de portée limitée et à grande échelle menés dans le cadre d'un processus d'évaluation pour déterminer si le SPP satisfait aux impératifs de performance contre les menaces définies dans l'évaluation de la menace ou la menace de référence. Cette question est examinée dans la section 9.

3.31. L'évaluation du SPP devrait correspondre à l'étape de la vie de l'installation à laquelle elle s'applique [17]. Il est souhaitable de faire appel à des experts indépendants pour examiner le SPP avant de demander à l'autorité compétente d'en approuver le fonctionnement. Lorsqu'il est fait appel à des experts indépendants, il conviendrait d'assurer la protection des informations sensibles conformément aux lois et prescriptions nationales pertinentes.

3.32. Lorsqu'un SPP est évalué en même temps que d'autres systèmes, tels que les systèmes de sûreté, l'évaluation devrait être confiée à une équipe intégrée composée de spécialistes de la protection physique, de l'intervention d'urgence, de l'exploitation, de la sûreté, de la comptabilité et du contrôle des matières nucléaires et d'autres disciplines pertinentes, dont la fiabilité a été vérifiée.

AUTRES CONSIDÉRATIONS RELATIVES À LA CONCEPTION

Intégration du système de protection physique

3.33. Un SPP intègre des mesures de détection, de retardement et d'intervention, et devrait être efficace contre l'enlèvement non autorisé et le sabotage [1, 2]. La conception du SPP devrait en principe intégrer l'exploitation, la sûreté, la comptabilité et le contrôle des matières nucléaires, la protection physique, la fiabilité et la sécurité des informations et la sécurité informatique dans une démarche équilibrée visant à satisfaire à toutes les prescriptions. Le processus de conception devrait améliorer le fonctionnement global de l'installation nucléaire et contribuer à satisfaire à toutes les prescriptions de la manière la plus efficace et efficiente. Toutefois, les différentes disciplines ont des priorités et des perspectives différentes.

Conduite des opérations

3.34. Les conditions de fonctionnement sont alignées sur les fins poursuivies par l'installation. Les conditions qui influenceront le SPP et qui devraient être prises en compte dans la phase de conception du système comprennent les heures de travail (en temps normal et dans des circonstances particulières), le nombre

de personnes ayant besoin d'accéder aux différentes parties de l'installation, la capacité des points de contrôle de l'accès et le nombre et les types d'entrées dans une zone sécurisée telle qu'une zone vitale.

Sûreté

3.35. Une gestion efficace de l'interface entre la sûreté et la sécurité constitue un élément important de ces deux programmes et est indispensable pour assurer une protection physique appropriée aux matières et aux installations nucléaires et pour préserver la santé et la sûreté des travailleurs et du public [2]. Les mesures de protection physique ne devraient pas compromettre la sûreté et les mesures de sûreté ne devraient pas compromettre la protection physique. Cette question est examinée plus avant dans la section 11.

3.36. La détermination et la protection des cibles d'un sabotage reposent en particulier sur une étroite coopération entre spécialistes de la protection physique et de la sûreté. Il conviendrait d'appliquer une approche graduée de manière à ne pas compromettre la sûreté, tout en rendant possible une protection efficace des cibles. L'exploitant devrait procéder à des analyses de détermination des cibles :

a) pour déterminer si le stock radioactif de chaque emplacement au sein de l'installation pourrait entraîner des conséquences radiologiques inacceptables telles que définies par l'État ;
b) pour recenser les équipements, systèmes ou dispositifs dont le sabotage pourrait conduire, directement ou indirectement, à des conséquences radiologiques inacceptables ;
c) pour identifier les systèmes de contrôle-commande numérique importants pour la sûreté et la sécurité.

3.37. Après la détermination des cibles, le SPP devrait être conçu (ou modifié) de façon à être efficace au regard des scénarios crédibles répertoriés dans l'énoncé de la menace applicable. Ce processus doit être mené à bien chaque fois qu'il y a une modification de l'évaluation de la menace ou de la menace de référence, une modification de la définition des conséquences radiologiques inacceptables donnée par l'État ou une modification importante du stock radioactif de l'installation nucléaire. Ce processus consiste à recenser les zones vitales (celles où se trouvent des matières nucléaires, des équipements, des systèmes ou des dispositifs dont le sabotage pourrait avoir de graves conséquences radiologiques), en tenant compte des systèmes de sauvegarde qui existent déjà [16].

3.38. La prise en compte simultanée des prescriptions de sûreté et de sécurité pendant la phase de conception d'une installation peut permettre l'exploitation efficace de synergies. Par exemple, la redondance des équipements ou des systèmes et leur séparation peuvent être utiles à la fois à la sûreté et à la sécurité, tandis que leur redondance sans leur séparation pourrait être utile à la sûreté, mais pas à la sécurité. La séparation d'équipements redondants peut protéger contre le sabotage en obligeant un agresseur à consacrer davantage de temps à la préparation de son acte de sabotage et à multiplier les équipements nécessaires à cette fin [10, 18].

3.39. D'autres systèmes de sûreté pourraient être conçus pour améliorer la sécurité ; c'est le cas des dispositifs de surveillance continue de l'air ou des avertisseurs de pression négative, qui offrent une protection au personnel, mais pourraient également être utilisés pour avertir d'une éventuelle tentative de sabotage ou d'enlèvement non autorisé. Ces systèmes pourraient être intégrés aux fins de la sûreté et de la sécurité en mettant en place une transmission des alarmes (automatique ou non) entre le personnel de sûreté et le personnel de sécurité si l'une des situations définies devait se produire.

3.40. Des mesures de sûreté et de radioprotection de base telles que d'épais murs de béton ou blindages peuvent également servir à augmenter le temps nécessaire à un agresseur pour atteindre un emplacement cible.

3.41. Les centrales nucléaires sont spécialement conçues pour résister à des sollicitations externes et internes extrêmes, telles que les vibrations, la chaleur, la surpression et l'impact, sans que la sûreté soit compromise. La publication n° 4 de la collection Sécurité nucléaire de l'AIEA, intitulée *Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage* [18], présente une méthodologie d'évaluation de la capacité d'un certain sous-ensemble d'une structure, d'un système et d'un composant liés à la sûreté de résister à des événements résultant d'actes de sabotage. Les présentes orientations portent notamment sur l'évaluation des aspects relatifs à la sauvegarde à prendre en compte pour protéger les centrales nucléaires contre le sabotage, notamment les attaques à distance.

Comptabilité et contrôle des matières nucléaires

3.42. Au niveau de l'installation, un solide système de comptabilité et de contrôle des matières nucléaires contribue à décourager et détecter l'enlèvement non autorisé de matières nucléaires en comptabilisant ces matières et en effectuant des contrôles rigoureux dans ce domaine [8]. Le système susvisé devrait comprendre

des moyens de recevoir et d'évaluer des alarmes et de déclencher une intervention si une alarme indique que des matières nucléaires pourraient avoir été enlevées sans autorisation ou sont utilisées de manière non autorisée. Un système efficace de comptabilité et de contrôle des matières nucléaires peut détecter un agresseur d'origine interne qui tente de commettre un acte malveillant concernant des dossiers conservés aux fins de cette comptabilité et de ce contrôle et peut corroborer l'évaluation correcte d'une irrégularité mettant en jeu des matières nucléaires [8]. De ce fait, le SPP et le système en question doivent fonctionner d'une manière coordonnée et complémentaire afin de réagir à tout un éventail de menaces. Les exploitants peuvent utiliser les orientations relatives à la mise en place d'un système de comptabilité et de contrôle des matières nucléaires aux fins de la sécurité nucléaire dans une installation nucléaire pour gérer efficacement les interfaces entre le SPP de l'installation et le système en question [2, 8, 10].

Sécurité de l'information et sécurité informatique

3.43. Les agresseurs souhaitant réaliser un enlèvement non autorisé de matières nucléaires ou se livrer à un acte de sabotage de matières et d'installations nucléaires peuvent tirer parti d'informations sensibles. Une information sensible peut se présenter sous des formes très diverses (des logiciels, par exemple), dont la divulgation, la modification, l'altération, la destruction ou le refus d'utilisation non autorisés pourrait compromettre la protection physique. Avant de commencer le processus en trois phases de conception et d'évaluation d'un SPP, les exploitants doivent établir des politiques, des plans et des procédures internes afin de préserver la confidentialité, l'intégrité et la disponibilité des informations sensibles qu'ils détiennent ou exploitent, conformément à la politique de sécurité nationale et aux lois et prescriptions nationales applicables à la sécurité de l'information. On trouvera des orientations générales sur la sécurité de l'information en rapport avec la sécurité nucléaire, dont un exemple de guide de classification destiné à aider à répertorier les informations sensibles, dans la publication n° 23-G de la collection Sécurité nucléaire de l'AIEA, intitulée *Sécurité de l'information nucléaire* [19], et les références [1, 2] donnent des orientations plus spécifiques sur la sécurité des informations sensibles en rapport avec la protection physique.

3.44. La sécurité informatique est un élément important de la conception d'un SPP et elle devrait être prise en compte dans toutes les phases de la conception et de l'évaluation de ce système. Des orientations générales sur la sécurité informatique pour la sécurité nucléaire figurent dans la référence [7]. Les publications de la collection Sécurité nucléaire de l'AIEA n° 42-G, *Sécurité informatique pour la sécurité nucléaire* [20] et n° 33-T, *Sécurité informatique des systèmes de contrôle-commande dans les installations nucléaires* [21] donnent

des orientations plus spécifiques sur la sécurité informatique pour les systèmes des installations nucléaires.

4. MATÉRIEL DE PROTECTION PHYSIQUE

4.1. Un SPP est un ensemble de mesures de protection physique intégrant les personnes, les procédures et les équipements. Ces mesures sont mises en œuvre et pérennisées grâce à des systèmes de gestion, comme le décrit la section 11.

4.2. Un SPP a pour objet de prévenir l'enlèvement non autorisé de matières nucléaires et le sabotage de matières et d'installations nucléaires, ainsi que d'offrir une protection contre de tels actes [1, 2]. Il atteint cet objectif grâce aux fonctions de détection (décèlement et évaluation), de retardement et d'intervention. La présente section examine ces fonctions principales et leur interaction.

4.3. Le SPP est conçu pour respecter le principe fondamental de défense en profondeur en créant des zones de sécurité à plusieurs niveaux ou concentrique axées sur les cibles identifiées [1, 2]. Dans la présente publication, le terme « zones de sécurité » est utilisé de manière générale pour désigner les zones d'accès limité, les zones protégées, les zones intérieures, les zones vitales et les chambres fortes se trouvant dans les limites d'une zone intérieure (voir la figure 2).

4.4. La conception d'un SPP pour une installation nucléaire est un processus complexe. Les concepteurs devraient coopérer au niveau national avec d'autres concepteurs et experts à la coordination de la conception du système et à la sélection du matériel. En cas de besoin, une assistance et des conseils supplémentaires peuvent être obtenus dans le cadre d'une coopération directe avec d'autres États ou l'AIEA.

DÉTECTION

4.5. Un système de détection d'intrusions est utilisé pour déclencher des alarmes (décèlement) que le PCS évalue pour déterminer si elles sont causées par des intrusions qui intéressent la sécurité nucléaire. Il s'ensuit que la probabilité de détection est le produit de la probabilité de décèlement et de la probabilité d'évaluation (voir la figure 3). Les systèmes de détection d'intrusions comprennent habituellement des capteurs de détection d'intrusions intérieurs et extérieurs, des

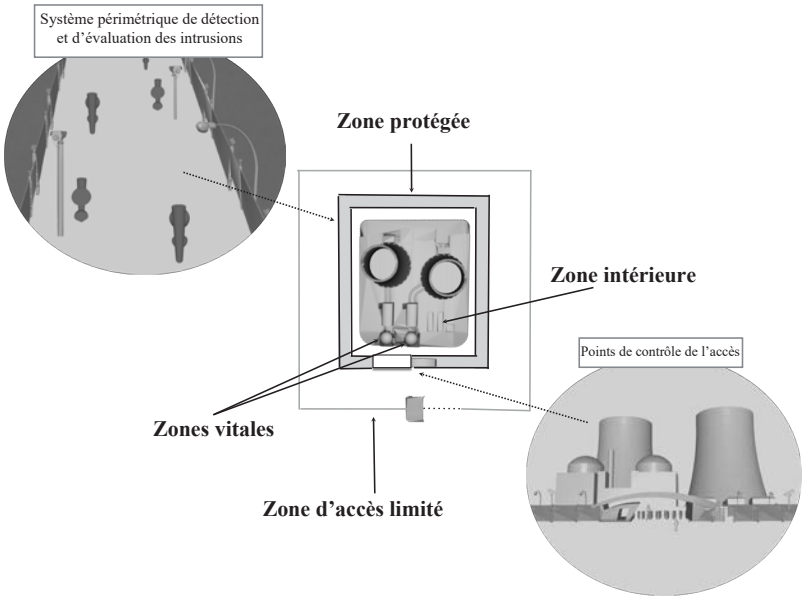


FIG. 2. Types de zone de sécurité

caméras de surveillance en circuit fermé, des mesures de contrôle de l'accès, des systèmes de transmission des alarmes et un personnel fonctionnant en symbiose. Le système de détection d'intrusions devrait détecter des agresseurs mettant en œuvre leurs moyens, définis dans l'évaluation de la menace ou la menace de référence applicable, pour tenter de réaliser un enlèvement non autorisé ou de se livrer à un acte de sabotage, ou pour faciliter la commission d'un tel acte.

4.6. Le concepteur d'un tel système devrait posséder une connaissance approfondie des caractéristiques opérationnelles, physiques et environnementales de l'installation à protéger (voir les sections 2 et 3). Les concepteurs de SPP devraient connaître parfaitement les technologies de décèlement et d'évaluation existantes, leur fonctionnement et leurs limites.

Caractéristiques de performance

4.7. La performance des capteurs de détection d'intrusions tient à leurs caractéristiques fondamentales, à savoir notamment la probabilité de décèlement, les taux de fausses alarmes ou d'alarmes intempestives, et leur éventuelle neutralisation.

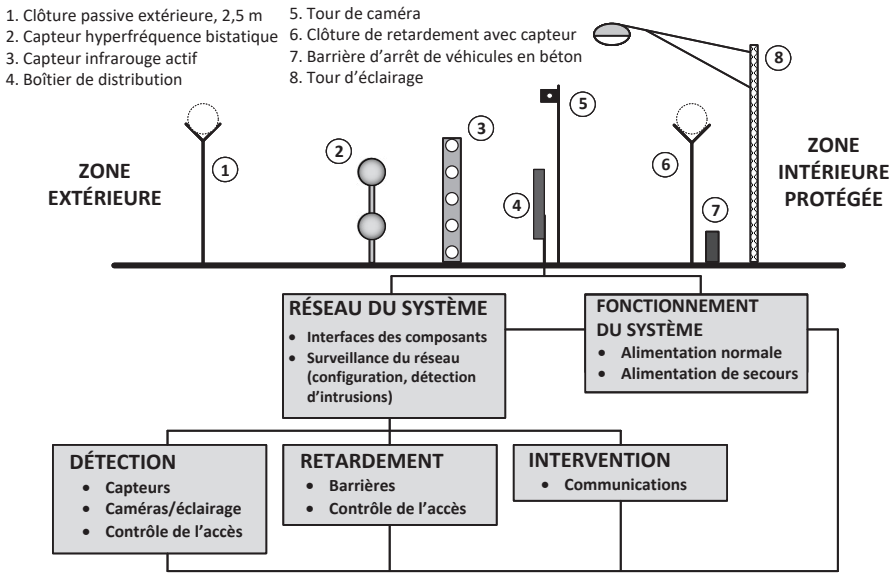


FIG. 3. Composants caractéristiques d'un système de détection périmétrique des intrusions

4.8. La probabilité de décèlement dépend du périmètre à couvrir et du modèle du capteur, des conditions d'installation, du réglage de sensibilité, des conditions météorologiques et des autres conditions environnementales, ainsi que de l'état du matériel. Elle pourrait aussi dépendre pour une bonne part des moyens dont dispose l'agresseur. Aucun capteur n'est efficace à 100 %, mais la probabilité d'une fausse alarme ou d'une alarme intempestive devrait être aussi faible que possible, et la probabilité de décèlement devrait être aussi forte que possible.

4.9. Les conditions varient en fonction des différentes installations et (même si certains fabricants de capteurs prétendent le contraire) il n'est pas possible d'assigner une probabilité de détection spécifique à un capteur ou à un ensemble de capteurs. De plus, la probabilité de décèlement varie en fonction de l'âge du matériel et de l'évolution des conditions dans lesquelles il est utilisé. De ce fait, cette probabilité devrait être vérifiée par des essais de fonctionnement périodiques (voir la section 8).

4.10. Le taux d'alarmes intempestives est le nombre d'alarmes déclenchées pendant une certaine période par des incidents non associés à une intrusion ou des incidents prévus, tels que les essais de fonctionnement des capteurs. Ces incidents peuvent tenir à des facteurs environnementaux, tels que le vent, la pluie ou les animaux sauvages, ou les alarmes déclenchées par inadvertance par le personnel

autorisé, ou encore à des erreurs d'installation ou de conception du système. Les taux d'alarmes intempestives sont généralement exprimés par un nombre moyen d'alarmes sur une certaine période (p. ex. une alarme intempestive par minute, par heure ou par jour) et peuvent être très différents en fonction des capteurs et des installations. Les alarmes intempestives déclenchées par le matériel lui-même sont appelées fausses alarmes (causées p. ex. par une erreur de conception ou la défaillance d'un composant) et il n'en sera plus question dans la présente section. Le contrôle et le maintien de l'environnement autour du capteur peuvent aider à réduire au maximum les alarmes intempestives et, de ce fait, contribuer à l'efficacité globale du SPP.

4.11. Les alarmes intempestives sont généralement classées en fonction de leur source. Les sources habituelles d'alarmes intempestives pour les capteurs extérieurs sont les mouvements de la végétation, les animaux sauvages et les conditions météorologiques (le vent, la pluie, la neige, le brouillard et la foudre, p. ex.). Ces alarmes peuvent également être déclenchées par les vibrations du sol, les interférences électromagnétiques, les rayonnements et les produits chimiques, ainsi que les effets acoustiques, thermiques et optiques.

4.12. Pour réduire les alarmes intempestives, il importe d'en repérer et comprendre les causes. Ces alarmes peuvent être réduites de trois façons : élimination de leur cause, diminution de la sensibilité du capteur, et utilisation de technologies permettant de filtrer et d'éliminer les alarmes de ce type.

4.13. Pour réduire les causes de ces alarmes, on pourrait d'abord détourner l'eau de pluie pour éviter que le capteur soit endommagé, ou installer une clôture pour réduire l'impact de la végétation apportée par le vent dans la zone considérée. On pourrait réduire certaines causes d'alarmes intempestives en modifiant les procédures de gestion, par exemple en couvrant le capteur installé dans une zone lorsque le personnel autorisé est présent.

4.14. La deuxième méthode consiste à réduire la sensibilité du capteur. Toutefois, il convient alors de veiller à ce que la réduction de sensibilité ne diminue pas de façon inacceptable la probabilité de déceler une véritable tentative d'intrusion.

4.15. On peut enfin mettre en œuvre des technologies de filtrage de certaines alarmes intempestives, comme dans l'exemple de la technologie à double usage : deux capteurs utilisant des technologies différentes selon une configuration en porte logique AND. La porte AND ne produit une alarme que si les deux capteurs sont activés, ce qui réduit la probabilité d'alarmes intempestives du type couramment rencontré avec l'une ou l'autre des technologies concernées.

Par exemple, un capteur infrarouge passif pourrait être placé avec un capteur hyperfréquences monostatique dans le même boîtier. Dans cette configuration, la sensibilité de chaque capteur pourrait être réglée à élevée sans provoquer les alarmes intempestives associées à l'utilisation d'un seul type de capteur.

4.16. Lorsque deux capteurs sont combinés selon une logique AND, la probabilité de décèlement sera plus faible que celle de chaque capteur pris isolément. Par exemple, les capteurs hyperfréquences présentent une plus forte probabilité de décèlement du mouvement dirigé directement vers le capteur ou s'en éloignant, et les capteurs infrarouges présentent une plus forte probabilité de décèlement du mouvement dans l'ensemble du champ visuel. En conséquence, la probabilité de décèlement avec les capteurs associés dans un boîtier unique sera plus faible que si deux capteurs sont installés séparément, perpendiculairement l'un à l'autre avec recoupement des modèles d'énergie et des champs visuels. Si une probabilité plus forte de décèlement est nécessaire, il pourrait être préférable de disposer de capteurs séparés.

4.17. De plus, les différents types de capteurs présentent des vulnérabilités différentes qui peuvent être exploitées. Le concepteur du SPP devrait donc chercher à mettre en place une défense en profondeur fondée sur une conception globale reposant sur l'utilisation de capteurs de types différents, mais complémentaires dont les zones de couverture se recoupent partiellement dans le secteur concerné, de sorte qu'un agresseur ait du mal à neutraliser plusieurs capteurs relevant de technologies différentes en utilisant la même méthode. Les capteurs complémentaires améliorent la performance globale du système, exprimée selon les trois principales caractéristiques des capteurs.

4.18. Il faudrait également prendre en considération la disponibilité du système de détection des intrusions, à savoir la capacité du système d'exercer ses fonctions à tous moments et compte tenu de l'éventail de conditions météorologiques attendu tout au long de la durée de vie du système. À cette fin, on peut prévoir des composants redondants et divers, des composants à durée de vie plus longue et des capteurs appropriés aux conditions météorologiques attendues, et élaborer des programmes de pérennisation bien conçus, s'agissant notamment de la maintenance préventive (dont il est question dans la section 11).

4.19. Il est souvent nécessaire d'éliminer tout obstacle autour des capteurs extérieurs pour qu'ils puissent fonctionner et fournir des éléments visuels supplémentaires pour aider à évaluer les causes des alarmes déclenchées par les capteurs. Les concepteurs d'un système de détection des intrusions devraient chercher à mettre en place des conditions de détection uniformes sur toute la

longueur du périmètre, ce qui est généralement obtenu en maintenant une zone dégagée parallèlement aux clôtures du périmètre. La zone dégagée est destinée à maintenir les personnes, les animaux et les véhicules à l'écart de la zone de détection. Elle est habituellement débroussaillée et l'on a fait disparaître les lignes aériennes de transport de force, entre autres structures aériennes. Dans les zones où le capteur primaire ne peut pas être déployé dans de bonnes conditions, comme dans le cas d'un portail, un capteur différent (un capteur infrarouge actif, par exemple) peut faire l'affaire.

Conditions environnementales

4.20. Bien des conditions environnementales peuvent produire différents types de « bruit » dans les gammes d'énergie que les capteurs de détection d'intrusions sont conçus pour déceler. Ces sources de bruit peuvent dégrader la performance des capteurs et ces derniers peuvent déclencher une alarme même en l'absence de tout agresseur. Les paragraphes 4.21 à 4.28 décrivent les facteurs qui peuvent dégrader la performance d'un capteur et montrent comment atténuer ces effets.

4.21. Les facteurs environnementaux généraux susceptibles de dégrader cette performance sont notamment l'énergie électromagnétique, les rayonnements ionisants, certains produits chimiques et des phénomènes acoustiques, thermiques, optiques, sismiques et météorologiques. Ces facteurs influent sur la sélection de la technologie des capteurs appropriée et pourraient nécessiter l'application de mesures d'atténuation spécifiques.

4.22. Étant donné que les capteurs intérieurs ont moins de blindage électrique que les capteurs extérieurs, les sources d'énergie électromagnétique peuvent affecter particulièrement la performance de certains types de systèmes de capteurs et augmenter la fréquence des alarmes intempestives. De plus, ces capteurs pourraient être placés dans des espaces intérieurs à proximité immédiate de nombreuses formes d'énergie électromagnétique. Ces sources sont par exemple la foudre, les équipements de distribution d'électricité, les lignes de transport de force et les transmissions par radiofréquence (y compris par télécommande). La construction du bâtiment ou de la salle à surveiller par un capteur intérieur de détection d'intrusions joue un rôle important s'agissant de déterminer la nature de l'énergie électromagnétique présente. Si la structure est principalement en bois ou en béton, dont aucun ne procure de blindage électromagnétique, des sources extérieures peuvent générer un bruit de fond électromagnétique élevé. On peut réduire les effets de l'énergie électromagnétique parasite en assurant le blindage électromagnétique de tous les composants du système (y compris tous

les chaînons de voies de transmission des données) et la mise à la terre électrique de tous ces composants.

4.23. Les rayonnements ionisants peuvent endommager certains composants de la plupart des types de capteurs, en particulier les composants semiconducteurs, les câbles à fibre optique et les objectifs d'appareils photos. Une conception et le choix de composants appropriés peuvent réduire la dégradation de la performance des capteurs. En particulier, le rayonnement neutronique dégrade la performance des dispositifs et circuits intégrés à semiconducteurs, le degré de dégradation dépendant principalement de la radioexposition totale, de sorte que dans des zones soumises à des niveaux de rayonnements élevés, les capteurs peuvent devoir être fréquemment remplacés.

4.24. L'emploi de substances chimiques dans certaines parties d'une installation nucléaire peut nuire au fonctionnement des capteurs (et d'autres composants électroniques ayant des fonctions relatives à la sécurité nucléaire). L'exposition des cartes électroniques aux substances corrosives, en particulier lorsque le taux d'humidité est élevé, peut provoquer le dépôt de résidus chimiques sur les circuits et une corrosion importante des composants. Cela peut réduire la performance et la fiabilité des composants des capteurs. L'électronique des capteurs devrait être protégée de façon à réduire les effets nocifs de l'exposition aux substances corrosives. La demande de miniaturisation a fait apparaître de nouvelles combinaisons de matériaux, et la corrosion pourrait avoir sur ces derniers des effets différents de ceux subis par les matériaux plus anciens. En conséquence, la maintenance et les essais des capteurs devraient être conçus de façon à garantir leur efficacité dans l'environnement dans lequel ils sont utilisés.

4.25. L'énergie acoustique est générée par un grand nombre de sources, et celle qui est générée par des sources extérieures peut être transmise dans une zone à protéger. Les formes d'énergie acoustique susceptibles d'affecter la performance des capteurs intérieurs de détection d'intrusions sont notamment le bruit généré par les phénomènes météorologiques, les appareils de ventilation, de climatisation et de chauffage, les téléviseurs et les téléphones, et des sources extérieures comme les aéronefs, les véhicules routiers et les trains.

4.26. Les modifications de l'environnement thermique peuvent générer des stimuli qui affectent la performance des capteurs intérieurs de détection d'intrusions. Ces modifications entraînent notamment une répartition inégale de la température, qui peut provoquer un mouvement de l'air dans la zone concernée, ainsi que l'expansion et la contraction des bâtiments et de ce qui s'y trouve. Les causes des modifications de l'environnement thermique sont notamment le temps qu'il fait,

les appareils de chauffage et de climatisation, les machines qui produisent de la chaleur, l'éclairage intérieur, les réactions chimiques et radioactives productrices de puissance thermique, et les fluctuations de la lumière du soleil à travers les fenêtres et les lucarnes.

4.27. Les sources des phénomènes optiques qui affectent les capteurs intérieurs de détection d'intrusions sont notamment l'énergie lumineuse du soleil, l'éclairage intérieur, les surfaces fortement réfléchissantes et l'énergie infrarouge et ultraviolette générée par d'autres équipements.

4.28. Les sources d'interférence d'origine sismique qui peuvent affecter les capteurs sont des sources tant naturelles qu'artificielles. La principale source naturelle d'interférence d'origine sismique est l'énergie éolienne, qui est transmise au sol par les clôtures, les poteaux et les arbres, en particulier. Les sources artificielles d'interférence d'origine sismique sont par exemple la circulation et les équipements industriels lourds.

Classification des capteurs

4.29. Les capteurs sont passifs ou actifs, et peuvent être installés de manière discrète ou visible. Les capteurs de détection d'intrusions peuvent être volumétriques, linéaires ou ponctuels. Les applications des capteurs (c'est-à-dire leurs modes d'installation et d'utilisation) sont notamment le câble enfoui, l'association à une clôture, le capteur autonome, le suivi de terrain, la pénétration d'enceinte, le mouvement intérieur, l'objet et la ligne de visée.

4.30. Les capteurs passifs réagissent à un certain type d'énergie émise par un objet d'intérêt (p. ex. l'énergie mécanique dégagée par un être humain marchant sur le terrain ou escaladant une clôture) ou à un changement intervenu dans un champ énergétique naturel causé par l'objet, tel qu'un changement du champ magnétique local dû à la présence d'un objet métallique.

4.31. Les capteurs actifs transmettent un type d'énergie et réagissent aux changements affectant l'énergie ultérieurement reçue (par transmission ou réflexion) du fait de la présence ou du mouvement d'un objet d'intérêt, par exemple un faisceau électromagnétique qui est temporairement bloqué par une personne ou un objet qui le traverse.

4.32. Les capteurs actifs sont plus susceptibles que les capteurs passifs d'être affectés par les conditions environnementales car ils transmettent et reçoivent tout à la fois des signaux. Il s'ensuit que, dans un même environnement, les

alarmes intempestives sont généralement moins nombreuses dans le cas des capteurs passifs.

4.33. Les modèles d'origine de la plupart des capteurs ont des caractéristiques qui les rendent propres à une utilisation aussi bien discrète que visible, mais ils peuvent habituellement, au besoin, être modifiés pour passer d'une utilisation discrète à une utilisation visible (p. ex. dans un but de dissuasion) ou l'inverse (pour dissimuler la technologie).

4.34. Les capteurs discrets sont soustraits aux regards, par exemple en étant enfouis dans le sol ou encastrés dans un mur. Un agresseur a plus de mal à les repérer et à les localiser que dans le cas des capteurs visibles – encore que les capteurs actifs discrets puissent être détectés à l'aide d'appareils électroniques – et ils peuvent donc être plus efficaces contre un agresseur qu'une surveillance visible ne décourage pas.

4.35. Un agresseur n'a aucune peine à repérer les capteurs visibles : ils peuvent par exemple être fixés à une clôture ou installés sur une autre structure d'appui. Les capteurs visibles pourraient dissuader un agresseur. Ils sont habituellement plus faciles à installer et à entretenir que les capteurs discrets.

Type de capteur

4.36. Les capteurs volumétriques décèlent une intrusion dans un volume d'espace : une alarme est déclenchée lorsque le capteur décèle l'entrée d'un objet dans son volume. Le volume du capteur n'est habituellement pas visible et est conçu de façon à rendre difficile son identification précise par l'agresseur. Les caractéristiques de ce volume sont basées sur divers facteurs, notamment la fréquence d'onde du capteur et la forme de l'onde en fonction de la configuration de l'antenne (p. ex. espacement des câbles, hauteur de montage, sensibilité, alignement).

4.37. Les capteurs linéaires décèlent une intrusion le long d'une ligne droite : une alarme est déclenchée si un objet touche ou franchit la ligne de détection. La zone de décèlement d'un capteur linéaire est généralement facile à identifier si l'alignement du capteur est visible (ou si la ligne suit quelque chose d'évident, comme une clôture).

4.38. Les capteurs ponctuels décèlent généralement un objet spécifique dans un lieu spécifique : une alarme est déclenchée si quelqu'un ou quelque chose s'approche de l'objet, le touche ou le déplace.

Applications des capteurs

4.39. Les capteurs peuvent être utilisés à l'extérieur ou à l'intérieur d'un bâtiment. Pour un usage extérieur, il faut tenir compte des conditions environnementales, et les capteurs sont généralement autonomes, fixés à une clôture ou focalisés sur une clôture (« associés à une clôture ») ou enfouis dans le sol. Les applications intérieures des capteurs sont moins affectées par les conditions environnementales et pourraient inclure le décèlement de la pénétration de limite, du mouvement intérieur et de la proximité d'un objet. Les systèmes d'alerte rapide installés au-delà de la limite de l'installation pourraient également utiliser des capteurs. Selon l'application, les capteurs pourraient également être des capteurs à ligne de visée ou de suivi de terrain.

4.40. Les systèmes d'alerte rapide peuvent laisser aux forces d'intervention plus de temps pour se déployer ou affronter l'agresseur potentiel avant qu'il n'atteigne la zone d'intérêt. Ces systèmes reposent habituellement sur un radar de surveillance au sol longue portée et courte portée, un système d'imagerie thermique à balayage et un radar-laser. La portée efficace de ces systèmes s'établit sur une échelle allant de centaines de mètres à des dizaines de kilomètres, ce qui peut fournir quelques secondes ou minutes supplémentaires pour l'intervention. Ces systèmes reposent sur une ligne de visée entre les capteurs et l'agresseur, mais ils peuvent être installés dans des zones situées en dehors de la limite de sécurité de l'installation qui ne se trouvent pas dans la ligne de visée des autres capteurs et systèmes d'évaluation. Dans ces applications, les capteurs sont conçus pour être discrets et entièrement autonomes. Toutefois, ils posent d'importants problèmes de conception et de fonctionnement, qui peuvent en empêcher l'utilisation efficace. On trouvera ci-après une description de certains de ces problèmes.

4.41. Les systèmes d'alerte rapide installés au-delà de la limite de l'installation n'atteignent habituellement pas le niveau de performance qui serait attendu des capteurs extérieurs dans l'installation, tels que les capteurs associés à une clôture. Il est difficile de définir des impératifs de performance et de concevoir des systèmes capables d'y satisfaire à coup sûr du fait de la nature de ces systèmes et des vastes superficies qu'ils peuvent devoir couvrir. On peut s'attendre à voir la performance varier en fonction de facteurs propres à l'installation, tels que l'environnement et la topographie.

4.42. Les systèmes à ligne de visée devraient être conçus de façon à fournir une vue directe de la zone d'intérêt et, de ce fait, fonctionner de la façon la plus efficace dans des zones ouvertes. Dans les zones où les animaux sauvages ou la végétation abondent, le taux d'alarmes intempestives peut être élevé. Pour que certaines

applications aient le maximum d'efficacité, comme dans le cas de l'utilisation de capteurs infrarouges passifs, le système lui-même devrait en principe avoir des paramètres et des fonctions limiteurs de portée, ou des capacités de masquage, afin de ne pas tenir compte des alarmes déclenchées par des déplacements dans les zones périphériques. Les capteurs à ligne de visée pourraient nécessiter de très importants travaux de préparation du site pour niveler le terrain ou devoir être installés dans des zones de détection peu étendues, ce qui pourrait être très onéreux pour certaines installations.

4.43. Les capteurs de suivi de terrain sont capables de déceler des agresseurs dans des zones où les irrégularités du sol rendraient nécessaire, dans le cas des capteurs à ligne de visée, d'effectuer d'importants travaux de préparation du site et d'installer un grand nombre de capteurs (voir la figure 4). Un capteur de ce type peut être ou non associé à une clôture ou enfoui dans le sol. Les variations de terrain importantes, telles que les fossés de drainage, peuvent fournir des lieux où un agresseur peut éviter d'être détecté ; ces variations devraient être évitées ou éliminées.

4.44. Les capteurs à câble enfoui décèlent habituellement un franchissement de la limite de l'installation. Ils sont généralement enfouis dans le sol et ne sont pas visibles (capteurs discrets). Les capteurs à câble enfoui sont notamment du type sismique, magnétique, à câble coaxial à ouvertures et à fibre optique.

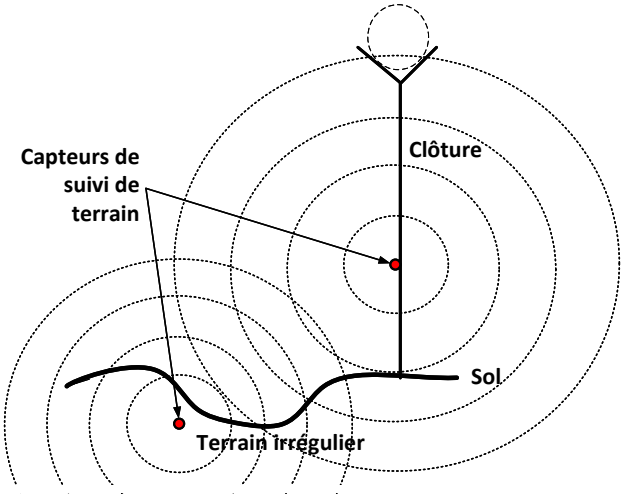


FIG. 4. Couverture des capteurs de suivi de terrain

4.45. Les capteurs associés à une clôture peuvent être montés sur une clôture ou former la structure de cette clôture, et nombre de ces capteurs peuvent aussi être considérés comme des capteurs de suivi de terrain. Les capteurs montés sur des clôtures sont notamment les capteurs à câble à fibre optique, les capteurs à capacitance et les capteurs de vibrations. Les capteurs qui peuvent former la structure de la clôture sont notamment les capteurs à câble dynamométrique.

4.46. Les capteurs autonomes sont utilisés pour les périmètres et, parfois, pour des zones à l'intérieur de l'installation. Les technologies sont notamment les capteurs infrarouges laser actifs et passifs, les capteurs hyperfréquences bistatiques et monostatiques, et les capteurs de mouvement vidéo.

4.47. Les capteurs de détection de franchissement de limite servent à détecter le franchissement des limites des bâtiments, y compris les plafonds et les planchers des salles, ainsi que les murs et les ouvertures qui y sont pratiquées (p. ex. portes, fenêtres, évents). Les technologies mises en œuvre sont notamment les capteurs électromécaniques, les capteurs de vibrations, les capteurs de bris de vitre et les capteurs de proximité infrasoniques et à capacitance.

4.48. Les capteurs de mouvement intérieurs sont utilisés pour déceler les mouvements dans un espace intérieur. Il peut s'agir de capteurs infrarouges et hyperfréquences.

4.49. Les capteurs d'objet (ou capteurs de proximité) concernent une cible spécifique au sein de l'installation. Il peut s'agir de capteurs de pression, de poids, à champ électrique, à capacitance, de mouvement vidéo et électromécaniques.

Capteurs extérieurs

4.50. Chaque installation nucléaire présente sa propre combinaison de conditions environnementales qui peuvent affecter la sélection des capteurs extérieurs. Ces conditions sont les suivantes : l'environnement physique, qui influe sur le choix des types de capteurs pour les systèmes à capteurs périmétriques ; les environnements naturel et industriel, qui influent sur le taux d'alarmes intempestives, et la topographie du périmètre, qui détermine la forme et l'étendue de l'espace disponible pour la détection, c'est-à-dire la largeur et le terrain de la zone dégagée. Il s'ensuit que le SPP conçu pour une installation nucléaire a peu de chance d'être optimal pour une autre.

4.51. Même si l'on comprend beaucoup mieux depuis quelques années les interactions entre les capteurs de détection d'intrusions et l'environnement, il est

souhaitable de mettre en place une zone d'essais sur site en utilisant différents capteurs possibles avant de choisir un système complet. C'est un moyen de confirmer le choix des capteurs et d'ajuster la conception du SPP définitif. Les essais devraient être effectués en toutes saisons afin d'évaluer la performance des capteurs dans les diverses conditions environnementales auxquelles l'installation devra concrètement faire face.

Capteurs associés à des clôtures

4.52. Les capteurs de vibrations des clôtures réagissent aux perturbations mécaniques de la clôture et sont destinés principalement à déceler un agresseur qui tente d'escalader la clôture ou de s'ouvrir un passage à travers celle-ci. Plusieurs types de transducteurs sont utilisés pour déceler le mouvement ou les vibrations de la clôture. Les capteurs de vibrations des clôtures réagissant à chaque perturbation mécanique de la clôture, il importe de prendre en considération les alarmes intempestives, par exemple celles qui sont dues aux vents forts (et à la pluie ou aux débris apportés par le vent), à la grêle ou aux vibrations causées par la circulation et les machines. Une clôture bien construite, avec des poteaux rigides et une structure compacte, peut limiter autant que possible les cas d'alarmes intempestives.

4.53. Certaines configurations de capteurs de vibrations des clôtures utilisent des câbles dynamométriques. Ces capteurs sont fixés aux clôtures et sont conçus principalement pour déceler toute personne escaladant ou coupant la clôture.

4.54. Les clôtures en fils métalliques tendus sont des capteurs associés à des clôtures qui sont faits d'un grand nombre de fils horizontaux parallèles à forte résistance à la traction reliés sous tension à des transducteurs situés près du point médian de la portée du fil. Ces transducteurs réagissent à la déflexion du fil qui se produit lorsqu'un agresseur le coupe, l'escalade pour passer de l'autre côté de la clôture ou sépare les fils pour passer à travers la clôture. Il s'agit habituellement de fil de fer barbelé, et les transducteurs sont des interrupteurs mécaniques, des extensomètres ou des éléments piézoélectriques. Les clôtures en fils métalliques tendus peuvent être installées sur un ensemble de poteaux existants ou sur une rangée indépendante de poteaux en mode autonome.

Capteurs sismiques

4.55. Les capteurs sismiques sont des capteurs passifs, discrets, enfouis dans le sol et de suivi de terrain. Ils réagissent aux perturbations du sol dues au passage d'un agresseur marchant, courant, sautant ou rampant.

4.56. Un capteur sismique comprend habituellement une chaîne de géophones, munis chacun d'une bobine conductrice et d'un aimant permanent. La bobine ou l'aimant est en position fixe, l'élément qui ne l'est pas étant libre de vibrer pendant une perturbation sismique ; dans l'un ou l'autre cas, un courant électrique est généré dans la bobine. On peut réduire les signaux parasites dus à des vibrations produites à une plus grande distance des capteurs sismiques en alternant la polarité des bobines de la chaîne de géophones.

4.57. La sensibilité de ces capteurs dépend fortement du type de sol dans lequel ils sont enfouis, et la profondeur d'enfouissement optimale dépend du sol. Un enfouissement moins profond augmente la probabilité de décèlement, mais réduit la zone de décèlement, tandis qu'un enfouissement plus profond réduit la probabilité de décèlement tout en élargissant la zone de décèlement. En procédant à de courtes sections d'essai sur site et en enfouissant les capteurs à des profondeurs différentes, on peut déterminer la profondeur optimale. La largeur d'une zone de décèlement pour des agresseurs qui marchent est habituellement comprise entre 1 et 2 mètres.

4.58. La sensibilité des capteurs sismiques diminue généralement dans un sol gelé. Dans les installations où le sol gèle en hiver, on peut procéder à un ajustement saisonnier des capteurs de pression et des capteurs sismiques afin d'obtenir une sensibilité équivalente tout au long de l'année si la sensibilité réduite en hiver n'est pas acceptable.

4.59. Nombre de sources de bruit sismique peuvent affecter ces capteurs et déclencher des alarmes intempestives. La principale source naturelle d'alarmes intempestives est l'énergie éolienne, qui est transmise au sol par les clôtures, les poteaux et les arbres. Les sources sismiques artificielles sont notamment les véhicules et les équipements industriels lourds. Avec les capteurs sismiques, il est difficile de distinguer les vibrations légères, causées par exemple par des pas, à proximité du capteur, de vibrations plus fortes, dues par exemple aux véhicules circulant plus loin. Ils sont plus couramment utilisés aux frontières qu'aux périmètres des installations.

Capteurs de pression

4.60. Un capteur de pression se compose de deux tubes remplis de liquide enfouis dans des tranchées peu profondes. Il réagit comme un capteur sismique en décelant les faibles différences de pression liées à une pression exercée à proximité du capteur (par des pas, p. ex.).

Capteurs de détection de champ magnétique

4.61. Les capteurs de détection de champ magnétique sont des capteurs volumétriques passifs, associés à une clôture et de suivi de terrain, et ils peuvent être discrets ou visibles. Ils réagissent aux modifications du champ magnétique local dues au mouvement de matériaux métalliques se trouvant à proximité. Ils peuvent déceler des agresseurs et le sens de leur mouvement, ainsi que les objets métalliques (des armes, p. ex.) qu'ils portent.

4.62. Un capteur de ce type se compose d'une série de boucles ou bobines de fil métallique enfouies dans le sol. Le mouvement de matériaux métalliques à proximité d'une boucle ou bobine modifie le champ magnétique local et induit un courant électrique. Les capteurs de détection de champ magnétique sont exposés aux perturbations électromagnétiques locales, telles que la foudre, et il peut être difficile de dire si un agresseur a déclenché une alarme en portant une petite arme à proximité du capteur ou en utilisant un grand véhicule à l'extérieur du périmètre.

4.63. Un capteur de ce type peut être conçu pour être utilisé sous l'eau ou sur la terre au niveau des limites pour détecter rapidement une intrusion dans la zone protégée.

Capteurs à câble coaxial à ouvertures

4.64. Les capteurs à câble coaxial à ouvertures sont généralement des capteurs volumétriques actifs, visibles ou discrets, enfouis dans le sol et de suivi de terrain. On les appelle également capteurs à câble coaxial à dispersion ou à câble rayonnant. Un capteur de ce type crée autour du câble un champ électromagnétique qui est perturbé lorsqu'un agresseur se trouve à proximité du capteur.

4.65. Ce capteur tire son nom de la construction du câble coaxial du transducteur, dans lequel le conducteur extérieur n'assure pas le blindage complet du conducteur central, de sorte qu'une partie du signal rayonné « se disperse » au niveau des bornes du conducteur extérieur. Le volume que ces capteurs peuvent détecter s'étend nettement au-dessus du sol, pour atteindre 0,5 à 1 mètre au-dessus de la surface, et jusqu'à 1 à 2 mètres au-delà de la largeur de la séparation des câbles. La sensibilité de ces capteurs dépend de la conductivité du sol.

4.66. Certains câbles coaxiaux à ouvertures contiennent un blindage en feuilles, une encoche remplaçant les bornes : une enveloppe intérieure semiconductrice permet à une seule enveloppe extérieure de contenir les deux câbles. On peut alors installer plus facilement le capteur en utilisant une seule tranchée, sans

avoir besoin de prévoir un espacement entre les câbles. Toutefois, le volume de décèlement est, dans ce cas, légèrement inférieur à celui d'un système à double câble présentant un large espacement entre les câbles.

4.67. Dans les versions antérieures de cette technologie, une alarme unique était déclenchée lorsque quelque chose était détecté dans une zone s'étendant généralement jusqu'à 100 mètres des câbles, et le système n'autorisait qu'un seul seuil d'alarme pour chacune des zones de ce type. Les versions plus récentes indiquent, avec une précision de quelques mètres, le lieu où quelque chose a été détecté, et les seuils d'alarme peuvent varier sur toute la longueur des câbles, ce qui permet d'adapter le réglage de sensibilité aux différents moyens d'enfouissement.

4.68. La présence de métal ou d'eau dans la zone de détection peut causer deux types de problèmes si l'on utilise ces capteurs. En particulier, le mouvement d'objets métalliques et le mouvement d'eau sont des sources importantes d'alarmes intempestives, car ils fournissent de nombreuses occasions de détection. Même l'eau stagnante peut contribuer à ce problème. Le second problème est le suivant : les objets métalliques fixes et l'eau stagnante déforment le champ de rayonnement, éventuellement de façon à créer des zones où la détection n'est pas efficace. Il s'ensuit que ces capteurs ne devraient être utilisés que si les objets métalliques, les lignes de transport de force, les clôtures et les poteaux, les conduites d'eau souterraines et les câbles électriques peuvent être exclus du volume de décèlement.

Capteurs à fibre optique

4.69. Les capteurs à fibre optique sont des capteurs linéaires passifs ou actifs, enfouis dans le sol ou associés à une clôture, et de suivi de terrain, et ils peuvent être discrets ou visibles. Les fibres transparentes d'un câble à fibre optique guident la lumière de l'une de leurs extrémités à l'autre et sont entourées par un matériau de gainage. Le gainage est conçu de façon que la lumière soit réfractée vers l'âme en fibre (au cœur du câble) ; les câbles en fibre optique n'ont donc pas besoin d'être droits. La figure de diffraction (tacheture) et l'intensité de la lumière à l'extrémité du câble à fibre optique sont fonction de la forme de la fibre sur toute sa longueur. Une très faible modification de la forme de la fibre peut être décelée à l'aide de capteurs de pointe et d'un traitement informatique du signal à l'extrémité, jusqu'à une distance de 100 mètres ou au-delà.

4.70. On peut utiliser des capteurs de continuité à fibre optique pour détecter le franchissement d'une limite structurelle, tel le percement d'un mur ou d'un

plafond. Des capteurs à fibre optique à microcourbure peuvent être utilisés en tant que capteurs de vibrations ou capteurs de pression.

4.71. Une fibre monomode peut également servir de capteur en fractionnant la lumière émise par la source et en l'envoyant dans les deux sens autour d'une boucle. En cas de perturbation de la fibre, les deux faisceaux lumineux reviennent selon différentes phases, le changement de phase indiquant l'importance de la perturbation. Un seul brin de câble à fibre optique, enfoui dans le sol à une profondeur de quelques centimètres, peut donc déclencher très efficacement une alarme lorsqu'un agresseur marche sur le sol au-dessus de la fibre. Pour accroître la probabilité qu'un agresseur marche au-dessus de la fibre, on donne habituellement à celle-ci la forme d'une grille enfouie juste au-dessous de la surface.

4.72. Pour les applications montées sur une clôture, les câbles à fibre optique peuvent être montés sur la clôture en tant que type de capteur de vibrations des clôtures ou prendre la forme d'un maillage qui peut être installé sur une clôture pour créer un capteur associé à une clôture. Ces clôtures à maillage utilisent habituellement un type de capteur de continuité pour indiquer qu'un agresseur perce un trou dans la clôture. La partie supérieure de la clôture est généralement configurée pour que la fibre soit déformée si un agresseur tente d'escalader la clôture, déclenchant alors une alarme.

4.73. Les sources d'alarmes intempestives pour les capteurs à fibre optique à microcourbure sont les mêmes que pour les capteurs de vibrations, à savoir les vibrations causées par des sources extérieures, telles que les machines rotatives, les avions volant à basse altitude ou les trains ou les gros véhicules circulant à proximité. Certaines alarmes intempestives peuvent être évitées en ajustant la sensibilité du capteur, ou éliminées par filtrage en fréquence, par comptage ou par chronométrage.

Capteurs sonars

4.74. Les capteurs acoustiques sonars sont des capteurs volumétriques actifs, discrets, autonomes et de suivi de terrain. Un système de capteurs sonars utilise habituellement des capteurs acoustiques et peut être conçu pour protéger les zones d'eau à proximité des installations en décelant et en suivant les agresseurs ou les objets pénétrant dans la zone contrôlée ou protégée. Les capteurs sonars détectent de façon fiable les objets en mouvement sous l'eau, même lorsque les conditions du milieu marin sont défavorables. Plusieurs de ces systèmes peuvent être utilisés dans des zones de détection se chevauchant dans le cadre du SPP global.

4.75. Le sonar fonctionne en émettant des signaux hydroacoustiques pulsés et en recevant les signaux d'écho réfléchis par les objets en mouvement sous l'eau. Les signaux du module d'antenne sont transmis par le câble principal au dispositif d'hydroacoustique. Un sonar peut être installé au fond d'une masse d'eau et sur un ouvrage d'amarrage, une jetée ou une plateforme de génie hydraulique. Le type de configuration et la structure, le choix de l'itinéraire pour la pose des câbles principaux et leur protection sont fixés par la conception du SPP et sont fonction du terrain subaquatique et des conditions opérationnelles.

Capteurs radars

4.76. Les capteurs radars sont des capteurs volumétriques actifs, visibles, autonomes et à ligne de visée. Les dispositifs radars sont conçus pour émettre un signal radioélectrique et détecter les modifications du signal réfléchi pour détecter la présence d'objets dans la zone protégée. Ils servent à surveiller une zone contrôlée et à détecter et suivre les agresseurs et les objets, tels qu'un petit bateau ou un nageur. Les capteurs radars peuvent déterminer exactement le lieu où se trouve un agresseur, ainsi que sa vitesse et son itinéraire.

Capteurs radars laser

4.77. Les capteurs radars laser sont des capteurs volumétriques ou linéaires actifs, visibles, autonomes et à ligne de visée. Un laser émet un faisceau de lumière pour balayer une zone et mesure le temps nécessaire au retour de la lumière réfléchie à l'émetteur afin de calculer la distance qui le sépare de l'objet. La présence d'un agresseur en mouvement modifie cette distance entre deux balayages, ce qui déclenche une alarme.

Capteurs intérieurs

4.78. Le choix des capteurs intérieurs devrait recenser les équipements et méthodes d'installation qui permettent le mieux d'atteindre les objectifs de détection d'intrusions dans une installation donnée. Il faudrait à cette fin tenir compte des interactions entre les équipements, l'environnement et les agresseurs potentiels. Les capteurs intérieurs offrent un niveau supplémentaire de défense en profondeur contre les agresseurs extérieurs et une protection contre les actes malveillants que pourraient commettre des agresseurs d'origine interne n'ayant pas l'autorisation d'accéder à la zone protégée (p. ex. une zone intérieure ou vitale).

4.79. Il est généralement plus facile de sélectionner les capteurs intérieurs appropriés que les capteurs extérieurs, car les environnements bâtis sont

habituellement plus prévisibles, mesurables et contrôlables. Toutefois, pour choisir le système optimal de capteurs intérieurs, il faut savoir si et dans quelle mesure les différents capteurs sont susceptibles de causer des alarmes intempestives dans l'environnement en question. En particulier, des capteurs de mouvement (hyperfréquences et infrarouges) peuvent être installés pour assurer une couverture acceptable moyennant des ajustements de sensibilité (manuels ou automatiques) et une compensation thermique numérique afin d'éviter les alarmes intempestives produites par les sources les plus courantes.

4.80. La sélection des technologies de détection et le positionnement des capteurs appropriés peuvent permettre à un système de détection d'intrusions de fonctionner dans des conditions optimales (voir la figure 5).

Capteurs de pression

4.81. Les capteurs de pression sont des capteurs ponctuels passifs, discrets et de détection d'objets et de franchissement de limite. Ils prennent souvent la forme d'un tapis qui peut être placé autour d'un objet ou sous cet objet. Les tapis-contact contiennent une série de commutateurs ruban positionnés parallèlement les uns aux autres sur toute leur longueur. Ces commutateurs sont faits de deux bandes

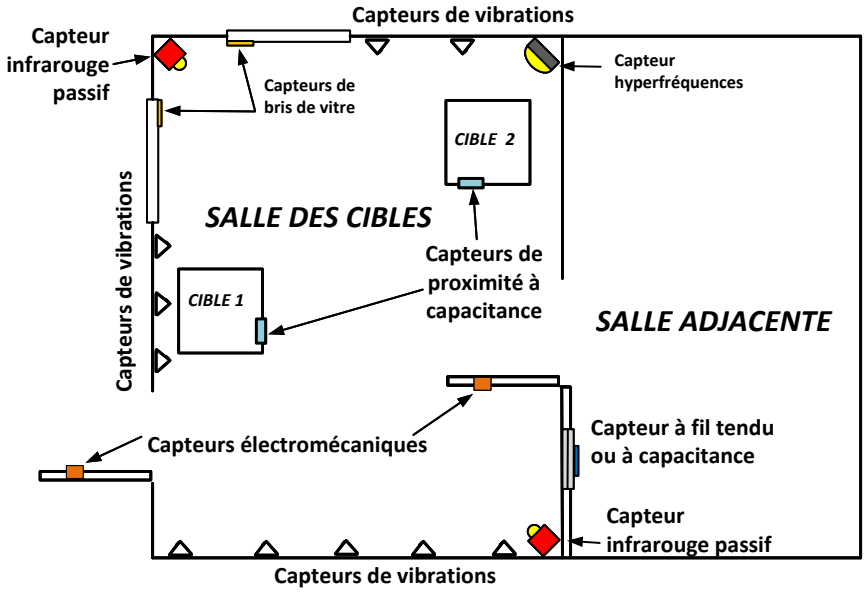


FIG. 5. Positionnement des capteurs intérieurs

de métal prenant la forme d'un ruban séparées par un matériau isolant, de sorte que, lorsqu'une certaine pression (fixée selon l'application) est exercée sur un point quelconque du ruban, les bandes de métal établissent un contact électrique et déclenchent une alarme. Les tapis-contact utilisés dans les applications de sécurité peuvent être dissimulés sous des revêtements de sol.

Capteurs à fil tendu

4.82. Les capteurs à fil tendu (capteurs de continuité) sont des capteurs linéaires passifs, discrets et de franchissement de limite. Ils sont habituellement fixés aux murs, plafonds, planchers ou fenêtres ou logés à l'intérieur pour détecter un franchissement. Le capteur se compose de petits conducteurs électriques ; il détecte le changement de courant et déclenche une alarme si l'un des conducteurs est cassé. Les conducteurs pouvant se présenter dans n'importe quelle configuration, un capteur peut être conçu pour protéger une zone ayant une forme inhabituelle. Les grilles et écrans à fil tendu peuvent servir à détecter un franchissement, par exemple par les orifices d'aération, les planchers, les murs, les plafonds, les armoires de rangements verrouillées, les chambres fortes et les lucarnes. Pour cette classe de capteurs, les taux d'alarmes intempestives sont très bas, car il faut qu'un fil soit cassé pour déclencher une alarme, et après chaque alarme, le capteur doit être réparé ou remplacé. De même, les capteurs de continuité basés sur une rupture de connexion électrique peuvent aussi utiliser des câbles à fibre optique ou des circuits imprimés.

Capteurs de bris de vitre

4.83. Les capteurs de bris de vitre sont des capteurs linéaires passifs, visibles et de détection de franchissement de limite. Ils emploient la technologie des chocs ou la technologie acoustique et détectent le bris d'une vitre d'une fenêtre. Leur efficacité dépend de caractéristiques telles que le type et l'épaisseur du verre, la distance entre le capteur et la fenêtre, et la présence éventuelle de couvre-fenêtre (p. ex. rideaux, stores) ou d'autres objets entre la vitre et le capteur. Les capteurs de chocs montés directement sur la vitre sont susceptibles de donner de meilleurs résultats. Les sources d'alarmes intempestives sont notamment le tonnerre, les bangs soniques, le matériel lourd ou les claquements de portes. Les capteurs de vibrations et de bris de vitre peuvent être complétés par des contacteurs magnétiques permettant de détecter l'ouverture d'une fenêtre sans bris de vitre.

4.84. Les capteurs acoustiques de bris de vitre sont habituellement montés sur un plafond ou un mur à une distance spécifiée des fenêtres protégées. Afin de déclencher une alarme, la plupart des capteurs de ce type doivent détecter le son

basse fréquence initial de l'impact sur la vitre suivi immédiatement du son de fréquence plus élevée du bris de vitre. Des alarmes intempestives peuvent être déclenchées par des sources de bruit de fréquences similaires, telles que celui de clés tombant sur un bureau.

4.85. Les capteurs de vibrations sont des capteurs linéaires passifs, visibles et de détection de franchissement de limite qui peuvent être installés sur des murs, des planchers et des plafonds pour déceler les tentatives de pénétration de surfaces afin d'accéder à la salle. Ces capteurs peuvent n'être que légèrement différents des capteurs de vibrations des clôtures en décelant les différentes fréquences qui seraient associées au bris de la surface. Ils peuvent utiliser les technologies à fibre optique, piézoélectrique ou « jiggle switch ».

Capteurs intérieurs et extérieurs

4.86. Certains capteurs peuvent être utilisés pour des applications tant intérieures qu'extérieures, quitte à adapter l'installation aux différents environnements. Les éléments à prendre en considération dans l'installation de ces capteurs sont notamment les suivants :

a) emplacement (p. ex., près de la cible ou à une limite) ;
b) montage ;
c) résistance à la neutralisation par manipulation frauduleuse, masquage, mystification ou autre tactique de l'agresseur ;
d) nécessité d'être à l'épreuve des intempéries (p. ex. l'eau, les températures extrêmes, la poussière) ;
e) niveaux d'intensité lumineuse et variations de ces niveaux ;
f) facilité d'accès à des fins de maintenance ;
g) spécifications du fabricant ;
h) sources d'éventuelles alarmes intempestives.

Capteurs infrarouges actifs

4.87. Les capteurs infrarouges actifs sont des capteurs linéaires actifs, visibles et à ligne de visée et peuvent être associés à une clôture ou autonomes ou détecter le franchissement d'une limite. Le plan vertical étroit dans lequel ce capteur fonctionne ne fournit pas de couverture en volume importante. Ces capteurs peuvent être utilisés sur de courtes portées pour combler les lacunes constatées au niveau de la zone de couverture, comme pour les portails, les portes et les portiques. Ils peuvent également être utilisés dans des applications de longue portée jusqu'à 100 mètres.

4.88. Les capteurs infrarouges actifs émettent depuis une diode électroluminescente un faisceau infrarouge à travers une lentille collimatrice et reçoivent le faisceau traversant une lentille collectrice qui focalise l'énergie sur une photodiode. Le capteur détecte le changement d'énergie du faisceau reçu lorsqu'un objet opaque bloque le faisceau ou modifie les caractéristiques de réflexion.

4.89. Les capteurs à faisceau unique sont disponibles pour les systèmes point à point, mais les capteurs multifaisceaux sont en principe utilisés pour les applications de sécurité nucléaire, car il est très facile de neutraliser ou d'éviter un capteur à faisceau unique. La figure 6 présente un exemple de système point à point composé de capteurs multifaisceaux disposés en deux séries verticales de modules émetteurs (E) et récepteurs (R) (le nombre et la configuration des modules sont l'affaire du fabricant). La « clôture » de faisceaux multiples qui en résulte déclenche une alarme si l'un quelconque des faisceaux uniques est interrompu. Les capteurs multifaisceaux incorporent généralement un type de logique qui déclenche une alarme si un agresseur tente de mystifier un récepteur en dirigeant sur lui une autre source infrarouge.

4.90. Si la « visibilité » entre les deux séries est réduite, par exemple par le brouillard atmosphérique, la neige, la fumée ou la poussière, le système pourrait produire des alarmes intempestives. De plus, la chute d'objets, les petits animaux ou d'autres objets en mouvement pourraient obstruer le faisceau infrarouge suffisamment pour déclencher une alarme.

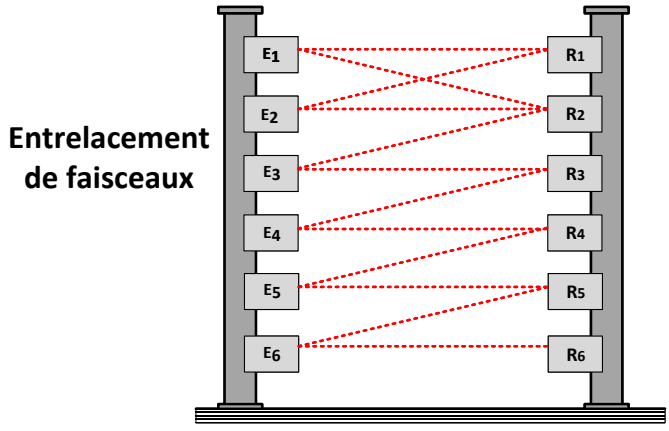


FIG. 6. Système infrarouge point à point actif utilisant des faisceaux multiples pour créer un entrelacement de faisceaux

4.91. Avec les capteurs infrarouges actifs, la surface du sol doit être plane car le faisceau se propage en ligne droite : si cette surface est convexe, elle bloquera le faisceau ; si elle est concave, un agresseur pourrait passer sous le faisceau sans être détecté. Les capteurs à double technologie peuvent pallier cette limite.

Capteurs infrarouges passifs

4.92. Les capteurs infrarouges passifs sont des capteurs volumétriques passifs, visibles et à ligne de visée qui peuvent être autonomes ; ils sont le plus souvent utilisés pour la détection de mouvement intérieur. Ils détectent des changements d'énergie thermique causés, par exemple, par une personne pénétrant dans le volume du capteur. Il s'agit habituellement d'un accroissement d'énergie thermique dû au fait que la température de l'agresseur est plus élevée que la température d'arrière-plan ; dans un environnement où la température est élevée, ces capteurs pourraient également détecter un agresseur dont la température est moins élevée que la température d'arrière-plan. Des lentilles spéciales focalisent le faisceau infrarouge sur le dispositif de détection du capteur et créent un champ visuel spécifique ; selon les lentilles utilisées, ce champ visuel peut offrir une visualisation étendue sur une courte distance ou une visualisation étroite sur une longue distance. Les lentilles grand-angulaires permettent une détection volumétrique, comme à l'intérieur d'une pièce, tandis que les lentilles à angle faible peuvent protéger une zone longue et étroite, comme un couloir ou un périmètre. Par ailleurs, les lentilles segmentent le champ visuel en zones sensibles et zones non sensibles.

4.93. Les capteurs infrarouges passifs devraient, si possible, être montés de sorte que le mouvement d'un agresseur soit susceptible de traverser la ligne de visée, pour laquelle la sensibilité est plus élevée. Des alarmes intempestives pourraient être déclenchées par les conditions atmosphériques, des débris apportés par le vent et des animaux, et la détection pourrait ne pas être fiable en cas de forte pluie. Le capteur infrarouge passif est le plus sensible lorsque la température de l'arrière-plan est nettement différente de celle d'un agresseur. La portée de ces capteurs peut dépasser 100 mètres. Comme il s'agit de dispositifs optiques, le seul moyen de limiter la portée maximale consiste à diriger le capteur sur un objet solide, comme le sol, à l'extrémité de la zone de détection souhaitée (voir la figure 7).

4.94. La figure 8 présente un modèle du capteur infrarouge passif intérieur le plus habituel. La subdivision du champ visuel en segments à angle solide indiqués est accomplie par la lentille segmentaire. Ces lentilles sont soit des lentilles du type

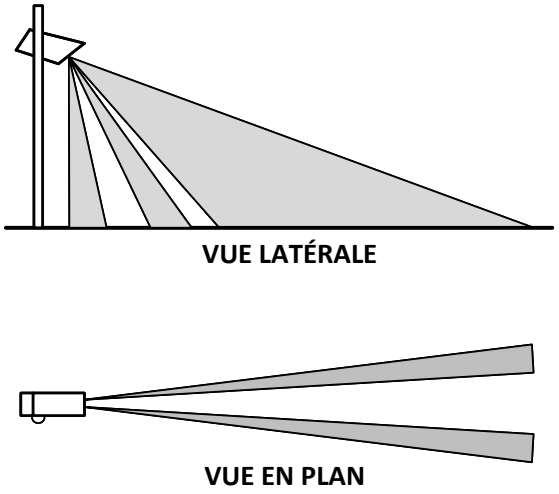


FIG. 7. Couverture des capteurs infrarouges passifs

de Fresnel, placées devant un capteur pyroélectrique, soit des lentilles de type miroir segmenté, qui renvoie l'énergie sur le capteur.

4.95. Les capteurs infrarouges passifs sont le plus sensibles lorsqu'ils détectent un mouvement dans leur champ de vision et le moins sensibles dans le cas d'un mouvement dirigé directement vers le capteur ou s'en éloignant (c'est le contraire pour les capteurs hyperfréquences), car le mouvement dans leur champ de vision se traduit par un plus grand nombre de segments absorbés sur une distance plus courte. Cette caractéristique devrait être prise en considération pour déterminer l'endroit où monter le capteur.

4.96. Pour réduire les alarmes intempestives causées par les variations de la chaleur émise par le sol au passage de nuages, les capteurs comparent l'énergie thermique reçue à partir de deux modèles de détection en forme de rideau. Une personne entrant dans une zone cause un déséquilibre. Les changements météorologiques devraient affecter à égalité les deux zones afin d'empêcher le déclenchement d'une alarme. Une application intérieure ne peut utiliser qu'un seul capteur.

4.97. Par les autres sources d'alarmes intempestives, on peut citer les insectes sur la lentille et d'autres sources d'énergie infrarouge, telles que les sources de chaleur (p. ex. les radiateurs, les chauffe-eaux, les canalisations d'eau chaude) ou les surfaces chaudes (p. ex., les rayons du soleil traversant les fenêtres peuvent créer localement des surfaces chauffées susceptibles d'émettre de l'énergie dans

la longueur d'onde correspondante). Les capteurs à double technologie peuvent pallier cette limite.

Capteurs à champ électrique ou à capacitance

4.98. Les capteurs à champ électrique (y compris les capteurs à capacitance) sont des capteurs volumétriques, linéaires ou ponctuels actifs, visibles et de suivi de terrain et ils peuvent être associés à une clôture ou autonomes ou détecter le franchissement d'une limite. Les capteurs intérieurs de ce type créent un circuit électrique résonant entre un objet métallique protégé et une unité de commande, ce qui en fait des capteurs actifs. La capacitance entre l'objet métallique protégé et le sol devient une composante de la capacitance totale d'un circuit accordé d'un oscillateur. La fréquence d'oscillation du circuit accordé pourrait être fixe ou varier.

4.99. Pour les applications périmétriques, la sensibilité de certains capteurs à champ électrique peut être augmentée de façon à étendre leur volume d'un mètre au

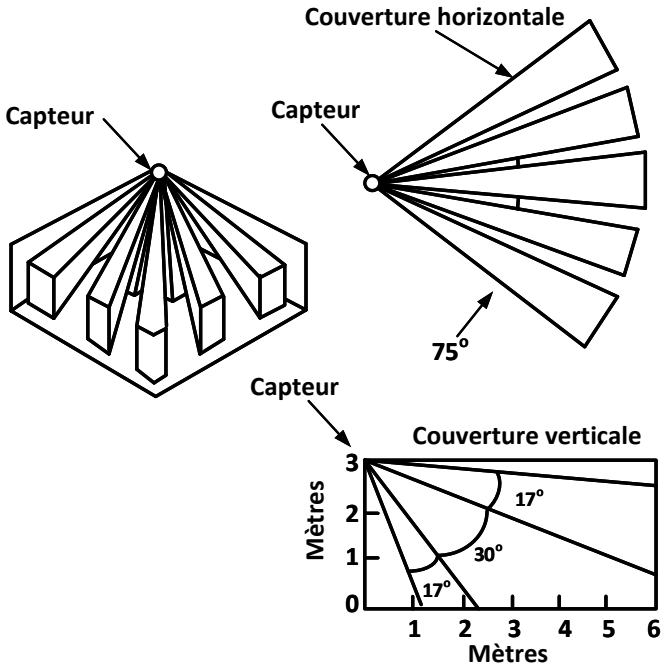


FIG. 8. Modèle de capteur infrarouge passif (reproduit avec l'aimable autorisation des Laboratoires nationaux Sandia)

maximum au-delà du fil métallique ou du plan dans lequel il se trouve. Toutefois, une sensibilité élevée multiplie habituellement les alarmes intempestives, et les capteurs à champ électrique pourraient être exposés à la foudre, à la pluie et au mouvement de la clôture ou de petits animaux. Les tempêtes de verglas pourraient causer des dommages importants aux fils et aux isolateurs muraux. Une bonne mise à la terre électrique de ces capteurs peut contribuer à réduire les alarmes intempestives, et les autres objets métalliques (la clôture, p. ex.) se trouvant dans le volume du capteur devraient être bien mis à la terre, car une mise à la terre défectueuse ou intermittente est une source d'alarmes intempestives. Étant donné que le volume du capteur est relativement important et s'étend au-delà du plan de la clôture, les capteurs à champ électrique sont plus difficiles que les autres capteurs associés à une clôture à neutraliser en creusant au-dessous ou en passant par-dessus la clôture.

4.100. La performance des capteurs à champ électrique montés sur leurs propres poteaux est généralement améliorée parce que la sensibilité plus élevée peut servir à élargir le volume du capteur, puisque l'on verra diminuer le taux d'alarmes intempestives dû au mouvement de la clôture.

4.101. Ce type de capteur peut également être utilisé pour déceler le franchissement d'une limite par les ouvertures des bâtiments existantes à ferrements, telles que les grilles, les conduits de ventilation, les cadres de fenêtre et les portes.

4.102. Pour les applications intérieures, les capteurs de proximité à champ électrique peuvent servir à protéger des objets ou des zones définies à l'intérieur des bâtiments (p. ex., les technologies sûres ou sensibles utilisées dans une zone de travail). Pour les applications dans lesquelles l'objet à protéger doit être mis à la terre, on peut considérer cet objet comme le plan de sol, et la mise à la terre peut être réalisée à l'aide d'une couverture de capacitance drapant l'objet. Si la couverture est suffisamment grande pour couvrir entièrement l'objet, toute tentative faite pour accéder à celui-ci déplace la couverture, ce qui modifie la capacitance et déclenche une alarme. Ces capteurs peuvent détecter des modifications de capacitance ne dépassant pas quelques picofarads.

4.103. La sensibilité des capteurs à champ électrique peut être affectée par une variation d'humidité relative et la proximité d'autres objets métalliques de l'objet protégé. Les variations d'humidité relative modifient les caractéristiques diélectriques et la conductivité atmosphérique. Si la sensibilité du capteur est réglée de façon à déceler un agresseur à plusieurs mètres de l'objet, cette variation de conductivité pourrait suffire à déclencher une alarme intempestive. Les capteurs

utilisant un circuit à autoéquilibrage s'ajustent automatiquement aux variations d'humidité relative et à la proximité d'objets métalliques de l'objet protégé. Des alarmes intempestives pourraient néanmoins être déclenchées si l'objet se trouve dans une zone d'intense circulation piétonnière.

Capteurs hyperfréquences

4.104. Les capteurs hyperfréquences sont des capteurs volumétriques actifs, visibles, à ligne de visée, autonomes ou de mouvement intérieur. En règle générale, on utilise des capteurs hyperfréquences bistatiques, dotés de deux antennes hyperfréquences identiques situées aux deux extrémités de la zone du capteur. L'une des antennes est reliée à un émetteur hyperfréquences et l'autre à un récepteur hyperfréquences. Le récepteur détecte les changements affectant l'énergie du faisceau direct entre les antennes et les signaux hyperfréquences réfléchis par le sol et d'autres objets. Les capteurs hyperfréquences réagissent aux modifications de la somme vectorielle du signal reçu causées par des objets se déplaçant dans la partie du faisceau émis qui se trouve dans le champ de vision du récepteur. Un agresseur en mouvement crée donc de nouvelles réflexions à mesure qu'il s'approche du capteur ou lorsqu'il bloque le signal, et augmente ou diminue le signal reçu en fonction de la phase du signal.

4.105. Les critères de détection par hyperfréquences sont définis en fonction de ce qui suit :

a) La surface du sol doit être plate de façon que l'objet ne soit pas protégé contre le faisceau hyperfréquences, ce qui empêcherait sa détection.
b) Pour surmonter les conséquences de la diminution de la capacité de détection dans les premiers mètres devant les antennes, les antennes des capteurs adjacents devraient se chevaucher de façon à couvrir cette zone.
c) Le volume de détection des capteurs hyperfréquences bistatiques est plus important que celui de la plupart des autres capteurs de détection d'intrusions : la section efficace du volume peut avoir jusqu'à 4 mètres de largeur et 3 mètres de hauteur. Les capteurs hyperfréquences peuvent également être empilés pour obtenir des volumes de détection plus importants.

4.106. Ces capteurs peuvent tolérer un éventail relativement large de conditions environnementales sans provoquer d'alarmes intempestives. Toutefois, la zone de détection ne devrait pas être encombrée par la neige et la végétation. Pour réduire au minimum les alarmes intempestives dues aux réflexions depuis les eaux de surface (pluie ou fonte de la neige), les surfaces plates de la zone de détection devraient être en pente ou disposer d'un autre moyen de drainage de l'eau. Le

gravier est souvent utilisé pour réduire la fréquence des alarmes intempestives due à l'eau stagnante.

4.107. Dans le cas des capteurs hyperfréquences monostatiques, l'émetteur et le récepteur se trouvent dans le même élément. L'énergie hyperfréquence transmise par faisceau radiofréquence est pulsée par l'émetteur et le récepteur détecte les modifications survenues dans le faisceau réfléchi. Un agresseur en mouvement provoque une légère modification de la fréquence réfléchie et, de ce fait, déclenche une alarme. Ces capteurs sont « crénelés en distance », ce qui veut dire que l'exploitant peut fixer la distance au-delà de laquelle le mouvement ne déclenchera pas d'alarme. Les installations monostatiques sont généralement utilisées dans un volume fixe (p. ex. un couloir) ou au niveau des portails et des portiques.

4.108. La détection est basée sur le décalage Doppler entre le signal émis et le signal reçu causé par un objet en mouvement dans le champ d'énergie. Les capteurs hyperfréquences monostatiques sont le plus sensibles au mouvement dirigé directement sur le capteur ou s'en éloignant car ce mouvement maximise le changement d'hyperfréquences. Ces capteurs devraient en principe être positionnés de façon que le mouvement d'un agresseur depuis les points d'entrée probables vers les objets protégés soit approximativement orienté vers le capteur ou s'en éloigne. La forme de la zone de détection est régie par la conception de l'antenne (voir la figure 9).

4.109. Le crénelage en distance peut servir à réduire la distance de détection efficace, en particulier si le capteur doit être utilisé en un lieu où l'énergie hyperfréquence peut traverser les murs de la zone ou de la salle protégée. Les hyperfréquences traversent la plupart des types de verre, de plâtre, de gypse, de contreplaqué et d'autres matériaux couramment utilisés dans les murs. Cela peut provoquer des perturbations indésirables au niveau des capteurs. Les objets métalliques, tels que les meubles de grande taille, les écrans ou les clôtures se trouvant dans la zone protégée, peuvent créer des « zones d'ombre », dans lesquelles la couverture est incomplète.

4.110. Pour les applications intérieures, les capteurs hyperfréquences devraient en principe être montés près du plafond de la zone protégée et orientés vers la couverture souhaitée, mais à bonne distance des objets métalliques qui pourraient réfléchir l'énergie hyperfréquence et provoquer des alarmes intempestives.

Capteurs de mouvement vidéo

4.111. Les capteurs de mouvement vidéo sont des capteurs volumétriques passifs, visibles ou discrets, autonomes ou de mouvement intérieur. Ces capteurs traitent le signal vidéo envoyé par des caméras de TVCF qui sont utilisées en intérieur comme en extérieur. Ces caméras sont généralement installées sur des tours, des plafonds ou des murs pour fournir une vue de la zone d'intérêt, et elles peuvent être utilisées conjointement à des fins de détection, de surveillance et d'évaluation d'alarme et en tant qu'archive visuelle. Il pourrait y avoir lieu de prévoir un éclairage artificiel pour les caméras lumière du jour fonctionnant en continu.

4.112. Les capteurs de mouvement vidéo dotés d'une capacité d'analyse vidéo (modules de matériel, matériel et logiciel vidéo de traitement des alarmes) peuvent être adjoints aux systèmes de caméras analogiques ou numériques qui utilisent des caméras lumière du jour, des caméras dans le proche infrarouge, l'imagerie thermique et les vues à 360°. Cette technologie, modulaire, peut être installée avec la caméra ou au PCS.

4.113. Les capteurs de mouvement vidéo détectent un changement de niveau de signal pour une certaine partie de la scène observée. Selon l'application, cette

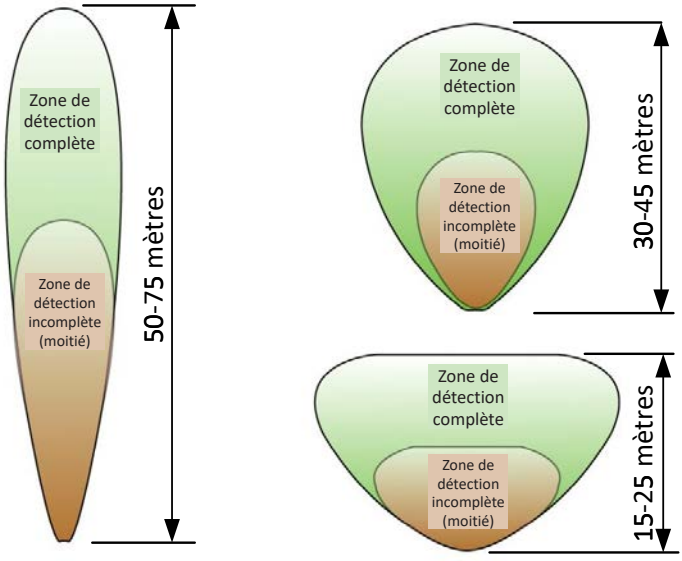


FIG. 9. Modèles habituels de détection hyperfréquence monostatique

partie peut être un grand rectangle, une série de points discrets ou une grille rectangulaire de points.

4.114. Ces capteurs sont plus susceptibles de détecter un mouvement dans l'ensemble du champ visuel qu'un mouvement vers la caméra ou s'en éloignant. L'arrière-plan de la zone de détection devrait de préférence être d'une couleur neutre, car il est plus facile pour un agresseur de se fondre dans un arrière-plan très clair ou très foncé. Une visibilité réduite, par exemple, par le brouillard, la neige ou une forte pluie pourrait également diminuer la probabilité de détection.

4.115. Les sources potentielles d'alarmes intempestives pour les capteurs de mouvement vidéo utilisés à l'extérieur sont notamment le mouvement des supports de caméra instables, les variations de luminosité dues, par exemple, aux nuages, à des objets réflecteurs et aux phares de véhicules, les objets en mouvement, comme les oiseaux et d'autres animaux sauvages, les débris apportés par le vent et les précipitations sur la caméra ou à proximité. On peut diminuer l'impact de certaines de ces sources en utilisant un écran limitant le champ de vision de la caméra.

Capteurs de vibrations

4.116. Les capteurs de vibrations sont des capteurs linéaires passifs, visibles et qui peuvent être enfouis dans le sol, associés à une clôture ou capables de détecter un franchissement de limite. Les capteurs de vibrations intérieurs englobent les capteurs de bris de vitre. Les capteurs de vibrations détectent le mouvement de la surface à laquelle ils sont fixés : un impact sur la surface la fait vibrer à une certaine fréquence qui dépend de sa construction et, dans une moindre mesure, de celle de l'objet ayant causé l'impact. Ces capteurs sont conçus pour réagir aux fréquences associées à des occurrences de bris de vitre ou d'autres objets et de pénétration, telles que l'entrée par effraction (fréquences généralement supérieures à 4 kHz) et ne pas tenir compte des vibrations normales des bâtiments, comme celles causées par les appareils de climatisation ou de chauffage.

4.117. Ces capteurs pourraient déclencher des alarmes intempestives s'ils sont montés sur les murs ou structures exposés à des vibrations extérieures, et il n'est pas conseillé de les utiliser sur des structures susceptibles de subir fréquemment des vibrations sévères (dues, p. ex., aux machines rotatives). Toutefois, si les structures sont exposées à des impacts occasionnels, les capteurs de vibrations pourraient être efficaces s'ils sont équipés d'un accumulateur à impulsions ou d'un circuit compteur.

Capteurs électromécaniques

4.118. Les capteurs électromécaniques sont des capteurs linéaires ou ponctuels actifs ou passifs, visibles ou discrets conçus pour la détection de franchissement de limite et d'objets. Le type le plus courant est un commutateur relativement simple servant généralement à détecter l'ouverture de portes et de fenêtres. La plupart des commutateurs de ce type sont magnétiques et se composent d'un élément de commutation et d'un élément magnétique. La figure 10 montre un commutateur à lames magnétique et ses composants en position fermée et ouverte.

4.119. L'élément de commutation, qui contient un commutateur à lames magnétique, est monté sur la partie fixe de la porte ou de la fenêtre. L'élément magnétique, qui contient un aimant permanent, est monté sur la partie mobile de la porte ou de la fenêtre, et se trouve adjacent à l'élément de commutation lorsque la porte ou la fenêtre est fermée. L'espace entre l'élément de commutation et l'élément magnétique est ajusté de sorte que le champ magnétique créé par l'aimant permanent maintienne le commutateur à lames en position fermée (ou sûre). L'ouverture de la porte ou de la fenêtre déplace l'aimant, ce qui réduit le champ magnétique et met le commutateur en position ouverte (celle de l'alarme).

4.120. On peut compléter l'ajustement à l'aide d'un aimant de polarisation pour empêcher la neutralisation du commutateur : on parle alors de commutateur magnétique symétrique. On peut aussi prévoir des commutateurs à lames multiples et des aimants multiples, des dispositifs de détection de pannes de fusibles et de chutes de tension, et un blindage. Certaines unités incorporent des électroaimants internes, qui ont des interactions complexes avec les aimants permanents mobiles,

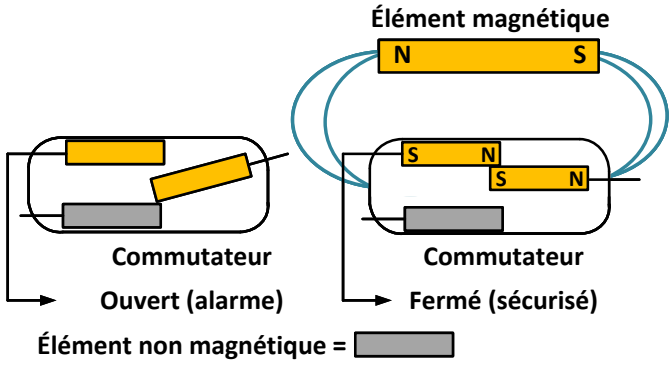


FIG. 10. Commutateur à lames magnétique

ce qui accroît la complexité de ces unités et les rend plus difficiles à neutraliser. De plus, certains modèles sont conçus pour pouvoir s'autovérifier.

4.121. Un commutateur à effet Hall contient des bascules électroniques au lieu de commutateurs à lames mécaniques et doit être alimenté. Il est destiné à fournir un niveau de sécurité plus élevé que les commutateurs magnétiques symétriques. Comme les autres commutateurs magnétiques, il se compose d'un élément de commutation et d'un élément magnétique, mais son fonctionnement repose sur les dispositifs à effet Hall de l'élément de commutation, qui mesurent la force du champ magnétique de l'élément magnétique. Une alarme est déclenchée si un changement suffisant du champ magnétique se produit. Les commutateurs magnétiques symétriques et les capteurs à effet Hall offrent tous une meilleure protection contre la manipulation frauduleuse et la neutralisation, y compris par les agresseurs d'origine interne, que le commutateur magnétique simple.

Capteurs d'imagerie thermique

4.122. Les capteurs d'imagerie thermique sont des capteurs volumétriques passifs, discrets, à ligne de visée, autonomes ou de mouvement intérieur. Les caméras d'imagerie thermique permettent de reconnaître et d'identifier différents types d'agresseurs, même dans de mauvaises conditions météorologiques ou d'éclairage et à différentes distances.

Récapitulation des technologies de capteurs

4.123. Le tableau 1 récapitule les différentes technologies de capteurs de détection d'intrusions en fonction des différents modes de fonctionnement, types de capteurs et applications de détection.

Évaluation des alarmes

4.124. La dernière phase du processus de détection est l'évaluation des alarmes, qui consiste à :

a) déterminer la cause de chaque alarme ;
b) décider si l'alarme est déclenchée par un agresseur ou est une alarme intempestive (p. ex. une alarme anodine due à un événement environnemental ou une fausse alarme) ;
c) s'il est confirmé que l'alarme est causée par un agresseur, fournir des renseignements sur ce dernier : qui fait quoi, où et quand et combien sont-ils ?

TABLEAU 1. TYPES DE CAPTEURS ET APPLICATIONS CARACTÉRISTIQUES

Capteur	Méthode[a]	Type de capteur[b]	Application[c]
Extérieur			
Sismique	P	L	CE, ST
Détection de champ magnétique	P	V	CE, AC, ST
À câble coaxial à ouvertures	A	V	CE, ST
À fibre optique	A, P	L	CE, AC, ST
À câble dynamométrique	P	L	AC
Sonar	A	V	AUT, ST
Radar	A	L, V	AUT, LV
Radar laser	A	L, V	AUT, LV
Pression	P	L	CE, ST
Intérieur			
Pression	P	P	FL, O
Fil tendu	P	L	FL
Bris de vitre	P	L	FL
Les deux			
Actif infrarouge	A	L, V	FL, AUT, AC, LV
Passif infrarouge	P	V	AUT, MI, LV
À champ électrique	A	L, P, V	FL, AUT, AC
À capacitance	A	V	FL, AUT, AC
Hyperfréquences	A	V	AUT, MI, LV
Mouvement vidéo	P	V	AUT, MI, LV
Vibrations	P	L	CE, FL, AC
Électromécanique	A, P	L, P	FL, O
Imagerie thermique	P	V	AUT, MI, LV

[a] Actif (A), passif (P).

[b] Capteur linéaire (L), ponctuel (P), volumétrique (V).

[c] Associé à une clôture (AC), autonome (AUT), câble enfoui (CE), franchissement de limite (FL), ligne de visée (LV), mouvement intérieur (MI), objet (O), suivi de terrain (ST).

4.125. L'évaluation des alarmes fait appel à un personnel compétent qui tire parti des technologies vidéo, d'éclairage et de communication appropriées.

4.126. Les alarmes peuvent être évaluées à l'aide des éléments visuels fournis par les technologies vidéo et/ou le personnel. Les deux méthodes d'évaluation reposent sur un bon éclairage et des lignes de visée appropriées. L'évaluation

vidéo peut réduire la durée habituelle d'une évaluation et, de ce fait, le délai d'intervention.

4.127. L'évaluation vidéo englobe habituellement les images de caméras fixes qui permettent l'enregistrement d'événements, la lecture instantanée et la prise de vues image par image, et de caméras dotées de fonctions de pivotement horizontal et d'inclinaison verticale ainsi que de fonctions de contrôle manuel ou de recherche intelligente (p. ex. déplacement automatique de la caméra qui indique l'endroit du mouvement détecté).

4.128. Lorsqu'elle est effectuée par le personnel, l'évaluation consiste à utiliser les observations faites par les gardiens, les forces d'intervention ou d'autres personnes, en fonction du plan de sécurité de l'installation. Ce mode d'évaluation pourrait être nécessaire si le système d'évaluation vidéo ne fonctionne pas (p. ex. parce qu'il est en maintenance ou parce que les conditions météorologiques sont mauvaises), n'est pas adapté à une situation donnée ou n'est pas disponible. Pour procéder à cette évaluation, le personnel doit se trouver dans l'endroit approprié pour observer la situation, et la probabilité d'une évaluation correcte par lui de cette situation diminue à mesure qu'augmente le temps qu'il lui faut pour atteindre cet endroit. Étant donné que les variables d'évaluation dépendent du SPP et de l'état de l'installation, la probabilité d'évaluation doit être prise en considération au moment de déterminer la probabilité de détection.

4.129. Les technologies permettant de classer les alarmes selon leur degré de priorité peuvent aider à évaluer celles-ci. Quand plusieurs alarmes sont déclenchées en même temps, le système d'alarme pourrait avoir la capacité de les classer automatiquement par ordre d'importance pour le PCS.

Technologie vidéo

4.130. Les applications de la technologie vidéo sont notamment les suivantes :

a) Évaluation des alarmes pour déterminer rapidement et précisément la menace pesant sur l'installation. Cela permet, le cas échéant, de déclencher une intervention appropriée.
b) Détection d'intrusions, y compris l'utilisation de capteurs de mouvement vidéo et de caméras de surveillance.
c) Contrôle de l'accès pour le personnel et les véhicules. Un logiciel de reconnaissance faciale peut être utilisé pour faciliter l'identification du personnel. Les technologies vidéo peuvent également aider à commander à

distance le matériel de sécurité (p. ex., les portes automatiques ou le matériel destiné à arrêter les véhicules).

d) Détection d'articles interdits, notamment le matériel de surveillance placé sous les véhicules et les caméras endoscopiques d'inspection.

e) Prise de conscience de la situation, pour renseigner les forces d'intervention sur les actions de l'agresseur et les endroits où il se trouve pendant une attaque.

f) La vidéo pré-incident renseigne sur la situation qui précède le moment où une alarme est déclenchée ou lui est concomitante, aux fins d'évaluation de l'alarme.

g) La vidéo post-incident renseigne sur l'agresseur et les outils qu'il a avec lui et peut fournir des indications sur sa cible, ce qui peut aider les forces d'intervention à l'intercepter.

h) La vidéo enregistrée (pré- et post-incident) peut servir, après un incident détecté, à appuyer les enquêtes et les poursuites.

4.131. Pour être efficaces, ces différentes applications nécessitent des résolutions vidéo différentes. La résolution vidéo détermine le degré de netteté des détails d'une image et dépend des éléments du système vidéo (notamment la lentille, la caméra, le système de transition vidéo, le matériel d'enregistrement, la compression des données, l'écran de visualisation des images). La résolution peut être perdue en plusieurs points du système (voir la figure 11). Le système vidéo devrait être fréquemment testé en tant que système afin de s'assurer que la combinaison de ses éléments fournit la résolution nécessaire dans toutes les conditions de fonctionnement (p. ex. différentes configurations ou fluctuations de la bande passante). Le type d'évaluation aux fins de laquelle il est prévu d'utiliser l'emplacement d'une caméra devrait déterminer la résolution nécessaire, et le système devrait être choisi de façon à fournir cette résolution.

4.132. Les trois niveaux génériques de résolution à prendre en considération sont ceux nécessaires à la détection, à la classification et à l'identification, encore que ces niveaux dépendent également de l'objet à évaluer et du niveau d'évaluation requis (p. ex. la classification d'une image en tant qu'être humain ou animal nécessite une résolution inférieure à celle qu'exige l'identification d'une personne particulière).

4.133. La résolution globale du système devrait être évaluée compte tenu de la caméra, de la lentille, du système de vidéotransmission, du système d'enregistrement vidéo, des méthodes de compression et de la résolution de l'écran du moniteur. Les systèmes de sécurité vidéo disponibles sur le marché pourraient offrir des résolutions descendant jusqu'à 10 pixels/m, mais cette résolution n'est

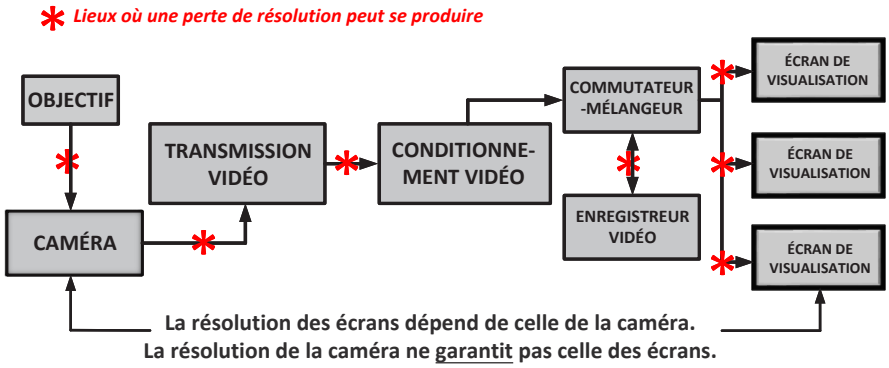


FIG. 11. Schéma du système de caméra montrant les points où la résolution peut être perdue

d'ordinaire pas suffisante pour les besoins de la protection physique. La résolution vidéo n'est pas seulement une affaire de pixels/m, mais dépend également de facteurs tels que la taille du capteur d'image, le champ de vision, l'arrière-plan et la bande passante. La résolution nécessaire dépend du but poursuivi. En règle générale, il est suggéré de disposer d'une résolution de 25 pixels/m pour détecter la présence d'un objet dans la zone d'intérêt. Une résolution augmentée jusqu'à environ 125 pixels/m permet de classifier un objet et, de ce fait, fournit suffisamment d'informations pour déterminer ce qui est présent en fonction de la classe (animal, débris apporté par le vent ou être humain). Selon toute probabilité, l'identification d'une personne nécessitera une résolution encore supérieure, d'environ 250 pixels/m, pour permettre d'identifier précisément une personne sur la base de son apparence physique.

Caméras

4.134. La fonction de base d'une caméra consiste à convertir une image optique de la scène physique en un signal (vidéo) électrique, se prêtant à une transmission vers un autre lieu pour affichage. La plupart des caméras utilisent des composants à semiconducteurs et ont diverses caractéristiques pour optimiser l'image qu'elles produisent. Le fabricant spécifie le format et la résolution des images produites par la caméra.

4.135. Les caméras devraient être montées sur une tour ou un support stable à une hauteur compatible avec l'usage prévu pour le système. Par exemple, une caméra de reconnaissance faciale peut être montée à hauteur de tête, tandis qu'une caméra destinée à surveiller une zone peut l'être à une hauteur beaucoup plus élevée afin d'en élargir le champ de vision. L'installation des caméras doit tenir compte des

éléments suivants : le champ de vision, les objets se trouvant dans le champ de vision, l'accessibilité aux fins de maintenance (p. ex. utilisation de tours pliantes) et la protection contre les agresseurs, d'origine interne ou externe, et contre le soleil. Par exemple, on peut protéger les caméras contre les agresseurs d'origine interne ou externe en les installant entre les clôtures intérieures et extérieures du périmètre et en ne permettant qu'au personnel de maintenance autorisé d'accéder à cette zone. Il peut être difficile d'atténuer les effets du lever et du coucher du soleil, car celui-ci ne se lève et ne se couche jamais à la même heure. En plaçant les caméras plus haut pour qu'elles regardent vers le bas, on peut contribuer à atténuer ces effets, mais on réduit alors la longueur des zones de détection.

4.136. Le contrôle du diaphragme, la durée d'exposition et l'amplification du signal électronique permettent à la plupart des caméras de produire une image de la luminosité moyenne de la scène. Les points lumineux dans le champ de vision de la caméra augmentent la luminosité moyenne, ce qui amène la caméra à compenser en réduisant la production moyenne de signaux vidéo. En conséquence, les parties sombres de l'image tendent à devenir trop sombres. Le nombre et l'intensité des zones lumineuses et obscures dans le champ de vision de la caméra pour lesquelles celle-ci est en mesure de compenser sont limités : c'est ce que l'on appelle la plage dynamique de la caméra.

4.137. Dans des conditions de faible luminosité, la plupart des caméras compensent automatiquement le manque d'éclairement lumineux en augmentant tout à la fois la durée d'exposition (contrôle de l'obturateur) et le gain d'amplification, compte tenu du niveau de luminosité globale fixé par l'utilisateur. Les caméras à objectif à diaphragme automatique compensent la modification des niveaux de luminosité en ouvrant ou en fermant le diaphragme. Certaines caméras numériques permettent à l'utilisateur de programmer la compensation du niveau d'éclairement lumineux. On peut également hiérarchiser l'ordre dans lequel le contrôle du diaphragme, le contrôle de l'obturateur et le gain d'amplification sont utilisés pour contrôler l'éclairement lumineux.

4.138. La cadence de prise de vue est le nombre d'images prises par seconde de vidéo. La vitesse d'obturation correspond à la durée pendant laquelle chaque image est exposée. Si cette vitesse est trop longue, l'image sera floue. Le dénominateur de la vitesse d'obturation devrait être approximativement égal au double du nombre d'images par seconde enregistrées.

4.139. Pour compenser la faible luminosité, le contrôle de l'obturateur permet d'ouvrir celui-ci pour allonger la durée d'exposition. Les durées d'exposition longues donnent des images floues pour les objets en mouvement, tandis que

les gains d'amplification plus élevés sur les signaux très bas niveau de lumière produisent des images plus granuleuses ; aucun de ces deux résultats n'est souhaitable pour une évaluation vidéo. Les fabricants de caméras indiquent souvent une sensibilité correspondant à différentes conditions d'essai et différents paramètres, notamment le niveau minimal d'éclairement lumineux de l'imageur de la caméra qui est considéré comme pouvant donner une image utilisable. Ces spécifications ne prennent pas en compte la baisse du niveau d'éclairement lumineux causée par l'objectif de la caméra, si bien que la quantité de lumière qui doit entrer dans l'objectif pour atteindre le niveau minimal d'éclairement de l'imageur peut être nettement supérieure au niveau spécifié. Les spécifications peuvent également ne pas indiquer les conditions d'éclairement et les conditions sur les lieux en fonction desquelles a été déterminée la sensibilité de la caméra. Outre le niveau minimal d'éclairement, il faut disposer des renseignements ci-après :

a) état de la vidéo de sortie (p. ex. signaux de sortie de la caméra, gain, durée d'exposition) ;
b) transmittance de l'objectif (c'est-à-dire le pourcentage de la lumière incidente apparaissant devant l'objectif qui est transmis à l'imageur) ;
c) nombre f de l'objectif (c'est-à-dire le niveau de réduction de la lumière sur l'imageur, déterminé par l'ouverture du diaphragme) ;
d) réflectance de la scène d'essai (c'est-à-dire le pourcentage de lumière incidente sur une scène renvoyé à sa source).

4.140. Dans certains cas, la sensibilité revendiquée par le fabricant pourrait être irréaliste et indiquer une performance meilleure que celle qui peut être obtenue dans les installations réelles. Une réflectance de scène exagérément élevée, des durées d'exposition dont la longueur est inacceptable et une bien trop grande ouverture de diaphragme (nombre f faible) sont autant de facteurs susceptibles de donner lieu à une sensibilité plus élevée pendant les essais que dans les conditions réelles. De plus, ces paramètres sont généralement déterminés pour une caméra appelée à enregistrer une scène statique : si la nécessité d'observer efficacement un mouvement est également prise en compte, la sensibilité effective de la caméra pourrait être nettement inférieure à celle revendiquée par le fabricant.

4.141. Les imageurs de caméra sont sensibles à une région spécifique du spectre électromagnétique. Si le spectre de sortie (couleur) de la source d'éclairement et la réponse spectrale de l'imageur ne sont pas compatibles, il faudra soit augmenter la lumière pour obtenir un éclairement suffisant, soit disposer d'une source de lumière différente. Les différences physiques entre les imageurs influent négativement sur la faible performance (sensibilité) lumineuse de la caméra, le plus souvent d'un facteur deux.

4.142. L'imageur doit être sensible à la couleur de la lumière produite par la source d'éclairage. Les caméras noir et blanc ont besoin de moins d'éclairement que les caméras couleur pour produire le même niveau de sortie vidéo. Si une source d'énergie dans le proche infrarouge est utilisée, une caméra noir et blanc peut produire une image vidéo visible même si la lumière proche infrarouge n'est pas visible par l'œil.

4.143. Lorsque l'évaluation des alarmes repose sur des systèmes vidéo, il faudrait de préférence utiliser plusieurs caméras à cette fin. Par exemple, si un capteur périmétrique couvre une longue distance, il pourrait être nécessaire de disposer de plusieurs caméras pour que l'évaluation des alarmes puisse se faire dans toute la zone de détection. Le déclenchement automatique des caméras dans les zones de détection voisines, en particulier là où les zones de couverture des capteurs se recoupent partiellement, pourrait également être utile.

4.144. Par ailleurs, il faudrait examiner et prendre en compte les facteurs influant sur le fonctionnement de la caméra. Par exemple, dans un climat très froid, on peut utiliser un mécanisme de réchauffement du boîtier de la caméra pour maintenir une température minimale. On pourrait également prendre des mesures visant à prévenir l'accumulation de neige et de glace, qui pourrait affecter la performance de la caméra.

4.145. Certains systèmes vidéo d'évaluation des alarmes utilisent un plus petit nombre de caméras, mais prévoient des supports panoramiques basculants et des objectifs zoom (on parle alors souvent de caméras VPIZ). Ces caméras peuvent être rapidement réorientées pour visualiser la zone où une alarme a été déclenchée, souvent en une fraction de seconde. Les systèmes anciens étaient à commande manuelle, mais les systèmes VPIZ actuels peuvent être programmés et préréglés de façon que la caméra s'oriente automatiquement vers le lieu où une alarme a été déclenchée dès la réception de celle-ci. De cette façon, une seule caméra peut couvrir jusqu'à quatre ou cinq zones équipées d'alarmes. Toutefois, la vitesse de réaction est essentielle : si la caméra réagit trop lentement, un agresseur pourrait se trouver hors de son champ de vision avant qu'elle ne focalise sur la zone où l'alarme a été déclenchée.

4.146. Cette approche présente certains inconvénients importants. Si plusieurs alarmes sont déclenchées simultanément dans les zones couvertes par une seule caméra VPIZ, le système ne peut pas enregistrer toutes ces scènes et un ordre de priorité doit être établi pour déterminer l'alarme vers laquelle la caméra devra se tourner. De plus, l'utilisation de caméras VPIZ ne permet pas d'enregistrer une pré-alarme, car il est peu probable que la caméra soit orientée vers la source d'une

alarme immédiatement avant celle-ci. Enfin, il faut prévoir des opérations de maintenance et des réparations plus fréquentes dans le cas du support panoramique basculant mécanique.

4.147. Une caméra fixe est à préférer à des caméras VPIZ pour l'évaluation immédiate d'une détection, mais ces dernières pourraient être utiles pour la surveillance post-alarme d'un événement ou d'une zone. Elles sont également utiles pour suivre un agresseur au-delà du lieu où l'alarme a été déclenchée.

4.148. On peut aussi utiliser des caméras d'imagerie thermique dans le cadre d'un système de télévision en circuit fermé. Ces caméras permettent de détecter, de reconnaître et d'identifier différents types d'objets dans de mauvaises conditions météorologiques et d'éclairage à différentes distances.

Objectifs

4.149. Les principaux paramètres de sélection des objectifs de caméras sont des variables interdépendantes (comme le format, la distance focale, le champ de vision et le nombre f). Le choix des valeurs dépend des objectifs du concepteur, notamment de la manière dont le système vidéo s'articulera avec les autres systèmes de sécurité. Le nombre f et le réglage du diaphragme déterminent la zone mise au point, aussi appelée profondeur de champ. Quelle que soit la caméra, la zone d'évaluation doit être nette ou avoir une profondeur de champ qui permette d'obtenir des images ayant la résolution nécessaire dans toutes les conditions d'éclairage.

4.150. D'autres caractéristiques peuvent améliorer la performance de l'objectif. Certains objectifs prévoient un réglage automatique de l'ouverture du diaphragme, notamment des filtres gris neutres placés au centre de l'objectif, qui, en liaison avec le circuit de la caméra, permettent d'ajuster automatiquement les niveaux de lumière. Il est alors possible de réduire davantage de lumière intense lorsque l'ouverture du diaphragme est plus petite que le filtre gris neutre. Certains objectifs ont des revêtements spéciaux destinés à renforcer ou à filtrer et éliminer certaines longueurs d'onde de la lumière pour optimiser la performance de l'objectif à des fins données. Par exemple, certains objectifs renforcent la transmission du proche infrarouge (longueurs d'onde comprises entre 800 et 1 100 nm), qui peut être utilisé par les caméras à semiconducteurs.

4.151. Les objectifs devraient être sélectionnés de façon à fournir la résolution et le champ de vision nécessaires. Lorsqu'un système vidéo est conçu pour être utilisé sur un périmètre, on peut déterminer, à partir d'une « approximation de la

distance et de la largeur », la longueur maximale de la zone qui peut être évaluée avec une caméra et un objectif donnés (voir la figure 12). Le champ de vision inférieur (généralement indiqué au bas de l'écran) est normalement plus étroit que la largeur de la zone, et le champ de vision supérieur est normalement plus large que le champ de vision en limite de résolution. La caméra ne peut pas visualiser une zone non visible entre la caméra et le champ de vision inférieur.

Système de vidéotransmission

4.152. Un système de vidéotransmission a pour fonction de relier les caméras aux écrans de visualisation vidéo du PCS sans effets indésirables sur le signal vidéo. Le système comprend habituellement des caméras, des systèmes de transmission avec ou sans fil, un matériel de traitement et des composants de stockage et d'affichage. La majorité des applications requièrent également un système d'éclairage. Les systèmes vidéo peuvent être analogiques ou numériques, ou un mélange des deux.

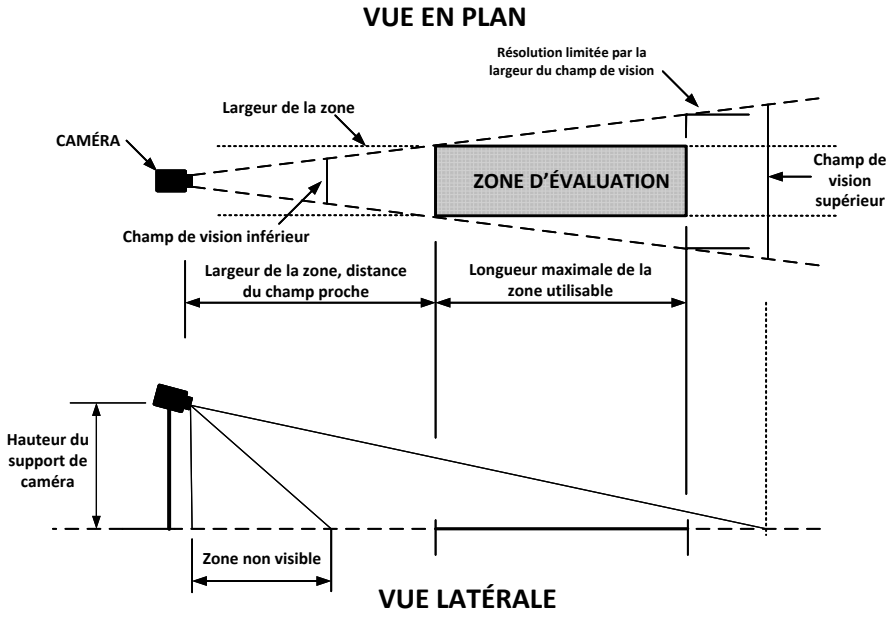


FIG. 12. Géométrie de la zone d'évaluation du périmètre

4.153. Les signaux vidéo envoyés par plusieurs caméras peuvent être transmis en réseau de plusieurs façons, par exemple :

a) câble coaxial (numérique et analogique) ;
b) fibre optique (numérique et analogique) ;
c) liaisons hyperfréquences, systèmes optiques (infrarouge) ou autres systèmes sans fil (numérique ou analogique) ;
d) connexion réseau (numérique).

4.154. La figure 13 montre un système analogique pour lequel l'écran de visualisation devrait avoir une résolution correspondant étroitement à celle des caméras utilisées dans le système d'évaluation. Pour les systèmes numériques, la résolution de l'écran de visualisation devrait être au moins aussi élevée que celle de l'imageur de la caméra.

4.155. La mise en place d'un système numérique repose généralement sur des composants (caméras, mémoires, écrans de visualisation) connectés par un réseau. Les concepteurs de systèmes doivent choisir un système analogue ou numérique pour obtenir la qualité d'image (notamment la résolution), la disponibilité et la fiabilité nécessaires pour l'application. Les considérations de sécurité pour les réseaux de vidéotransmission font l'objet de la section 6.

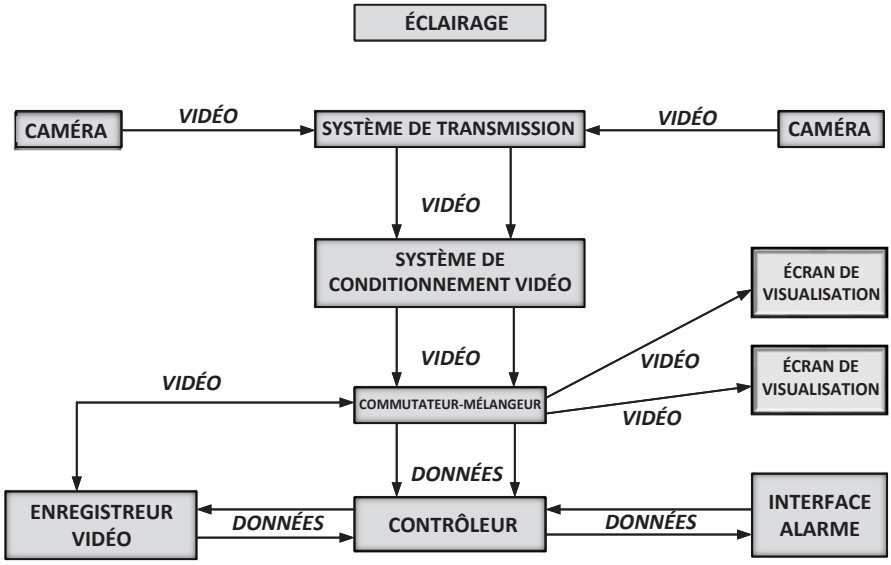


FIG. 13. Composants analogiques d'un système vidéo

4.156. La capacité du réseau numérique doit être prise en considération lors de la conception d'un tel système. Le nombre de caméras et la cadence de prise de vue et la résolution des images affichées influent sur l'efficacité du système vidéo : plus le réseau comporte de caméras et plus la cadence de prise de vue est élevée, plus forte est la probabilité que la vidéo soit lente ou « se fige ». Les techniques de compression numérique peuvent améliorer la capacité du réseau, mais influent négativement sur la résolution à l'écran.

4.157. La transmission câblée utilise soit des signaux électriques transportés par des câbles en cuivre, soit des signaux optiques transportés par des câbles à fibre optique. L'utilisation de câbles en cuivre (coaxiaux, p. ex.) pourrait entraîner une certaine dégradation du signal s'il n'est pas conditionné par des égaliseurs, des transformateurs d'isolement ou des caleurs. Les câbles à fibre optique sont moins touchés par la perte de signal, mais pourraient nécessiter des composants supplémentaires pour la conversion analogique-numérique du signal.

4.158. Les boucles de masse, le bruit induit et les sautes de puissance dues aux éclairs peuvent endommager le matériel électrique, mais ne concernent pas les câbles à fibre optique. Avec la transmission par fibres optiques, il n'est pas nécessaire de conditionner le signal à l'aide d'égaliseurs, de transformateurs d'isolement ou de caleurs, mais il pourrait y avoir lieu de prévoir des répéteurs pour fournir une puissance de signal suffisante pour les très longs câbles.

4.159. Nombre de systèmes vidéo analogiques anciens utilisant plus de caméras qu'il n'y a d'écrans de visualisation au PCS, on utilise un matériel de commutation pour connecter plusieurs signaux vidéo à un ou plusieurs dispositifs de contrôle (écrans de visualisation, magnétoscope). En général, le système d'alarme associé s'articule avec le système de commutation de telle façon que le déclenchement d'une alarme dans une zone quelconque fait automatiquement s'afficher les signaux de sortie de la caméra associés sur un écran local.

4.160. Les types de systèmes de commutation analogique sont notamment les suivants :

a) Commutation manuelle par contacteur bouton-poussoir, de sorte que le signal vidéo est transmis par le commutateur-mélangeur sans conditionnement ni base de temps électronique.
b) Commutation séquentielle, qui consiste à balayer une à une toutes les séquences de signaux de sortie de la caméra, la cadence de balayage ou le nombre de fois qu'une même image est affichée étant généralement ajustable.

c) Commutation activée par l'alarme : le signal vidéo provenant de la caméra dans la zone où se produit l'alarme est automatiquement envoyé vers la sortie quelle que soit l'entrée sélectionnée avant le déclenchement de l'alarme.
d) Commutation à distance, qui implique une commutation multiple, dont une partie est effectuée à distance avant que les signaux ne parviennent au PCS.

4.161. Les systèmes modernes utilisent un logiciel multiplex numérique pour gérer les images de caméras. Un multiplexeur est un dispositif qui sélectionne un signal d'entrée analogique ou numérique entre plusieurs signaux et le transmet en tant que signal de sortie unique.

Enregistrement vidéo

4.162. Les systèmes d'enregistrement vidéo fournissent des données historiques à étudier ultérieurement, notamment en utilisant les fonctions de relecture et de pause, pour aider l'évaluation et constituer un journal d'audit. Les systèmes d'enregistrement vidéo peuvent utiliser des enregistreurs analogiques (c'est-à-dire des magnétoscopes à bande) ou numériques. Les enregistrements numériques peuvent également être utilisés aux fins d'évaluation en temps réel.

4.163. Le nombre de caméras, le nombre d'images enregistrées par seconde (habituellement entre 2 et 30) pour chaque caméra, la résolution de ces images et la durée de stockage déterminent la capacité de stockage nécessaire pour les enregistrements vidéo. La quantité de données enregistrées tient compte de l'équilibre à trouver entre les besoins du système vidéo à utiliser aux fins d'évaluation et la capacité de stockage disponible. Par exemple, une qualité vidéo globale élevée favorise la lecture en direct pour une évaluation en temps réel, des images en haute résolution peuvent permettre d'identifier un agresseur (au lieu d'indiquer simplement qu'un agresseur est présent) et une cadence de prise de vue rapide peut aider à évaluer ce que fait un agresseur, mais il faut pour cela stocker un plus grand nombre de données. Les systèmes de gestion vidéo peuvent comprimer les données vidéo à stocker et ajuster automatiquement la qualité des images selon qu'il s'agit d'une situation d'alarme (cadence de prise de vue rapide et résolution élevée) ou d'une situation normale (cadence de prise de vue lente et basse résolution).

4.164. Les enregistreurs vidéo numériques peuvent être commandés par un système informatique qui s'articule avec la fonction de surveillance du capteur d'un SPP, de sorte que, lorsqu'un capteur génère une alarme, l'enregistreur peut recevoir comme instruction de lire la vidéo pré- et post-alarme provenant de la caméra qui couvre la zone dans laquelle se trouve le capteur.

4.165. On peut réduire la taille des fichiers vidéo stockés en diminuant la durée de l'enregistrement et la cadence de prise de vue et en compressant les fichiers. Pour visualiser une image enregistrée compressée, on commence par la décompresser, mais les détails de l'image provenant du fichier décompressé pourraient être dégradés par rapport à l'image originale d'avant la compression. On voit que la qualité globale de l'image extraite des données vidéo enregistrées est fonction de la résolution de la caméra, de la cadence de prise de vue, de la résolution de l'image capturée et du degré de compression appliqué.

4.166. Il faudrait installer au PCS un nombre suffisant d'écrans de visualisation vidéo pour permettre une évaluation rapide et efficace sans interférence provenant d'autres contrôles et sorties de systèmes.

4.167. Le contrôleur vidéo est la principale interface SPP interconnecté/système vidéo. Ce contrôleur contrôle automatiquement les entrées et les sorties du multiplexeur, surveille l'enregistreur et affiche les scènes sur l'écran de visualisation. Le contrôleur vidéo peut faire partie intégrante du logiciel et du matériel d'alarme, de communication et d'affichage, qui sont généralement intégrés aux systèmes d'enregistrement numérique et en réseau.

Éclairagisme

4.168. Un éclairage de sécurité adéquat est nécessaire pour les zones ou structures qui forment le périmètre d'une installation nucléaire où sont utilisés des systèmes de détection des intrusions et d'évaluation des alarmes. L'éclairage peut également permettre d'évaluer les alarmes déclenchées dans des zones telles que les zones vitales, les zones d'entreposage de matières nucléaires et les zones intérieures, ou les zones où se trouvent des services de distribution ou des infrastructures essentielles de protection physique.

4.169. L'éclairage de sécurité est installé aux fins suivantes :

a) télévision en circuit fermé (notamment les capteurs de mouvement vidéo) pour la détection (en particulier l'évaluation des alarmes) et la surveillance des agresseurs ;
b) dissuasion d'agresseurs ;
c) zones de dissimulation éventuelle ;
d) points de contrôle de l'accès (p. ex. permettre l'identification des personnes et des véhicules, et la détection d'articles interdits) ;
e) activités des gardiens et des forces d'intervention.

4.170. L'éclairage de sécurité aide à protéger les gardiens et les forces d'intervention en réduisant les possibilités pour un agresseur de rester inaperçu. Lorsque l'éclairage de sécurité est déficient, on peut prévoir, entre autres dispositions, des postes de sécurité supplémentaires, des patrouilles et des dispositifs de vision nocturne.

4.171. Au moment de planifier un système d'éclairage de sécurité, il faudrait prendre en considération le contraste entre un agresseur et l'arrière-plan. Par exemple, les couleurs claires des parties inférieures des bâtiments et structures ou du sol pourraient rendre plus visible un agresseur portant des vêtements sombres.

4.172. Tout système d'éclairage proposé devrait être planifié en même temps que les autres systèmes de sécurité, notamment les systèmes de télévision en circuit fermé et les systèmes de détection d'intrusions. L'utilisation d'un éclairage de sécurité peut également affecter la sûreté nucléaire opérationnelle et les questions générales de santé et de sûreté, et il importe de comprendre ces interfaces et les priorités associées. Il faudrait veiller à ce que les pannes d'éclairage soient signalées rapidement et qu'il y soit remédié de même : certains systèmes déclenchent une alarme en cas de panne d'éclairage.

4.173. Lorsque l'éclairage n'est pas disponible ou ne peut pas être utilisé, on peut avoir recours à une caméra d'imagerie thermique. Celle-ci tire parti du rayonnement thermique émis par les objets pour produire une image sans éclairage : tous les objets émettent un rayonnement thermique, qui n'est pas visible, et les objets plus chauds (comme le corps humain) apparaissent plus clairs sur l'image que les objets plus froids. L'image ainsi produite ressemble en général à une photo en noir et blanc, bien que certains systèmes appliquent différentes couleurs à l'image pour représenter différentes températures.

4.174. Si la législation ou les politiques environnementales locales exigent d'un exploitant qu'il réduise la consommation d'électricité ou abaisse les niveaux d'intensité lumineuse, les caméras bas niveau de lumière, les appareils d'éclairage infrarouge discrets, les systèmes d'éclairage par détection de mouvement et les systèmes d'éclairage à diodes électroluminescentes peuvent être envisagés comme des solutions alternatives à faible consommation d'énergie.

Types de systèmes d'éclairage

4.175. Le type de système d'éclairage devrait être sélectionné sur la base des prescriptions de sécurité applicables à l'installation. L'éclairage de sécurité se

décline selon quatre approches : éclairage permanent, éclairage auxiliaire, éclairage amovible et éclairage de secours.

4.176. L'éclairage permanent est le type d'éclairage de sécurité le plus couramment utilisé. Une série de luminaires fixes sont disposés de façon à éclairer en permanence une zone donnée dans des conditions de faible luminosité, avec des cônes de lumière qui se recoupent partiellement. L'éclairage auxiliaire est disposé de façon similaire, mais les luminaires sont normalement éteints pendant la nuit et sont allumés automatiquement ou manuellement si une activité suspecte éveille l'attention des gardiens ou si elle est détectée par des capteurs. Si l'éclairage auxiliaire est utilisé, il importe de le gérer avec soin car il peut avoir des effets indésirables (p. ex. en avertissant des agresseurs que leur présence a été détectée). L'éclairage amovible comprend des groupes intégrés de luminaires et de générateurs amovibles manuels qui peuvent fonctionner à l'endroit et au moment voulus, qu'il fasse nuit ou non. Ce type de système vient généralement compléter l'éclairage permanent ou auxiliaire ou est utilisé à titre de mesure compensatoire. L'éclairage de secours peut faire double emploi avec tous les systèmes susmentionnés, mais prend le relais lorsque l'alimentation électrique normale est en panne ou que le système d'éclairage normal ne fonctionne pas pour d'autres raisons. L'éclairage de secours repose sur un système d'alimentation sans coupure, tel que les générateurs et batteries installés ou portatifs.

Éclairement lumineux

4.177. Naturel ou artificiel, l'éclairement lumineux se mesure en lux. Lorsqu'il s'adapte à de faibles niveaux de luminosité et lorsque le contraste entre l'objet et l'arrière-plan est bon, l'œil peut voir un agresseur à un niveau d'éclairement d'environ 1 lux, mais ce niveau doit être beaucoup plus élevé lorsqu'il s'agit de reconnaître une personne. L'œil met d'ordinaire entre 5 et 20 minutes pour s'adapter à des niveaux de faible luminosité, selon l'âge de la personne ; il conviendrait d'en tenir compte au moment de planifier une stratégie relative aux patrouilles que les gardiens sont appelés à effectuer.

4.178. Pour garantir que l'éclairement lumineux renvoyé à la caméra dans des conditions de faible luminosité soit suffisant et que le contraste entre les agresseurs et l'arrière-plan ait toutes chances d'être adéquat, la surface du sol de la zone d'évaluation devrait être suffisamment réfléchissante.

4.179. L'éclairement lumineux et la réflexion sont généralement mesurés à l'aide d'un luxmètre à une certaine distance de la zone d'évaluation, à une distance du sol comprise entre 15 et 30 cm. L'éclairement moyen dans une zone

couverte par un certain nombre de luminaires est calculé en procédant à plusieurs mesures effectuées en des lieux équidistants de l'aire globale de la surface. Cette mesure est appelée « éclairement horizontal de la scène » ou simplement « éclairement de la scène ».

4.180. L'éclairement moyen de la scène devrait être suffisant pour favoriser l'évaluation vidéo et l'évaluation visuelle par les gardiens et les forces d'intervention. Par exemple, pour une zone dégagée de tout obstacle, un éclairement de la scène moyen de 10 lux pour une surface dont la réflectivité entre 25 et 35 % peut fournir une luminosité suffisante aux fins de l'évaluation.

4.181. Le ratio lumière/obscurité à l'intérieur d'une zone donnée influe également sur la capacité de faire des évaluations. La figure 14, où le ratio lumière/obscurité est d'environ 20/1, montre d'importants angles morts de couverture. Ces derniers sont nettement réduits dans la figure 15, où le ratio lumière/obscurité est d'environ 4/1. Un éclairage de ratio lumière/obscurité de 6/1 ou moins donne en général un contraste suffisant aux fins d'évaluation. Au moins 75 % du champ de vision de la caméra devrait de préférence présenter au moins l'éclairement minimal moyen et un ratio lumière/obscurité acceptable.

FIG. 14. Scène à ratio lumière/obscurité élevé, d'environ 20/1 (reproduit avec l'aimable autorisation des Laboratoires nationaux Sandia)

4.182. Étant donné que la plupart des applications d'éclairage utilisent des ampoules qui produisent de la lumière visible, l'estimation de la lumière nécessaire peut être entachée d'erreurs si le spectre de l'imageur de la caméra, qui englobe la partie infrarouge du spectre, n'est pas pris en considération.

Disposition de l'éclairage

4.183. Pour éviter que les caméras ne soient orientées directement sur une source de lumière, tous les luminaires devraient en principe se trouver au-dessus des caméras et hors de leur champ de vision (voir la figure 16). Afin d'éviter les effets potentiels de la rétrodiffusion par la poussière ou le brouillard, la source de lumière ne devrait pas être montée directement au-dessus de la caméra. On peut aussi réduire ces effets au minimum en fixant un parasoleil au verre de protection du boîtier de la caméra. Les poteaux d'éclairage périmétrique devraient être installés à l'intérieur du périmètre concerné, pour éviter qu'un agresseur ne puisse s'en servir pour escalader la clôture délimitant le périmètre.

4.184. On peut modéliser un système d'éclairage proposé pour estimer les niveaux d'éclairement de la scène et les ratios lumière/obscurité. Il faudrait de préférence tester physiquement la conception d'un tel système avant de l'installer dans la configuration définitive de l'éclairage périmétrique. On peut réaliser ce

FIG. 15. Scène à ratio lumière/obscurité faible, d'environ 4/1 (reproduit avec l'aimable autorisation des Laboratoires nationaux Sandia)

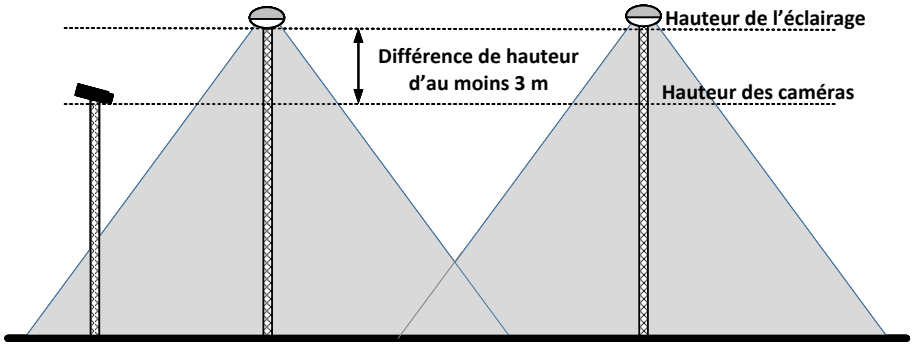


FIG. 16. Différence de hauteur proposée entre l'éclairage extérieur et les caméras

test en installant au moins cinq luminaires (pour les installations en une seule ligne) et en mesurant l'éclairement selon les critères indiqués plus haut.

4.185. Il sera vraisemblablement nécessaire d'ajuster et de modifier l'ensemble du système d'éclairage après son installation de façon à obtenir la performance prévue. Par exemple, les essais de caméras font souvent apparaître des réflexions ou des points lumineux non identifiés qu'il convient de corriger.

4.186. Il faudrait envisager de disposer l'éclairage d'une façon similaire pour les applications intérieures. Les niveaux normaux d'éclairage intérieur permettent d'utiliser une caméra vidéo d'une sensibilité moindre que celle qui est nécessaire pour les applications extérieures. Les sources d'éclairement infrarouge proche peuvent être utilisées à l'intérieur pour que la surveillance vidéo garde une certaine discrétion.

Prescriptions d'éclairage

4.187. L'éclairage périmétrique doit respecter des prescriptions spécifiques selon que le périmètre est isolé, semi-isolé ou non isolé. Dans le cas des périmètres clôturés isolés, les clôtures sont situées à au moins 30 m des bâtiments ou zones d'exploitation. Dans le cas des périmètres clôturés semi-isolés, les zones d'approche dégagées de tout obstacle sont délimitées par des clôtures situées à 20 ou 30 m. Dans le cas des périmètres clôturés non-isolés, les clôtures sont immédiatement adjacentes aux zones d'exploitation. Par exemple, on peut contrôler l'éclairage de façon que l'itinéraire des patrouilles effectuées par les gardiens se trouve dans une relative obscurité, tandis que la zone dégagée ou la zone surveillée est éclairée. Les prescriptions de sûreté de l'État ou de l'exploitant

devraient être prises en compte lorsque les gardiens effectuent des patrouilles dans les zones faiblement éclairées (p. ex. pour éviter tout risque de trébuchement).

4.188. Les prescriptions d'éclairage sont différentes pour les points de contrôle de l'accès. Les points de contrôle de l'accès pour les piétons doivent être suffisamment éclairés pour que leur personnel puisse reconnaître les personnes et examiner leurs moyens d'identification. Les prescriptions peuvent être différentes lorsque les points d'accès sont dotés de systèmes automatisés de contrôle. L'entrée des véhicules peut nécessiter un éclairage supplémentaire pour faciliter la fouille des véhicules et l'identification de leurs occupants. Les points d'accès moins utilisés peuvent avoir les mêmes niveaux d'éclairage que le périmètre avoisinant, avec la possibilité d'augmenter ces niveaux en fonction des besoins. Les postes de garde installés aux points de contrôle de l'accès nécessitent des niveaux d'éclairement intérieur qui permettent aux gardiens de voir les véhicules et les piétons qui s'approchent tout en réduisant autant que faire se peut la mesure dans laquelle l'intérieur du bâtiment peut être vu de l'extérieur.

4.189. À l'intérieur du périmètre de l'installation, d'autres zones et structures peuvent avoir besoin d'éclairage, comme les zones ouvertes, les zones d'entreposage, les zones de travail, les jetées, les quais et d'autres zones et structures sensibles, dont chacune peut avoir ses propres prescriptions d'éclairage. Les zones ouvertes non occupées et les zones d'entreposage extérieures (p. ex. les zones d'entreposage de matières, les voies ferrées de garage et les zones de stationnement) devraient normalement être éclairées de façon que les gardiens puissent les examiner dans de bonnes conditions lorsqu'ils effectuent des patrouilles. En principe, une zone ouverte adjacente à un périmètre devrait être éclairée selon les mêmes prescriptions que le périmètre. L'éclairage des zones d'entreposage extérieures devrait prévoir un éclairage suffisant dans les allées, passages et renfoncements pour éliminer les zones sombres où un agresseur pourrait se cacher.

4.190. L'éclairement est tout particulièrement nécessaire dans le cas des approches de voie d'eau, des jetées et des quais s'ils sont présents dans une installation. On peut utiliser des projecteurs pour éclairer une zone donnée ou pour des raisons spécifiques si nécessaire. Cet éclairage ne devrait pas contrevenir aux règles et règlements régissant l'utilisation de la mer ou des voies de navigation intérieures (c'est-à-dire qu'il ne devrait pas être éblouissant pour les pilotes).

Types de lampes et leurs caractéristiques

4.191. Pour choisir le type de lampe nécessaire, il convient de tenir compte des caractéristiques du système d'évaluation et des autres systèmes d'éclairage de sécurité (p. ex. si l'évaluation repose sur du matériel infrarouge, un éclairage approprié est nécessaire). Les types de lampes couramment utilisés à des fins de sécurité sont notamment les suivants :

a) Lampes à incandescence : La lumière est émise par un filament porté à incandescence à l'intérieur d'un globe sous vide.
b) Lampe fluorescente : La lumière est produite par un arc électrique dans un tube rempli de vapeur de mercure basse pression. La vapeur émet un rayonnement ultraviolet qui est converti en lumière visible par la poudre fluorescente déposée sur la surface intérieure du tube.
c) Lampe à décharge à haute intensité : La lumière est générée par interaction directe d'un arc avec un gaz. Les gaz utilisés dans les lampes à décharge à haute intensité sont notamment la vapeur de mercure, les halogénures métalliques et la vapeur de sodium haute et basse pression. L'argon est généralement ajouté pour favoriser l'ignition, et d'autres poudres ou vapeurs peuvent l'être pour améliorer le rendu des couleurs.
d) Lampe électroluminescente : La lumière est générée à partir d'une diode à semiconducteurs. Les lampes électroluminescentes contiennent un ensemble de diodes électroluminescentes dans une enveloppe appropriée.
e) Lampe proche infrarouge : La lumière est générée par des ensembles de diodes électroluminescentes ou d'ampoules à incandescence, et la lumière visible est éliminée par des filtres extérieurs.

Postes de sécurité

4.192. Un PCS (ou une station de surveillance si un PCS n'est pas nécessaire) a pour fonction d'assurer une surveillance permanente des alarmes, une évaluation des alarmes à l'aide de caméras de surveillance en circuit fermé, une surveillance en circuit fermé et la communication avec les gardiens, le personnel de l'installation et les forces d'intervention (voir la figure 17) [1, 2]. Dans certains cas, le personnel du PCS utilise du matériel de contrôle des accès à distance. Par ailleurs, un PCS tient des registres à des fins diverses, notamment les enquêtes sur les incidents. S'agissant des installations abritant des matières nucléaires de catégorie I ou de catégorie II, ou d'installations dont le sabotage pourrait avoir de graves conséquences radiologiques, telles que déterminées par l'autorité compétente, le PCS devrait se trouver dans la zone protégée et être occupé en permanence, et l'accès à ce poste devrait être contrôlé. Un PCS n'est

FIG. 17. Poste central de sécurité (reproduit avec l'aimable autorisation des Laboratoires nationaux Sandia)

pas recommandé pour les autres installations nucléaires, mais le terme PCS, utilisé dans la présente publication par souci de simplicité, fait référence au lieu d'exercice des fonctions susmentionnées.

4.193. Un PCS doit être conçu et fonctionner d'une manière analogue à la salle de commande d'un réacteur nucléaire et appliquer les mêmes méthodes de gestion des interfaces homme-machine. Bien que mise au point pour les industries de type process, l'utilisation de la norme ANSI/ISA-18.2-2016, *Management of Alarm Systems for the Process Industries* de l'Institut national américain de normalisation et de l'International Society for Automation [22], peut être envisagée lors de la conception d'un PCS pour une installation nucléaire.

4.194. Tous les systèmes de sécurité physique (notamment les systèmes de détection des intrusions, les systèmes de contrôle des accès et les systèmes d'évaluation et de surveillance par caméras en circuit fermé) devraient être intégrés dans le PCS et gérés comme il convient. Le PCS devrait permettre de surveiller et d'évaluer les alarmes transmises par tous les capteurs et se doter

d'un réseau spécifique, redondant, sécurisé et diversifié de communications voix-données intérieures et extérieures. Dans l'exercice de ses fonctions, le PCS tire profit des recommandations ci-après :

a) Tous les capteurs installés dans l'installation devraient transmettre leurs signaux directement au PCS.
b) Si une alarme n'est pas surveillée au PCS, des procédures explicites devraient être en place pour assurer une bonne communication avec le poste central pour intervention immédiate. Celle-ci ne devrait pas être conditionnée à une évaluation par le personnel de l'installation.
c) Le personnel de l'installation devrait être à même de fournir au PCS des informations sur les incidents qui se produisent, notamment l'accès non autorisé, l'introduction d'articles interdits, le déclenchement d'alarmes de sûreté (p. ex. les alarmes dues aux rayonnements) ou tout autre incident ou activité suspect.

Suivi des alarmes

4.195. Le personnel d'un PCS a pour fonctions principales de suivre les alarmes transmises par les capteurs, d'évaluer toutes les alarmes reçues et, en cas de besoin, de prendre les mesures d'intervention appropriées. Ce personnel doit s'acquitter de toutes ses fonctions dans le respect des procédures approuvées.

Évaluation et surveillance

4.196. Les alarmes peuvent être évaluées directement à partir d'images de caméras de surveillance en circuit fermé et/ou, indirectement, par les gardiens ou les forces d'intervention évaluant la cause de l'alarme et la signalant au PCS. Celui-ci devrait utiliser ces images et toutes alarmes ultérieures pour suivre (c'est-à-dire assurer la surveillance de) la cause de l'alarme. Le chemin suivi par l'agresseur et une description détaillée de ses mouvements, de son apparence, de ses armes et de ses actions devraient être fournis aux gardiens et aux forces d'intervention. L'utilisation de systèmes de surveillance en circuit fermé dotés de caméras VPIZ correctement placés peut renforcer la capacité de surveillance. La technologie vidéo qui inclut la relecture et la prise de vues image par image, l'enregistrement fractionné et une interface homme-machine ergonomique permet une évaluation en temps réel.

Communication

4.197. Les systèmes de communication entre le PCS, les gardiens, les forces d'intervention et les responsables de l'installation devraient être dédiés, sécurisés, redondants et diversifiés, immédiats et fiables. De plus, le personnel du PCS devrait communiquer efficacement avec d'autres organisations, telles que les organismes d'intervention d'urgence et les organisations intervenant dans la maintenance du SPP, et leur faire prendre conscience de la situation. Les communications du PCS servent à déclencher une intervention et à renseigner le personnel investi de fonctions de commandement et de contrôle pendant une intervention en cas d'événements de sécurité nucléaire.

Contrôle des accès

4.198. Un système de contrôle de l'accès permet de surveiller et de contrôler le mouvement des personnes autour d'une installation, et complète d'autres systèmes de sécurité et de gestion des situations d'urgence.

4.199. Les systèmes de contrôle des accès peuvent être intégrés au PCS dans le cadre d'un réseau de sécurité ou utilisés en tant que systèmes indépendants et autonomes. Dans les deux cas, tout système en réseau devrait être sécurisé.

4.200. Les systèmes de contrôle des accès recueillent et stockent des données sur l'accès autorisé par l'intermédiaire d'un point de contrôle de l'accès et sur les tentatives infructueuses faites pour obtenir un accès non autorisé. Ils peuvent également être configurés de façon à afficher les demandes d'accès ou à assurer des fonctions de contrôle automatisées. Le système de détection d'intrusions devrait être intégré au système de contrôle de l'accès de façon que l'accès autorisé ne génère pas d'alarmes intempestives.

4.201. Certains systèmes de contrôle des accès sont configurés de manière à autoriser une personne à vérifier à distance si une autre personne a le droit d'accéder à la zone concernée et, le cas échéant, à autoriser l'accès, par exemple en déverrouillant à distance le verrou final de la porte. En pareil cas, le système de contrôle de l'accès peut afficher une photographie stockée de la personne qui demande l'accès et des images de surveillance en circuit fermé de la zone concernée. L'exploitant peut ensuite déterminer s'il y a lieu d'autoriser ou de refuser l'accès.

Tenue des registres

4.202. Tous les incidents importants en rapport avec le contrôle de l'accès, les alarmes et les évaluations vidéo devraient être enregistrés et archivés pour examen ultérieur. Les systèmes de sécurité interconnectés (alarmes, caméras, systèmes d'enregistrement) devraient avoir une fonction d'horodatage de façon que tous les éléments du système utilisent la même référence temporelle.

4.203. La capacité du système de contrôle des accès d'enregistrer le lieu et le moment où une personne est entrée dans une zone donnée de l'installation et l'a quittée est précieuse du point de vue tant de la sécurité que de la gestion de la sûreté. Par exemple, les registres de contrôle de l'accès peuvent servir à vérifier que toutes les personnes qui se trouvaient dans un bâtiment sont bien recensées à la suite d'une évacuation d'urgence.

4.204. On peut aussi utiliser les registres d'alarmes automatisés pour recueillir et analyser les fausses alarmes et les alarmes intempestives, et des tendances peuvent être analysées pour faciliter l'établissement des calendriers de maintenance. Les registres d'alarmes et d'évaluation vidéo peuvent également être utilisés aux fins des enquêtes sur les événements de sécurité nucléaire ou les situations d'urgence déclenchées par de tels événements. On peut également examiner les registres écrits et automatisés d'exploitation pour vérifier que les essais d'alarmes ont été effectués à la fréquence requise et que des mesures compensatoires ont été mises en place en cas de besoin. Les informations obtenues au PCS devraient être stockées en toute sécurité.

Interface humaine

4.205. Le PCS devrait disposer d'un personnel permanent dont la fiabilité et l'aptitude ont été vérifiées grâce à une sélection minutieuse et qui possède les connaissances et compétences correspondant aux tâches assignées. Le PCS peut appliquer en son sein des mesures telles que la règle des deux personnes ou la télésurveillance afin de réduire la menace d'origine interne, ces mesures pouvant être requises pour certaines de ses fonctions, telles que la mise d'un capteur en mode accès (non sécurisé) ou l'ouverture à distance d'une porte haute sécurité.

4.206. Un PCS devrait disposer d'un personnel suffisamment nombreux pour surveiller et évaluer les alarmes et déclencher une intervention en cas de besoin, et recevoir et évaluer les informations provenant d'autres sources. Durant un événement de sécurité nucléaire, le personnel du PCS devrait être capable de communiquer des renseignements détaillés sur l'incident à la direction de

l'installation et de donner aux membres compétents de l'installation des conseils sur l'intervention à mener.

4.207. Le personnel du PCS devrait bien connaître les technologies de sécurité et avoir été longuement formé et mis à l'épreuve avant que des tâches ne lui soient confiées. En règle générale, ce personnel est composé de gardiens ou de membres des forces d'intervention, qui connaissent et comprennent l'installation, les opérations et les procédures de sécurité, et les plans d'urgence. On trouvera des orientations sur les plans d'urgence dans la publication n° 39-T de la collection Sécurité nucléaire de l'AIEA, intitulée *Élaboration d'un plan d'intervention spécialisé en sécurité nucléaire pour les installations nucléaires* [23]. Les fonctions du PCS et de son personnel devraient faire l'objet d'exercices réguliers.

Facteurs humains

4.208. La conception des systèmes au sein du PCS doit, dans un premier temps, recenser les fonctions que le personnel devra exercer et les interfaces qui lui seront nécessaires à cette fin. Il pourrait y avoir lieu d'afficher des informations telles que l'état du système, l'aménagement d'une installation nucléaire, l'état des alarmes et les informations concernant les écrans de visualisation et le contrôle de l'accès afin de faciliter l'exercice de ces fonctions. Le moment où ces informations sont affichées pour l'exploitant (p. ex. toujours, lors d'une alarme ou sur demande) et la manière dont elles le sont, et les cas où elles ne devraient pas l'être, comme lorsqu'une alarme est associée à une porte manipulée par une personne autorisée, devraient faire l'objet d'une attention particulière. Cette approche pourrait être modifiée en fonction des activités menées dans l'installation à différents moments de la journée.

4.209. Le processus d'évaluation des alarmes est très fortement tributaire de décisions humaines. Une grande installation nucléaire pourrait avoir des centaines de caméras et capteurs à surveiller, qui peuvent tous déclencher des alarmes. La possibilité de déclencher rapidement une intervention appropriée et précise dépend de l'aptitude du personnel du PCS à interpréter les données et à prendre les décisions appropriées. Le pupitre de commande du PCS devrait être conçu pour que le personnel n'ait pas à traiter un trop grand nombre d'informations d'un seul coup. En ce qui concerne les systèmes de grande taille, plusieurs opérateurs, ayant chacun leur poste de sécurité, peuvent être prévus pour surveiller le système de sécurité et maintenir le contrôle sur celui-ci, mais dans ce cas, il convient d'examiner attentivement, au stade de la planification et de la conception, les relations et interactions entre opérateurs et leurs équipements. Si un seul opérateur est assigné au PCS, le système peut prévoir de surveiller son état de santé et

de prévenir d'autres membres compétents du personnel si l'intéressé n'est plus capable de remplir ses fonctions.

4.210. Une attention particulière devrait être portée à l'aménagement des systèmes matériels et logiciels au moment de la conception d'un PCS. L'espace de travail devrait être confortable et facile à utiliser par le nombre d'opérateurs attendus. Les opérateurs devraient pouvoir voir les équipements et écrans nécessaires et se voir les uns les autres, entendre les communications et les indicateurs sonores d'alerte et s'entendre les uns les autres, et contrôler les commandes informatiques et faire fonctionner le matériel de communication.

Aménagement et conception

4.211. On peut considérer l'espace de travail du PCS comme une série de zones qui diffèrent du point de vue de l'accessibilité et de la visibilité. L'espace prévu pour tous les écrans et commandes devrait être suffisant pour qu'ils puissent remplir la fonction qui leur est assignée. Les écrans principaux devraient être bien visibles par l'opérateur en position de travail normale sans qu'il ait besoin de modifier beaucoup la direction de son regard ou la position de sa tête. L'opérateur devrait être capable de contrôler rapidement et avec précision toutes les fonctions nécessaires. Il faudrait envisager d'appliquer des techniques telles que les lettres de taille variable, les arrière-plans grisés pour le contraste et l'utilisation de la couleur pour améliorer la présentation visuelle des informations.

4.212. Le concepteur devrait choisir les périphériques d'entrée (p. ex. une souris, un clavier ou un simple bouton-poussoir) les mieux adaptés à la fonction qu'ils doivent remplir. Le matériel de communication (microphones et téléphones, p. ex.) devrait être à la portée des opérateurs. L'emplacement du matériel auxiliaire devrait être choisi en fonction de son importance et de sa fréquence d'utilisation.

4.213. La conception doit également faire une place aux techniques d'organisation et de gestion des informations affichées afin d'en faciliter l'interprétation par l'opérateur et d'améliorer l'efficacité des mesures à prendre. Les techniques de gestion du matériel associé au pupitre de commande sont notamment les suivantes :

a) Signaux audibles destinés à prévenir l'opérateur qu'une alarme a été déclenchée ; des sons différents sont prévus pour indiquer telle ou telle classe d'alarme ou alarme prioritaire.
b) Codage de couleurs (ou symbole clignotant) sur l'écran pour mettre l'information en relief ou aider à la classer par catégories (voir la figure 18).

c) Écrans distincts pour les graphiques et le texte pour différents types de données.
d) Représentation graphique multicouche avec les liens entre les couches. Par exemple, un plan de niveau peut indiquer qu'une alarme a été déclenchée dans une salle donnée (voir la figure 19), et le lien vers cette salle fait apparaître la salle et le capteur qui produit l'alarme.
e) Textes affichés avec des descriptions ou des boîtes de dialogue fournissant des informations supplémentaires (voir la figure 20).

4.214. La configuration du système de gestion des alarmes devrait lui permettre de distinguer entre les alarmes et de les classer par ordre d'importance en fonction du lieu où elles sont déclenchées (p. ex. une alarme dans une zone sensible passe avant une alarme au niveau du périmètre) et de leur motif (p. ex. une intrusion, une défaillance du système, une panne d'électricité, une activité non autorisée ou une manipulation frauduleuse). Ce système devrait fournir des alarmes dans l'ordre où elles se sont produites ou, aux fins de l'évaluation de plusieurs alarmes simultanées, selon l'ordre de priorité établi en fonction de l'importance du bien protégé. Les alarmes sont affichées pour l'opérateur dans un ordre décroissant de priorité, mais elles finissent toutes par être évaluées. Par exemple, dans un système de détection périmétrique des intrusions, l'ordre de priorité des alarmes peut être établi en prenant en compte les éléments ci-après :

a) le nombre de capteurs installés dans une zone donnée qui produisent une alarme ;
b) le temps écoulé entre les alarmes déclenchées dans la zone ;
c) l'ordre dans lequel les alarmes se produisent par rapport à la configuration physique des capteurs ;
d) la présence ou l'absence d'alarmes dans les zones adjacentes.

4.215. En ce qui concerne les installations abritant des matières nucléaires de catégorie I ou de catégorie II et où toute activité non autorisée pourrait avoir de graves conséquences radiologiques, le PCS devrait normalement se trouver à une bonne distance des limites du périmètre, dans une structure durcie (p. ex. un bunker). Il faudrait envisager d'installer le PCS à bonne distance des murs extérieurs du bâtiment qui l'abrite afin de renforcer sa protection contre une attaque directe ou à distance. L'accès à un PCS doit être strictement contrôlé. Le contrôle de l'accès peut être manuel, un opérateur déverrouillant la porte d'entrée après une vérification d'identité par vidéo, ou automatique. Pour empêcher toute personne d'entrer sans autorisation dans le PCS en suivant une personne autorisée, on peut utiliser deux portes équipées de systèmes d'interverrouillage et surveillées en circuit fermé, avec un dispositif de contrôle de l'accès renforcé.

FIG. 18. Écran texte signalant une alarme sur le pupitre de commande (reproduit avec l'aimable autorisation des Laboratoires nationaux Sandia)

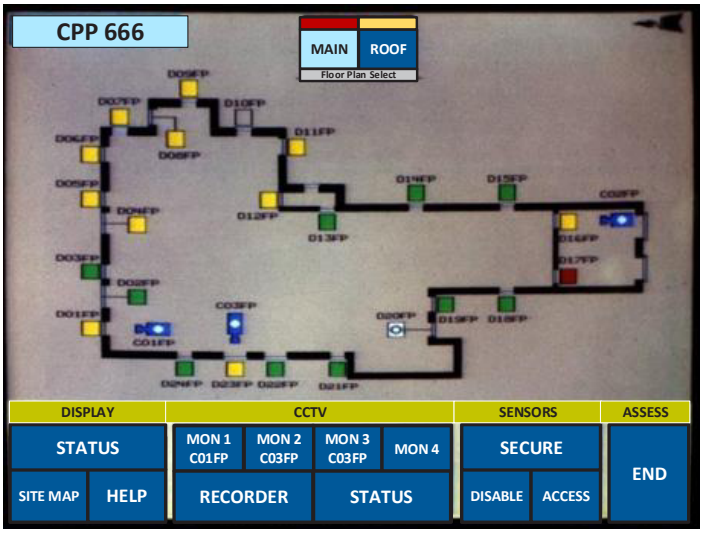


FIG. 19. Écran carte affichant le plan de niveau de l'installation (reproduit avec l'aimable autorisation des Laboratoires nationaux Sandia)

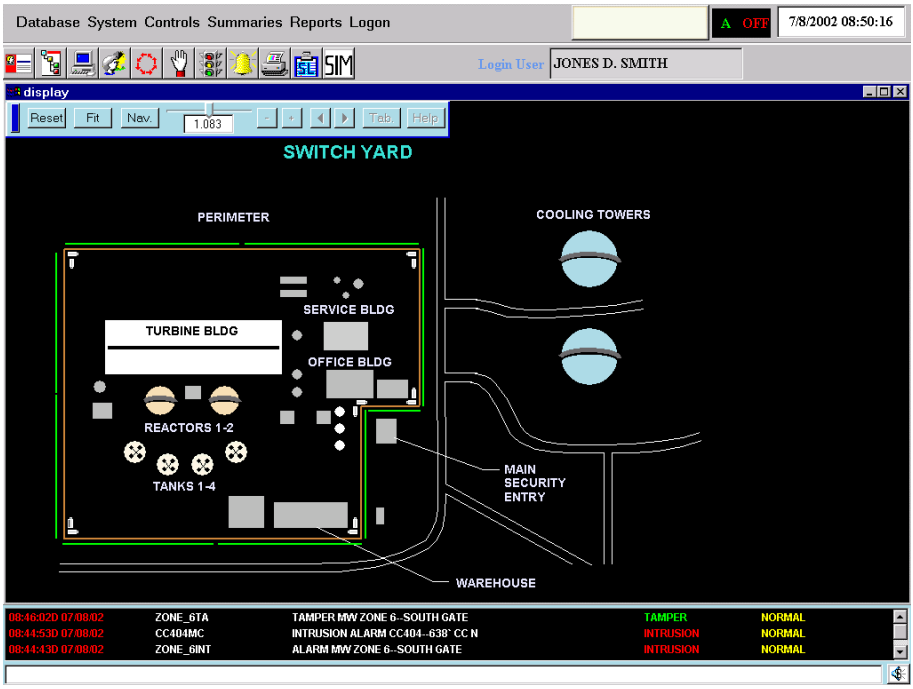


FIG. 20. Plan de niveau affichant les informations transmises par le capteur qui a produit l'alarme (reproduit avec l'aimable autorisation des Laboratoires nationaux Sandia)

4.216. Il faudrait appliquer au PCS des mesures de sécurité informatique, telles que le contrôle de l'accès aux équipements en réseau et le contrôle de l'accès aux informations et la détection des tentatives d'accès aux informations [7, 21].

4.217. Le PCS devrait pouvoir continuer de fonctionner pendant les arrêts programmés ou non, les situations d'urgence nucléaire ou radiologique et les événements de sécurité nucléaire. Les systèmes associés au PCS devraient, dans la mesure du possible, être redondants, diversifiés et protégés contre les manipulations frauduleuses. En ce qui concerne l'alimentation électrique, le PCS devrait disposer d'au moins deux sources indépendantes d'alimentation sans coupure et, en cas de besoin, d'un générateur de secours.

4.218. Un PCS pouvant être un point de défaillance unique pour un SPP, il est souhaitable de mettre en place un poste de secours qui pourrait prendre la relève si le PCS était inutilisable, par exemple en cas de défaillance matérielle ou humaine, d'attaque menée contre le poste central ou d'une évacuation rendue nécessaire, notamment, par un incendie, un tremblement de terre, une inondation ou le rejet

de radionucléides. Les fonctions de secours devraient prévoir la surveillance et le contrôle des alarmes, la surveillance en circuit fermé et les communications. Le poste de secours devrait être séparé du poste central et se trouver à un endroit accessible en fonction des besoins, et devrait être testé régulièrement.

Systèmes de communication vocale

4.219. Il importe de prévoir une communication vocale fiable entre le PCS, les équipes d'intervention d'urgence, le personnel de l'installation, les gardiens et les forces d'intervention sur site et hors site. Il devrait notamment être possible :

a) de communiquer à tout moment et dans des conditions différentes (p. ex. dans les situations normales et les situations d'urgence) ;
b) d'utiliser un moyen de communication sécurisé en cas de besoin ;
c) de communiquer rapidement avec les autorités compétentes et les forces d'intervention hors site en cas de besoin ;
d) de disposer d'un moyen de communication secondaire ou de remplacement lorsque le moyen principal n'est pas disponible.

4.220. Il faudrait concevoir des systèmes de communication qu'il soit difficile de perturber en prévoyant plusieurs moyens de communication, tels que les radios bidirectionnelles, les téléphones portables, les interphones et les téléphones fixes. Nombre de systèmes de communication vocale fonctionnent sur un réseau informatique qui peut utiliser la technologie sans fil pour transmettre les signaux. La sécurité de ces réseaux est abordée dans la section 6.

Systèmes radio

4.221. Les gardiens et les forces d'intervention utilisent couramment un système de radios portables à piles et à faible consommation d'énergie. Elles sont faciles à utiliser et ne nécessitent guère d'infrastructure mis à part l'alimentation électrique pour la recharge périodique des piles. En général, une radio fonctionne sur une fréquence parmi plusieurs ou permet de capter une chaîne parmi plusieurs. Pour obtenir une communication fiable entre deux radios, la portée ne doit pas dépasser un niveau compris entre 2 et 5 km selon le terrain, l'aménagement de l'installation et l'état de la pile et de l'antenne. Des émetteurs plus puissants et des récepteurs plus sensibles, communément appelés stations de base, peuvent être utilisés dans les postes de sécurité et les postes fixes. On utilise également des systèmes mobiles susceptibles de faire passer la portée pour une communication fiable jusqu'à plus de 20 km. Les systèmes radio utilisés par les forces d'intervention pour leurs communications fonctionnent en général sur des chaînes dédiées et une

fréquence spécifique, en utilisant la modulation de fréquence à bande étroite et la transmission en clair (c'est-à-dire que les signaux vocaux transmis ne sont pas codés ou brouillés).

4.222. Les systèmes de radio en clair ont des inconvénients ; ils sont en particulier susceptibles d'interception, de tromperie (p. ex., un agresseur surveillant les communications radio pour connaître les protocoles et envoyer de faux messages pour perturber la réponse) et de brouillage (transmission de signaux sur le canal de fréquences d'un système de communication pour masquer les communications souhaitées). Les systèmes radio à signal vocal crypté sont plus sécurisés (p. ex. ils résistent mieux à l'interception ou à la transmission de messages trompeurs). Les systèmes à radiofréquence sont vulnérables au brouillage car le signal brouilleur peut être émis à distance. On peut améliorer la résistance au brouillage d'un réseau de communications en utilisant des radios plus puissantes, dont le brouillage nécessite un matériel plus puissant, des technologies radio plus poussées ou des systèmes de communication multiples. En elles-mêmes, les radios à signal crypté n'empêchent pas le brouillage, car un signal crypté peut être brouillé de la même façon qu'un signal clair. Les systèmes radio mieux sécurisés, qui résistent mieux au brouillage, sont plus complexes et onéreux, et, en général, réduisent la durée de vie des piles des radios et se ressentent davantage du bruit dans le canal de communication, ce qui en réduit la portée de communication réelle.

4.223. Selon la configuration de l'installation, sa taille et les types de bâtiments se trouvant sur le site, les systèmes radio peuvent subir une perte de signal, et il pourrait être nécessaire d'augmenter la puissance du signal des radios portatives à l'aide d'un répéteur à radiofréquence. Ce répéteur reçoit les signaux vocaux transmis par les radios portatives et les transmet sur une fréquence distincte à toutes les autres radios du système. De plus, placé sur un lieu élevé, un répéteur peut augmenter la portée.

4.224. On devrait pouvoir avoir recours à un large éventail de méthodes de communication pour que les gardiens et les forces d'intervention puissent communiquer pendant un événement de sécurité nucléaire. On pourrait ainsi faire appel à des systèmes utilisés régulièrement à d'autres fins, tels que les téléphones fixes et les interphones, et les systèmes conçus spécifiquement pour les situations d'urgence. Un ensemble diversifié de méthodes de communication peut créer un système qui soit solide, fiable et pouvant résister à l'interception, à la tromperie et au brouillage. On peut aussi équiper les radios d'« alarmes de contrainte » qui préviennent le PCS que la personne qui utilise une radio pourrait bien transmettre des messages trompeurs sous la contrainte.

Systèmes de fouille

4.225. Les personnes, véhicules et matières entrant dans les zones de sécurité ou les quittant peuvent être soumis à une fouille à laquelle procèdent des gardiens, des chiens et des systèmes de fouilles à l'aide de technologies telles que des détecteurs de métaux, de rayonnements et d'explosifs. Les fouilles à l'entrée visent à prévenir l'introduction d'articles interdits. Les fouilles à la sortie sont principalement destinées à empêcher l'enlèvement non autorisé de matières nucléaires. Si un système automatisé de fouille ou un chien déclenche une alarme, les gardiens peuvent procéder à une fouille manuelle pour déterminer si l'alarme est intempestive ou valide et, en cas de besoin, déclencher une intervention.

Fouilles manuelles

4.226. Une fouille manuelle est habituellement une technique de contrôle secondaire utilisée pour fouiller des personnes, des colis et des véhicules une fois qu'une alarme initiale a été déclenchée. L'efficacité des fouilles manuelles effectuées par les gardiens dépend de leur formation et des procédures suivies : en particulier, les gardiens doivent être capables de repérer les types d'articles interdits recherchés, par exemple la taille, la masse et la forme qu'ils sont susceptibles d'avoir. En principe, tout article peut faire l'objet d'une fouille manuelle, qu'il s'agisse d'un petit colis ou d'une personne, d'un véhicule ou d'un grand conteneur d'expédition.

Fouilles de véhicules

4.227. Étant donné qu'il est difficile de procéder à une fouille minutieuse dans le cas d'un véhicule, l'opérateur peut exiger que les véhicules demeurent en dehors de la limite de l'installation. Si les véhicules sont autorisés sur le site, un portique de contrôle d'accès ou un dispositif d'immobilisation d'un véhicule peut isoler ce dernier pendant la fouille (voir la figure 21).

Détection des métaux

4.228. Des détecteurs de métaux sont habituellement utilisés pour fouiller les personnes à l'entrée et à la sortie ; on peut les diviser en deux grandes catégories :

a) Les détecteurs actifs de métaux, qui transmettent l'énergie électromagnétique et détectent le métal en captant la réponse du champ transmis à la présence de l'objet métallique.

b) Les magnétomètres, qui captent les distorsions locales du champ magnétique terrestre causées par la présence de matériaux ferromagnétiques.

4.229. Certaines formes de matières nucléaires et de matériaux de blindage ne pouvant pas être détectées par de simples détecteurs de métaux, les portiques et dispositifs portatifs tirent communément parti d'autres technologies de détection des métaux en utilisant en particulier des détecteurs à champ pulsé et à onde entretenue.

Portique de détection de métaux

4.230. Un signal sinusoïdal permanent est appliqué à la bobine de l'émetteur sur un côté du portique du détecteur. Cette bobine produit un champ magnétique de faible intensité (habituellement de 50 μT ou moins). Les bobines du récepteur sont montées sur l'autre côté du portique, de sorte qu'une personne contrôlée passe entre les bobines de l'émetteur et du récepteur. Le signal est détecté par les bobines du récepteur avant d'être analysé. En l'absence de métal dans le portique, le signal n'est pas modifié.

4.231. Dans un détecteur de métaux à champ pulsé, les bobines à faible inductance de l'émetteur produisent de très courtes impulsions d'énergie magnétique (pouvant ne pas dépasser 50 μs) entre 200 et 400 fois par seconde. Pendant l'impulsion, le signal reçu n'est pas pris en considération, mais après la fin de chaque impulsion, il est analysé pendant une courte période (en général

FIG. 21. Portique de contrôle d'accès des véhicules (reproduit avec l'aimable autorisation des Laboratoires nationaux Sandia)

quelques dixièmes de milliseconde). En l'absence de métal dans le portique, le signal de sortie du récepteur n'est que le bruit électromagnétique de fond (en général très faible). En présence d'un objet métallique, l'impulsion magnétique induit un courant de Foucault dans le métal, qui décroît rapidement (en fonction de la résistivité du métal), mais se maintient suffisamment longtemps pour être présent lors de l'analyse du signal reçu. Le signal est ensuite amplifié et la phase détectée ; si le signal dépasse un seuil retenu, une alarme est déclenchée. La grande majorité des portiques de détection des métaux utilisés aujourd'hui appliquent cette technique.

4.232. Pour contrôler les personnes passant par les points de contrôle et de fouille, on peut utiliser des portiques permettant de faire subir à un grand nombre de personnes un contrôle visant à détecter la présence de métaux à l'entrée comme à la sortie.

4.233. Les alarmes de détecteur de métaux devraient également être déclenchées en cas de panne d'électricité, de défaillance d'équipements ou de manipulation frauduleuse. L'environnement d'un portique de détection de métaux peut en affecter la performance. C'est notamment le cas des éléments suivants :

a) Objets métalliques en mouvement, des portes, par exemple, à quelques mètres de distance, produisant des alarmes intempestives.
b) Objets métalliques immobiles, notamment les barres d'armature pour plancher, qui déforment le champ magnétique et créent des zones de sensibilité plus élevée ou plus faible.
c) Appareils électriques, tels que radios, dispositifs à rayons X et ordinateurs fonctionnant à proximité de détecteur de métaux, qui déclenchent des alarmes intempestives.
d) Mouvement du plancher sous le détecteur de métaux au passage des personnes dans la zone, ce qui déclenche des alarmes intempestives. Les canalisations d'eau dans les murs ou sous le plancher pourraient aussi faire bouger les tuyaux métalliques.

Détecteurs de métaux portatifs

4.234. La plupart des détecteurs de métaux portatifs utilisent la technologie de l'onde entretenue. Ils génèrent un champ magnétique en régime permanent dans la gamme de fréquence de 100 Hz à 25 kHz. (Les premiers portiques de détection des métaux utilisaient également cette technique, mais ils ont été largement remplacés par les détecteurs à champ pulsé.)

4.235. Les détecteurs de métaux portatifs doivent être utilisés à une très petite distance de la personne à contrôler. À la distance de fonctionnement normale par rapport au corps, ils sont très sensibles et peuvent déceler des objets beaucoup plus petits que dans le cas d'un portique de détection. En particulier, ils pourraient mieux convenir pour contrôler de plus petites quantités de métaux qui pourraient servir à protéger des matières nucléaires enlevées. L'efficacité d'un détecteur de métaux portatif dépend fortement de la technique mise en œuvre par la personne chargée du contrôle. Un contrôle rigoureux effectué selon une procédure bien conçue peut être très efficace, mais il prend beaucoup de temps. Les détecteurs portatifs sont donc le plus souvent utilisés comme méthode secondaire lorsque les portiques de détection ont généré des alarmes, et chaque point de contrôle devrait être équipé d'un détecteur de métaux portatif.

Détection d'explosifs

4.236. Les méthodes d'absorption des rayons X ou d'activation et d'absorption neutroniques sont communément appliquées à la détection d'explosifs dans les chargements et les bagages. Ces méthodes de détection d'explosifs ne sont pas utilisées pour le contrôle des personnes.

4.237. Des méthodes actives et passives ont été mises au point pour la détection de traces de vapeurs d'explosifs, qui utilisent généralement les systèmes de spectrométrie de mobilité ionique et des chiens dressés. Les petits colis font l'objet d'une inspection visant à détecter la présence d'explosifs et suivant ces approches pour déceler la présence de traces d'explosifs sur les surfaces qui ont été contaminées par les personnes ayant manipulé des explosifs ou qui ont été en contact avec des explosifs. Par ailleurs, ces méthodes sont généralement appropriées à la fouille des personnes.

4.238. La technologie des ondes millimétriques de faible énergie peut être utilisée pour fouiller les personnes, et les méthodes d'imagerie par rayons X peuvent l'être pour fouiller les colis.

4.239. Les appareils de détection d'explosifs en vrac mesurent les caractéristiques des matériaux en vrac pour déceler la présence d'explosifs. Ces caractéristiques sont notamment le coefficient d'absorption des rayons X, le coefficient de rétrodiffusion X, la constante diélectrique, les interactions du rayonnement gamma ou neutroniques, et les émissions d'hyperfréquences ou infrarouges. L'analyse des mesures de ces paramètres peut fournir des estimations de la masse, de la densité, de la teneur en azote et du numéro atomique équivalent du matériau concerné. Les explosifs n'ont aucune de ces caractéristiques en propre, mais

elles peuvent indiquer que des explosifs sont très probablement présents, et le taux de fausses alarmes peut être suffisamment faible pour permettre la détection automatique des matériaux qui pourraient être des explosifs. Si le système génère une alarme, un opérateur peut procéder à un contrôle (une évaluation) secondaire pour déterminer la présence d'explosifs.

Absorption des rayons X

4.240. Dans la plupart des cas, les détecteurs d'explosifs en vrac à rayons X sont des versions modifiées de scanners de colis. Ces appareils servent donc habituellement un double objectif : le colis peut faire l'objet à la fois d'une fouille pour déterminer la présence d'armes ou d'autres articles interdits et d'un contrôle pour déterminer celle d'explosifs. Les simples détecteurs à rayons X monoénergie ne donnent pas suffisamment d'informations pour la détection automatisée d'explosifs et nécessitent une interprétation de l'image par un opérateur. Les détecteurs à double énergie (habituellement autour de 100 et 160 keV) mesurent le ratio énergie reçue/énergie transmise aux deux énergies et, en le comparant aux coefficients d'atténuation connus, peuvent calculer le numéro atomique équivalent pour la région examinée. Aux fins d'affichage, on ajoute des couleurs aux images pour indiquer les matières à numéro atomique bas ou élevé, ce qui peut aider le personnel à interpréter ces images. Les tomodensitomètres peuvent extraire suffisamment d'informations pour calculer la masse, la densité et le coefficient d'absorption massique de la matière concernée. L'analyse de la rétrodiffusion peut déterminer le numéro atomique équivalent d'une matière en examinant l'énergie des rayons X rétrodiffusée vers la source (principalement du fait de la rétrodiffusion Compton, qui est la plus efficace pour les matières riches en hydrogène, comme les explosifs, les plastiques et la nourriture).

Activation et absorption neutroniques

4.241. Les détecteurs à activation de neutrons thermiques et à absorption de neutrons rapides pulsés peuvent également servir à détecter la présence d'explosifs. Les détecteurs de neutrons thermiques peuvent déterminer la teneur en azote d'une matière : l'absorption nucléaire d'un neutron thermique par ^{14}N génère ^{15}N dans un état excité, qui n'est pas stable et émet un rayonnement gamma de fréquence caractéristique. La quantité de rayonnement de cette fréquence indique la teneur en azote, et comme la plupart des explosifs sont riches en azote, ces appareils peuvent détecter leur présence. Les détecteurs de neutrons rapides pulsés peuvent fournir une approximation de la teneur de la matière en hydrogène, carbone et oxygène qui, associée aux mesures de la teneur en azote déterminée par les neutrons thermiques, peut identifier plus précisément la matière en question.

Toutefois, les systèmes de détection de neutrons rapides pulsés sont onéreux, de grande taille et lents, si bien que l'on utilise souvent l'activation de neutrons thermiques pour les petits colis très nombreux et la détection de neutrons rapides pulsés pour un petit nombre de véhicules et les grands conteneurs d'expédition.

Détection de traces de vapeurs d'explosifs

4.242. La détection de vapeurs d'explosifs est difficile car la concentration d'explosifs de grande puissance en phase vapeur peut être très faible (voir le tableau 2). Les pressions de vapeur sont même plus faibles si l'explosif est emballé dans un gel ou solvant à base de pétrole.

4.243. Dans un système de spectrométrie de mobilité ionique, les molécules de l'échantillon d'air sont d'abord ionisées avant de passer dans une région de dérive par un obturateur qui s'ouvre à des intervalles de temps en millisecondes, ce qui crée des impulsions d'ions. À l'intérieur de la région de dérive, les ions se séparent selon leur masse, les plus légers progressant plus vite que les plus lourds. À la fin de la région de dérive, les ions entrent en collision avec une plaque de Faraday, qui enregistre le courant de sortie en fonction du temps écoulé depuis l'entrée des ions dans la région de dérive.

TABLEAU 2. PRESSION DE VAPEUR DES MOLÉCULES D'EXPLOSIFS À TEMPÉRATURE AMBIANTE ET À LA PRESSION ATMOSPHÉRIQUE (20 °C, 100 kPa)

Explosif	Entrant dans la composition de	Pression de vapeur (parties par milliard)
Dinitrate d'éthylèneglycol	Dynamite	92 000
Nitroglycérine (NG)	Dynamite	340
Dinitrotoluène (DNT)	TNT militaire	300
Trinitrotoluène (TNT)	TNT militaire	8
Cyclotriméthylènetrinitramine (RDX)	C-4, Semtex	0,006
Tétranitrate de pentaérythritol (PETN)	Detasheet, Semtex	0,002

4.244. Très sensibles, les détecteurs utilisant la spectrométrie de mobilité ionique permettent de détecter la dynamite, le TNT militaire et les explosifs plastiques. Cette sensibilité et la relative facilité d'utilisation et de maintenance font que cette technologie est largement utilisée pour déceler la présence d'explosifs. Toutefois, il peut être difficile d'éliminer les résidus d'explosifs se trouvant dans l'instrument après la détection de quantités importantes, car on peut encore y détecter des traces de très petite taille (quelques nanogrammes, p. ex.) de certains explosifs.

4.245. La sensibilité de la plupart des détecteurs d'explosifs du commerce est la meilleure lorsqu'ils sont utilisés avec des échantillons prélevés sur les surfaces, ce qui consiste à passer un substrat sur une surface susceptible d'avoir été contaminée. Le substrat est ensuite placé dans une unité de chauffage, qui désorbe les particules d'explosifs qui se sont accumulées sur le substrat et les apporte au détecteur pour analyse.

4.246. Pour contrôler un grand nombre de personnes passant par des points de contrôle sensibles, tels que ceux installés dans les zones d'embarquement des aéroports, on a mis au point des portiques de sécurité pour les personnes.

4.247. Par ailleurs, des chiens dressés à la recherche d'explosifs sont largement utilisés à cette fin. Toutefois, ils doivent subir un dressage permanent pour continuer d'identifier même les explosifs ou autres matières à la recherche desquels ils ont été dressés. De plus, la fiabilité de la détection dépend de l'état de santé et de la disposition du chien, ainsi que de la vigilance et de la compétence du maître-chien. Les chiens sont généralement dressés pour identifier entre six et dix odeurs et peuvent n'être capables de les identifier que pendant une courte période chaque jour. En conséquence, on privilégie de plus en plus les détecteurs d'explosifs technologiques pour faire subir aux personnes un contrôle visant à détecter la présence d'explosifs.

Imagerie par rayons X et imagerie par ondes millimétriques

4.248. Les appareils disponibles dans le commerce peuvent utiliser la rétrodiffusion de rayons X de faible énergie pour visualiser les matières se trouvant sur le corps des personnes contrôlées. Ces appareils peuvent générer une image des articles interdits, notamment les explosifs cachés sous les vêtements des personnes à contrôler. Ces dernières reçoivent habituellement une très faible dose de rayonnements ionisants. Des préoccupations relatives à la protection de la vie privée sont associées à la visualisation du corps d'une personne à travers ses vêtements. Ces préoccupations pourraient être en partie apaisées par une analyse automatisée de l'image produite qui indique simplement à l'opérateur

si la personne concernée doit subir aussi une fouille manuelle. On trouvera des recommandations dans la publication n° SSG-55 de la collection Normes de sûreté de l'AIEA, intitulée *Radiation Safety of X Ray Generators and Other Radiation Sources Used for Inspection Purposes and for Non-medical Human Imaging* [24].

4.249. L'imagerie par ondes millimétriques ou ondes térahertziennes est une autre technologie disponible dans le commerce pour générer une image des personnes ; elle utilise des rayonnements dont les fréquences rendent la plupart des vêtements transparents, mais qui sont réfléchis par la peau. Les métaux absorbant fortement ces fréquences, les images peuvent faire apparaître des articles interdits, tels que des armes de poing, des couteaux et des explosifs. Pour traiter les questions liées au respect de la vie privée, on peut utiliser des logiciels permettant de modifier ou d'anonymiser les images.

4.250. Qu'il s'agisse des dispositifs de rétrodiffusion des rayons X ou de ceux qui utilisent l'imagerie par ondes millimétriques, un contrôle secondaire, impliquant généralement une fouille manuelle, est nécessaire pour confirmer les indications fournies par ces dispositifs techniques.

4.251. Le contrôle des véhicules et des conteneurs de fret de grande taille nécessite l'emploi de rayons X d'énergie plus haute que dans le cas des petits colis. Les systèmes à rayons X à énergie comprise entre 320 et 630 keV sont le plus souvent utilisés pour fouiller les véhicules. Certains systèmes de contrôle de véhicules utilisent les rayons gamma, les radionucléides tels que le ^{137}Cs (utilisant l'émission de 661 keV du produit de filiation du ^{137m}Ba de courte période) et le ^{60}Co (1 173 et 1 333 keV) fournissant un rayonnement plus pénétrant même que dans le cas des systèmes à rayons X de haute énergie. Pendant le contrôle effectué à l'aide de ces systèmes de haute énergie, utilisant les rayons X ou les rayons gamma, les occupants du véhicule doivent en sortir.

Détection des matières nucléaires

4.252. Les détecteurs de matières nucléaires ont pour fonctions de déceler et, après une évaluation appropriée, détecter l'enlèvement non autorisé de matières nucléaires sur les personnes, dans les colis ou dans les véhicules quittant une zone de sécurité. Deux méthodes sont communément utilisées pour déceler des matières nucléaires ; elles mettent en jeu des portiques ou des dispositifs portatifs :

a) La méthode passive décèle le rayonnement gamma et le rayonnement neutronique émis par les matières nucléaires.

b) La méthode active repose sur l'activation neutronique pour déceler des matières nucléaires protégées.

4.253. Le rayonnement émis par des matières nucléaires peut être détecté en utilisant l'un ou l'autre des matériaux de détection suivants : les scintillateurs cristallins ou organiques (dans une matrice plastique), les semiconducteurs (corps solides) qui conduisent l'électricité lorsqu'ils sont exposés à un rayonnement, et les détecteurs proportionnels contenant un gaz qui peut détecter les neutrons.

Détection de rayonnement gamma

4.254. Les scintillateurs détectent le rayonnement gamma à partir de la décroissance radioactive des matières nucléaires : des photons sont produits lorsque le matériau scintillateur absorbe le rayonnement ionisant. En règle générale, les scintillateurs sont cristallins (iodure de sodium) ou organiques (plastiques), ces derniers étant largement utilisés dans le cas des portiques pour piétons.

4.255. Un scintillateur à iodure de sodium dopé au thallium [NaI(Tl)] couplé à un tube photomultiplicateur est communément utilisé pour détecter et identifier le rayonnement gamma. Les cristaux d'iodure de sodium pur scintillent efficacement lorsqu'ils sont refroidis à 77 K environ, mais nettement moins bien à la température ambiante normale. L'adjonction de thallium non seulement augmente l'efficacité à des températures de fonctionnement normales, mais aussi modifie la longueur d'onde de la lumière de scintillation, si bien que le NaI(Tl) est transparent à ses propres scintillations. Ces systèmes présentent un inconvénient : l'exposition à de petites quantités d'humidité fait passer la couleur du NaI(Tl), ce qui diminue sa lumière de scintillation et nuit à la fiabilité de la détection et de l'identification du rayonnement gamma. Un détecteur NaI(Tl) peut être utilisé pour distinguer des rayons gamma d'énergie variable et, de ce fait, peut servir à distinguer entre les radionucléides, mais il ne peut pas détecter les neutrons. Toutefois, d'autres scintillateurs, tels que le bromure de lanthane, pourraient fournir une résolution en énergie légèrement meilleure que le NaI(Tl).

4.256. Les scintillateurs plastiques émettent des photons lorsque des rayons de haute énergie (p. ex., rayons X, rayons gamma, neutrons) arrivent sur le plastique. Toutefois, les photons n'indiquent pas l'énergie du rayonnement incident qui a produit la scintillation ; ils ne peuvent donc pas identifier les radionucléides. Le matériau plastique est moins cher (par unité de surface) que les scintillateurs cristallins décrits plus haut, mais il est moins efficace. Globalement, les scintillateurs plastiques sont plus sensibles à un moindre coût, mais ne fournissent pas de résolution en énergie. Par ailleurs, ils peuvent détecter des neutrons dans

une certaine mesure et sont communément utilisés pour le contrôle des personnes par rayonnement.

4.257. Les détecteurs à semiconducteurs tels que ceux qui utilisent le germanium de haute pureté et le tellurure de cadmium-zinc peuvent indiquer l'énergie des rayons gamma qui arrivent sur le cristal. Cela permet d'identifier les radionucléides car l'énergie des rayons gamma émis est caractéristique de la décroissance d'un radionucléide spécifique. C'est particulièrement utile pour distinguer la source des alarmes intempestives. Par exemple, une personne ayant récemment subi une procédure médicale utilisant un isotope radioactif tel que le ^{99m}Tc émet un niveau de rayonnement gamma détectable, mais un détecteur à semiconducteurs peut distinguer le spectre énergétique des rayons gamma de celui des radionucléides que cette personne pourrait avoir reçus dans une installation nucléaire. Les cristaux semiconducteurs ont une excellente efficience (sensibilité par unité de surface) et une bonne résolution en énergie, mais ils sont plus onéreux (par unité de surface) que les scintillateurs plastiques. Les détecteurs au germanium nécessitent un refroidissement à azote liquide onéreux, tandis que les détecteurs à tellurure cadmium-zinc peuvent fournir une résolution en énergie raisonnable à la température ambiante normale. Par ailleurs, les détecteurs à semiconducteurs peuvent détecter les neutrons dans une certaine mesure.

Détection de neutrons

4.258. La détection de neutrons est des plus utiles pour détecter les matières nucléaires, parce que certaines de ces matières (en particulier les isotopes du plutonium) émettent des neutrons qui sont difficiles à protéger et que le fond de rayonnement neutronique est généralement très faible. Les détecteurs de neutrons peuvent donc être très sensibles, et la détection de neutrons peut être un indicateur fiable de la présence de matières nucléaires.

4.259. Un détecteur de neutrons déclenche une alarme en cas d'augmentation statistiquement significative des niveaux de fond normaux. Il faudrait choisir un seuil d'alarme qui soit proche du niveau de fond normal, mais pas au point de provoquer un grand nombre d'alarmes intempestives. On établit le niveau de fond de référence à partir de la moyenne des intervalles de comptage, cette moyenne étant continuellement actualisée. En règle générale, pour un portique de contrôle des personnes, le comptage des signaux reprend chaque fois qu'une personne quitte le portique et chaque comptage est comparé au seuil d'alarme, compte tenu du niveau de fond moyen ; une alarme est déclenchée si le comptage dépasse le seuil d'alarme.

4.260. De plus, des alarmes devraient également être générées en cas de panne d'électricité, de défaillance d'équipements, de niveau de fond trop élevé ou trop faible, ou de manipulation frauduleuse des équipements.

Détection par activation neutronique

4.261. La détection par activation neutronique consiste à diriger un faisceau de neutrons, à partir d'une source telle que l'isotope ^{252}Cf, vers une cible, généralement un conteneur qu'il est difficile de fouiller par un autre moyen (un conteneur de fret, p. ex.), afin de détecter la présence d'uranium. La source est utilisée pour diriger une impulsion de neutrons vers le conteneur – le plus souvent pendant quelques secondes –, puis blindée pour stopper les neutrons incidents. Tout neutron retardé émis par des fragments de fission d'uranium est ensuite compté pour indiquer si des matières nucléaires sont présentes dans le conteneur ou non. Cette méthode de fouille ne devrait être utilisée que pour les conteneurs.

Portique de détection de matières nucléaires

4.262. Des équipements de détection des rayonnements peuvent être installés dans des portiques pour détecter la présence de matières nucléaires dans les véhicules et les autorails (voir les figures 22 et 23). Les détecteurs peuvent être montés sur une fondation en béton ou sur les murs ; on peut utiliser un seul détecteur ou en empiler plusieurs pour que la hauteur de la zone de détection corresponde à celle des véhicules. On peut aussi doter les portiques d'une surveillance vidéo pour enregistrer le processus de détection et étayer par des éléments probants l'évaluation des alarmes. Les matières nucléaires peuvent être détectées dans des véhicules à l'arrêt ou en mouvement.

Dispositifs portatifs de détection de matières nucléaires

4.263. On peut utiliser des détecteurs portatifs pour contrôler des personnes, des colis et des véhicules pour y détecter la présence d'un large éventail de matières nucléaires ; on peut aussi adapter ces dispositifs à certains types de matières nucléaires. Les détecteurs portatifs sont principalement utilisés comme dispositifs de contrôle secondaire et pour contrôler des zones ou volumes très importants, là où un portique de détection n'est pas efficace. La procédure de contrôle et le temps qu'elle prend, ainsi que l'avantage de pouvoir détecter des quantités de matières nucléaires plus petites sont analogues aux avantages et limites du détecteur de métaux à main présenté plus haut. Chaque point de contrôle doté d'un portique de détection de matières nucléaires devrait également être équipé d'un détecteur de rayonnement portatif.

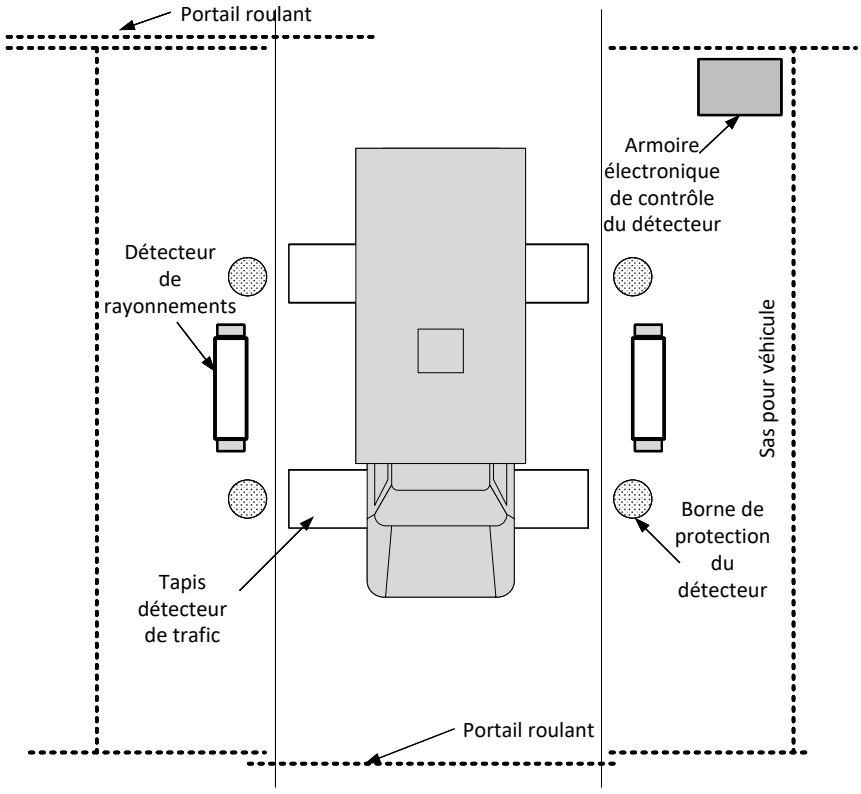


FIG. 22. Configuration des portiques de détection de matières nucléaires dans les véhicules

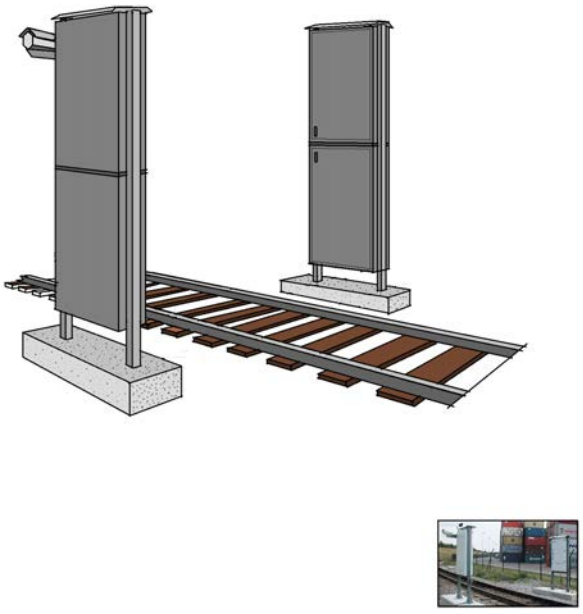


FIG. 23. Moniteur de surveillance en circuit fermé des matières nucléaires dans les autorails

Matières nucléaires protégées

4.264. L'utilisation combinée des détecteurs de métaux et des détecteurs de matières nucléaires est indispensable pour détecter des matières nucléaires protégées. Le détecteur de métaux devrait pouvoir détecter des quantités relativement faibles de métaux lourds, comme le plomb. La résistance de ces métaux étant en général plus forte que dans le cas de ceux qui ont un nombre atomique plus bas, ils peuvent être plus difficiles à détecter. Dans tous les cas, la sensibilité de fonctionnement des détecteurs doit être très élevée, ce qui augmente le taux d'alarmes intempestives ; il pourrait de ce fait être nécessaire de prévoir une zone où le personnel puisse retirer les objets métalliques de ses vêtements (p. ex. retirer des chaussures à coquille d'acier).

Récapitulation des technologies utilisées par les systèmes de fouille

4.265. Le tableau 3 récapitule les différentes technologies de fouille en fonction des différentes applications et des différents modes de classification.

TABLEAU 3. CLASSIFICATION DES SYSTÈMES DE FOUILLE ET APPLICATIONS CARACTÉRISTIQUES

Type de fouille	Articles généralement inspectés	Portativité[a]	Principe de fonctionnement[b]	Interaction[c]	Type d'alarme[d]
Détection de métaux					
Portique	Personnes	Fixe intégré	Électro-magnétique	Active Passive	Alarme
Portatif	Personnes	Mobile	Électro-magnétique	Active	Alarme
Détection d'explosifs					
Absorption des rayons X	Véhicules Conteneurs de fret Articles portés à la main	Fixe	Écran de visualisation Rayons X	Active	Interprété
Activation et absorption neutroniques	Véhicules Conteneurs de fret Articles portés à la main	Fixe	Écran de visualisation Rayonnement	Active	Interprété
Traces de vapeur	Personnes Articles portés à la main	Fixe Mobile	Analyse du gaz	Active	Alarme Interprété
Chiens dressés	Personnes Véhicules Conteneurs de fret Articles portés à la main	Mobile	Odeurs d'explosifs	Sans objet	Interprété
Détection de matières nucléaires					

TABLEAU 3. CLASSIFICATION DES SYSTÈMES DE FOUILLE ET APPLICATIONS CARACTÉRISTIQUES (suite)

Type de fouille	Articles généralement inspectés	Portativité[a]	Principe de fonctionnement[b]	Interaction[c]	Type d'alarme[d]
Portique : gamma et neutrons	Personnes Véhicules Conteneurs de fret Articles portés à la main	Fixe Intégré	Rayonnement	Passive	Alarme
Portique : activation neutronique	Véhicules Conteneurs de fret	Fixe Autonome	Rayonnement	Active	Alarme Interprété
Portatif : gamma et neutrons	Personnes Véhicules Conteneurs de fret Articles portés à la main	Mobile	Rayonnement	Passive	Alarme Interprété
Portiques combinés de détection de métaux et d'explosifs					
Imagerie par rayons X (rétrodiffusion basse énergie)	Personnes	Fixe	Écran de visualisation Rayons X	Active	Interprété
Imagerie à rayonnement électro-magnétique et à ondes millimétriques	Personnes	Fixe	Écran de visualisation Rayonnement	Active	Interprété
Détection combinée de métaux, de matières nucléaires et d'explosifs					

TABLEAU 3. CLASSIFICATION DES SYSTÈMES DE FOUILLE ET APPLICATIONS CARACTÉRISTIQUES (suite)

Type de fouille	Articles généralement inspectés	Portativité[a]	Principe de fonctionnement[b]	Interaction[c]	Type d'alarme[d]
Inspection manuelle	Personnes Véhicules Conteneurs de fret Articles portés à la main	Fixe Mobile	Écran de visualisation Miroirs Toucher	Active	Interprété

[a] Le système peut être fixe, intégré (combiné avec d'autres applications), autonome (non combiné avec d'autres applications) ou mobile (peut être déplacé d'un lieu dans un autre).
[b] Type de technologie utilisé.
[c] Interaction active ou passive avec l'article faisant l'objet d'une fouille.
[d] Alarme audible ou visuelle ou interprétée par l'opérateur.

SYSTÈMES DE CONTRÔLE DE L'ACCÈS

4.266. Les systèmes de contrôle de l'accès servent à prévenir ou à détecter l'entrée non autorisée dans les zones de sécurité (p. ex., les zones d'accès limité, les zones protégées, les zones intérieures et les zones vitales). Ils devraient réserver l'entrée et la sortie aux personnes et aux véhicules autorisés, et favoriser la prévention et la détection des déplacements non autorisés de matières nucléaires, d'informations sensibles et d'articles interdits ou de matériel vers et depuis les zones de sécurité. Des orientations générales sur le contrôle de l'accès figurent dans la référence [2]. Les clés, serrures, combinaisons, mots de passe et dispositifs connexes utilisés pour contrôler l'accès aux zones de sécurité et au matériel de protection physique devraient être protégés en conséquence.

4.267. Un système de contrôle de l'accès peut être :

a) autonome : c'est le cas, par exemple, d'une serrure de porte ;
b) interconnecté : un groupe de dispositifs de contrôle de l'accès contrôlés au niveau local ;
c) intégré : un système de contrôle de l'accès intégré à un système de détection des intrusions.

4.268. En règle générale, le nombre des personnes autorisées à accéder à chaque niveau successif d'une zone de sécurité diminue du fait des politiques tendant à restreindre l'accès aux zones de haute sécurité. Le système de contrôle de l'accès peut et, de ce fait, devrait prévoir pour chaque niveau successif des mesures d'une rigueur croissante : pour déterminer le matériel et les processus de contrôle à mettre en place, il faudrait prendre en compte le nombre de personnes autorisées qui doivent passer par chaque point d'accès et les prescriptions de sécurité. Les contrôles d'accès peuvent utiliser une chose qu'une personne possède, comme des données d'identification, une chose qu'elle connaît, comme un numéro d'identification personnel, ou une caractéristique qui lui est propre, comme ses empreintes digitales. Le système de contrôle de l'accès devrait être supervisé par des gardiens de façon à détecter toute tentative de neutraliser ou d'éviter le système et à déclencher une intervention.

4.269. S'agissant des systèmes de contrôle de l'accès intégrés aux systèmes de détection d'intrusions, les prescriptions applicables aux voies de transmission entre les serveurs et les dispositifs de contrôle de l'accès sont examinées à la section 6. Ce type de système de contrôle de l'accès a besoin de communiquer avec le sous-système qui décèle l'état (ouvert ou fermé) d'un point d'accès pour pouvoir enregistrer avec précision le moment où une personne franchit ce point et vérifier ensuite que l'état de ce dernier est correct. De plus, le système de contrôle de l'accès doit communiquer à un certain niveau avec le système de transmission et d'évaluation des alarmes. Si les deux systèmes ne sont pas intégrés, il devrait exister entre eux au moins une certaine interaction permettant de déterminer si l'accès qui a été enregistré est autorisé ou non et, dans ce dernier cas, de déclencher une alarme. Les deux systèmes peuvent être intégrés dès lors que le système gère les alarmes et les messages de contrôle de l'accès selon l'ordre de priorité correct.

4.270. La figure 24 présente un exemple de configuration des éléments d'un portique de contrôle de l'accès. L'ordre dans lequel se présentent les dispositifs de fouille peut varier, mais toutes les opérations de fouille doivent être achevées avant qu'une personne ne soit autorisée à entrer dans la zone de sécurité.

Contrôle de l'accès des personnes

4.271. Un système de contrôle de l'accès des personnes vérifie l'identité et l'autorisation de la personne cherchant à entrer dans une zone de sécurité. L'autorisation est habituellement fondée sur le besoin d'accéder à une zone pour y mener des activités autorisées. Les systèmes électroniques de contrôle automatisé de l'accès ont une liste d'accès, habituellement une base de données électroniques, qui contient des données sur les personnes ayant l'autorisation d'accéder. Ces

systèmes devraient de préférence être conçus pour créer des enregistrements horodatés pour tous les événements ou alarmes générés dans le système. Les dispositifs modernes de contrôle de l'accès peuvent stocker les données les plus récentes, de sorte qu'ils peuvent fonctionner en mode secours en cas de perte d'alimentation des réseaux. Les paragraphes 4.272 à 4.295 décrivent différentes mesures de contrôle de l'accès des personnes.

Données d'identification

4.272. Les mesures de contrôle de l'accès fondées sur quelque chose qu'une personne possède (données d'identification, telles qu'un badge d'identification avec photo) impliquent généralement un contrôle visuel par un gardien. Certains badges contiennent également des données d'identification codées qui peuvent être utilisées dans les systèmes automatisés de contrôle de l'accès. Si ces badges servent à faire fonctionner un système de contrôle de l'accès (p. ex., à ouvrir une porte, un tourniquet ou un portail), ils devraient être gérés et contrôlés de la même manière qu'un système de contrôle utilisant un dispositif de verrouillage et des clés (voir les paragraphes 4.299 à 4.309).

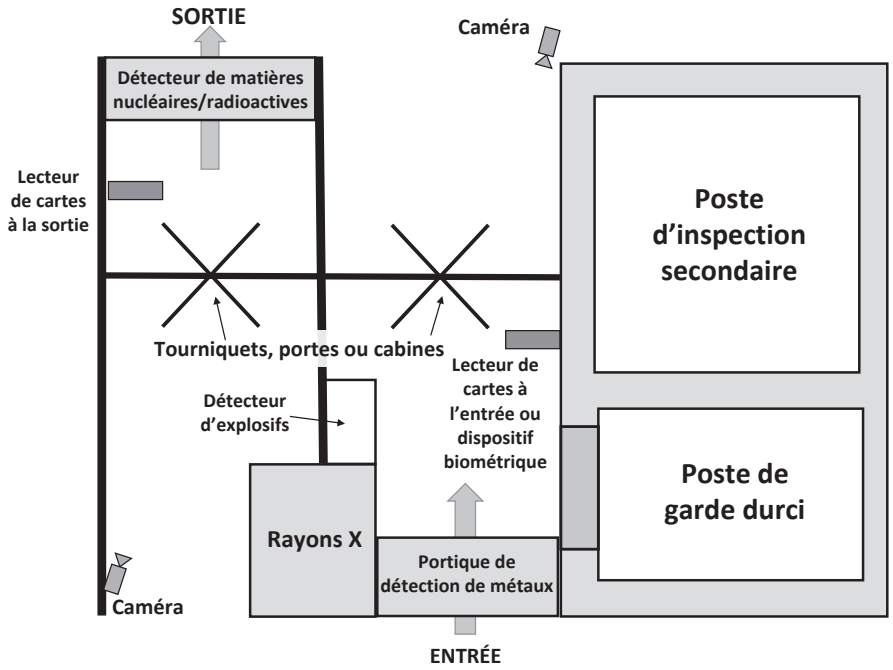


FIG. 24. Exemple de configuration des éléments d'un point de contrôle d'accès

4.273. Le badge d'identification avec photo est un type de données d'identification communément utilisé pour le contrôle de l'accès des personnes, mais c'est le moins sécurisé. Une personne peut fabriquer un faux badge ou modifier son apparence de façon à ressembler à la photo qui figure sur un badge qu'elle a volé. Étant donné que ce type de badge est vérifié manuellement, une erreur du gardien peut en réduire l'efficacité, surtout lorsqu'un grand nombre de personnes entrent dans une installation. En règle générale, ces badges demeurent en la possession de la personne en dehors des heures de travail.

4.274. Dans un système d'échange de badges, lorsqu'une personne présente un badge, le gardien compare ce badge et la personne avec la photo figurant sur un autre badge conservé au point de contrôle de l'accès. S'ils correspondent, le gardien échange les badges et autorise l'entrée. Le badge est conservé au point de contrôle jusqu'à ce que la personne quitte la zone, moment où les badges sont de nouveau échangés ; le badge qui a servi à l'échange et a été porté à l'intérieur de la zone de sécurité n'en sort donc jamais. Cela réduit le risque qu'un badge soit contrefait, perdu ou volé, mais n'évite pas l'erreur humaine ni n'empêche une personne de modifier son apparence de façon qu'elle corresponde à l'image figurant sur un badge perdu ou volé.

4.275. Dans un système d'images stockées, un gardien vérifie l'identité d'une personne sur la base de caractéristiques visuelles. Une image stockée de manière sécurisée est affichée sur un écran de contrôle vidéo ou écran d'ordinateur et comparée à une image en temps réel de la personne demandant à entrer. Les systèmes d'images stockées ne reposent pas sur une caractéristique mesurable unique, comme des empreintes digitales, et ne sont donc pas considérés comme une forme de vérification biométrique. Toutefois, ils sont plus sûrs que les systèmes d'identification manuelle de photos car il est difficile de manipuler frauduleusement une image stockée de manière sécurisée.

4.276. Une donnée d'identification codée peut prendre la forme d'un badge dans et sur lequel sont stockées des informations qui peuvent être lues par un système électronique de contrôle de l'accès. Les systèmes disponibles dans le commerce qui utilisent des données d'identification codées prévoient des caractéristiques telles que des codes d'autorisation uniques, une autorisation d'accès à durée limitée et/ou pour une zone spécifique, et l'enregistrement de chaque passage par chaque point d'accès. Voici des exemples de tels systèmes :

a) Le codage sur piste magnétique est largement utilisé dans les systèmes de cartes de crédit commerciales. Une piste de matériaux magnétiques sur l'un des bords du badge contient des données codées qui sont lues lorsque la carte

passe dans un lecteur à fente ou est insérée dans un lecteur. La technologie des pistes magnétiques est très utilisée du fait d'un coût relativement faible et d'un haut degré de fiabilité.

b) La technologie fondée sur le signal Wiegand utilise un code d'identification produit par une série de fils parallèles aux propriétés magnétiques spéciales intégrés dans une carte. Les fils sont généralement disposés sur deux rangs et le codage est « fixé » pendant la fabrication de la carte. On fait glisser les cartes dans la fente d'un lecteur, comme pour lire les cartes à pistes magnétiques. Cette technologie est largement utilisée dans le secteur du contrôle d'accès.

c) Les codes-barres sont couramment utilisés dans le commerce de détail pour identifier automatiquement les produits au point de vente et ils peuvent être utilisés sur des données d'identification codées. Les différentes largeurs des barres et les espaces entre elles établissent le code, et la carte est lue par un capteur optique qui balaie le code-barres et transmet l'information à un décodeur. Il est facile de reproduire un code-barres à l'aide d'une imprimante ou une photocopieuse. Les codes-barres bidimensionnels peuvent stocker davantage d'informations que les codes-barres unidimensionnels.

4.277. Les badges de proximité peuvent être lus sans être insérés dans un lecteur. Le badge électronique d'identification de proximité utilise un petit transpondeur (émetteur) à radiofréquence et doit être alimenté en électricité d'une manière ou d'une autre. Les badges de proximité passifs sont alimentés par un signal radiofréquence généré par le lecteur à mesure qu'il lit le badge. Les badges de proximité actifs sont alimentés par une pile longue durée. Les badges actifs ont été largement remplacés par des badges passifs. Les badges anciens étaient en lecture seule, un code spécifique étant établi au moment de la fabrication, mais les badges plus récents sont en lecture/écriture et programmables, ce qui permet à l'administrateur du système de programmer un badge en fonction des besoins du système. Les systèmes tout récents sont protégés par un mot de passe et peuvent crypter des données et utiliser la communication cryptée entre le badge et le lecteur. Le système est conçu de façon que le badge ne puisse être lu que par le lecteur du même système.

4.278. La carte à puce (ou carte à puce intelligente) est de la même taille qu'une carte de crédit bancaire et dispose d'un circuit intégré. Elle peut communiquer avec un lecteur par l'intermédiaire de contacts disposés sur sa surface ou d'une communication radiofréquence à faible consommation d'énergie (carte à puce sans contact). Les cartes à puce sont dotées d'un microprocesseur qui peut également contenir d'autres informations concernant, par exemple, les

transactions financières, la formation du personnel, les dossiers médicaux ou la gestion des biens.

Numéros d'identification personnels

4.279. Nombre de systèmes de contrôle de l'accès demandent à l'utilisateur de saisir un numéro d'identification personnel (NIP) mémorisé pour accéder à la zone concernée. Dans un système reposant sur la seule saisie d'un NIP, l'utilisateur saisit son NIP sur un clavier pour accéder à la zone concernée : le NIP n'identifie pas sans équivoque la personne si d'autres personnes figurant dans la base de données du système ont le même NIP. L'utilisation du seul NIP ne fournit pas un niveau de sécurité élevé, car un agresseur pourrait se procurer le NIP par l'observation ou la contrainte. S'il n'empêche pas la saisie répétée d'un NIP erroné, le système pourrait être neutralisable.

4.280. L'utilisation d'un NIP combiné à l'une des données d'identification énumérées plus haut fournit un système plus sécurisé. Par exemple, une personne demandant à accéder à la zone concernée pourrait insérer une donnée d'identification codée dans le système avant de saisir un NIP sur un clavier. Ce numéro peut ensuite être comparé au numéro crypté stocké dans le fichier d'accès de cette personne, et si les numéros sont identiques (et si la personne est investie du mandat approprié), elle peut accéder à la zone concernée. Ce système n'est toutefois pas non plus sans défauts, car une personne pourrait donner le NIP et la donnée d'identification à un agresseur.

4.281. Les systèmes sont généralement plus sécurisés si les NIP sont créés de façon aléatoire et transmis aux utilisateurs au lieu de leur permettre de les créer eux-mêmes. De plus, le système devrait protéger le NIP en le cryptant avant de le transmettre sur un réseau ou de le stocker.

Systèmes d'identification biométrique

4.282. Les systèmes d'identification biométrique utilisent une caractéristique physique ou physiologique propre à une personne pour vérifier son identité. Les systèmes disponibles dans le commerce utilisent des caractéristiques telles que le poids, la géométrie de la main ou du doigt, la forme des veines, les empreintes digitales, la reconnaissance faciale et la forme des yeux. Les facteurs à prendre en considération en choisissant un système sont notamment la mesure dans laquelle la caractéristique peut identifier sans équivoque une personne, la variabilité de cette caractéristique chez cette personne et la difficulté qu'il y a à mettre en œuvre le système qui traite cette caractéristique. Les systèmes biométriques

peuvent servir à valider d'autres données d'identification utilisées pour le contrôle de l'accès ou être utilisés seuls. Dans le premier cas, le système utilise la première donnée d'identification pour identifier le bon dossier (p. ex. NIP ou carte d'identification radiofréquence), puis vérifie que les données biométriques associées sont correctes. Lorsqu'il est utilisé seul, le système biométrique pourrait devoir rechercher dans la base de données le bon dossier, ce qui allonge le délai de traitement et de vérification, surtout si cette base est grande. Dans les États où la législation requiert l'anonymat, certains systèmes sont conçus de façon à empêcher la reconstruction des données biométriques d'une personne (p. ex., les empreintes digitales ne peuvent pas être récupérées).

4.283. Pour toute caractéristique biométrique, certaines personnes ne peuvent pas être identifiées sans équivoque de cette manière ; d'autres méthodes doivent alors être disponibles. De plus, si une personne doit porter un équipement de protection individuel avant d'entrer dans une zone donnée, cet équipement pourrait empêcher l'utilisation de l'identification biométrique. On pourrait, par exemple, mettre en place des mesures de contrôle de l'accès réalistes pour les personnes portant des gants ou des masques respiratoires : une personne portant des gants ne peut pas être identifiée par la géométrie de la main ou les empreintes digitales, et un masque respiratoire pourrait empêcher d'utiliser les systèmes d'identification reposant sur la reconnaissance faciale, la forme des yeux ou l'iris.

4.284. Chaque mesure de contrôle d'accès biométrique a un taux de fausses acceptations (le pourcentage de fois où le système valide l'identité d'une personne non autorisée) et un taux de faux rejets (le nombre de fois où une personne autorisée se voit refuser l'accès à la zone concernée). D'autres défaillances du système peuvent être dues aux caractéristiques ou aux actions de la personne, comme dans le cas d'empreintes digitales illisibles. Ces facteurs devraient être pris en considération pour choisir un système de contrôle de l'accès biométrique.

4.285. Une bascule peut être intégrée aux systèmes de contrôle de l'accès des personnes : le poids de la personne autorisée est enregistré à l'entrée aux fins d'une comparaison ultérieure. Si le poids de la personne correspond par la suite au poids enregistré (avec une tolérance spécifiée), l'association avec d'autres mesures de contrôle de l'accès, telles que les cartes et les NIP, renforce la crédibilité de la vérification de l'identité. Par ailleurs, les bascules réduisent le risque de voir des personnes donner à d'autres des données d'identification ou de voir plusieurs personnes non autorisées accéder simultanément à la zone considérée.

4.286. Les systèmes reposant sur la géométrie de la main caractérisent la forme de celle-ci, en mesurant trois caractéristiques dimensionnelles de la main, telles

que la largeur et la longueur des doigts et l'épaisseur de la main. Une caméra à semiconducteurs photographie la main, y compris en vue latérale pour montrer l'épaisseur de celle-ci. Un éclairement infrarouge et une plaque réfléchissante fournissent à la caméra une image en silhouette de la main. Le système mesure la longueur et la largeur de certaines parties de la main et crée une représentation (ou modèle) numérique de celle-ci, qu'il compare à la main d'une personne demandant à accéder à la zone concernée. Si l'image lue et le modèle stocké correspondent compte tenu des limites de tolérance admissibles, la vérification se passe bien.

4.287. La géométrie de deux doigts est une version simplifiée de ce système, qui permet de vérifier l'identité d'une manière analogue, le système ne mesurant alors que l'index et le majeur.

4.288. La forme des veines, en particulier dans certaines parties de la main, est une caractéristique utile pouvant servir à identifier une personne. Les systèmes de vérification biométrique de l'identité disponibles dans le commerce utilisent la forme des veines de la paume, des doigts et du dos de la main. Utilisée en association avec une caméra à semiconducteurs, la lumière du proche infrarouge peut pénétrer la peau à une profondeur suffisante pour fournir des images claires des veines de certaines parties de la main.

4.289. Les systèmes reposant sur les empreintes digitales utilisent les terminaisons et les bifurcations des crêtes comme éléments caractéristiques d'une empreinte digitale, encore que certains systèmes utilisent l'ensemble de l'empreinte à des fins de comparaison. Tous les systèmes d'identification des empreintes digitales dépendent, pour une identification fiable, d'un positionnement correct du doigt et d'une analyse et d'une comparaison précises de l'empreinte. Pour offrir une assurance supplémentaire, les systèmes modernes prévoient également un contrôle du pouls. Il existe des capteurs à imagerie directe qui utilisent des dispositifs à semiconducteurs pour acquérir des images d'empreintes digitales à l'aide de méthodes capacitives, thermiques ou reposant sur un champ électrique. Ces dispositifs sont communément utilisés dans des applications telles que l'ouverture de session informatique sécurisée, et utilisent l'imagerie ultrasonore ou optique.

a) L'imagerie ultrasonore représente les couches inférieures de la peau et est, de ce fait, plus solide dans le cas d'empreintes digitales « endommagées » par une couche superficielle de la peau sèche ou usée. Cette méthode est plus lente que l'imagerie optique car le transducteur ultrasonique effectue un balayage ligne par ligne.
b) Les méthodes optiques utilisent un prisme et une caméra à semiconducteurs pour obtenir une image de l'empreinte digitale. Une image d'empreintes

digitales sèches ou usées est plus difficile à obtenir à l'aide des méthodes optiques, mais l'application aux plaques optiques de revêtements spéciaux permet d'améliorer la qualité de l'image en assurant un bon couplage optique entre la plaque et l'empreinte.

4.290. Les systèmes de reconnaissance faciale utilisent les caractéristiques distinctives du visage d'une personne pour vérifier son identité. La plupart des systèmes obtiennent l'image du visage à l'aide d'une caméra vidéo, mais certains d'entre eux peuvent obtenir des images thermiques à l'aide d'un imageur infrarouge. Les caractéristiques distinctives sont extraites de l'image et comparées à leurs enregistrements préalablement stockés. L'identité est vérifiée si les images correspondent dans la tolérance spécifiée. Ces systèmes doivent être conçus de manière à pouvoir gérer de façon fiable les variations de présentation du visage et de l'éclairage.

4.291. Comme les empreintes digitales, les caractéristiques de la forme de l'œil sont uniques et il existe des systèmes de vérification de l'identité fondés sur la reconnaissance des formes caractéristiques de la rétine et de l'iris. La forme unique des vaisseaux sanguins qui irriguent la rétine peut être évaluée optiquement à travers le cristallin : un chemin circulaire autour du centre de vision est balayé à l'aide d'une lumière d'une très faible intensité fournie par des diodes électroluminescentes infrarouges, et l'intensité de la lumière réfléchie par la position du faisceau pendant le balayage indique l'emplacement des vaisseaux sanguins de la rétine.

4.292. Les systèmes biométriques fondés sur l'iris utilisent une caméra vidéo pour représenter la structure de l'iris. Les images sont obtenues à l'aide d'une caméra située à environ 25 cm de l'iris, donc sans contact physique entre le visage et le lecteur et sans lumière artificielle projetée dans l'œil (celui-ci est éclairé de l'extérieur par la lumière visible). C'est pour ces raisons que la technologie de la lecture de l'iris est souvent préférée à celle du lecteur d'images rétiniennes. Elle peut toutefois présenter des inconvénients, parmi lesquels les rejets erronés de personnes portant des lunettes, la durée relativement longue de l'opération (entre 4 et 5 secondes pour les utilisateurs chevronnés et jusqu'à 15 secondes pour les nouveaux utilisateurs) et le fait que chez environ 2 % de la population, l'iris a une couleur ou une structure qui ne peut pas être reconnue par le système.

Suivi du personnel

4.293. Nombre de systèmes de contrôle de l'accès permettent de suivre le personnel à l'intérieur d'une installation en enregistrant les données d'identification

aux points d'entrée et de surveillance. Le système enregistre ainsi les zones visitées par une personne et peut restreindre l'accès à certains sites, d'une façon générale ou à certains moments (p. ex. en dehors des heures de travail). Un système de suivi du personnel protège contre le non-respect des procédures, comme dans le cas de la suppression, de l'échange ou de l'utilisation identique consécutive des données d'identification, et permet de détecter les manquements à la règle des deux personnes.

4.294. Les données de suivi du personnel sont stockées dans un journal permanent renseignant sur les accès par date, zone, personne ou autres paramètres. S'ils sont établis comme il convient, les registres de contrôle de l'accès peuvent être utilisés pendant l'enquête menée sur un événement de sécurité nucléaire pour identifier d'éventuels suspects ou s'assurer que les gardiens s'acquittent correctement de leurs tâches de patrouille. De plus, le fait qu'une installation dispose d'un système de suivi de ce type pourrait dissuader le personnel d'accomplir des actes non autorisés. Les demandes d'accès autorisé à des zones de sécurité ou à des systèmes importants pour la sûreté ou la sécurité, qu'elles soient approuvées ou rejetées, devraient en principe être réexaminées régulièrement pour confirmer que l'accès reste nécessaire pour les personnes concernées ou pour aider à identifier d'éventuelles activités liées à une menace d'origine interne.

Règle des deux personnes pour le contrôle de l'accès

4.295. Certains systèmes automatisés de contrôle de l'accès appliquent une règle des deux personnes en conditionnant l'autorisation d'accès à une zone à la saisie dans le système de deux séries de données d'identification ou de caractéristiques biométriques. Cela pourrait par exemple s'appliquer à l'entrée dans une zone de haute sécurité et à la sortie de cette zone afin de s'assurer qu'une personne n'y entre ou n'y demeure pas seule. La règle des deux personnes peut également s'appliquer à l'ouverture d'armoires contenant du matériel de sécurité ou des composants du système d'alarme, à l'entrée dans les salles de traitement du contrôleur pendant la maintenance ou à certaines fonctions du personnel du PCS, telles que l'ouverture à distance d'une porte de sécurité.

Contrôle de l'accès des véhicules

4.296. Les véhicules peuvent faire l'objet de procédures de contrôle de l'accès à l'entrée ou à la sortie de zones de sécurité. Dans certains cas, la vérification de l'autorisation du chauffeur et des occupants suffit et il n'est pas nécessaire de présenter une autorisation distincte pour le véhicule. Pour les zones de haute

sécurité, on peut utiliser un système d'enregistrement des véhicules pour réserver l'entrée aux seuls véhicules autorisés.

4.297. Selon l'installation, les méthodes de contrôle de l'accès des véhicules peuvent être automatisées ou manuelles. Dans le cas d'une petite installation, on peut utiliser une liste manuelle de véhicules autorisés afin de limiter l'accès des véhicules aux zones de sécurité. Pour les installations de grande taille et complexes, on peut établir une base de données automatisée pour les véhicules autorisés et attribuer des données d'identification pour l'accès de ces véhicules, comme pour les systèmes de contrôle de l'accès des personnes, ou utiliser une technologie automatisée d'identification des véhicules (p. ex. la reconnaissance des plaques d'immatriculation ou une puce intégrée au véhicule). On peut aussi utiliser les bases de données d'images pour identifier les véhicules autorisés et déterminer s'ils ont été modifiés par rapport à la configuration autorisée.

Contrôle de l'accès dans les situations d'urgence

4.298. En prévision d'une situation d'urgence, il faudrait mettre au point des méthodes pour faciliter l'accès des équipes d'intervention d'urgence. À cet égard, ces équipes peuvent être accompagnées par des personnes autorisées lorsqu'elles interviennent dans des zones de sécurité. Des orientations supplémentaires sur ce sujet sont fournies dans la référence [2].

Serrures et clés

4.299. Éléments essentiels d'un SPP, les serrures assurent à la fois des fonctions de contrôle de l'accès et des fonctions de retardement. Une barrière physique, une porte, par exemple, peut être franchie par percement ou en neutralisant le mécanisme de verrouillage. Les serrures devraient être choisies de façon à retarder un agresseur au niveau ou aussi près que possible de la barrière : il pourrait alors y avoir lieu d'intégrer le mécanisme de verrouillage dans la barrière elle-même. Les serrures sont communément classées selon le mécanisme de verrouillage ; il peut notamment s'agir de serrures à combinaison, de serrures à clé et de serrures électroniques.

4.300. Les serrures à combinaison se présentent sous la forme d'une serrure auberonnière à coffret, montée sur ou dans une barrière, ou d'un cadenas séparé. Ces serrures peuvent être à cadran unique ou multiple, à poussoir ou électroniques. Une serrure à cadran multiple comporte plusieurs disques rotatifs dont chacun a plusieurs positions (en général au nombre de dix, numérotées de 0 à 9) et est communément utilisée sur les petits conteneurs, les serviettes porte-documents

et les bicyclettes, mais est facile à neutraliser. Dans une serrure mécanique à poussoir, une série de boutons sont pressés les uns après les autres (et dans le bon ordre) pour activer des liens entre une porte et un bouton extérieur afin d'ouvrir la serrure. Une serrure de ce type n'offre qu'un nombre relativement réduit de combinaisons possibles ; on peut donc la neutraliser simplement en essayant chaque combinaison possible jusqu'à trouver la bonne. Une serrure à combinaison à cadran unique est une serrure mécanique à cadran rotatif, qui est en contact avec plusieurs disques ou cames parallèles. Les serrures de ce type sont généralement ouvertes en faisant tourner le cadran alternativement dans le sens des aiguilles d'une montre sur une certaine distance (habituellement sous la forme d'étapes numérotées) et dans le sens inverse des aiguilles d'une montre. Les cames ont habituellement une indentation ou encoche ; lorsque la bonne combinaison est saisie, toutes les encoches s'alignent et reçoivent le loquet qui ouvre la serrure. Certaines serrures à combinaison à cadran unique peuvent être neutralisées assez facilement, mais il existe des modèles haute sécurité qui sont difficiles à neutraliser. Les serrures à combinaison électronique présentent de nombreuses caractéristiques que ne possèdent pas les autres types de serrures à combinaison : certaines d'entre elles peuvent être neutralisées comme les autres serrures à combinaison, mais en général plus difficilement.

4.301. Les serrures à clé peuvent être des serrures à garnitures, à paillettes (ou disque), à levier ou à goupilles, ce dernier type étant le plus communément utilisé. Comme dans le cas des serrures à combinaison, une serrure à clé devrait en principe pouvoir être réglée de façon à n'accepter qu'une parmi un grand nombre de clés possibles. Il existe des barillets haute sécurité qui permettent de mieux contrôler les clés en réservant toute commande de fourniture ou de copie de clés, de clés brutes ou de barillets aux personnes munies d'une autorisation écrite, et en réservant la fabrication et la fourniture de certaines configurations de clés spécifiques à des utilisateurs spécifiques. Les serrures à clé permettent d'utiliser un passe-partout : la plupart des clés n'ouvrent qu'une certaine serrure, mais un passe-partout peut servir à ouvrir n'importe quelle serrure de ce type. L'utilisation de ce système impose de mettre en place des mesures de contrôle supplémentaires, car si un passe-partout est perdu ou volé, il peut servir à ouvrir plusieurs serrures différentes de l'installation concernée.

4.302. Une serrure électronique comprend un ferme-porte automatique sur la porte, un dispositif de saisie, un dispositif de commande et une serrure, généralement mécanique, qui est enclenchée ou activée lorsque la bonne combinaison est saisie ou le bon jeton est présenté au dispositif de saisie. Ces systèmes peuvent utiliser des badges de données biométriques, des cartes à pistes magnétiques, des cartes de proximité, des cartes à puce ou une combinaison. Les

serrures électroniques permettent d'isoler la partie de la serrure qui contient le code de celle qui est exposée et peuvent être programmées en vue de différentes utilisations et facilement intégrées aux systèmes d'alarme. En cas de panne d'électricité, un système de serrure électronique peut être conçu de façon que la serrure reste verrouillée ; en d'autres termes, les portes restent fermées pour le personnel de la partie non protégée de la zone concernée, mais il est possible de sortir de celle-ci depuis la partie sécurisée. Nombre de serrures électroniques sont équipées d'une serrure auberonnière dans la porte et, souvent, d'une clé physique adaptée au barillet – la clé prioritaire d'urgence – qui peut servir à ouvrir la serrure pendant une panne d'électricité.

4.303. L'exploitant de l'installation devrait mettre en place un système de contrôle utilisant un dispositif de verrouillage et des clés et assigner des rôles et responsabilités spécifiques en matière de contrôle pour tous les dispositifs de verrouillage utilisés dans l'installation, à savoir les serrures, les clés et les autres mesures de contrôle de l'accès. Les paragraphes 4.304 à 4.306 décrivent les composants d'un système de contrôle utilisant un dispositif de verrouillage et des clés.

4.304. Il conviendrait normalement d'établir une hiérarchie des serrures et des clés, pour classer les serrures, clés et autres dispositifs de contrôle de l'accès en groupes de mesures qui sont nécessaires pour fournir des niveaux analogues de sécurité dans le cadre d'une approche graduée. Par exemple, les serrures, clés et autres dispositifs de contrôle de l'accès utilisés dans le cadre du SPP pourraient être rangés dans la catégorie « serrures et clés de sécurité » pour les distinguer des « serrures et clés administratives » utilisées dans d'autres parties de l'installation.

4.305. Il faudrait mettre au point des mesures de contrôle utilisant des serrures et des clés pour les serrures et clés de sécurité, assorties de mesures proportionnées aux conséquences potentielles de leur perte ou de leur neutralisation. Par exemple, toutes les clés donnant accès à une zone vitale devraient faire l'objet de mesures de contrôle strictes de façon qu'une personne non autorisée ne puisse pas les utiliser pour y accéder, alors que s'il s'agit des clés d'un bureau administratif ne contenant pas de matières sensibles, le contrôle de la porte pourrait être minimal. Les serrures de sécurité, barillets, clés brutes et données d'identification (cartes et badges) de rechange devraient être entreposés dans un lieu sécurisé.

4.306. On peut utiliser une liste des personnes autorisées à accéder aux clés de sécurité. Les clés et les combinaisons ne devraient être attribuées qu'aux personnes qui sont des utilisateurs autorisés et qui doivent utiliser une clé ou une combinaison de sécurité pour faire leur travail. Un système de contrôle utilisant

un dispositif de verrouillage et des clés devrait inclure des procédures permettant de vérifier l'identité de la personne demandant les clés ou les combinaisons et de s'assurer que celle-ci est autorisée à accéder à toutes les zones accessibles à l'aide de ces clés ou combinaisons.

4.307. Il conviendrait de mettre en place un système de gestion de l'inventaire aux fins de comptabilité et de contrôle des serrures de sécurité, clés et données d'identification utilisées, ainsi que des pièces de rechange entreposées. Les serrures et clés de sécurité devraient avoir une caractéristique unique, telle qu'un numéro d'identification unique, et il faudrait tenir et entreposer dans un lieu sécurisé un registre des serrures, barillets, clés, clés brutes et données d'identification. Le registre devrait indiquer le nombre de clés pour chaque serrure et l'endroit où elles se trouvent, et toutes les fois où une serrure a été changée, ressaisie ou permutée. L'inventaire des serrures, clés et autres dispositifs de sécurité devrait être examiné et actualisé à une fréquence prédéfinie. Il conviendrait, pour remédier à la perte ou au vol de clés, de données d'identification ou d'articles similaires, de mettre en place des mesures telles que la ressaisie ou le changement des serrures, ou le changement des combinaisons ou des codes. Un processus de notification devrait être mis en place pour signaler la perte ou le vol de clés et de données d'identification de sécurité.

4.308. Il existe des systèmes automatisés de contrôle par clés qui contrôlent la délivrance des clés, les suivent jusqu'à leur restitution et procèdent à des contrôles et à des inventaires automatisés.

4.309. Il faudrait mettre en place un système de gestion des combinaisons et des NIP afin d'en contrôler la délivrance aux membres autorisés du personnel. Les registres de combinaisons, de NIP et de modèles biométriques devraient être sécurisés de manière appropriée. Il faudrait tenir des registres du personnel autorisé à connaître les combinaisons et les NIP, qui indiqueraient également les dates auxquelles ces combinaisons ou NIP ont été changés pour la dernière fois et celles auxquelles ils doivent être changés. Les combinaisons et NIP devraient être changés périodiquement, lorsque le personnel autorisé à les connaître n'a plus besoin d'accéder à la zone considérée ou lorsqu'il apparaît que les NIP pourraient avoir été compromis.

Scellés ou dispositifs indicateurs de fraude

4.310. Les scellés ou dispositifs indicateurs de fraude peuvent être utilisés avec des serrures et des alarmes comme indicateurs supplémentaires d'une tentative non autorisée d'ouvrir une porte ou un conteneur. S'ils sont utilisés, ces dispositifs

devraient faire l'objet de contrôles périodiques destinés à vérifier l'existence d'éventuelles irrégularités. Des informations supplémentaires sur les dispositifs indicateurs de fraude figurent dans la référence [8].

RETARDEMENT

4.311. La fonction de retardement, principalement assurée par des barrières, vise à augmenter le temps dont un agresseur a besoin pour commettre un acte malveillant (en particulier la période qui suit la détection et la notification d'intervention) en dressant des obstacles sur tous les chemins qu'il est susceptible d'emprunter, afin de laisser suffisamment de temps à la force d'intervention pour réagir et intervenir. Les barrières complètent les mesures de contrôle de l'accès et favorisent habituellement la détection sur le périmètre d'une zone de sécurité, et peuvent servir à atténuer les conséquences d'une attaque à distance. Elles pourraient dissuader certains agresseurs et neutraliser certaines tentatives de commission d'actes malveillants. Elles pourraient parfois être fournies par des éléments naturels sur le site d'une installation, comme des escarpements, des collines ou de très longues distances, mais le retardement devrait en principe être assuré par des barrières artificielles planifiées et positionnées avec soin sur le chemin suivi par l'agresseur. Outre le retard causé par la barrière elle-même, la distance entre la barrière et la cible protégée pourrait représenter un moyen supplémentaire de retardement. Le retardement fourni dépend de la nature des obstacles physiques employés et des capacités de l'agresseur. Des orientations sur les barrières physiques figurent dans la référence [2].

4.312. Les barrières devraient être envisagées compte tenu de l'objectif de l'agresseur (habituellement l'enlèvement non autorisé ou un acte de sabotage) et de ses capacités telles qu'elles sont définies dans l'évaluation de la menace ou la menace de référence. Si l'objectif est l'enlèvement non autorisé de matières, les barrières qui sont franchies ou détruites par l'agresseur à son entrée dans l'installation ne constitueront plus un moyen de retardement à sa sortie. Certaines barrières, telles que les sorties de secours, pourraient retarder jusqu'à un certain point un agresseur essayant d'entrer dans l'installation, mais elles doivent, pour des raisons de sécurité, permettre au personnel de l'évacuer rapidement.

4.313. Le tableau 4 donne une vue d'ensemble des types de barrières avec les fonctions qui leur sont associées, leur emplacement habituel, leurs limites, les éventuelles mesures compensatoires (mesures temporaires pouvant être appliquées en cas de défaillance de la barrière) et les moyens de garantir l'intégrité de ces barrières.

TABLEAU 4. TYPE DE BARRIÈRE

Type	Emplacement	Fonction	Limites	Mesures compensatoires éventuelles	Mesures visant à garantir l'intégrité
Barrières faible sécurité	Limites de l'installation	Délimiter l'installation	Pas de retardement	Patrouille de gardiens	Contrôle visuel
Clôtures de sécurité	Limites de l'installation Zones de sécurité	Délimiter l'installation Aider à déceler et à évaluer par retardement Pourraient faire partie du système de détection	Retardement limité	Poste de garde	Contrôle visuel Pourraient comporter des capteurs
Barrières d'arrêt de véhicules	Habituellement à la limite de la zone de sécurité	Empêcher l'entrée non autorisée de véhicules	Les barrières sont conçues pour un certain angle d'impact et un poids et une vitesse maximaux d'un seul véhicule Des chicanes limitent les vitesses d'approche	Dispositifs ou obstacles temporaires	Contrôle visuel et essais fonctionnels quotidiens des barrières mobiles

TABLEAU 4. TYPE DE BARRIÈRE (suite)

Type	Emplacement	Fonction	Limites	Mesures compensatoires éventuelles	Mesures visant à garantir l'intégrité
Barrières structurelles (bâtiments)	Peuvent être utilisées comme limite d'une zone de sécurité	Retarder	Pas de protection contre les attaques menées à distance Il pourrait y avoir lieu de renforcer certains éléments pour maintenir l'équilibre (p. ex. installer des grilles aux fenêtres)	Gardiens Forces d'intervention Obstacles mobiles	Contrôle visuel Pourraient comporter des capteurs
Tourniquets et portes	Aux limites ou à l'intérieur de la zone de sécurité	Autoriser l'entrée dans une zone de sécurité	Le compromis pourrait être difficile à trouver entre le retardement et la barrière fixe associée	Gardiens Forces d'intervention Obstacles mobiles	Contrôle visuel Pourraient comporter des capteurs Essais de fonctionnalité de tous systèmes de retardement actif (p. ex., goupilles de verrouillage de porte)

TABLEAU 4. TYPE DE BARRIÈRE (suite)

Type	Emplacement	Fonction	Limites	Mesures compensatoires éventuelles	Mesures visant à garantir l'intégrité
Barrières antifranchissement de limite	Lieux spécifiques	Assurer un retardement équilibré	Le compromis pourrait être difficile à trouver entre le retardement et la barrière fixe associée	Gardiens Forces d'intervention Obstacles mobiles	Contrôle visuel Pourraient comporter des capteurs
Barrières spécialisées (blocs, dispositifs d'arrimage)	Lieux spécifiques, pour augmenter le retardement (p. ex. les emplacements cibles)	Assurer un retardement équilibré	Impact sur la sûreté/ impact opérationnel	Gardiens Forces d'intervention Obstacles mobiles	Contrôle visuel
Barrières remplaçables	Emplacements cibles	Retarder	Sûreté Utilisation limitée Problèmes d'accès à des espaces confinés	Gardiens Activation manuelle en cas de défaillance de l'activation électronique	Maintenance et essais

TABLEAU 4. TYPE DE BARRIÈRE (suite)

Type	Emplacement	Fonction	Limites	Mesures compensatoires éventuelles	Mesures visant à garantir l'intégrité
Barrières en milieu marin	Limites fluviales	Retarder une attaque venue d'un cours d'eau	Pourraient être difficiles à concevoir et à déployer (marées, courant)	Gardiens Drones	Contrôle visuel Essais de fonctionnalité de tous systèmes de retardement actif

4.314. On peut utiliser plusieurs modèles différents de barrières pour mettre en œuvre une approche axée sur la défense en profondeur afin de faciliter l'évaluation des alarmes et l'interception de l'agresseur à des endroits prévus à l'avance. Il conviendrait d'envisager d'installer les barrières à côté des systèmes de détection afin que l'agresseur se heurte à une barrière juste après le décèlement de l'attaque. Cette pratique retarde l'agresseur à l'endroit où il a été détecté et accroît la probabilité d'une évaluation précise et, par conséquent, d'une détection (voir la section 9).

4.315. Pour être équilibrée, la conception d'une barrière doit, dans la mesure du possible, veiller à ce que chaque aspect de la configuration de la barrière permette un retardement équivalent. Dans la conception d'un système de retardement équilibré, il devrait être tenu compte de ce qui suit :

a) mettre en place des barrières et autres mesures de retardement au plus près de la cible afin de ralentir le plus possible l'agresseur ;
b) utiliser des barrières composées de matériaux différents et dont la neutralisation demanderait des méthodes et des outils différents ;
c) disposer les barrières d'arrêt de véhicules aux extrémités des zones de détection ;
d) limiter l'utilisation par l'agresseur de véhicules à proximité de la cible ;
e) obliger un agresseur à pied à porter des outils et des armes (et la matière cible dans le cas d'un enlèvement non autorisé) ;
f) empêcher qu'un véhicule ne soit utilisé comme bélier ou poste de combat, ou pour acheminer des explosifs, à l'emplacement cible ;
g) utiliser des barrières dans les espaces confinés pour réduire autant que faire se peut la liberté de mouvement de l'agresseur.

Barrières faible sécurité

4.316. Les barrières faible sécurité sont généralement installées le plus à la limite externe d'une installation et le sont principalement à des fins de sûreté (dans le cas, p. ex., de projets de construction) et ne retardent que faiblement un agresseur. Elles sont souvent utilisées pour délimiter l'installation (p. ex. pour définir la zone dans laquelle le fait de pénétrer sans autorisation constitue une infraction) et maintenir les animaux à l'écart de la zone de détection. Les barrières faible sécurité sont habituellement des clôtures en bois, en tissu et en barbelé.

Clôtures de sécurité

4.317. Les clôtures de sécurité sont installées aux limites des zones de sécurité. Elles ont un but dissuasif et peuvent retarder un agresseur dans une certaine mesure, et sont souvent utilisées conjointement avec des systèmes de détection d'intrusions. Elles peuvent appuyer les fonctions de décèlement et d'évaluation. Par exemple, on peut en installer en parallèle pour créer une zone dégagée autour d'une zone de sécurité. On peut installer des capteurs, de l'éclairage et des caméras dans la zone dégagée pour mettre en place un système de détection périmétrique des intrusions.

4.318. Une clôture de sécurité comprend généralement des panneaux, des montants, de la quincaillerie et des fondations. Comme le montrent les figures 25 et 26, les panneaux de clôture de sécurité sont habituellement de quatre types : à mailles losangées, à mailles soudées, à mailles en métal déployé (normal ou aplati), en métal, en métal tissé et en béton armé.

4.319. Les clôtures devraient être construites de manière à prévenir le creusement de tunnels souterrains. On y parvient habituellement en réalisant des fondations profondes ou en béton.

4.320. La conception de la clôture devrait tenir compte des systèmes de détection associés et des capacités des agresseurs. Au moment de choisir un matériau pour une clôture, s'agissant en particulier de remplacer une clôture existante, il faudra prendre en considération l'incidence sur les stratégies applicables aux patrouilles de gardiens et la surveillance en circuit fermé, car les différents matériaux pourraient modifier la visibilité à travers la clôture. À des fins spécifiques, on peut utiliser d'autres matériaux pour une clôture (le verre de sécurité, p. ex.).

4.321. Les clôtures de sécurité pourraient être utilisées dans le cadre du système de détection lui-même. C'est par exemple le cas des clôtures avec câble à fibres optiques, capteur dynamométrique et capteur de vibrations (voir la figure 27).

4.322. Les clôtures de sécurité devraient faire l'objet d'un contrôle visuel régulier pour s'assurer qu'elles demeurent capables de remplir leur fonction de retardement. Si cette fonction est temporairement perturbée (p. ex. lors de la réparation d'une clôture endommagée), on peut prendre, en cas de besoin, des mesures compensatoires telles que l'installation de postes de garde pour assurer les fonctions de détection et de retardement.

Utilisation de rouleaux de ruban barbelé

4.323. Le placement de rouleaux de ruban barbelé sur les clôtures ou à proximité renforce leur capacité de retarder un agresseur. S'il vient coiffer une clôture existante, ce ruban peut constituer un ajout efficace, car un agresseur

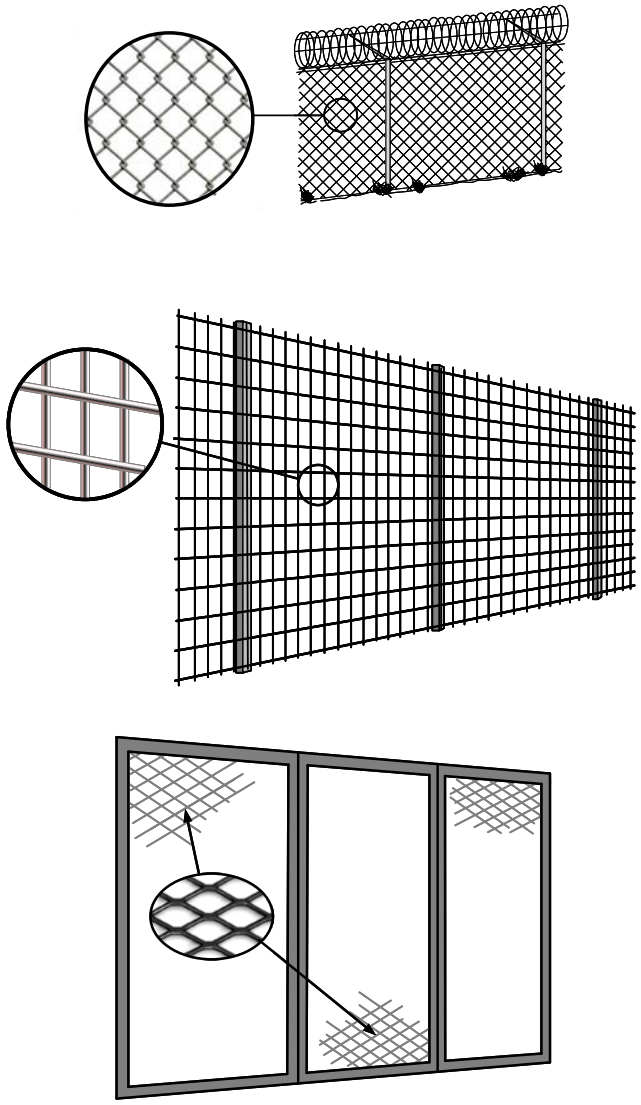


FIG. 25. Types de panneaux de clôture de sécurité. (De haut en bas) À mailles losangées, à mailles soudées et à mailles en métal déployé

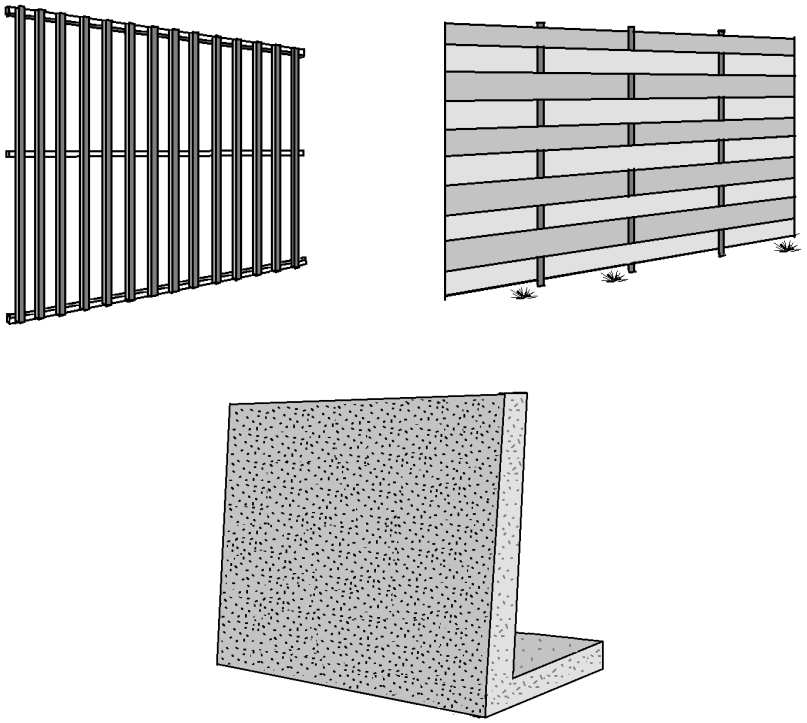


FIG. 26. Types de panneaux de clôture de sécurité. (De haut en bas) En métal, en métal tissé et en béton armé

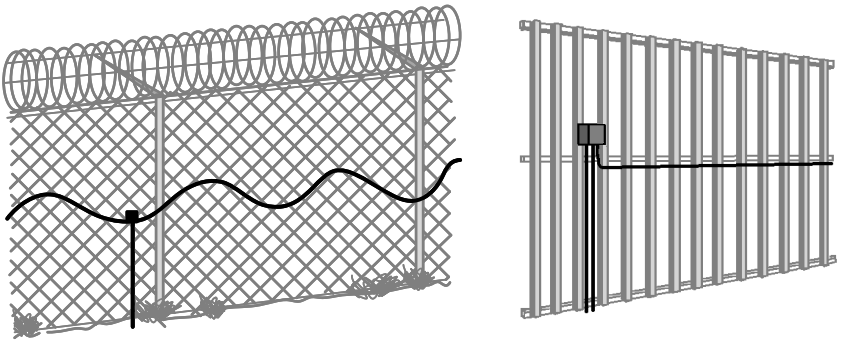


FIG. 27. Clôture de sécurité avec câble de capteur de vibrations (à gauche) et câble à fibres optiques (à droite)

devra avoir des outils supplémentaires pour pouvoir escalader la clôture (voir la figure 28). S'il utilise le ruban barbelé, l'exploitant de l'installation devra prendre en considération l'évaluation de la menace ou la menace de référence, les conditions environnementales, les éventuelles incidences sur la sûreté ou implications juridiques, la capacité structurelle de la barrière existante de soutenir le rouleau de ruban barbelé et les éventuelles conséquences pour les activités de maintenance (p. ex. l'accès aux capteurs et aux caméras).

4.324. Une autre amélioration consiste à installer un rouleau de ruban barbelé horizontalement sur le sol, contre une clôture ou entre les clôtures (voir la figure 29). L'installation de rouleaux de ruban barbelé entre deux clôtures périmétriques peut éviter les lésions accidentelles aux passants circulant en dehors et à l'intérieur de l'installation. Lorsqu'ils sont placés horizontalement, ces rouleaux devraient être fixés au sol et il faudrait empêcher la prolifération de la végétation ou l'accumulation de débris dans les rouleaux.

Barrières d'arrêt de véhicules

4.325. Les barrières d'arrêt de véhicules sont conçues pour prévenir tout accès non autorisé de véhicules à une installation en dissipant l'énergie cinétique du véhicule. Il peut s'agir de structures fixes installées parallèlement aux clôtures de sécurité ou d'éléments amovibles déployés devant des barrières routières ou ferroviaires. Un système de barrières d'arrêt de véhicules devrait pouvoir arrêter un véhicule défini (conformément à l'évaluation de la menace ou à la menace de référence) à une distance spécifique des zones intérieures et vitales, indépendamment de l'endroit où l'attaque est lancée. Il conviendrait d'équilibrer les capacités d'arrêt des barrières fixes et amovibles afin d'éviter toute vulnérabilité dans la série de barrières d'arrêt de véhicules.

4.326. La pénétration d'un véhicule est un succès s'il fonctionne toujours après avoir traversé la barrière ou si celle-ci n'est plus un obstacle parce qu'elle a été retirée, franchie ou percée, par exemple par un véhicule précédent.

4.327. La conception de ces barrières devrait tenir compte des considérations ci-après :

a) la menace (en utilisant l'évaluation de la menace ou la menace de référence) que la barrière vise à enrayer (p. ex. le type, la taille et le poids du véhicule, la vitesse et l'angle d'impact, d'autres caractéristiques physiques) ;
b) les conditions de fonctionnement de l'installation pertinentes, telles que le débit de véhicules ;

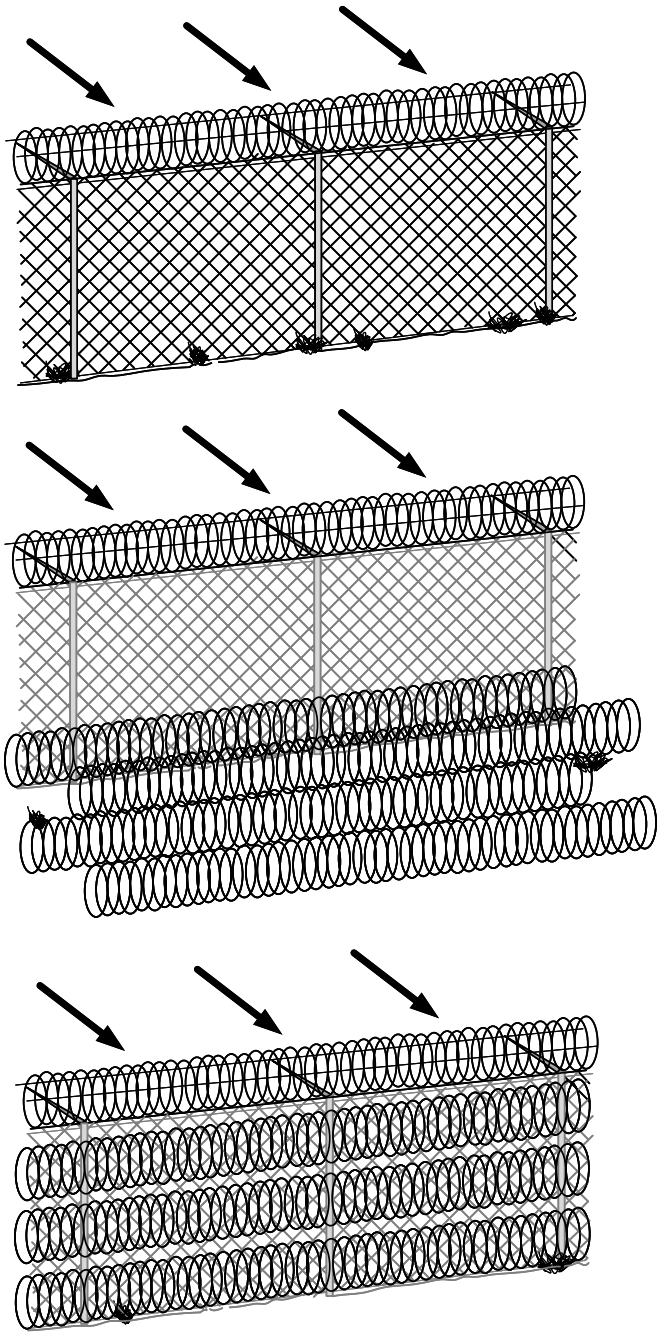


FIG. 28. Clôture de sécurité avec rouleaux de ruban barbelé

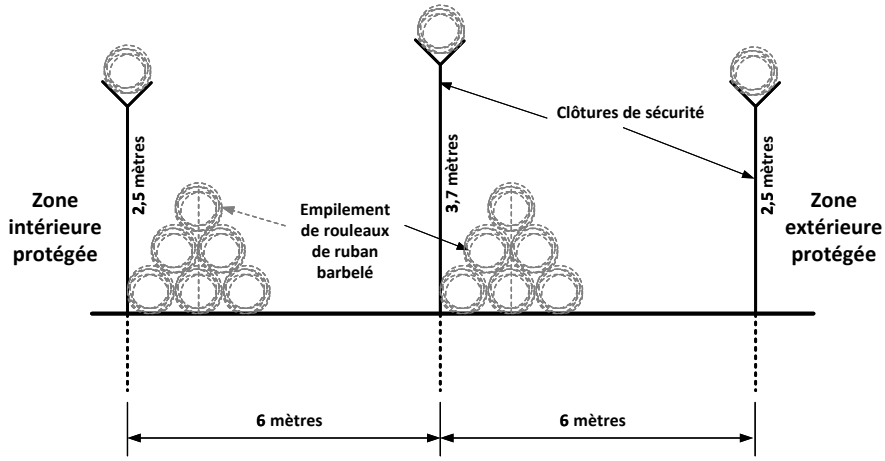


FIG. 29. Configuration de clôtures de sécurité avec rouleaux de ruban barbelé

c) les limites de ces barrières s'agissant de protéger l'installation contre des types inhabituels de véhicules (p. ex. petites camionnettes de livraison, motocyclettes, véhicules de chantier, petits véhicules tout-terrain) ;
d) les zones à protéger (pour choisir les meilleurs endroits où installer ces barrières) ;
e) les considérations propres à l'installation, telles que le terrain, l'aménagement des routes à l'intérieur et autour des zones contrôlées, les voies d'approche potentielles et les conditions environnementales.

4.328. Il faudrait choisir les barrières qui offrent la meilleure protection contre la menace définie et soient adaptées à une situation et à un environnement donnés, et elles devraient être installées correctement :

a) Les barrières installées en dehors d'une zone de détection devraient être conçues de façon à être difficiles à neutraliser par un agresseur. Grâce à cette précaution, ainsi qu'aux patrouilles régulières, il sera difficile pour un agresseur de retirer les barrières sans se faire repérer et déclencher une intervention. Par exemple, des tuyaux de grand diamètre remplis de béton enfouis profondément dans le sol, associés à l'organisation aléatoire de patrouilles, seraient difficiles à retirer sans que la patrouille le détecte, ce qui pourrait rendre une surveillance continue de la zone moins indispensable.
b) Les barrières relativement faciles à neutraliser devraient être installées à l'intérieur d'une zone de détection de façon à permettre de détecter toute manipulation frauduleuse de la barrière.

c) La hauteur et la construction d'une barrière devraient être choisies de façon à être les plus efficaces contre les véhicules prévisibles selon l'évaluation de la menace ou la menace de référence.

4.329. La plupart des barrières d'arrêt de véhicules permanentes sont conçues pour arrêter les véhicules au moyen de l'une ou plusieurs des méthodes suivantes :

a) Un dispositif d'arrêt de véhicules absorbe la plus grande partie de l'énergie cinétique du véhicule et applique une force de résistance faible à modérée pour stopper progressivement le véhicule sur une distance relativement longue. Ce sont par exemple une série de poids qui s'arriment successivement au véhicule à mesure qu'il passe à travers la barrière, et des câbles qui se fixent à des systèmes de freinage pour dissiper l'énergie du véhicule.
b) Un atténuateur de choc absorbe la plus grande partie de l'énergie cinétique du véhicule et applique une force de résistance importante pour stopper le véhicule à une distance raisonnable. On utilise par exemple des conteneurs en plastique remplis de liquide et des fûts en acier vides soutenus par des supports robustes.
c) Un dispositif à inertie échange la quantité de mouvement et l'énergie cinétique avec le véhicule au moment de l'impact. Ce dispositif applique une force de résistance importante pour stopper le véhicule à une distance raisonnable. On utilise par exemple de petites formes en béton et de petits fûts remplis de sable qui ne sont pas ancrés dans le sol.
d) Un dispositif rigide applique une force de résistance importante pour stopper les véhicules à une très courte distance. Le véhicule dissipe la presque totalité de sa propre énergie cinétique à mesure qu'il se déforme au moment de l'impact. On utilise par exemple des formes en béton massives et des structures en acier massives qui sont bien ancrées dans le sol. Le taquet déraileur de train est un type de dispositif rigide.

4.330. Les barrières d'arrêt de véhicules sont potentiellement vulnérables aux points d'accès. Il est fréquent que les routes d'approche conduisent directement à un point d'accès, qui est de ce fait susceptible d'être défoncé par un véhicule, mais l'orientation des barrières d'arrêt de véhicules et des routes peut réduire la probabilité de franchissement d'une barrière. Les routes d'approche présentant de multiples virages et barrières (des chicanes, p. ex.) de chaque côté de la zone du point d'accès réduisent la vitesse d'approche et de départ des véhicules.

4.331. Il faudrait envisager d'installer des barrières amovibles disposées en chicane aux points d'accès. Ce système permet de fermer et de verrouiller une barrière amovible avant de débloquer et d'ouvrir l'autre, de sorte que la zone

délimitée par les barrières constitue une zone d'attente pour un véhicule à fouiller avant son entrée ou à sa sortie. D'autres méthodes pourraient permettre d'obtenir un effet similaire (p. ex. en utilisant des véhicules, des conteneurs ou de lourds sacs de chantier comme barrières temporaires). L'attention portée à l'emplacement des contrôles opérationnels et des systèmes hydrauliques et électriques associés d'une barrière d'arrêt de véhicules peut aider à améliorer la fiabilité de ces barrières.

4.332. En règle générale, les barrières amovibles ne sont pas conçues pour arrêter les véhicules non autorisés, mais pour être déplacées afin de laisser entrer les véhicules autorisés. Elles peuvent être de divers types, à savoir notamment : bornes rétractables, barrières escamotables et barrières levantes (voir la figure 30).

Barrières structurelles

4.333. Les barrières structurelles sont des éléments de construction qui, tels les murs, planchers, plafonds et toits en béton, peuvent servir de barrières de retardement. Ces barrières structurelles peuvent aussi être des structures autonomes intérieures qui pourraient également retarder un agresseur. Elles peuvent aussi protéger les gardiens ou les membres des forces d'intervention.

4.334. Les murs, planchers, toits et plafonds en béton sont conçus pour supporter des charges structurelles et non pas, en principe, pour retarder la pénétration dans une installation. La méthode classique de construction d'un mur repose sur une ossature en bois, des briques, des blocs de maçonnerie ou du béton. Les murs en béton sont construits avec la résistance et l'épaisseur du béton et les dimensions et l'espacement de matériaux de confortement (barres d'armature) qui répondent aux prescriptions structurelles. Toutefois, pour fournir les durées de retardement nécessaires à la protection physique, notamment la protection contre les attaques à distance, il pourrait y avoir lieu de fixer des normes plus strictes pour la conception de ces barrières ou de prévoir des mesures de renforcement supplémentaires.

4.335. Les spécifications des barrières structurelles devraient prendre en compte les capacités des menaces définies dans l'évaluation de la menace ou la menace de référence. En règle générale, les méthodes d'intrusion qu'un agresseur pourrait utiliser pour neutraliser une barrière structurelle sont notamment les outils manuels, électriques et thermiques, les explosifs et le matériel de construction et de démolition lourd, utilisés seuls ou en parallèle.

4.336. La conception et la construction d'une nouvelle installation devraient si possible lui donner des caractéristiques la rendant intrinsèquement capable d'offrir des durées de retardement importantes. De cette façon, non seulement elle

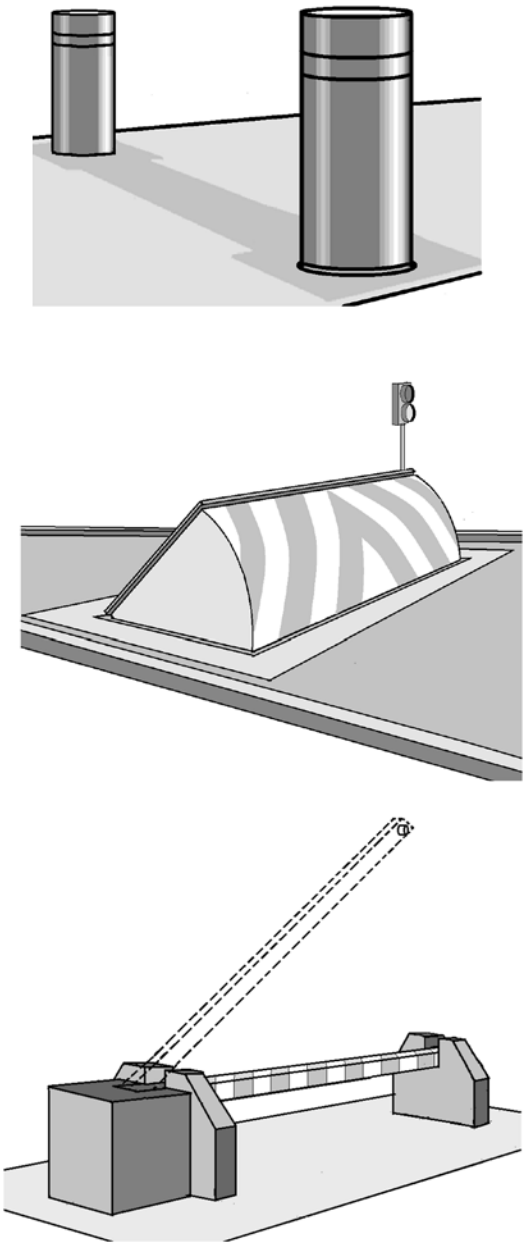


FIG. 30. Barrières d'arrêt de véhicules amovibles. (Du haut en bas) Bornes rétractables automatiques ou manuelles ; barrière escamotable, et barrière levante

serait protégée contre les menaces actuelles, mais elle pourrait l'être également contre les menaces et capacités nouvelles et émergentes. Il est également possible de concevoir et de construire de nouvelles barrières structurelles pour offrir un retardement supplémentaire et, dans certains cas, on peut rendre plus robustes les structures existantes en ajoutant des caractéristiques permettant d'augmenter la durée de retardement. Les méthodes utilisées pour augmenter la durée offerte par les barrières structurelles sont notamment les suivantes :

a) La construction d'au moins deux murs parallèles en béton armé proches l'un de l'autre. Ce faisant, on obtient un délai d'intrusion plus long que dans le cas d'un seul mur dont l'épaisseur serait égale à la somme des épaisseurs des murs distincts, car le percement de plusieurs murs multiplie les efforts à fournir par l'agresseur et nécessite le transfert d'outils d'un mur au mur suivant.
b) La construction d'au moins deux murs en béton armé avec des matériaux de remblai (roches, p. ex.) disposés entre les murs.
c) L'utilisation de plusieurs matériaux pour construire un mur composite, comme dans le cas d'un mur en béton revêtu de plaques d'acier. Cette méthode allonge la durée de retardement et augmente la complexité de la neutralisation de cette barrière.
d) Les améliorations du toit, notamment à l'aide de membranes à écrans enrobés, de plusieurs centimètres d'isolant rigide, de béton armé de barres d'acier déformé et de mailles d'acier expansé, et de grandes barres d'armature posées en rangs ou en couches dans le béton.
e) La confortation des barres d'armature dans un mur en béton. Cette méthode peut allonger le délai d'intrusion dans la plupart des cas de figure. Une explosion pourrait percer le béton, mais le matériau d'armature reste généralement intact et doit être enlevé avant l'intrusion. Comme il faut plus de temps pour enlever une barre d'armature que pour enlever le béton, il pourrait être avantageux d'ajouter des barres, d'augmenter leur taille ou de réduire l'espacement entre elles.
f) Une couverture de terre ou d'autres morts-terrains, pour retarder l'accès au mur lui-même.
g) Installation de barrières sous la ligne de toiture. Celles-ci pourraient être plus efficaces contre l'intrusion que celles qui seraient installées dans le toit lui-même, et pourraient être utilisées dans certaines structures existantes sans nécessiter de modifications importantes. L'installation de ces améliorations sous la ligne de toiture offre à la structure une certaine protection contre les attaques directes et pourrait rendre nécessaire une deuxième tentative d'intrusion. Cette deuxième tentative pourrait également être contrée, car elle aurait lieu dans un espace confiné et l'intrusion pourrait nécessiter des

outils différents. La distance optimale sous le toit pourrait être de 30 cm environ et elle pourrait limiter encore les actions ultérieures de l'agresseur car l'espace concerné serait remblayé à l'aide de débris. Les matériaux d'amélioration sont notamment la toile de criblage pour carrière, l'acier expansé, le maillage de chambre forte ou le caillebotis.

4.337. Lorsqu'il s'agit de protéger les gardiens et le personnel d'intervention, la conception des barrières devrait prendre en considération la résistance des barrières aux effets balistiques et des explosifs ou à une entrée par effraction. Si la barrière est destinée à servir de poste de combat, on pourrait prévoir des meurtrières (ou ouvertures) et un vitrage pare-balles.

Tourniquets et portes

4.338. Pour une conception équilibrée des barrières, la durée de retardement aux points d'accès en deçà d'une série de barrières devrait être égale à celle des structures des barrières avoisinantes. Les points d'accès des personnes dotés de fonctions de retardement à la limite d'une zone de sécurité sont par exemple des tourniquets en métal et durcis, des portiques pour les personnes (p. ex. une cabine avec une porte équipée d'un système d'interverrouillage ou entrée sécurisée) et des portes grillagées et barrières de porte en acier durci (voir les figures 31 à 33).

4.339. Il conviendrait de ne pas réduire la valeur d'un mur en tant que barrière en installant des portes, cadres de porte, gonds ou autres ouvertures standard. On peut allonger les délais nécessaires pour franchir les points d'accès en utilisant des matériaux plus épais ou composites. Les portes résistantes aux explosifs et les portes pare-balles, ainsi que les grilles anti-accès forcé pourraient nettement augmenter la résistance à l'intrusion. Les portes et leurs cadres, gonds, boulons et serrures devraient être renforcés de manière à offrir le même retardement que les planchers, murs et plafonds de la structure. Par exemple, les casemates haute résistance d'entreposage de matières nucléaires de catégorie I doivent avoir des portes blindées de même résistance.

4.340. Il conviendrait d'accorder une attention particulière à l'interaction entre les aspects liés à la sûreté et à la sécurité en ce qui concerne les points d'accès qui sont situés sur les itinéraires d'évacuation hors d'une structure et qui assurent des fonctions de retardement. Il pourrait y avoir lieu de mettre en place des mesures telles que le confinement à distance (y compris le blocage temporaire du mécanisme d'ouverture des portes de secours) en cas d'alarme évaluée et de surveillance visuelle de la situation. On pourrait aussi envisager d'installer des

FIG. 31. Tourniquet en métal (à gauche) et tourniquet durci (à droite) (reproduit avec l'aimable autorisation des Laboratoires nationaux Sandia)

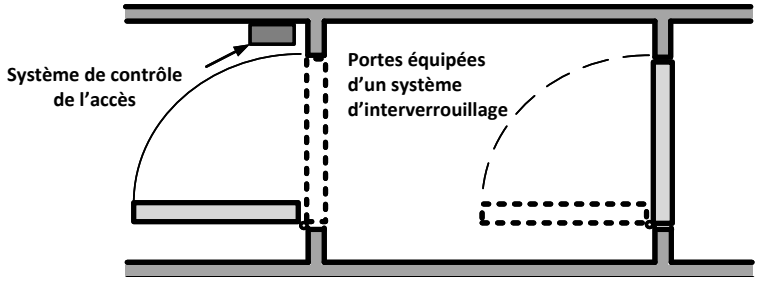


FIG. 32. Portique pour le personnel (entrée sécurisée)

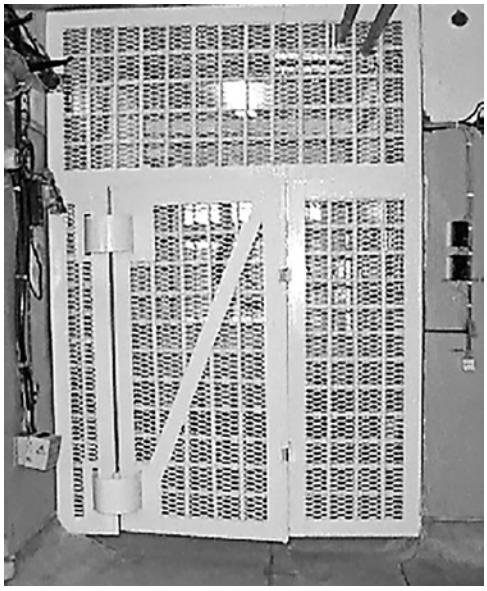


FIG. 33. Porte grillagée en acier durci (gardée ou non)

portes équipées d'un système d'interverrouillage ou d'ajouter un dispositif de séparation (p. ex. des tourniquets durcis).

4.341. Étant donné que l'amélioration et le renforcement ultérieur des points d'accès existants seront relativement onéreux, il conviendrait d'en réduire le nombre au minimum.

4.342. Les portes standard utilisées par le personnel sont généralement faites de tôles en acier léger, pour lesquelles les durées de retardement peuvent varier selon les outils utilisés. On pourrait considérer que l'amélioration des portes existantes, notamment le renforcement du battant, du cadre, des charnières, des dispositifs de sortie, des lucarnes, du vitrage et des serrures, et la protection contre les tentatives de franchissement à l'aide d'outils à main, électriques ou thermiques, allonge leur durée de retardement et équilibre le système de barrières global. On peut utiliser les méthodes énumérées ci-après :

a) Éliminer l'ensemble des lucarnes, boutons extérieurs, entrées de clé et autres ouvertures inutiles.
b) Doubler les battants à l'aide de plaques d'acier.
c) Ajouter des charnières robustes pour supporter tout poids supplémentaire.

d) Ajouter des noyaux de bois entre les plaques pour augmenter la durée de retardement pour les outils de coupage thermique.
e) Souder ou fixer avec un boulon une bande de tôle mince en acier à la porte. Cette bande devrait être de la même hauteur que la porte et large d'au moins 5 cm, et recouvrir sur 2,5 cm le cadre de la porte adjacent.
f) Injecter dans le cadre un mélange de béton à au moins 45 cm au-dessus de la gâche.
g) Percer des trous dans le cadre pour pouvoir injecter des deux côtés du cadre et souder une plaque de métal sur les trous.
h) Souder le haut de la fiche à la charnière.
i) Utiliser des charnières avec goujon.
j) Prévenir l'enlèvement de la porte du côté de la charnière en utilisant une bande d'acier en Z fixée à l'aide de boulons ou soudée à l'arrière du battant de la porte. Si les charnières sont enlevées et qu'une tentative soit faite pour disjoindre la porte de son cadre, une partie de la bande en Z entrera en contact soit avec la surface intérieure du cadre, soit avec l'arrière du butoir.
k) Protéger les fermetures antipaniques en ajoutant une plaque d'acier durci du côté intérieur de la porte. La plaque de métal, à laquelle est fixé un élément en acier imperçable, empêche d'attaquer la fermeture antipanique au ciseau et au crochet en fil métallique. On peut ainsi allonger considérablement le délai d'intrusion si l'espace entre la barre antipanique et la partie horizontale de la plaque est attaqué.
l) Utiliser une seule serrure classique dotée d'un système à pênes dormants de haute sécurité.
m) Ajouter une deuxième porte ou un grillage du côté intérieur de la porte existante pour équilibrer le retardement à l'intérieur de la structure.

4.343. Dans les nouvelles installations ou lorsqu'il faut remplacer un bloc-porte, on peut installer des portes haute sécurité offrant une protection balistique et pouvant résister à une tentative d'accès forcé pour faire face à la menace définie par l'évaluation ou à la menace de référence.

Barrières antifranchissement de limite

4.344. Nombre de limites, telles que le mur d'un bâtiment, prévoient des ouvertures pour les fenêtres et l'accès des sociétés assurant des services publics. Étant donné que ces ouvertures compromettent l'intégrité du mur originel, on utilise des barrières pour qu'il soit plus difficile pour une personne non autorisée de se servir de ces ouvertures pour franchir la limite.

4.345. Il conviendrait d'améliorer les fenêtres pour équilibrer le retardement, de façon qu'elles ne soient pas le maillon faible d'un système de barrières. Les fenêtres standard ne retardent pas les agresseurs et doivent être améliorées pour offrir une bonne résistance à l'intrusion. Si une fenêtre est en état de fonctionner, le mécanisme de verrouillage pourrait constituer un maillon faible qui, s'il est forcé, pourrait être ouvert. Lorsque des fenêtres sont installées dans des portes, les bandes de métal qui séparent le vitrage de la porte sont un maillon faible. L'emplacement de la fenêtre influe également sur l'amélioration à apporter : par exemple, les fenêtres proches du sol doivent être davantage renforcées que celles qui se trouvent à plusieurs mètres de hauteur. Le mécanisme de verrouillage d'une fenêtre devrait se trouver dans un endroit qui ne soit pas facilement accessible depuis l'extérieur. L'installation de dispositifs de verrouillage plus étoffés ou de fenêtres fixes pourrait être considérée comme une mise à niveau possible.

4.346. La solidité et le poids des matériaux des cadres de fenêtre sont très variables. Certains cadres spéciaux contiennent des matériaux dissimulés qui résistent aux outils de coupe, et on peut améliorer la fixation du cadre à la structure en utilisant des pièces de fixation supplémentaires ou plus lourdes ou en soudant la bride de fixation. Toutefois, ces améliorations n'allongeront la durée de retardement que si les matériaux verriers et les revêtements protecteurs sont également mis à niveau.

4.347. Les matériaux verriers standard sont très fragiles. Le verre trempé a amélioré les caractéristiques de résistance mécanique et de contrainte thermique par rapport à celles du verre standard. Le verre armé utilisé dans les portes et fenêtres coupe-feu incorpore dans sa masse un treillis en fil de fer qui augmente la résistance à l'intrusion. Ces matériaux verriers sont souvent améliorés à l'aide d'une grille de protection en acier expansé ou d'un autre grillage en métal.

4.348. Lorsqu'un niveau plus élevé de résistance à l'intrusion est nécessaire, on peut utiliser un verre de sécurité épais. Le verre feuilleté se compose d'au moins deux carreaux de verre recuit ou plaques de verre liées à une ou des couches de plastique. Il résiste mieux que le verre standard à l'accès forcé et peut remplacer la plupart des autres verres. Toutefois, certains types de verre feuilleté sont combustibles et les règlements de sécurité contre les risques d'incendie en limitent l'utilisation. Le vitrage composite en polycarbonate contient une solide couche intérieure de polycarbonate laminé entre deux couches extérieures de verre. Les matériaux composites peuvent être percés à l'aide d'outils à main et de haches d'incendie, mais l'utilisation des panneaux les plus épais augmente la résistance à l'accès forcé à l'aide d'outils en acier. La résistance aux impacts des polycarbonates est proche de celle du verre pare-balles. D'autres améliorations

sont possibles, notamment l'adjonction d'un écran ou d'une grille à l'intérieur de la lucarne ou du vitrage.

4.349. Les ouvertures utilisées par les services collectifs de distribution englobent tous les types d'ouvertures à chambranle autres que les portes et les fenêtres. Ces ouvertures sont très nombreuses dans les installations nucléaires : ce sont les conduits de ventilation, les tunnels d'accès aux services collectifs de distribution, les vides sanitaires, les convoyeurs, les trappes d'accès à la toiture, les ventilateurs d'extraction et les ouvertures de service, qui tous peuvent servir de voie d'accès à un agresseur. Dans les centrales nucléaires, ces ouvertures pourraient aussi inclure les canaux d'amenée et de décharge qui doivent être protégés. Les ouvertures utilisées par les services collectifs de distribution pourraient être relativement faciles à ouvrir et, de ce fait, devraient être reliées à un système d'alarme et barricadées. De plus, elles contiennent souvent des grilles de sûreté ou d'ornement, qui peuvent également faire office de barrières. On peut augmenter la résistance à l'intrusion de ces ouvertures en installant des revêtements protecteurs tels que des grilles, des barres, des treillis de métal expansé ou des écrans. De même, on peut prévoir des grilles à maillage en acier et en métal expansé, des barres de fer, des tubes ou des barreaux pour réduire la taille de ces ouvertures afin d'empêcher une personne de les utiliser. On peut emboîter des conduits ou des tubes pour empêcher l'accès aux gaines d'air, aux ponceaux ou aux grandes canalisations d'alimentation en eau.

Barrières spécialisées

4.350. Les barrières spécialisées utilisées pour certaines applications sont notamment les barrières amovibles placées autour des zones où se déroulent des activités de réparation et de maintenance ou qui doivent être protégées pour une autre raison pendant une période limitée (p. ex. les zones d'entreposage intermédiaire). Pour augmenter les durées de retardement offertes par les barrières existantes, on peut utiliser des blocs modulaires massifs, des conteneurs de fret, voire des véhicules en stationnement, par exemple devant l'entrée d'un lieu d'entreposage empruntée par les véhicules (voir la figure 34).

4.351. D'autres barrières spécialisées peuvent encore augmenter le délai d'intrusion directement aux endroits où l'enlèvement non autorisé de matières nucléaires est possible ou qui peuvent être la cible d'un sabotage. Ce sont les portes de salles d'entreposage haute résistance, les doubles cages en acier pour l'entreposage de matières nucléaires et les dispositifs d'arrimages spécialisés (voir les figures 35 et 36).

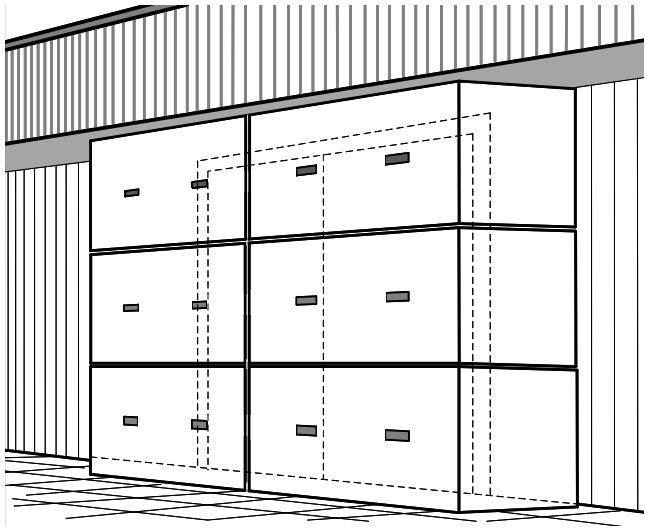


FIG. 34. Blocs modulaires massifs

Barrières remplaçables

4.352. Les barrières remplaçables peuvent être actives ou passives, et peuvent offrir un délai supplémentaire en allongeant le temps qu'il faut à un agresseur pour neutraliser une barrière physique en lui compliquant la tâche. Le matériau remplaçable est en principe entreposé sous forme compacte et, à l'issue d'une réaction chimique ou physique, il se dilate de façon à remplir l'ouverture ou l'espace lors d'une attaque. Les systèmes pyrotechniques d'obscurcissement par la fumée et les systèmes à mousse aqueuse sont deux exemples de barrières remplaçables.

4.353. Les systèmes à barrières remplaçables actives devraient être protégés contre la désactivation liée à une agression d'origine extérieure ou interne et être conçus de façon à éviter leur activation accidentelle pendant d'autres périodes (leur maintenance, p. ex.). Toutefois, ils devraient donner un niveau élevé d'assurance qu'ils s'activeront bien pendant une agression (fiabilité). La sûreté pourrait devoir être prise en considération si ces systèmes doivent être activés (correctement ou non) dans des espaces de travail confinés. Une mesure de défense en profondeur peut consister à déployer un obscurcissant dense associé à du fil barbelé ou fil muni de lames de rasoir, et elle peut allonger sensiblement la durée de retardement par rapport à l'utilisation du fil seul ou de l'obscurcissant seul. Certains systèmes de sûreté peuvent également servir de barrières remplaçables. Par exemple, un système à mousse aqueuse pour la lutte contre l'incendie peut également être

FIG. 35. Double cage en acier pour l'entreposage de matières nucléaires (reproduit avec l'aimable autorisation des Laboratoires nationaux Sandia)

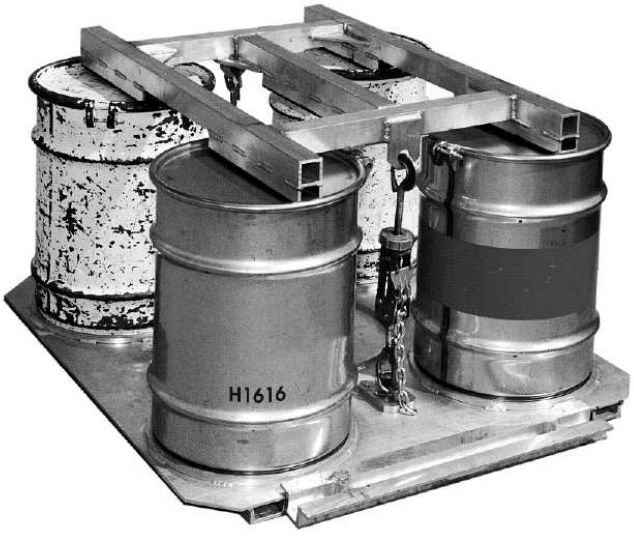


FIG. 36. Dispositif d'arrimage spécialisé

utilisé comme système à barrière remplaçable pour la sécurité, mais il devrait

l'être sans compromettre la sûreté ou la sécurité.

4.354. Les barrières remplaçables passives installées dans les portes ou d'autres lieux ne sont pas activées à distance ou depuis l'extérieur et sont relativement simples et peu onéreuses.

4.355. Les barrières remplaçables devraient en principe être associées à des barrières physiques importantes pour retarder le plus possible la progression vers la cible. Utilisées seules, les barrières remplaçables sont moins efficaces s'agissant d'allonger la durée de retardement, mais pourraient l'être davantage en tant que barrières à l'enlèvement non autorisé que contre le sabotage.

4.356. Toute utilisation de barrières remplaçables, en particulier des applications activées, devrait être étroitement coordonnée avec les mesures de sûreté pendant les activités de conception, d'installation, de maintenance et d'essais de façon que la sûreté du personnel ne soit pas compromise.

Barrières anti-agression aérienne

4.357. Si une menace aérienne est crédible, le positionnement stratégique de poteaux, de câbles ou d'autres barrières physiques (p. ex. des rouleaux de ruban barbelé) pourrait empêcher certains types d'aéronef d'atterrir dans l'installation. Ces barrières peuvent être installées au sol ou sur le toit de bâtiments.

Barrières en milieu marin

4.358. On pourrait envisager d'installer des barrières en milieu marin là où il est nécessaire de se protéger contre l'intrusion d'une embarcation. Ces barrières peuvent être fixes ou flottantes. Les barrières flottantes artificielles sont conçues selon un principe modulaire et faites de poutres en acier inoxydable ou de câbles armés, d'un dispositif spécial d'assemblage articulé et de mousse rigide haute densité injectée dans des coques de polyéthylène, et les modules peuvent être combinés en séries pour fournir la barrière de la longueur souhaitée. Ces dispositifs servent également à identifier la limite de l'installation dans la masse d'eau concernée.

4.359. Les barrières flottantes artificielles peuvent prendre des configurations différentes et être équipées de dispositifs de sécurité supplémentaires, tels que les barrières de surface, les filets immergés et les dispositifs de détection (voir la figure 37).

4.360. Les barrières déployables sous l'eau peuvent être commandées par un treuil électrique à distance, depuis le PCS ou manuellement. Ces barrières peuvent être des écrans, des maillages ou d'autres matériaux pour clôtures.

4.361. Les barrières flottantes artificielles sont habituellement fixées sur un ouvrage d'amarrage sur le rivage ou ancrées sur le lit de la masse d'eau. Pour une longue barrière, il pourra falloir multiplier les points d'ancrage intermédiaires pour qu'elle soit solidement maintenue en place. La configuration de l'installation dépend des conditions opérationnelles, notamment de la profondeur de l'eau, de la direction du vent et de la marée. Ces barrières peuvent être installées sur des rivières, des lacs, des canaux, des zones au large des côtes et d'autres zones d'eau. Une attention particulière devrait être accordée à l'ancrage de ces barrières lorsqu'elles sont installées à proximité ou au niveau des canaux d'amenée ou d'évacuation de l'eau de refroidissement, en raison des forts courants qui pourraient être générés.

4.362. D'autres barrières en milieu marin pourraient être des structures fixes ancrées au rivage, avec barrières immergées et capacités de détection (voir la figure 38). Certains ouvrages longitudinaux de protection ou murs anti-tsunamis en béton armé peuvent également servir de barrières en milieu marin.

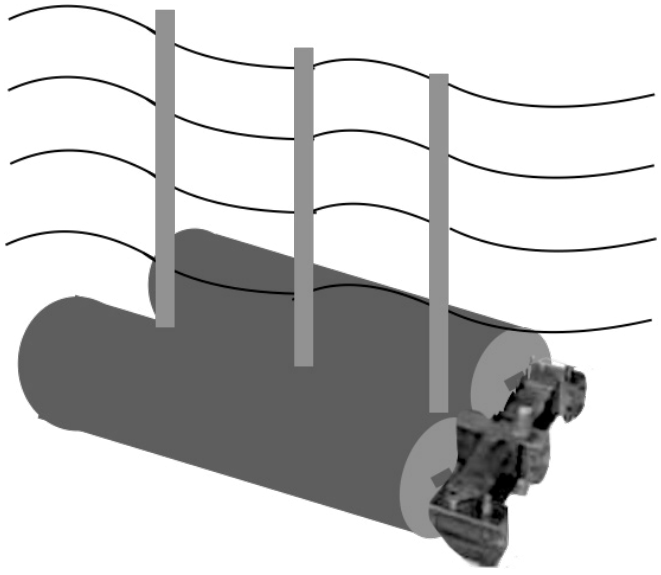


FIG. 37. Double barrière flottante avec barrière de surface et dispositif de détection

FIG. 38. Barrière ancrée sur le littoral (reproduit avec l'aimable autorisation de la Commission canadienne de sûreté nucléaire)

Rôle des barrières en cas d'attaque de sabotage à distance

4.363. La conception des mesures d'atténuation concernant les attaques de sabotage à distance devrait prendre en considération la solidité des dispositifs de sauvegarde et des caractéristiques de fonctionnement (p. ex. le confinement des réacteurs, la redondance, la séparation physique des équipements essentiels), ainsi que la protection contre l'incendie, la radioprotection et les mesures de préparation et d'intervention en cas d'urgence déjà en place dans l'installation. Outre l'utilisation de barrières, on pourrait envisager d'augmenter les patrouilles effectuées par les gardiens et les forces d'intervention sur les lieux pouvant être ciblés en vue d'attaques à distance, afin de dissuader et de déstabiliser tout agresseur. Lorsque les mesures existantes ne suffisent pas pour faire face à des attaques à distance, on devrait envisager de mettre en place les mesures de protection supplémentaires suivantes :

a) Augmenter la distance de sécurité en étendant la zone d'accès limité ou en créant de plus vastes zones dégagées en dehors du périmètre et en éliminant les zones de dissimulation.
b) Installer des structures ou des écrans pour obscurcir les espaces situés entre les zones depuis lesquelles une attaque à distance pourrait être menée et les cibles, ce qui réduit de ce fait la capacité de surveillance de l'agresseur et d'identification de ses cibles et des zones vulnérables spécifiques, et permet au personnel d'intervention de se mettre à l'abri.
c) Mettre en place des barrières physiques à proximité ou au niveau des cibles afin d'atténuer les conséquences d'une attaque à distance. Ces barrières peuvent être des couches de matériaux de différentes densités permettant

de diminuer les effets de l'onde de choc produite par une attaque avec explosifs. L'utilisation de barrières multiples espacées à l'extérieur ou à l'intérieur de la structure pourrait faire détoner prématurément les explosifs, ce qui obligerait les agresseurs à multiplier les attaques précises. La nature de la menace et les prescriptions nationales pourraient également influer sur l'emplacement des barrières, notamment la distance entre celles-ci et l'installation.

d) Modifier l'aménagement des installations et les durcir en :
   i) construisant ou déplaçant en sous-sol les emplacements d'entreposage cibles ;
   ii) déplaçant les cibles dans des salles durcies d'entreposage de matières à l'intérieur d'une structure moins résistante qui, lors d'une attaque, s'effondre et ensevelit la salle d'entreposage durcie ;
   iii) ajoutant un terrain de couverture épais aux installations déjà existantes ou prévues.

5. INTERVENTION

5.1. Les gardiens assurent le contrôle des accès, font fonctionner un PCS, escortent des personnes, effectuent des patrouilles, évaluent les alarmes, interviennent en temps utile et communiquent avec le PCS ou le centre de surveillance [2]. En matière d'intervention, leurs fonctions consistent à se préparer à se déplacer, à communiquer et à neutraliser les agresseurs tels qu'ils sont définis dans une évaluation de la menace ou la menace de référence. L'équipement des forces d'intervention pourrait englober les technologies d'aide à l'appréciation de la situation et à une intervention efficace. La présente section décrit les aspects importants à prendre en considération en matière d'équipement, de qualifications et de formation.

ÉQUIPEMENT

5.2. Les gardiens et le personnel d'intervention devraient disposer de l'équipement leur permettant de remplir leurs fonctions habituelles et d'intervention. Leur équipement approprié dépend de nombreux facteurs, notamment des fonctions qu'ils doivent assurer, des prescriptions opérationnelles et de sûreté de l'installation (p. ex. l'utilisation d'un équipement de protection individuel), des facteurs environnementaux et de l'équipement spécifique nécessaire pour prévenir

l'enlèvement non autorisé de matières nucléaires ou le sabotage de matières et d'installations nucléaires.

5.3. Afin que les forces d'intervention puissent exercer leurs fonctions consistant à se déplacer (c'est-à-dire à se déployer vers un lieu approprié), à communiquer et à neutraliser un agresseur, leur équipement pourrait inclure des véhicules (p. ex. des véhicules, aéronefs et bateaux durcis), du matériel de communication et des armes.

5.4. L'équipement pourrait inclure des technologies d'aide à l'appréciation de la situation, telles qu'un système de suivi du personnel d'intervention et un système de drones aériens (SDA). Les systèmes de suivi permettent au responsable du commandement tactique et au personnel d'intervention de surveiller à distance les lieux où se trouvent ce personnel et les véhicules. Grâce aux technologies telles qu'un système de drones aériens, le responsable du commandement tactique peut suivre en temps réel le déroulement d'un événement de sécurité nucléaire.

5.5. Il faudrait également veiller à ce que le personnel d'intervention dispose d'un équipement de protection, tel que des postes durcis et des véhicules blindés. Les postes de combat durcis peuvent être utilisés pour retarder les agresseurs, mais, dans ce cas, il faudrait protéger ces postes pour que ces derniers ne puissent pas s'en emparer avant l'arrivée des forces d'intervention. Les véhicules tels que les aéronefs ou les véhicules terrestres peuvent réduire le délai d'intervention et être utilisés comme plateformes d'armes stables. S'ils sont dotés d'un blindage approprié, ils peuvent aussi protéger dans une certaine mesure les équipes d'intervention hors site contre des agresseurs armés.

QUALIFICATIONS

5.6. L'État devrait définir des prescriptions minimales de qualification pour les gardiens et les membres des forces d'intervention recrutés par l'exploitant (par opposition aux membres des forces de l'ordre locales ou des forces armées). Les exploitants devraient veiller à ce que les gardiens et les membres des forces d'intervention (y compris les candidats suivant une formation) satisfassent aux exigences en matière de santé, d'aptitude physique, de précision et d'aptitude au maniement des armes à feu, de connaissance des procédures et politiques, et de communication orale et écrite.

FORMATION

5.7. La formation et l'évaluation devraient permettre de faire en sorte que les intéressés puissent remplir efficacement les fonctions qui leur sont assignées dans les conditions habituelles et durant un événement de sécurité nucléaire. Les résultats de la formation et des évaluations peuvent, en sus d'autres méthodes, servir à estimer l'efficacité d'une intervention s'agissant d'intercepter et de neutraliser des adversaires tels que définis dans l'évaluation de la menace ou la menace de référence (voir également la section 9).

5.8. La formation devrait reposer sur les prescriptions, plans et procédures établis, et être dispensée dans un environnement aussi réaliste que possible. Elle devrait s'appuyer sur une série de scénarios qui tiennent compte des capacités de l'agresseur telles qu'elles sont définies par l'évaluation de la menace ou la menace de référence. La formation, les exercices sur table, les exercices partiels ou complets des forces d'intervention et les exercices d'attaque simulée (c'est-à-dire les essais de performance à grande échelle) peuvent servir à évaluer l'état de préparation des gardiens et des forces d'intervention, à recenser les domaines dans lesquels des améliorations sont nécessaires, et à faire en sorte que les plans et procédures soient appropriés et efficaces. Les exercices devraient normalement prévoir de tester ce qui suit :

a) connaissance du profil professionnel exigé et des procédures de travail ;
b) plans d'intervention (accès, fermeture ou confinement) ;
c) aptitude au maniement des armes à feu, y compris dans des conditions de faible luminosité ;
d) emploi d'une force non létale ;
e) suivi de l'agresseur.

6. RÉSEAUX ET SYSTÈMES D'APPUI DU SYSTÈME DE PROTECTION PHYSIQUE

RÉSEAUX DU SYSTÈME DE PROTECTION PHYSIQUE

6.1. Il conviendrait de définir les prescriptions concernant les réseaux du SPP au stade de la conception, chaque fois que des modifications sont prévues et lorsque des changements sont apportés à l'évaluation de la menace et à la menace de référence. La conception des réseaux de communication, d'électricité et des autres

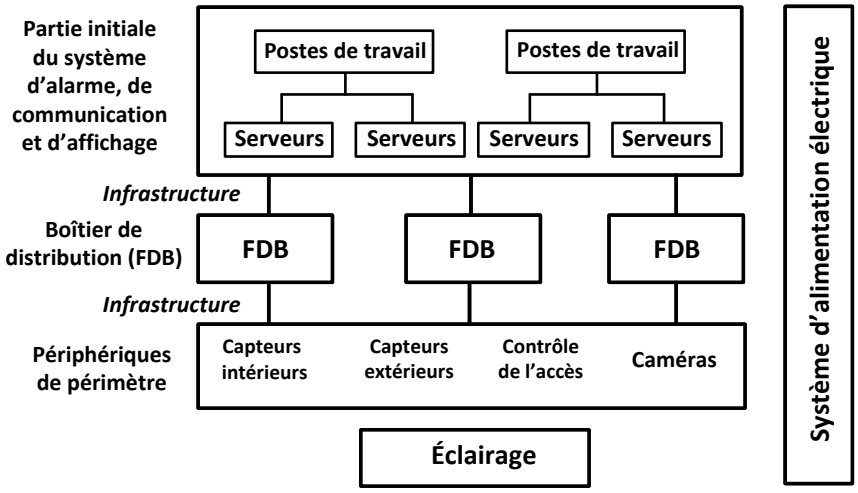


FIG. 39. Réseau type de SPP et dispositifs associés

systèmes d'appui devrait être intégrée à la conception du SPP (voir la figure 39). Le SPP devrait être conçu de manière à pouvoir résister aux cyberattaques et les détecter (pour d'autres orientations sur la sécurité informatique, voir les références [10, 17 à 21]).

6.2. L'intégration des réseaux du SPP devrait s'accomplir d'une manière sécurisée, compte tenu du fait que l'intégration et le couplage des systèmes peuvent augmenter la complexité du réseau et pourraient multiplier pour un agresseur les possibilités de le compromettre. Il s'ensuit que les prescriptions de sécurité informatique concernant les systèmes informatisés, réseaux et systèmes numériques devraient être prises en considération dès le début du processus de conception du réseau du SPP.

6.3. Les systèmes et réseaux informatiques à protéger selon la recommandation énoncée dans la référence [1] sont ceux qu'utilise le SPP pour protéger contre un enlèvement non autorisé de matières nucléaires ou un acte de sabotage et ceux qui sont utilisés pour la comptabilité et le contrôle des matières nucléaires et pour la sûreté. Les cyberattaques peuvent avoir les objectifs suivants :

a) surmonter les obstacles liés à la confidentialité pour acquérir des informations sensibles sur ces systèmes (voir aussi la section 3) ;
b) compromettre l'intégrité des informations sur ces systèmes (p. ex. en modifiant les dossiers conservés aux fins de la comptabilité et du contrôle

des matières nucléaires afin de dissimuler un enlèvement non autorisé de telles matières) ;

c) rendre impossible l'accès à un système (p. ex. en mettant hors service un système important pour le SPP ou en empêchant la transmission d'une alarme au PCS) ;

d) utiliser de façon malveillante une fonction du système (p. ex. en déverrouillant une porte télécommandée).

6.4. Une attention particulière devra être accordée à la question de la sécurité des ordinateurs et réseaux du SPP au regard de scénarios dans lesquels un système est compromis en prélude à une attaque physique (c'est-à-dire dans le cadre d'une « attaque combinée »). En pareil cas, la cyberattaque pourrait se produire immédiatement avant l'attaque proprement dite, mais elle pourrait être menée beaucoup plus tôt. Si la compromission d'un système ou réseau informatique du SPP est détectée, il conviendrait de prendre des mesures pour déterminer si elle vise à modifier le système pour faciliter une attaque physique à venir.

6.5. Le SPP d'une installation nucléaire utilise habituellement des systèmes informatiques de types très divers, notamment des systèmes reposant sur les technologies de l'information et de la communication (qui conservent et transmettent des informations, notamment des informations sensibles), des systèmes informatiques intégrés et des systèmes de contrôle-commande (qui contiennent des codes logiciels, mais dont l'intégrité et la disponibilité pourraient être essentielles pour la sûreté). Le SPP s'articule normalement avec les opérations, la comptabilité et le contrôle des matières nucléaires et les systèmes de sûreté, notamment ceux qui concernent la préparation et la conduite des interventions d'urgence. On trouvera des orientations concernant un SPP intégré dans la référence [2] et la protection de systèmes informatiques dans les références [7, 20], notamment des orientations sur l'établissement d'un programme de sécurité informatique efficace dans les installations nucléaires. Des orientations sur la protection des systèmes de contrôle-commande informatisés sont présentées dans la référence [21].

Conception du réseau

6.6. Les conceptions de réseau de SPP varient selon la taille et les prescriptions de l'installation nucléaire. Il y a beaucoup de variables à prendre en considération pour concevoir un réseau qui réponde aux besoins actuels tout en conservant des possibilités d'adaptation et de croissance. La conception d'un tel réseau devrait se conformer aux prescriptions de l'architecture de sécurité informatique défensive

et du programme de sécurité informatique de l'installation [7]. Les aspects importants à prendre en considération sont notamment les suivants :

a) Hiérarchie : La conception d'un réseau hiérarchisé permet au concepteur de diviser un modèle complexe en éléments plus petits et plus simples. Cela peut aussi l'aider à concevoir pour le réseau une infrastructure fiable dont pourrait profiter la sécurité informatique.
b) Modularité : L'organisation en zones des différentes fonctions exécutées par des systèmes en réseau facilite la conception du réseau. De plus, la modularité peut stabiliser le fonctionnement, si bien que la défaillance d'un domaine fonctionnel (p. ex. une zone ou fonction) n'entraîne pas celle de l'ensemble du système.
c) Confidentialité : Il conviendrait de protéger les informations se rapportant au réseau (p. ex. les bases de données, fichiers et documents, modifications et simulateurs associés) pour qu'elles ne soient pas rendues disponibles ou divulguées à des personnes, entités ou processus non autorisés.
d) Disponibilité : Le réseau devrait rester disponible et exécuter les fonctions requises dans les conditions environnementales et de fonctionnement attendues (c'est-à-dire normales, anormales, situation d'urgence) durant une période définie. Les conditions anormales pourraient être des défaillances de matériel et de logiciel, un très fort volume de trafic de données, une configuration inhabituelle de ce trafic, des incidents de déni de service et d'autres événements non planifiés.
e) Souplesse : La possibilité de modifier des parties du réseau, d'ajouter de nouvelles fonctions, d'augmenter la capacité future du réseau sans qu'une importante mise à niveau soit nécessaire (p. ex. sans remplacer des matériels importants) ou de permettre d'apporter à l'avenir des modifications aux opérations.
f) Intégrité : Il faudrait mettre en place des mesures de protection des éléments du réseau pour garantir leur intégrité tout au long de leur durée de vie utile. Au nombre des méthodes permettant de garantir l'intégrité du réseau figurent des caractéristiques de conception concernant le contrôle de l'accès physique et logique aux équipements, la détection de l'accès non autorisé au réseau et à l'intérieur de celui-ci, et la protection des données sous-jacentes.
g) Complexité : Il faudrait trouver un compromis entre la complexité du réseau et les prescriptions de protection de l'installation nucléaire et des opérations, ainsi que les exigences de maintenance.

6.7. Pendant la conception du réseau du SPP, les besoins en matière de sécurité des informations et de protection physique des lignes de communication et des nœuds de réseau devraient être pris en considération. Le système devrait être doté des

moyens lui permettant de détecter et d'enregistrer les défaillances tant explicites qu'implicites de composants (p. ex. dispositifs, algorithmes, signaux) [7]. Une attention particulière devrait être accordée aux mesures de protection à mettre en place aux limites des zones de sécurité informatique (c'est-à-dire les pare-feux, la limitation du trafic de données), ainsi qu'aux contrôles physiques et administratifs.

6.8. La conception du système devrait prendre en compte la qualité et l'environnement opérationnel des composants à installer. Les modes de défaillance devraient être évalués afin de comprendre les conséquences potentielles d'une défaillance. Par exemple, dans un « réseau arborescent », tous les composants reliés à une « branche » pourraient être affectés, tandis que les autres branches ne le seraient pas, et l'installation d'un équipement redondant sur la même branche du réseau aurait pour seul résultat que la même défaillance toucherait les deux séries d'équipements.

6.9. Les réseaux de communication de données utilisent des architectures différentes pour transmettre les informations d'un dispositif à un autre. L'architecture de réseau est une méthode de connexion de dispositifs à un même réseau informatique. Le type d'architecture choisi détermine le coût, la solidité et la fiabilité du réseau, et différentes architectures peuvent être utilisées pour répondre à différents besoins.

Réseaux de communication

6.10. Les réseaux et dispositifs de communication du SPP devraient s'articuler avec le SPP global. La conception d'un SPP automatisé devrait séparer les fonctions critiques de ce dernier, telles que la détection périmétrique des intrusions, la surveillance du périmètre et le contrôle de l'accès, des autres réseaux de l'installation. La séparation des fonctions fournira une architecture qui permettra la mise en place de mesures de sécurité informatique plus efficaces.

6.11. Le SPP automatisé d'une installation pourrait comprendre :

a) un système d'acquisition et de traitement des données d'alarme (matériel d'affichage et d'évaluation) utilisé pour contrôler le système de détection d'intrusions ;
b) un système de contrôle de l'accès, notamment des systèmes automatisés d'assignation de l'authentification et d'identification du personnel autorisé ;
c) une évaluation et surveillance vidéo ;
d) des systèmes de communication (vocale et données), notamment avec les gardiens et les forces d'intervention ;

e) des éléments de sécurité informatique et de sécurité des réseaux.

6.12. Les dispositifs des sous-systèmes du SPP susmentionnés produisent, reçoivent et traitent divers types de signaux (p. ex. alarmes de capteur et signaux vidéo pour l'évaluation, les communications relatives au contrôle de l'accès et l'état général du système). Pour les sous-systèmes du SPP, toutes les mesures de communication peuvent être intégrées dans un même réseau ou réparties entre plusieurs réseaux. L'intégration à un réseau permet de transférer l'information entre les périphériques et les ordinateurs qui exécutent la fonction de serveurs pour le traitement des données d'entrée.

6.13. Les réseaux de communication de données peuvent comprendre :

a) des dispositifs de protection physique (p. ex., capteurs, caméras, alarmes) ;
b) des périphériques en interaction avec les utilisateurs (p. ex. lecteurs biométriques, serrures de porte électromagnétiques) ;
c) des contrôleurs de dispositifs assurant le traitement des signaux envoyés par plusieurs capteurs ;
d) des dispositifs de distribution (p. ex. commutateurs-mélangeurs et routeurs) ;
e) des serveurs de base de données qui traitent les signaux envoyés par des dispositifs de distribution intermédiaires ;
f) des postes de travail pour les équipements du SPP attribués au PCS, aux gardiens et aux forces d'intervention.

6.14. Là où cela est possible, il faudrait utiliser des voies de transmission des données redondantes et diverses ; les systèmes sont communément conçus de manière qu'un système secondaire puisse prendre automatiquement le contrôle en cas de défaillance du système principal. La redondance offre un système de communication plus sécurisé en obligeant un agresseur à neutraliser ou à compromettre deux voies de transmission distinctes.

Méthodes de cryptage

6.15. On pourrait crypter les données à transmettre s'il est impossible de contrôler l'accès physique aux lignes de communication du SPP. Toutefois, le cryptage et le décryptage des signaux peuvent entraîner des retards importants en matière de communication. Les risques associés à l'allongement des délais de communication doivent être évalués et pris en compte lors de la conception du réseau du SPP. L'utilisation du cryptage devrait être évaluée lors de la réalisation de l'inventaire détaillé des actifs sur lequel appuyer la classification des systèmes informatiques selon leur importance [19].

Technologie de transmission

6.16. Les sous-systèmes de câblage d'un SPP se subdivisent entre réseaux de signaux et réseaux d'alimentation électrique. Le SPP et les sous-systèmes d'éclairage devraient bénéficier d'une alimentation sans interruption (c'est-à-dire qu'une source d'alimentation de remplacement ou de secours est nécessaire en toutes circonstances).

6.17. Les communications de données du SPP peuvent utiliser les lignes filaires, la fibre optique ou, exceptionnellement, les liaisons sans fil (voir le tableau 5). Les lignes de communication filaire sont actuellement la principale méthode de transfert de données.

6.18. Les signaux sans fil peuvent être vulnérables à différents types de cyberattaques, notamment le déni de service (ou de disponibilité) [7]. Toute décision d'utiliser la technologie sans fil pour les communications d'un SPP devrait être prise au regard des risques, et l'utilisation de cette technologie est normalement déconseillée dans le cas des systèmes qui requièrent le niveau de sécurité le plus élevé [7].

6.19. Lorsque l'on envisage d'utiliser des systèmes de capteurs sans fil, il convient de tenir compte des possibilités de collisions, d'évanouissement du signal, d'interférences et de brouillage. Il y a collision lorsque au moins deux signaux sont reçus simultanément, le récepteur ne pouvant alors en lire aucun. L'évanouissement du signal se produit lorsque la distance entre l'émetteur et le récepteur est trop longue ou que la transmission est bloquée par un matériau tel qu'un objet ou une structure métallique de grande taille. Il y a interférence lorsque d'autres sources émettant dans la même gamme de fréquence recouvrent partiellement le signal envoyé par le capteur ou l'émetteur. Le brouillage est une interférence intentionnelle mise en œuvre par un agresseur pour empêcher les signaux d'alarme de parvenir au récepteur. De plus, les signaux sans fil sont susceptibles d'être interceptés et falsifiés.

SYSTÈMES D'APPUI DU SYSTÈME DE PROTECTION PHYSIQUE

Systèmes d'alimentation électrique et de secours

6.20. Le système d'alimentation électrique a pour but de fournir une source d'alimentation fiable au SPP et aux sous-systèmes dans les conditions de fonctionnement normales et les situations d'urgence. La redondance peut

TABLEAU 5. TYPES DE CONNEXION POUR LES LIGNES DE COMMUNICATION

Méthode	Type	Avantages et inconvénients de l'utilisation dans un réseau de SPP
Fil métallique		
Câble coaxial	Impulsions électriques (tension, p. ex. RJ45)	Méthode classique Utilisé dans les équipements de télévision et de radio Grande résistance au bruit et grande résistance mécanique
Paire torsadée	RS-232 (norme de communication) ou câble de catégorie 6	RS-232 a une longueur maximale de câble limitée allant de 15 m (câbles standard) à 300 m (câbles spéciaux)
Fibre optique	Impulsions lumineuses	La fibre optique n'est pas affectée par la foudre, les problèmes de mise à la terre ou d'autres sources de rayonnement électromagnétique 100 fois plus rapide que le câble coaxial 1 000 fois plus rapide que la paire torsadée Il faut un émetteur et un récepteur pour convertir le signal électrique en lumière et reconvertir celle-ci en un signal électrique Rayon de courbure limité Si elle traverse un champ de rayonnement, la fibre peut être endommagée ou « obscurcie »
Fibre multimode	Plusieurs rayons ou modes	Une grande longueur de câble pourrait entraîner une perte de signal
Fibre monomode	Un seul rayon ou mode	Le signal est transmis sur une plus longue distance qu'avec la fibre multimode La fibre monomode est plus chère que la fibre multimode
Transmission sans fil	Utilisation d'ondes électromagnétiques, de radiofréquences, d'hyperfréquences ou de rayonnements infrarouges (pour les très courtes distances)	À utiliser en l'absence de connexions filaires Les signaux transmis sans fil sont extrêmement vulnérables à une attaque La transmission sans fil devrait être réservée aux applications à très faible risque Elle ne devrait pas être utilisée dans un SPP assigné au niveau de sécurité le plus élevé Les signaux sans fil n'ont pas de limites claires

empêcher la défaillance de certains composants de causer celle de l'ensemble du système. En fonction des prescriptions, l'électricité peut être fournie par l'une ou une combinaison des méthodes suivantes :

a) alimentation par un réseau de distribution hors site ;
b) alimentation sans interruption avec batteries ;
c) groupes électrogènes de réserve.

6.21. Dans le cas des installations les plus sensibles, il pourrait être souhaitable d'avoir deux sources distinctes d'alimentation hors site pour réduire la probabilité d'une coupure. Ces sources hors site ne devraient pas être situées au même endroit de façon qu'un seul incident ne provoque pas d'interruption d'alimentation. Les autres aspects à prendre en considération en ce qui concerne les sources d'alimentation du SPP sont l'approvisionnement électrique et la compatibilité avec le réseau de distribution (p. ex. les lignes de transport de force, les coffrets de distribution, les connexions et les conduits électriques), notamment les limites de charge pour tous les composants et sous-systèmes du SPP.

6.22. Si l'électricité de source hors site du SPP est coupée, une alimentation sans interruption devrait fournir immédiatement l'électricité nécessaire pour maintenir en état de fonctionnement les équipements du SPP considérés comme essentiels, tels que les capteurs, les alarmes, les composants concernant la communication et les caméras de surveillance. Une alimentation sans interruption, généralement à accumulateur, fournit au SPP une alimentation électrique temporaire jusqu'au transfert de la charge électrique entre la source normale d'électricité et la source de secours (qui est habituellement un groupe électrogène de secours). Le PCS devrait recevoir une indication acoustique et visuelle de toute coupure d'électricité et du rétablissement de celle-ci, notamment une indication de l'état du groupe électrogène de secours, le cas échéant. En règle générale, l'éclairage périmétrique n'utilise pas de source d'alimentation sans interruption ou à accumulateur en raison de sa forte consommation d'électricité.

6.23. L'alimentation sans interruption et les groupes électrogènes de secours pouvant fournir à un agresseur un itinéraire pour attaquer les systèmes du SPP, ils devraient faire l'objet de mesures de protection, notamment de sécurité informatique. Les aspects à prendre en considération pour assurer la protection de l'alimentation de secours sont notamment les suivants :

a) installation dans une zone contrôlée ou un bâtiment durci à l'intérieur du périmètre (dans certains cas à l'intérieur d'une zone vitale) ;

b) installation de capteurs pour détecter toute manipulation frauduleuse et tout accès non autorisé ;
c) démarrage automatique dès la coupure de l'électricité primaire ;
d) essais de maintenance réguliers en charge pour assurer le maintien de l'efficience et de l'efficacité ;
e) vérification périodique de la tension de sortie pour remédier à la surtension initiale ;
f) contrôle des accumulateurs d'alimentation sans interruption et des systèmes de charge, notamment de la durée de recharge, depuis le PCS ;
g) définir la charge admissible et la durée pendant laquelle les équipements du SPP peuvent fonctionner à l'aide d'une alimentation de secours (p. ex. stockage et fourniture de combustible suffisants) ;
h) mise en place d'une capacité suffisante d'alimentation du SPP, du PCS et du poste de secours ;
i) assurer l'alimentation électrique des équipements essentiels du SPP pour les maintenir en état de fonctionnement.

6.24. La capacité d'activer un réseau de secours offre une redondance qui permet aux équipements du réseau du SPP de fonctionner en cas d'endommagement de l'un de ses éléments, et peut atténuer l'incidence d'une défaillance totale de l'ensemble d'un sous-système ou de ses composants. Les réseaux de secours sont plus solides s'ils utilisent des technologies et des équipements différents (diversité) et s'ils ne sont pas interconnectés.

Prescriptions d'emplacement et de protection des équipements fixes

6.25. Les postes de travail utilisés pour la maintenance des équipements et dispositifs de réseau du SPP (en particulier les serveurs) devraient être installés dans une zone dont l'accès est contrôlé (p. ex. dans des meubles verrouillés ou des salles dotées d'un dispositif de contrôle de l'accès et d'alarme). La règle des deux personnes ou d'autres mesures peuvent être utilisées en ce qui concerne l'accès aux serveurs et postes de travail du réseau aux fins de la protection administrative des équipements et de la gestion de la configuration.

Aspects à prendre en considération concernant la protection des câbles du réseau

6.26. Chaque fois que cela est possible, les câbles de signal du SPP devraient tous être placés dans une zone protégée afin de limiter l'accès à ces câbles. Lorsque les câbles du réseau ne se trouvent pas dans une zone sécurisée et que des données sensibles sont transmises sur ces câbles, il faudrait crypter les données, mettre en

œuvre la surveillance du signal et protéger les lignes dans des gaines et boîtes de connexion métalliques, avec des joints soudés. Pour améliorer la protection, les gaines devraient de préférence être enfermées ou enterrées. Généralement exposés au niveau de leurs deux terminaux, les câbles sont particulièrement vulnérables à des attaques à ce niveau.

6.27. Il conviendrait également de contrôler et surveiller les lignes de communication utilisées pour transmettre des informations sensibles à l'aide de mesures de sécurité informatique afin de s'assurer que l'intégrité de la ligne et du signal est maintenue et d'indiquer d'éventuelles intrusions ou défaillances de composants [7]. Il faudrait envisager de contrôler les ports individuels, notamment leur arrêt, si l'on constate une activité malveillante potentielle.

Protection contre les manipulations frauduleuses

6.28. La protection contre les manipulations frauduleuses devrait être incorporée dans la conception du matériel et du système, par exemple au moyen de capteurs indiquant qu'un agresseur s'approche des équipements ou des lignes. Il conviendrait de mettre en œuvre une protection contre les manipulations frauduleuses ou une surveillance des lignes en ce qui concerne :

a) l'électronique et les coffrets de capteurs dans des boîtes de connexion, avec les interrupteurs de sécurité qui déclenchent une alarme en cas d'ouverture ;
b) les lignes de communication pour les alarmes, avec la surveillance des lignes pour détecter celles qui ont été coupées, déconnectées, court-circuitées ou contournées.

Maintenance et essais du réseau du système de protection physique

6.29. Les dispositifs du réseau du SPP sont en permanence exposés à des conditions de fonctionnement qui peuvent réduire la durée de vie des composants (p. ex. les conditions météorologiques, les chocs mécaniques, les variations de tension et les champs de rayonnements). La maintenance préventive périodique du réseau de protection physique augmentera la disponibilité du SPP et allongera sa durée de vie opérationnelle. Les activités de maintenance et d'essais du réseau du SPP devraient se conformer aux prescriptions de sécurité informatique.

6.30. Cette maintenance peut être préventive (planifiée) ou d'urgence (non planifiée, ou associée à un arrêt ou à un écart par rapport aux spécifications d'un composant du système). La maintenance périodique et les essais de fonctionnement peuvent aider à contrôler la performance et à assurer en permanence l'opérabilité,

la fiabilité, la disponibilité et l'efficacité du réseau s'agissant de recueillir et de transmettre les données envoyées par les sous-systèmes automatisés de protection physique.

6.31. L'exploitant devrait établir des procédures et des calendriers de maintenance préventive concernant les systèmes du réseau du SPP en fonction des types d'équipements installés et des conditions de fonctionnement et du registre d'entretien de ces équipements.

6.32. Il conviendrait de gérer le cycle de vie des composants et systèmes du réseau du SPP de façon à s'assurer que ces composants seraient remplacés avant que ne se produisent des défaillances dues au vieillissement ou à l'obsolescence, compte tenu des durées de vie revendiquées par les fabricants ou observées par le passé. Les activités énumérées ci-après peuvent faciliter la remise en état en cas de défaillance imprévue :

a) Conception modulaire, ce qui accélère le remplacement et la remise en service.
b) Sauvegarde fréquente des bases de données et de la configuration du système.
c) Procédures documentées de remise en état permettant au réseau de redevenir pleinement opérationnel après une panne.
d) Disponibilité de pièces de rechange et d'équipements originels ou compatibles. Il pourrait y avoir lieu de suivre les changements de vendeurs et de fournisseurs afin de garantir cette disponibilité.

7. TECHNOLOGIES NOUVELLES ET ÉMERGENTES

7.1. Les technologies nouvelles et émergentes doivent être évaluées (et, dans le cas des technologies de protection, adoptées selon que de besoin) pour répondre au développement technologique et aux menaces nouvelles et émergentes. Cette évaluation peut faciliter l'adoption de technologies qui réduisent les coûts, améliorent l'efficacité, atténuent les risques associés aux menaces nouvelles et émergentes, et améliorent la fonctionnalité et les capacités globales du SPP.

7.2. Pour être couronnée de succès, l'utilisation de la nouvelle technologie pour le SPP devrait reposer sur l'identification de la technologie disponible la plus appropriée au règlement d'un problème, l'utilisation de cette technologie

dans les limites de ses capacités nominales, l'intégration effective de différentes technologies et l'incorporation des seules technologies avancées qui ont fait leurs preuves. Il conviendrait d'examiner avec soin les revendications des fabricants quant à leur technologie, en prenant notamment en considération son adéquation aux besoins et à l'environnement d'une installation et sa fiabilité.

7.3. La présente section donne des orientations concernant l'évaluation des besoins ou lacunes technologiques constatés dans un SPP existant, le recensement des technologies susceptibles d'être retenues pour répondre à ces besoins ou combler ces lacunes, et l'évaluation de ces technologies avant leur achat et leur mise en œuvre. Un besoin ou une lacune technologique est une limite apparue dans le SPP actuellement mis en œuvre ou une incapacité de répondre à un besoin actuel ou futur. Théoriquement, la différence entre les technologies actuelles du SPP et les technologies nouvelles et émergentes porte simplement sur la question de savoir si une technologie du SPP donnée est communément utilisée dans les installations nucléaires d'un État.

7.4. Un État ou un exploitant pourrait élaborer un cadre structuré de gestion technologique qui permette d'intégrer les technologies nouvelles et émergentes du SPP aux systèmes existants. Ce cadre a pour objectif de recenser et de mettre au point des technologies nouvelles et émergentes de sécurité et de s'assurer de leur efficacité et de leur fiabilité dans l'environnement pertinent, ainsi que de leur disponibilité.

7.5. Il est souhaitable que ce cadre de gestion :

a) recense les menaces nouvelles et émergentes et détermine comment elles pourraient affecter l'installation, et définisse les mesures de sécurité nouvelles ou renforcées éventuellement nécessaires ;
b) inventorie les travaux de recherche-développement ou les nouvelles technologies qui pourraient aider à répondre aux menaces émergentes et aux besoins courants ;
c) recense les technologies qui sont le mieux à même de répondre à un besoin défini et ont fait l'objet d'essais et d'évaluations suffisants ;
d) intègre les technologies du SPP d'une installation nucléaire de façon à atteindre les objectifs généraux du système ;
e) s'assure que la nouvelle technologie est suffisamment éprouvée pour être utilisée dans une installation nucléaire.

7.6. Une proposition de cadre concernant les technologies nouvelles et émergentes prévoit des processus formalisés de conduite de l'évaluation des besoins, une

phase d'essais et d'évaluation, et le déploiement de la technologie concernée (voir la figure 40). Dans le cadre proposé, une évaluation des besoins sert à recenser les domaines dans lesquels la technologie pourrait remédier aux lacunes ou régler les problèmes existants, et les travaux de recherche-développement qui pourraient appuyer les technologies susceptibles de répondre aux besoins et aux menaces futurs. Les technologies susceptibles d'être retenues sont ensuite analysées pour déterminer celles qui pourront ou peuvent déjà apporter des solutions réfléchies et viables pour répondre aux besoins définis. La dernière étape consiste à accepter les technologies de sécurité abouties qui sont prêtes à être utilisées dans les installations en fonction des besoins et qui peuvent être intégrées à d'autres technologies de sécurité.

ÉVALUATION DES BESOINS

7.7. Une évaluation des besoins est un processus systématique servant à définir les besoins, à en examiner la nature et les causes, et à fixer des priorités pour l'action future à mener pour y répondre (voir la figure 41). Cette évaluation porte sur les objectifs à atteindre et non sur les moyens d'y parvenir. De nombreux facteurs peuvent influer sur les objectifs, tels que l'évolution des menaces, les modifications apportées aux prescriptions réglementaires ou aux opérations dans

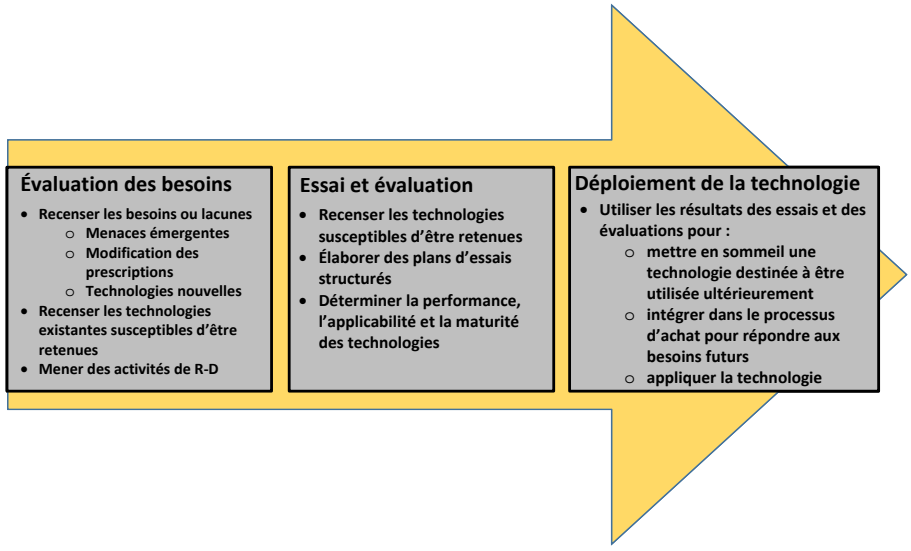


FIG. 40. Cadre proposé pour la gestion technologique

une installation nucléaire, ou la volonté d'améliorer l'efficacité ou l'efficience du SPP. Les résultats sont utilisés pour fixer des priorités et définir les critères concernant les solutions potentielles afin d'aider les décideurs à prendre les bonnes décisions quant à la meilleure répartition des ressources disponibles.

7.8. La première étape d'une évaluation des besoins consiste à déterminer l'état actuel du SPP existant et la menace actuelle. Les problèmes ou sujets de préoccupation sont recensés à partir de différentes sources, notamment des évaluations, d'analyses de la performance d'un SPP ou de l'évolution de la menace ou des modifications apportées aux prescriptions réglementaires ou aux opérations de l'installation. Il conviendrait, lorsque c'est possible, de construire des indicateurs mesurables des besoins. Par exemple, les capteurs existants pourraient avoir une probabilité de détection testée de 0,75, tandis que la performance souhaitée (ou requise) est une probabilité de détection de 0,80. Il faudrait également recenser les sources de données permettant d'analyser le problème de façon détaillée.

7.9. On recueille ensuite les données permettant d'analyser chaque problème recensé. Il conviendrait de procéder à une analyse des écarts pour identifier les domaines dans lesquels tel ou tel système doit être amélioré et, ce faisant, recenser les écarts entre la situation actuelle et la situation souhaitée. Une analyse causale est une analyse structurée visant à déterminer ce qui a causé le problème ou l'écart identifié de façon que les solutions éventuellement dégagées s'attaquent à la véritable cause du problème et non pas simplement à un symptôme. Par exemple, le capteur évoqué dans l'exemple précédent pourrait avoir une faible probabilité de détection du fait des limites de la communication entre le capteur et le système de transmission et d'affichage des alarmes, et non pas du capteur

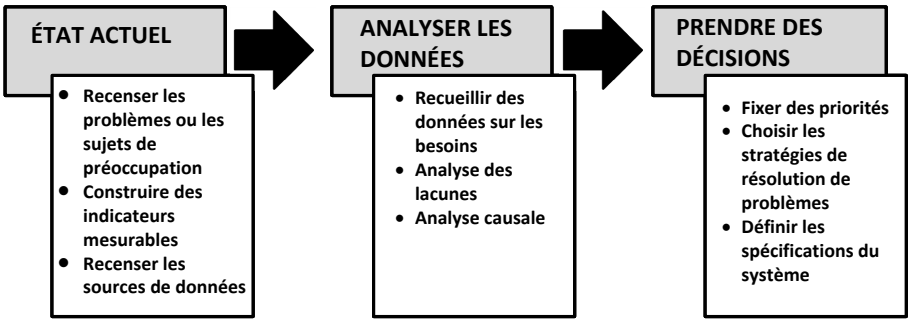


FIG. 41. Processus d'évaluation des besoins

lui-même. En pareil cas, le remplacement du capteur ne s'attaquerait pas à la cause profonde du problème.

7.10. Les résultats de la phase d'analyse de l'évaluation des besoins sont consignés pour fournir aux décideurs les informations qui leur permettent de fixer des priorités, de choisir des stratégies et d'élaborer des spécifications concernant les technologies du SPP susceptibles de répondre aux besoins définis qui doivent être examinées dans le cadre du processus d'essais et d'évaluation.

ESSAIS ET ÉVALUATION

7.11. La phase d'essais et d'évaluation consiste à fournir des informations aux décideurs en vérifiant et en validant les prescriptions de performance, en évaluant la mesure dans laquelle une technologie satisfait à ces prescriptions et en déterminant si les systèmes sont éprouvés, efficaces sur le plan fonctionnel et adaptés à l'usage prévu. Les essais et l'évaluation effectués pendant les premières phases de l'évaluation d'une technologie nouvelle visent à démontrer la faisabilité des approches conceptuelles, à évaluer les risques inhérents à la conception, à dégager d'autres conceptions, à comparer et analyser les équilibres à trouver, et à apprécier la possibilité de respecter les prescriptions opérationnelles. Avec la conception et le développement d'une technologie nouvelle, le processus itératif des essais passe progressivement des essais et de l'évaluation de la conception, qui concernent principalement la réalisation des objectifs de conception technique et la vérification des spécifications techniques, aux essais et à l'évaluation opérationnels, qui portent sur les questions liées à l'efficacité opérationnelle et à l'aptitude à répondre à un besoin défini.

7.12. Des processus formalisés d'essais et d'évaluation ont été mis au point pour le matériel, mais ils doivent être appliqués et adaptés pour que les logiciels puissent aussi être testés efficacement. Dans les deux cas, le processus d'essais et d'évaluation doit être rigoureux, logique, systématique et itératif, les premiers essais donnant lieu à la transmission de résultats d'essais et d'évaluation bien étayés et objectifs aux développeurs du système, aux utilisateurs et aux décideurs.

7.13. La plupart des processus d'essais et d'évaluation peuvent se décomposer en quatre phases principales :

1) Définition des objectifs des essais.
2) Élaboration d'un plan préalable aux essais (y compris les résultats escomptés de ces essais).

3) Réalisation des essais, à savoir :
   i) élaboration de plans d'essais détaillés ;
   ii) rassemblement des données d'essais ;
   iii) analyse des données d'essais ;
   iv) corroboration des résultats des essais.
4) Réalisation et enregistrement de l'évaluation postérieure aux essais.

7.14. Définis sur la base des résultats de l'analyse des besoins, les objectifs des essais pourraient se rapporter à des facteurs tels que les spécifications opérationnelles, les besoins des utilisateurs, les prescriptions environnementales ou opérationnelles, les prescriptions concernant l'interface humaine, la moyenne des temps de bon fonctionnement, la capacité d'intégration aux autres systèmes et la facilité de la maintenance.

7.15. L'analyse des objectifs de l'évaluation préalable aux essais sert à déterminer les types et les quantités de données nécessaires, les résultats escomptés des essais et les outils d'analyse nécessaires pour réaliser les essais et les évaluations. Cette analyse peut également être l'occasion de réfléchir à la manière de concevoir les scénarios d'essai, de mettre en place le cadre des essais et d'enregistrer ces derniers, ainsi qu'aux ressources nécessaires, à l'ordre à privilégier pour la réalisation des essais et à la façon d'évaluer leurs résultats.

7.16. La réalisation des essais consiste à élaborer des plans d'essais spécifiques, à réaliser les essais, à rassembler et analyser les données et à corroborer les résultats des essais. Ces derniers devraient être planifiés et réalisés de façon à fournir suffisamment de données à l'appui de l'analyse. Il faudrait ensuite vérifier l'exhaustivité, l'exactitude et la validité des données avant de les utiliser pour la dernière étape du processus.

7.17. Cette dernière étape est celle de l'évaluation postérieure aux essais, qui consiste à comparer les résultats mesurés (les données d'essais) aux résultats escomptés, à évaluer les données et à porter un jugement sur les plans technique et opérationnel. Si les résultats mesurés diffèrent des résultats escomptés, il conviendrait de réexaminer les conditions et procédures d'essai afin de déterminer si les écarts de performance sont réels ou découlent des conditions d'essai. Ces écarts pourraient tenir à des simulations informatiques inexactes [2], à des anomalies du matériel ou des conditions d'essai, à des erreurs instrumentales ou à des erreurs des processus d'essai. Les paramètres étudiés pour représenter l'environnement opérationnel, la performance des systèmes et le soutien logistique devraient être choisis avec soin, décrits de façon détaillée et enregistrés avant les essais. Pendant l'analyse des données, on peut utiliser la modélisation

et la simulation pour faciliter l'évaluation de la performance, de l'efficacité et de l'aptitude à répondre à un besoin défini.

DÉPLOIEMENT DE LA TECHNOLOGIE

7.18. Le déploiement de la technologie s'entend du processus consistant à ajouter une technologie nouvelle ou améliorée à un système existant. Il s'agit de déployer une technologie compatible avec les prescriptions de sécurité dans un délai raisonnable et au moindre coût. Les buts du déploiement de la technologie sont les suivants :

a) utiliser la meilleure technologie disponible toutes sources confondues, selon qu'il convient ;
b) déployer rapidement la technologie retenue ;
c) au besoin, rafraîchir la technologie utilisée pour que le SPP puisse fonctionner efficacement pendant toute la durée de vie du système.

7.19. Le déploiement de la technologie vise à :

a) améliorer et rafraîchir un SPP existant en fonction des besoins ;
b) maintenir les systèmes ou composants d'un SPP en état de fonctionner en mettant à jour les technologies afin de prévenir l'obsolescence d'un système existant ;
c) améliorer la fonctionnalité de ces systèmes ou composants en mettant à niveau une technologie ou en en ajoutant une nouvelle pour renforcer la capacité du SPP existant.

8. ESSAIS PÉRIODIQUES DES ÉQUIPEMENTS

TYPES D'ESSAIS

8.1. Les essais périodiques des équipements comprennent les essais de réception et les essais de durabilité, à savoir :

a) les essais de préréception, réalisés pendant l'installation pour s'assurer que tous les composants matériels et logiciels sont opérationnels et interagissent correctement ;

b) les essais de réception, réalisés pour montrer que les composants ou systèmes installés ont été mis en place comme prévu et fonctionneront comme prévu ;
c) les essais d'opérabilité et les essais fonctionnels, réalisés pour indiquer que les composants de protection physique fonctionnent comme prévu ;
d) les essais de maintenance et d'étalonnage, qui visent à déterminer si les composants et sous-systèmes du SPP sont correctement installés, alignés et étalonnés.

8.2. Ces différents types d'essais peuvent être effectués séparément, être combinés dans le cadre d'un processus global de maintenance et d'essais, ou appuyer un programme d'assurance de la qualité dans le cadre d'un système de gestion intégré (voir la section 11). Par exemple, les essais d'opérabilité et les essais fonctionnels peuvent être effectués séparément une fois par jour sur un certain élément du SPP. D'un autre côté, le même élément peut faire l'objet d'essais d'opérabilité, fonctionnels et d'étalonnage après la maintenance, avant l'essai de réception, et s'il donne satisfaction pour tous les essais, il est remis en service. Les paragraphes 8.3 à 8.16 décrivent en détail les différents types d'essais.

Essais de préréception

8.3. À la suite de l'installation de nouveaux SPP et sous-systèmes, tous les composants de protection physique devraient faire l'objet d'essais de préréception de façon que tous les composants matériels et logiciels soient opérationnels et interagissent correctement. Ce processus consiste à effectuer des essais point à point sur l'ensemble du réseau pour s'assurer que le système de transmission des alarmes fonctionne correctement de bout en bout et signale celles-ci à un PCS ou à un autre poste, selon le cas. Il s'agit de tester tous les matériels, logiciels, systèmes de communication vocale et de données, dispositifs d'éclairage et systèmes d'alimentation électrique et de secours. Ces essais s'inscrivent habituellement dans le cadre de la phase de construction d'une installation et sont effectués avant le transfert officiel entre le constructeur et l'exploitant.

Essais de réception

8.4. L'exploitant devrait effectuer des essais de réception pour s'assurer que les mesures du SPP sont pleinement fonctionnelles dans tous les aspects de l'exploitation et sont conformes aux spécifications de conception avant la réception. Ils devraient porter sur tous les composants du SPP et de ses sous-systèmes. C'est la partie la plus étoffée des essais : il s'agit notamment de vérifier la bonne installation de tous les composants et sous-systèmes, et d'établir et d'enregistrer les seuils de référence pour la performance, l'opérabilité et le

fonctionnement. Ces essais sont destinés à recenser tout problème opérationnel et de fonctionnalité qui doit être réglé pour que le système soit exploité conformément aux spécifications et prescriptions de conception. Il s'agit de tester tous les matériels, logiciels, systèmes de communication vocale et de données, dispositifs d'éclairage et systèmes d'alimentation électrique et de secours du SPP.

8.5. Les essais de réception devraient être soigneusement planifiés et consignés dans un plan où seraient énoncés les objectifs et la portée de ces essais, les autorisations correspondantes, les responsabilités, les méthodes d'essai, l'enregistrement des défaillances et des données, les spécifications concernant les ressources et le cadre des essais, et décrits tous les essais prévus. Les plans d'essais devraient comporter des spécifications, une description de chaque essai, les conditions d'essai initiales, la procédure d'essai détaillée, les résultats escomptés et tous facteurs spéciaux. Un plan d'essais de réception efficace est tributaire de spécifications de conception clairement définies, mesurables et faciles à tester.

Essais d'opérabilité et essais fonctionnels

8.6. Les essais d'opérabilité et les essais fonctionnels visent à faire en sorte que les mesures, composants et sous-systèmes du SPP fonctionnent initialement dès leur installation et continuent de fonctionner correctement. Ces essais sont effectués régulièrement pour déterminer les dysfonctionnements ou indisponibilités importants de composants ou sous-systèmes du SPP. Pendant ces essais, il ne s'agit pas de neutraliser le composant ou sous-système concerné ni de déterminer dans quelle mesure son fonctionnement donne satisfaction, mais uniquement de confirmer qu'il fonctionne. Par exemple, il pourrait être demandé aux gardiens de s'assurer régulièrement que le portique de détection de métaux est bien alimenté en électricité et de le franchir pour déterminer si les objets métalliques qu'ils ont normalement sur eux déclenchent bien une alarme visuelle et sonore, ou d'ouvrir une porte sur laquelle est fixé un commutateur magnétique symétrique et de confirmer le déclenchement d'une alarme. Ces essais pourraient également être effectués sur les sous-systèmes. Par exemple, il pourrait être demandé à un gardien en patrouille de se déplacer dans la zone surveillée en circuit fermé par un capteur volumétrique de détection d'intrusions afin de confirmer qu'une alarme est bien déclenchée. Le personnel du PCS déterminerait si l'alarme a été envoyée par le capteur et si la caméra appropriée a été activée et fournit une image de qualité suffisante pour établir qu'une personne a déclenché l'alarme.

8.7. Les essais d'opérabilité et les essais fonctionnels devraient normalement être effectués assez fréquemment (p. ex. une fois par équipe ou une fois par semaine, selon qu'il conviendra) pour garantir le fonctionnement continu des composants et

sous-systèmes. Il devrait être rapidement remédié aux problèmes éventuellement détectés par ces essais ou des mesures compensatoires devraient être mises en place jusqu'à ce que les mesures correctives aient produit leurs effets.

8.8. Ces essais peuvent être effectués manuellement par une personne ou à l'aide de dispositifs automatiques d'essai à distance. Les essais manuels impliquent par exemple l'utilisation d'un commutateur magnétique symétrique (voir plus haut) ou l'inspection d'un périmètre par un technicien à la suite d'un orage pour déterminer si des capteurs ou des caméras ont été endommagés ou semblent avoir été décentrés.

8.9. Il est nettement préférable que les composants du SPP fassent l'objet d'essais manuels. Dans certains cas, toutefois, par exemple, du fait de l'insuffisance des moyens humains ou de l'éloignement des systèmes de détection des intrusions, les essais manuels peuvent ne pas être possibles ou être difficilement réalisables. En pareil cas, on pourrait utiliser un dispositif à distance ou automatique, dans lequel le système de transmission et de contrôle des alarmes déclenche lui-même un signal d'essai. Par exemple, un essai automatique pourrait commencer ainsi : un système de détection d'intrusions produit un déclencheur d'essai transmis à un capteur spécifique à un moment aléatoire, et le capteur devrait répondre en déclenchant une alarme. Le système de détection d'intrusions vérifierait ensuite que l'alarme a été déclenchée dans le délai spécifié par le déclencheur et a été visée par l'exploitant dans un délai spécifié. Si un essai à distance ou automatique n'est pas effectué avec succès, un message d'alarme devrait être produit, indiquant la possibilité d'une défaillance ou d'une manipulation frauduleuse d'un matériel, laquelle devrait faire l'objet d'une enquête. Les techniques à distance et automatiques actuellement disponibles pourraient déterminer que le capteur fonctionne, mais ne peuvent pas tester son étalonnage ou son alignement et, de ce fait, un essai automatique à distance devrait compléter, et non pas remplacer, un essai manuel.

Essais de maintenance et d'étalonnage

8.10. Les essais de maintenance et d'étalonnage servent à déterminer si les composants et sous-systèmes du SPP sont correctement installés, alignés et étalonnés conformément aux spécifications. Ces essais seraient également effectués dans le cadre des essais de réception initiaux ou en lien avec ces derniers, ou à la suite d'activités de maintenance. Par exemple, un essai de maintenance ou d'étalonnage d'un portique de détection de métaux ou de rayonnements pourrait consister à franchir à de nombreuses reprises ce portique avec une source d'essai spécifiée afin de montrer que le détecteur a une probabilité de détection acceptable

pour cette source. Dans un autre exemple, un technicien qualifié pourrait tester un capteur périmétrique en marchant, courant, sautant, grimpant ou rampant (selon le cas) dans la zone de détection pour montrer que le capteur fournit la probabilité de décèlement voulue.

8.11. Des essais de maintenance et d'étalonnage bien conçus permettent de détecter si la performance des composants s'est dégradée avec le temps, si les pièces de rechange s'avèrent défectueuses ou si un composant aurait pu faire l'objet d'une manipulation frauduleuse. Ces essais devraient être effectués d'une manière cohérente et donner des résultats reproductibles, de sorte qu'un dispositif testé avec succès un jour mais sans succès le lendemain témoigne d'une dégradation de sa performance et non pas d'un manque de cohérence dans la manière dont l'essai a été effectué. La cohérence et la reproductibilité peuvent être au rendez-vous si l'on fournit une série détaillée de procédures et si la personne qui effectue les essais est qualifiée, ou si l'on utilise un dispositif d'essai homologué qui simule le passage d'un agresseur devant un capteur (p. ex. en utilisant un outil pour tirer le tissu d'une clôture avec une force pouvant correspondre à celle d'une personne qui escaladerait cette clôture).

Essais sur site

8.12. Étant donné que la conception et les conditions environnementales d'une installation sont particulières à celle-ci, l'exploitant devrait effectuer des essais de performance sur site pour établir et valider les valeurs utilisées dans les évaluations de l'efficacité du SPP (voir la section 9). Si l'installation est opérationnelle, il est nécessaire d'instaurer une coordination détaillée entre les opérations de l'installation et le personnel de sécurité de façon que les mesures de protection soient maintenues pendant la période des essais, notamment, le cas échéant, dans le cadre des mesures compensatoires approuvées précédemment. Si un essai fait apparaître une déficience ou si un élément de protection est neutralisé dans le cadre d'un essai (p. ex., une clôture est percée), des mesures compensatoires devraient être mises en place et des actions correctives engagées immédiatement. Les mesures compensatoires devraient être maintenues jusqu'à ce que les actions correctives soient achevées et évaluées.

UTILISATION DE BANCS D'ESSAI SPÉCIAUX

8.13. Les essais de performance effectués sur des bancs d'essai spéciaux à l'intérieur ou à l'extérieur de l'installation peuvent servir à tester l'efficacité d'un composant du SPP dans des conditions très diverses et en fonction de tactiques

très diverses. Un banc d'essai spécial permet d'effectuer des essais dans des conditions réalistes sans que les opérations ou la sécurité de l'installation en soient affectées. Le banc d'essai pourrait inclure les équipements nécessaires pour tester les systèmes et l'infrastructure intérieurs et extérieurs du SPP à l'appui des essais des capteurs et de la collecte et de l'enregistrement des données. Il pourrait également inclure les systèmes de contrôle de l'accès, les systèmes de retardement, les capteurs de détection d'articles interdits, l'éclairage, l'évaluation et les systèmes de distribution d'électricité, ainsi que les systèmes de transmission, de surveillance et d'enregistrement des alarmes.

8.14. À l'intérieur d'une installation, un banc d'essai offre la possibilité de tester et de suivre les mesures du SPP dans les conditions environnementales et industrielles propres à l'installation, afin de mieux comprendre comment ces facteurs affectent la performance et les taux d'alarmes intempestives. Ce banc d'essai peut également servir à évaluer les composants et sous-systèmes de protection physique avant la construction d'une installation. Il est souhaitable de surveiller et tester ces composants ou sous-systèmes en tenant compte de toutes les conditions météorologiques possibles.

8.15. On peut aussi utiliser un banc d'essai spécial pour obtenir des données de performance réalistes afin d'évaluer les technologies nouvelles et de former le personnel au fonctionnement et à la maintenance du SPP. Un banc d'essai peut servir à recenser les essais de maintenance et d'étalonnage spécifiques et à tester la performance d'une barrière ou d'un système de détection d'intrusions qui ne peut pas être testé dans l'installation elle-même pour des raisons de coût ou en raison de considérations propres à l'installation, telles que la sûreté du personnel (p. ex. dans une zone à forte intensité de rayonnement ou contaminée).

8.16. Ces essais peuvent fournir les données nécessaires pour établir les durées de retardement offertes par des barrières physiques spécifiques. Si ces essais sont dûment étayés, les résultats peuvent servir à constituer une bibliothèque de données relatives aux attributs des éléments du SPP (p. ex. les durées de retardement des barrières) pour faciliter l'utilisation de mesures de protection similaires dans d'autres installations nucléaires nationales sans avoir à renouveler les essais. De même, les durées de retardement des barrières peuvent être recueillies en fonction de tactiques très diverses, telles que les outils à main, les outils électriques, les explosifs et les véhicules.

9. ÉVALUATION DU SYSTÈME DE PROTECTION PHYSIQUE

9.1. L'évaluation du SPP vise à établir s'il satisfait aux prescriptions normatives ou aux objectifs de performance. Les méthodes et les sources utilisées pour recueillir, analyser et gérer les données sur lesquelles repose l'évaluation influent directement sur sa validité. L'évaluation doit porter sur toutes les mesures de protection physique, à savoir les personnes, les plans, les procédures et les équipements concernés, pour déterminer si le SPP dans son ensemble se conforme bien aux prescriptions et objectifs définis. La présente section donne un aperçu des méthodes qui peuvent servir à évaluer l'efficacité d'un SPP.

9.2. Les prescriptions de conception du SPP spécifiées au niveau national pourraient appartenir à l'un des types suivants :

a) Une approche réglementaire normative, selon laquelle l'État définit des prescriptions spécifiques en fonction des objectifs de protection physique qu'il fixe. Il est satisfait à une prescription normative si les mesures requises sont en place : par exemple, « une clôture à mailles losangées de 2,4 m est requise sur la limite de la zone d'accès limité ». Les prescriptions normatives pourraient inclure les critères de performance qui sont mesurés en termes techniques et non pas en termes d'efficacité par rapport à l'évaluation de la menace ou à la menace de référence.
b) Une approche réglementaire basée sur la performance, selon laquelle une prescription générale est spécifiée en fonction des objectifs généraux de l'ensemble du SPP par rapport à la menace définie dans l'évaluation de la menace ou la menace de référence. Par exemple, le respect d'une prescription basée sur la performance pourrait consister à prévenir le vol de matières nucléaires de catégorie I par un agresseur spécifique équipé de fusils, d'explosifs en vrac et d'un véhicule commercial, ou à détecter une intrusion dans une installation contenant des matières nucléaires de catégorie III et à la signaler immédiatement à la police locale et à l'autorité compétente dans les 24 heures.
c) Une approche réglementaire à la fois normative et basée sur la performance, selon laquelle certaines prescriptions pourraient être définies en termes d'efficacité par rapport à l'évaluation de la menace ou à la menace de référence, et certaines autres pourraient l'être en fonction de la présence ou de l'absence de l'une ou de plusieurs mesures spécifiques prescrites par l'État (répondant peut-être à des critères techniques connexes). De plus, d'autres prescriptions pourraient combiner ces deux aspects.

9.3. Pour mesurer l'efficacité d'un SPP conçu pour satisfaire à des prescriptions normatives, il suffit de déterminer s'il a été pleinement ou non satisfait à toutes les prescriptions spécifiques. Les prescriptions normatives peuvent généralement être évaluées par observation directe dans l'installation nucléaire ; on peut citer, par exemple, l'observation des plans et procédures opérationnels, les dossiers et journaux, la formation du personnel, les entretiens et les observations du fonctionnement du SPP.

9.4. Pour mesurer l'efficacité d'un SPP conçu pour satisfaire à des prescriptions de performance, il faut habituellement effectuer des essais de performance, tels que des exercices [2]. Dans le cas d'une installation en cours de conception, les essais de performance ne sont pas possibles ; d'autres méthodes, telles que la simulation par ordinateur, peuvent être utilisées. L'évaluation des prescriptions de performance pourrait inclure les études comparatives directes et les essais indépendants pour confirmer que chaque élément du SPP satisfait aux prescriptions et spécifications de performance.

9.5. Si une évaluation indique qu'un élément du système est défectueux ou ne fonctionne pas de manière satisfaisante, il pourrait être nécessaire de prendre immédiatement des mesures correctives, notamment des mesures compensatoires, et d'en informer l'autorité compétente, le cas échéant. Une évaluation du SPP peut également servir :

a) à améliorer l'efficacité du système en mettant en évidence les gains d'efficience et les déficiences ;
b) à ajuster les capacités du système lorsqu'elles dépassent nettement les prescriptions réglementaires ou n'y satisfont pas ;
c) à comparer l'efficacité de plusieurs modèles de SPP pour aider à choisir le meilleur.

9.6. Les études indépendantes, telles que celles que l'on doit au Service consultatif international sur la protection physique (IPPAS) de l'AIEA, pourraient également appuyer l'évaluation du SPP d'une installation.

VÉRIFICATION NORMATIVE

9.7. Selon l'approche réglementaire normative, l'État établit des prescriptions de protection physique spécifiques pour atteindre les objectifs de protection physique qu'il définit pour l'enlèvement non autorisé de chaque catégorie de matières nucléaires et pour chaque niveau de conséquences radiologiques des

actes de sabotage [2]. Ces prescriptions fournissent une série de dispositions ou critères de référence auxquels l'exploitant est tenu de se conformer pour chaque catégorie de matières et chaque niveau de conséquences radiologiques.

9.8. En règle générale, les prescriptions normatives peuvent être évaluées par observation directe, par la mise en place de mesures ou l'examen de dossiers, conjointement avec les essais des différents éléments du SPP. Les prescriptions normatives sont par exemple les suivantes :

a) Des caractéristiques particulières (p. ex., mur, clôture, caméra) doivent être présentes.
b) Une mesure de protection physique doit satisfaire à des paramètres directement mesurables (p. ex. une épaisseur minimale pour un mur ou une hauteur minimale pour une clôture).
c) Les équipements de protection physique doivent avoir un certificat ou autre document officiel qui en confirme les caractéristiques techniques.
d) Les gardiens doivent posséder certaines qualifications et certains types d'équipements, et savoir utiliser ces derniers.
e) Un capteur périmétrique doit être conçu, exploité et régulièrement testé de manière à fournir au moins une probabilité définie de décèlement avec au moins un niveau minimal de certitude concernant une personne rampant, marchant ou courant dans la zone de détection.

9.9. Une évaluation d'un SPP au regard des prescriptions normatives devrait toujours être effectuée avant les autres évaluations, par exemple si les prescriptions basées sur les résultats doivent également être évaluées.

Méthodes d'évaluation normative

9.10. Une évaluation d'un SPP au regard des prescriptions normatives consiste à comprendre les prescriptions, à recueillir des informations et à mettre celles-ci en regard des prescriptions afin de déterminer la conformité. Les méthodes énumérées ci-après sont utilisées pour acquérir les informations permettant de déterminer la conformité :

a) Examen de documents écrits, tels que plans, procédures, plans de séance de formation, journaux et dossiers.
b) Entretiens avec le personnel associé à la conception, à l'exploitation, à la gestion et à la maintenance du SPP. Des entretiens pourraient également être organisés avec le personnel de l'installation qui n'est pas directement

concerné par le SPP afin de mieux comprendre comment les mesures de protection physique sont mises en œuvre dans la pratique.

c) Observations directes de l'organisation, des pratiques et des systèmes en place pour le SPP et des mesures spécifiques prises dans les installations.

d) Utilisation de toutes les méthodes susmentionnées pour réaliser une évaluation objective de la conformité du SPP à chaque prescription normative.

ESSAIS DE PERFORMANCE

9.11. Les essais de performance servent à confirmer l'aptitude d'un SPP à satisfaire à des exigences de performance, mais ils peuvent aussi être requis lorsqu'une mesure prescrite doit répondre à un critère ou à une spécification technique.

9.12. Le choix des composants et mesures du SPP à tester pourrait être basé sur l'exploitation de l'installation, le calendrier des essais ou une exigence formulée par une autorité compétente. Les mesures spécifiques pourraient également être testées sur la base des enseignements tirés de l'expérience d'exploitation, des résultats des évaluations précédentes ou d'événements de sécurité nucléaire, ou d'autres informations faisant état d'une faiblesse potentielle dans le SPP.

9.13. Les essais de performance de certaines mesures de protection physique ou d'un ensemble de mesures du SPP peuvent être effectués pour des raisons diverses, à savoir notamment :

a) Essais visant à déterminer les valeurs des indicateurs de performance (p. ex., les probabilités de détection, les durées de retardement) indiquant le degré d'efficacité des mesures de protection physique prises à l'encontre d'agresseurs disposant de différents moyens, tels que spécifiés dans l'évaluation de la menace ou la menace de référence.

b) Essais visant à déterminer les méthodes qu'un agresseur pourrait utiliser pour neutraliser les mesures et sous-systèmes techniques (qui pourraient servir à appuyer les analyses par arbre de défaillances).

9.14. Les autres aspects à prendre en considération pour élaborer un programme d'essais de performance, y compris des exercices, à l'appui de l'évaluation du SPP sont notamment les suivants :

a) élaborer un plan pour confirmer la conformité aux prescriptions et la performance du SPP. Ce plan devrait fournir une base pour la conception et

la fréquence des essais de performance et les critères d'évaluation. Il devrait s'assurer que l'évaluation établisse s'il est répondu aux critères de fiabilité, d'opérabilité, de fonctionnalité, de préparation et de performance ;

b) veiller à ce que les essais de performance, y compris les exercices, soient effectués périodiquement en coordination avec des organismes d'intervention extérieurs, à une fréquence déterminée par l'autorité compétente ;

c) associer d'autres éléments de l'organisme exploitant (p. ex. l'intervention d'urgence, le personnel de l'installation, le personnel de la salle de commande) aux exercices afin de les rendre réalistes et de tester les différentes disciplines qui collaborent pendant un événement de sécurité nucléaire ;

d) étayer les résultats des évaluations, y compris les mesures correctives et, le cas échéant, communiquer les résultats et les constatations à l'autorité compétente ;

e) coopérer avec les autres exploitants ou organismes pour partager les enseignements tirés et les meilleures pratiques, notamment sur le processus d'évaluation et les résultats.

9.15. Le programme d'essais de performance du SPP devrait utiliser les données d'autres essais existants effectués par le personnel de maintenance dans le cadre du programme d'assurance de la qualité. Il est souhaitable que le programme d'essais de performance dispose d'éléments pour coordonner la conception, la planification et la conduite des essais, ainsi que la gestion des données tirées des essais, à savoir notamment :

a) intégrer les données tirées d'autres essais dans la maintenance et la formation, par exemple, afin de définir des objectifs et des méthodes d'essai communs et d'utiliser au mieux les données d'essais ;

b) assurer l'intégration des ressources au calendrier d'opérations de l'installation afin de réduire au minimum les perturbations ;

c) élaborer des plans d'essais pour définir les objectifs, les méthodes, les procédures et les critères relatifs aux essais ;

d) concevoir des essais permettant d'obtenir suffisamment de données pour appuyer l'évaluation quantitative avec un degré de fiabilité statistique approprié ;

e) faire effectuer les essais par un personnel qualifié, rompu au fonctionnement de l'élément du SPP faisant l'objet d'un essai, et selon les procédures qui s'y rapportent ;

f) faire effectuer les essais par un personnel impartial afin de garantir l'intégrité des données ;

g) gérer les différents attributs des données d'essais afin de comprendre comment les interpréter et les appliquer ;
h) élaborer un plan de gestion des données pour orienter la collecte, l'analyse et la maintenance des données d'essais.

9.16. Les essais de performance devraient être reproductibles et objectifs : les essais effectués par des experts différents utilisant le même plan d'essais devraient aboutir à des résultats comparables. La méthodologie des essais devrait être structurée de manière à garantir l'utilisation la plus efficiente et précise des résultats et observations tirés de chaque essai. Les normes internationales[5] peuvent fournir de bonnes pratiques concernant l'utilisation de l'échantillonnage de données et la conception des essais.

Méthodes d'évaluation de la performance

9.17. Les essais de performance utilisés pour l'évaluation englobent les exercices partiels ou complets et les exercices d'attaque simulée des forces d'intervention, et visent à déterminer si le personnel, les procédures et les équipements assurent les niveaux de performance nécessaires. Ces essais peuvent être conçus de manière à tester la performance d'un seul composant du SPP ou d'un sous-système du SPP global. Par exemple, un essai de portée limitée pourrait consister à mesurer les temps de réponse et d'évaluation pour une cible donnée ou à déterminer si un opérateur du PCS peut coopérer avec le système de détection des intrusions pour identifier la source d'une alarme dans une zone d'entreposage dans un délai fixé.

9.18. Lorsque cela est matériellement possible, on peut effectuer plusieurs essais de performance pour chaque élément de protection physique pour recueillir un éventail représentatif de données d'essais. Par exemple, trois essais pourraient être effectués pour déterminer les temps de réponse, soit un essai pour chacune des trois équipes d'intervenants. On peut faire des enregistrements vidéo des données d'essais.

9.19. Les données d'essais de performance pourraient être conservées dans une bibliothèque de données qui pourrait être utilisée pour justifier les hypothèses concernant les probabilités de détection, l'évaluation et les durées de retardement et d'intervention utilisées dans les évaluations de la protection physique. La section 8 présente d'autres informations sur la collecte des données d'essais.

---

[5] Par exemple, celles élaborées par le Comité technique 69 sur les applications des méthodes statistiques de l'Organisation internationale de normalisation.

Essais de performance de portée limitée

9.20. Les essais de performance de portée limitée peuvent servir à tester toute opération ou procédure, à confirmer qu'une politique est appliquée ou à vérifier l'existence de connaissances ou d'une compétence requises. Les techniques d'évaluation telles que les observations et les entretiens n'exigent pas de plans d'essais, mais les essais de performance de portée limitée devraient être formellement consignés et approuvés à l'avance. Il conviendrait de définir les critères d'essais réussite/échec et les résultats escomptés de façon que les méthodes de collecte et d'analyse des données soient utiles et d'un bon rapport coût-efficacité pour l'évaluation du SPP global. Les essais de performance de portée limitée peuvent être planifiés ou inopinés. Pendant tout processus d'évaluation, les techniques d'essais multiples devraient en principe être mises en œuvre pour déterminer si le personnel affecté aux activités du SPP s'acquitte efficacement de ses fonctions.

9.21. Les essais de performance de portée limitée peuvent servir à évaluer nombre de mesures du SPP sans perturber les opérations de l'installation ni utiliser des ressources importantes ou un grand nombre de personnes. Ces essais peuvent consister à observer directement une activité ou un processus donné ou à évaluer des actions ou interventions se rapportant à une situation anormale. Ils peuvent indiquer des moyens de protection spécifiques, tandis que les essais multiples concernant une série d'actions peuvent fournir des assurances accrues d'une capacité globale.

9.22. Les essais de performance de portée limitée peuvent porter sur l'évaluation de mesures, plans ou procédures spécifiques du SPP ou sur la collecte de données aux fins de la formation et de la qualification du personnel d'exploitation, des spécialistes de la sécurité et des gardiens.

Essais de performance à grande échelle

9.23. Les essais de performance à grande échelle englobent les exercices complets des forces d'intervention et les exercices d'attaque simulée. Les deux types d'exercices sont des essais intégrés conçus pour évaluer toutes les mesures mises en œuvre pour répondre à une attaque d'une installation par un agresseur spécifique. Alors qu'un exercice complet des forces d'intervention vérifie le plan, le calendrier et les procédures d'intervention, l'exercice d'attaque simulée permet, dans des conditions réalistes, d'évaluer et de vérifier l'efficacité du SPP. On peut recueillir des données pour confirmer des hypothèses, évaluer l'efficacité du SPP face aux menaces définies et évaluer la capacité de mettre en œuvre des stratégies

de protection, d'évaluer la formation et de recenser les domaines dans lesquels des améliorations sont nécessaires.

9.24. Les exercices d'attaque simulée nécessitent une planification poussée et une coordination étroite avec tous les éléments de l'organisme exploitant, notamment les responsables et le personnel de l'installation, les agents chargés de la protection physique, les membres des équipes d'intervention et le personnel d'intervention hors site. Exigeants et coûteux, ces exercices requièrent une planification minutieuse et une coordination attentive si l'on veut en tirer le maximum d'avantages. On peut utiliser des armes simulées pour recueillir des données sur un agresseur et la participation active des membres des forces d'intervention pendant l'exercice. Il faudrait utiliser un plan global d'exercices pour planifier, coordonner et exécuter un exercice d'attaque simulée et enregistrer les données utiles qui en sont tirées. Un plan d'exercice d'attaque simulée peut comprendre beaucoup d'éléments, mais il englobe normalement au moins les suivants :

a) objectifs d'essai clairs ;
b) scénarios d'attaque généraux et spécifiques ;
c) agresseurs et capacités spécifiques (indiqués dans l'évaluation de la menace ou la menace de référence) ;
d) installation(s) concernée(s) et limites de l'exercice ;
e) mesures compensatoires destinées à protéger l'installation pendant l'essai, notamment une force parallèle (force d'intervention supplémentaire en réserve), si nécessaire ;
f) mesures visant à protéger les participants pendant l'exercice, notamment les actions que ces derniers doivent mettre en œuvre si une véritable intervention est déclenchée pendant l'exercice ;
g) communication entre les participants et les forces parallèles pour que la sûreté ou la sécurité ne soient pas compromises ;
h) méthodologie des essais ;
i) calendrier.

Élaboration de scénarios

9.25. Les exercices d'attaque simulée et les essais de portée limitée s'appuient sur des scénarios d'attaque spécifiques. Lorsqu'ils élaborent de tels scénarios, les experts cherchent à mettre au point une série de scénarios pour faire face à la menace définie par l'évaluation ou la menace de référence. Ces scénarios peuvent impliquer des agresseurs externes ou des menaces d'origine interne, ou encore

des attaques révélant une collusion entre les deux. Les informations utilisées pour élaborer les scénarios proviennent de nombreuses sources, à savoir notamment :

a) caractéristiques de l'installation nucléaire ;
b) caractéristiques des cibles d'un enlèvement non autorisé et d'un sabotage ;
c) caractéristiques et capacités des agresseurs telles qu'elles sont énoncées dans l'évaluation de la menace ou la menace de référence ;
d) résultats d'analyses antérieures, telles qu'une analyse des chemins.

9.26. Les aspects à prendre en considération dans l'élaboration des scénarios d'agression sont notamment les suivants :

a) les capacités des agresseurs (notamment la combinaison de leurs tactiques, p. ex., la force, la furtivité ou la ruse) ;
b) les différentes conditions de fonctionnement de l'installation au moment de l'attaque (p. ex. une casemate d'entreposage de matières nucléaires ouverte ou fermée) ;
c) les informations dont un agresseur pourrait disposer ;
d) toute action mise en œuvre par un agresseur d'origine interne dans un scénario de collusion.

9.27. Lorsqu'une série de scénarios ont été mis au point, il faudrait en choisir un ou plusieurs pour le(s) tester dans le cadre d'un exercice d'attaque simulée ou pendant l'évaluation du SPP. On peut par exemple dégager le scénario le plus pessimiste ou des scénarios limitatifs (scénarios qui prévoient des essais du SPP plus difficiles et, de ce fait, peuvent servir à tester des scénarios moins exigeants), choisir un scénario permettant de tester une caractéristique spécifique du SPP ou tester un éventail de scénarios au fil du temps. Le scénario retenu, quel qu'il soit, doit permettre d'atteindre les objectifs d'essai.

9.28. Le choix des scénarios à tester déterminera dans quelle mesure les résultats donnent des informations utiles quant à l'efficacité du SPP. Dans certains cas, un SPP pourrait fonctionner mieux dans des scénarios d'attaque qui, avant les essais, semblent plus exigeants et moins bien dans des scénarios qui semblent moins exigeants. On voit que l'évaluation d'un éventail de scénarios peut donner une meilleure idée de l'efficacité du système. D'autres méthodes sont disponibles à cette fin, comme par exemple les exercices sur table et les simulations informatiques.

10. ANALYSE DU SYSTÈME DE PROTECTION PHYSIQUE

10.1. La présente section décrit le processus et les méthodes d'analyse utilisés pour évaluer les résultats des essais de performance, des modélisations et des simulations afin de déterminer la mesure dans laquelle un SPP satisfait aux exigences fixées en matière de performance sur la base d'une évaluation de la menace ou de la menace de référence ; ces méthodes d'analyse sont les suivantes :

a) Analyse des chemins : Méthode consistant à évaluer les chemins qui pourraient être exploités par l'adversaire afin de déterminer la probabilité que l'intervention peut l'intercepter avant qu'il n'atteigne son objectif.
b) Analyse de neutralisation : Méthode consistant à déterminer la probabilité que l'intervention peut stopper un agresseur avant qu'il n'atteigne son objectif ou lui faire abandonner la partie.
c) Analyse de l'agresseur d'origine interne : Méthode consistant à déterminer l'efficacité du SPP face à un acte commis par une personne bénéficiant d'un accès autorisé à une installation nucléaire.
d) Analyse de scénario : Méthode consistant à élaborer un plan (scénario) d'attaque spécifique et à évaluer le SPP pour déterminer son efficacité face à une attaque de ce genre.

10.2. Une analyse de l'efficacité d'un SPP vise à déterminer la probabilité qu'il offrira une protection appropriée contre l'enlèvement non autorisé de matières nucléaires ou le sabotage de matières et d'installations nucléaires. Les essais de performance représentent la méthode la plus importante permettant d'acquérir des informations sur l'efficacité d'un SPP, et les résultats de ces essais peuvent appuyer les méthodes d'analyse décrites dans la présente section. Par exemple, les essais de performance peuvent servir à déterminer la probabilité de détection par un système de détection périmétrique des intrusions dans une installation nucléaire, sur laquelle on peut ensuite s'appuyer pour réaliser une analyse des chemins [2]. L'analyse des chemins est une analyse complète de tous les chemins qu'un agresseur venu de l'extérieur de l'installation pourrait emprunter pour atteindre la cible. D'autres méthodes, telles que les résultats d'essais de performance, peuvent également être utilisées pour déterminer l'efficacité avec laquelle un SPP fait face à des menaces définies.

10.3. Les fonctions de détection et de retardement du SPP sont destinées à faciliter une intervention rapide pour faire face à un événement de sécurité nucléaire. La fonction d'intervention vise ensuite à intercepter et neutraliser ou

stopper d'une autre manière un agresseur avant qu'il n'atteigne son objectif ou à lui faire abandonner la partie. L'efficacité d'un SPP peut être exprimée de manière quantitative en tant que probabilité d'efficacité du système (P_E), sous la forme :

$$P_E = P_I \times P_N \quad (1)$$

où

P_E est la probabilité que le SPP satisfait aux exigences de performance le concernant ;

P_I est la probabilité que l'intervention intercepte l'agresseur, autrement dit qu'un nombre suffisant de membres des forces d'intervention convenablement formés et équipés arrivent à l'endroit approprié à temps pour empêcher l'agresseur de mener à bien un acte d'enlèvement non autorisé ou de sabotage.

et P_N est la probabilité conditionnelle que le SPP (y compris l'intervention) neutralise l'agresseur, étant donné qu'il y a interception.

10.4. L'analyse des chemins cherche à évaluer P_I, qui dépend du lien entre les capacités de détection, les durées de retardement et le délai écoulé entre le premier décèlement de l'agresseur et une intervention rapide. L'analyse de neutralisation vise à évaluer P_N, qui dépend du nombre, des armes, de la formation et de l'équipement de la force d'intervention par rapport à ceux de l'agresseur. Les analyses de neutralisation doivent tenir compte des prescriptions juridiques et réglementaires ainsi que de la qualité des plans d'intervention. Les analyses des chemins et de neutralisation servent à identifier les faiblesses potentielles ou effectives en prenant en considération les facteurs pertinents, à déterminer s'il est satisfait aux exigences de performance concernant P_I et P_N et à établir si le SPP dans son ensemble fournit une défense en profondeur et une protection équilibrée suffisantes.

ANALYSE DES CHEMINS

10.5. L'analyse des chemins produit des estimations de P_I pour chaque chemin crédible qu'un agresseur pourrait emprunter pour atteindre la cible définie, en évaluant pour chacun la probabilité de repérer l'agresseur alors qu'il est encore temps pour les forces d'intervention de l'intercepter avant qu'il ne puisse mener à

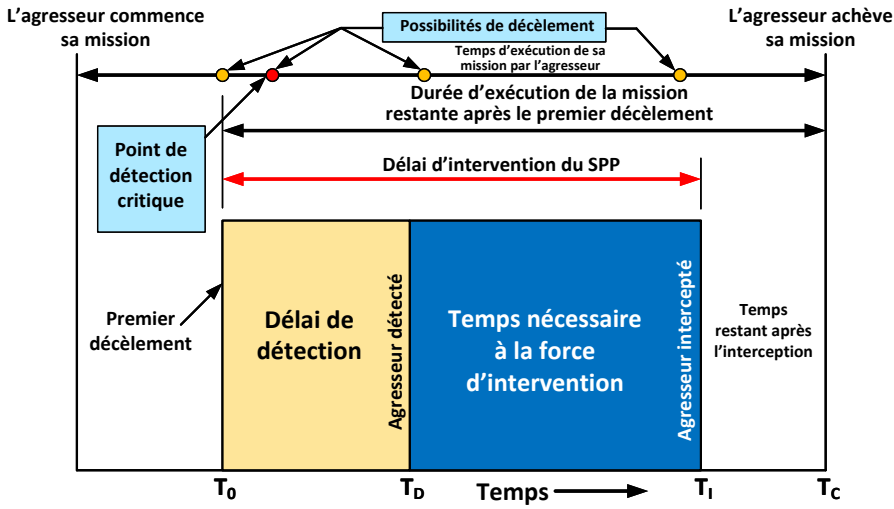


FIG. 42. Comparaison entre la chronologie de l'attaque et celle de l'intervention

bien un acte d'enlèvement non autorisé ou de sabotage. Elle peut servir à identifier les chemins où P_I est la plus faible, qui sont les chemins les plus vulnérables et sont parfois appelés chemins critiques. L'efficacité de la conception du SPP en matière d'interception est mesurée en tant que valeur de P_I pour un chemin particulièrement vulnérable : si P_I est trop faible pour le chemin le plus vulnérable, la conception du SPP est considérée comme inadéquate. P_I est déterminée pour un seul chemin en utilisant des chronologies comme celles indiquées dans la figure 42.

10.6. La figure 42 montre en haut la chronologie de l'attaque, en indiquant le temps qu'il reste à l'agresseur pour mener à bien toutes les tâches sur le chemin spécifié, ainsi que les possibilités de détection de l'agresseur par le SPP compte tenu de cette chronologie. À chacune de ces possibilités correspond une probabilité de détection, P_D, qui peut en principe être estimée sur la base des essais de performance. La dernière possibilité de détection qui permettrait de repérer l'agresseur à temps pour l'intercepter s'appelle le point de détection critique. Sous la chronologie de l'attaque, la figure montre le délai d'intervention du SPP et le temps d'exécution de sa tâche par l'agresseur restant sur le chemin après le premier décèlement, eu égard à chaque possibilité de détection. Le temps d'exécution de sa tâche par l'agresseur et le délai d'intervention du SPP sont généralement mesurés ou estimés quantitativement sur la base des essais de performance.

10.7. Une possibilité de détection associée au chemin est considérée comme se présentant en temps utile si le délai utilisé par le SPP pour l'intervention d'interception d'un agresseur après son premier décèlement est inférieur au temps dont ce dernier aurait besoin pour mener à bien l'acte projeté ; dans le cas contraire, la possibilité de détection n'est pas considérée comme se présentant en temps utile. Dans la figure 42, les deux premières possibilités de détection se présentent en temps utile et, dans ce cas, P_I est la probabilité que l'agresseur soit détecté au niveau d'une ou de ces deux possibilités sur le chemin spécifié. S'il existe K possibilités de détection en temps utile, P_I correspond à :

$$P_I = 1 - \left\{ \prod_{i=1}^{K} \left(1 - P_{Di}\right) \right\} \tag{2}$$

où

P_{Di} est la probabilité de détection associée à la possibilité de détection ;

K est le nombre de possibilités de détection en temps utile ;

et i est une seule possibilité de détection en temps utile.

10.8. L'analyse des chemins applique conceptuellement ce calcul de P_I à chaque chemin menant à la cible. Les chemins à évaluer sont définis en termes de niveaux concentriques de protection mis en place autour d'une cible donnée (voir la figure 43).

10.9. Le niveau correspondant à la zone protégée comprend deux barrières (portail, clôture), tandis que le deuxième niveau de protection en comporte quatre (porte 1, porte 2, mur 1, mur 2). Il existe donc huit chemins menant à la cible : {clôture, mur 1}, {clôture, mur 2}, {clôture, porte 1}, {clôture, porte 2}, {portail, mur 1}, {portail, mur 2}, {portail, porte 1}, {portail, porte 2}. Pendant l'analyse des chemins de cette installation fictive, P_I serait calculée pour chacun de ces huit chemins et celui pour lequel elle serait la plus faible serait identifié comme étant le plus vulnérable. Si cette valeur est suffisamment élevée, ce SPP pourrait être considéré comme fournissant une bonne capacité d'interception au niveau de cette cible.

10.10. En plus de calculer P_I pour le chemin le plus vulnérable, l'analyse des chemins peut établir si la défense en profondeur est adéquate en prenant en compte les mesures de protection qui seraient mises en place avant le point de détection critique de chaque chemin ou à ce niveau. Par exemple, l'installation fictive de la

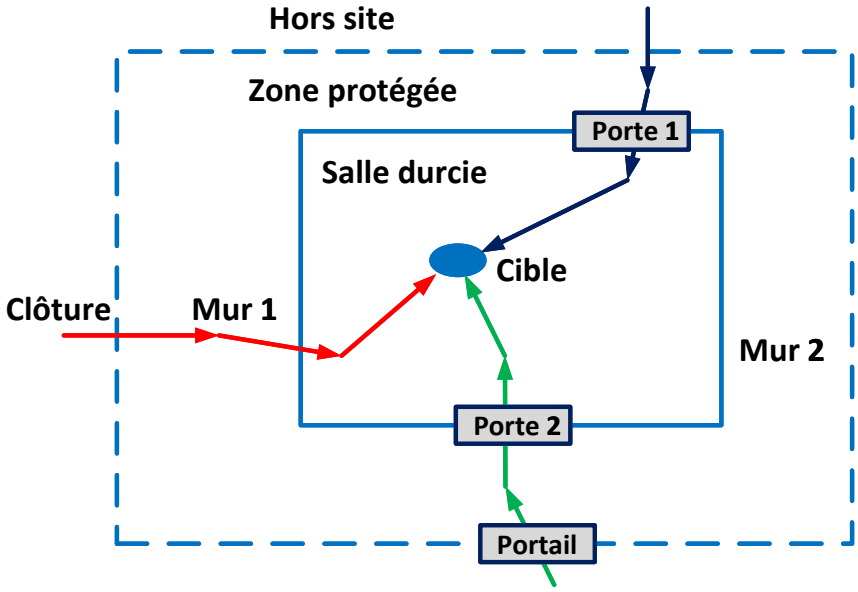


FIG. 43. Trois chemins pouvant être exploités par un agresseur indiqués pour une installation fictive comportant deux niveaux de protection

figure 43 n'aurait pas de défense en profondeur si un seul niveau était assuré en temps utile, par exemple si la clôture et le portail situés à la limite du périmètre fournissaient des possibilités de détection en temps utile, mais que ce ne soit pas le cas des quatre barrières de la zone intérieure. Si, en revanche, dans l'installation fictive de la figure 43, le point de détection critique se situe à la limite de la salle durcie, la clôture et le portail fournissent une défense en profondeur à la limite du périmètre, offrant ainsi deux possibilités de détection en temps utile.

ANALYSE DE NEUTRALISATION

10.11. Les analyses de neutralisation visent à évaluer P_N en tant que mesure de l'efficacité de l'intervention. Cette probabilité est établie à partir d'informations concernant l'intervention, la menace, le SPP et la méthodologie retenue pour déterminer la neutralisation. P_N est évaluée en examinant une série d'engagements au cours desquels deux forces en présence (la force d'intervention et la force adverse) utilisent des armes et des tactiques en tentant d'atteindre leurs objectifs respectifs. Le grand nombre de facteurs aléatoires pouvant influer sur l'issue d'un engagement multiplie les résultats possibles. Le résultat est défini comme une

« victoire du SPP » si la force adverse est tuée ou capturée ou abandonne. La probabilité de neutralisation, P_N, peut être définie par l'équation suivante :

$$P_N = \frac{\text{Nombre de victoires}}{\text{Nombre d'engagements}} \quad (3)$$

10.12. Pour que cette expression se vérifie, le nombre d'engagements du dénominateur devrait être considéré comme arbitrairement important. À mesure que ce nombre augmente, la proportion de victoires se rapprochera de la probabilité réelle de cet événement. En utilisant l'équation (3), tous les engagements devraient être modélisés à l'aide d'hypothèses identiques, telles que les mêmes conditions initiales, et il ne devrait y avoir que deux résultats possibles pour un engagement, une victoire ou une défaite des forces d'intervention.

10.13. Les méthodes de détermination de P_N sont notamment les suivantes :

a) avis d'expert ;
b) modèles mathématiques ;
c) simulations ;
d) analyse des résultats d'événements réels.

10.14. Chaque méthode a ses avantages et ses inconvénients en termes de temps nécessaire à sa mise en œuvre et de précision. Certaines méthodes ne tiennent compte que d'un petit nombre de facteurs, tandis que d'autres en prennent beaucoup plus en considération, mais aucune méthode ne peut prendre en compte l'ensemble des facteurs qui influent sur l'issue d'un seul engagement. Néanmoins, ces méthodes peuvent donner un aperçu de la solidité d'une intervention.

10.15. Les méthodes simples, telles que l'avis d'expert, pourraient nécessiter seulement des données sur le personnel et les armes (nombre et types) de part et d'autre, et le moment de leur engagement. Plus complexes, les simulations pourraient nécessiter une grande quantité de données, à savoir, notamment, les suivantes :

a) emplacements initiaux des forces d'intervention et des forces adverses ;
b) itinéraires de déploiement des forces d'intervention et emplacements finals ;
c) chemin emprunté par l'agresseur ;
d) plan d'attaque de l'agresseur ;
e) terrain ;
f) caractéristiques de construction ;

g) caractéristiques du SPP (p. ex. durées de retardement offertes par les barrières).

10.16. Lorsqu'elle est utilisée dans le cadre du processus de conception, l'analyse de neutralisation s'appuie sur une combinaison d'avis d'expert, de modèles mathématiques et de simulations. Elle pourrait notamment consister à examiner les questions générales liées à la planification de l'intervention, telles que les options en matière de plan d'intervention spécialisé, l'effectif et les armes des forces d'intervention, et la formation de ces forces (compte tenu des prescriptions réglementaires).

10.17. Cette analyse pourrait également comprendre un volet basé sur la performance qui pourrait examiner en détail la performance des forces d'intervention contre les forces adverses dans différents scénarios et différentes conditions. Selon cette approche, on crée un certain nombre de scénarios, dont chacun est défini par des informations et hypothèses relatives à l'agresseur et à la cible ou aux cibles à attaquer. Ces hypothèses sont notamment les mesures fournies par le SPP (notamment l'intervention), les capacités de l'agresseur et ses intentions et son plan d'attaque, notamment une série d'actions hypothétiques de l'agresseur et un ou plusieurs chemins susceptibles d'être empruntés par lui. Les scénarios à évaluer pourraient être connus au début de l'analyse de neutralisation ou être mis au point à mesure de la progression de cette analyse.

10.18. L'analyse de neutralisation portant sur les aspects du SPP liés à l'intervention, des hypothèses sont généralement formulées sur l'élément ou le niveau de protection du système sur le chemin emprunté par l'agresseur qui a abouti à la première détection de ce dernier. C'est cet élément ou ce niveau qui pourrait être choisi car le point de détection critique ou le premier élément ou niveau pris en compte fournit une forte probabilité de détection. On conduit ensuite des exercices d'efficacité, à savoir des exercices de portée limitée ou d'attaque simulée, ou des simulations à partir de cet élément ou niveau.

10.19. Comme il est souvent difficile de conduire un grand nombre d'essais, en particulier des exercices d'attaque simulée, on peut utiliser et formaliser des méthodes d'estimation de P_N à partir de l'ensemble d'échantillons disponible. L'une de ces méthodes est exprimée dans l'équation (4), qui est une approximation moins fiable lorsque la taille de l'échantillon est réduite. Il existe d'autres méthodes permettant d'estimer les probabilités à partir d'un échantillon de petite taille.

$$P_N = \frac{\text{Nombres de victoires simulées des forces d'intervention}}{\text{Nombre de simulations réalisées}} \quad (4)$$

PROBABILITÉ D'EFFICACITÉ D'UN SYSTÈME DE PROTECTION PHYSIQUE

10.20. Pour déterminer la probabilité de l'efficacité d'un SPP, une méthode consiste à évaluer P_E en tant que produit de P_I et de P_N pour un chemin donné, en déterminant l'emplacement du point de détection critique du chemin le plus vulnérable, avant de conduire des exercices ou de modéliser des scénarios permettant d'estimer P_N en commençant par les agresseurs au point de détection critique. Cette approche a un inconvénient : le point de détection critique se trouve habituellement à l'emplacement cible ou à proximité, et il n'est souvent guère pensable que la détection ne se ferait pas avant ce point.

10.21. Une autre méthode d'évaluation de P_E à partir de P_I et P_N consiste à choisir un emplacement sur le chemin d'un agresseur au point de détection critique ou encore avant ou après, puis à conduire des exercices ou simuler des scénarios pour estimer P_N alors que l'agression commence à cet emplacement. Dans ce cas, P_I est la probabilité cumulative de détection pour toutes les possibilités de décèlement sur ce chemin jusqu'à l'emplacement choisi. Selon cette approche, on peut analyser le scénario en utilisant le point de détection le plus probable. Dans ce cas, la valeur calculée de P_E n'égalera pas la valeur tirée de la méthode précédente si l'élément ou niveau choisi n'est pas le point de détection critique, puisque, dans cette situation, P_I ne serait pas égale à la valeur cumulative P_D correspondant à l'élément ou au niveau choisi.

ANALYSE DES MENACES D'ORIGINE INTERNE

10.22. On trouvera des orientations sur les mesures contre les menaces d'origine interne dans les références [8, 9]. Les paragraphes 10.22 à 10.26 décrivent une méthode d'analyse de la manière dont un SPP fait face aux menaces d'origine interne que représentent des personnes qui agissent seules ou en collusion avec des agresseurs externes. Les méthodes communément utilisées pour analyser les menaces d'origine interne sont notamment les avis d'expert, les analyses des chemins et les analyses de documents. Les agresseurs d'origine interne créent des difficultés particulières à un SPP car ils ont accès à des informations détaillées et sont à même d'utiliser des méthodes de neutralisation dont ne disposent pas

les agresseurs externes. Les agresseurs d'origine interne sont avantagés sur les plans suivants :

a) Accès : Accès autorisé aux installations nucléaires, notamment à une zone intérieure ou une zone d'accès limité.
b) Autorité : Pouvoir défini d'influencer ou de contrôler autrui. Par exemple, le supérieur d'un gardien pourrait avoir le pouvoir de lui ordonner de ne pas tenir compte de l'obligation de fouiller un véhicule pénétrant dans une zone protégée.
c) Connaissances : Les connaissances spécifiques qu'une personne pourrait avoir tirées de l'exercice de ses fonctions ou de son expérience. Il pourrait s'agir d'informations concernant, par exemple, la caractérisation et les opérations de l'installation, les mesures, capacités et fonctionnement du SPP, et les cibles.

10.23. Pour analyser les menaces d'origine interne, il convient de mettre au point des scénarios crédibles s'appuyant sur les cibles identifiées et les groupes d'agresseurs internes. Les scénarios devraient prendre en compte les menaces définies dans l'évaluation de la menace ou la menace de référence et décrire les tâches spécifiques qu'un agresseur interne devrait exécuter. Les menaces d'origine interne pourraient être :

a) passives : les personnes concernées sont disposées à renseigner des agresseurs externes, non à participer à une attaque ;
b) actives : les personnes concernées sont disposées à agir seules ou en collusion avec d'autres menaces internes ou avec des agresseurs externes pour commettre un acte d'enlèvement non autorisé et de sabotage. Une menace interne active pourrait ou non être disposée à recourir à la violence.

10.24. Pour analyser les menaces internes passives, il importe de déterminer les informations qu'un agresseur interne pourrait fournir et d'élaborer des scénarios impliquant des agresseurs qui disposent de ces informations. L'efficacité du SPP est établie en testant sa performance dans le cadre de ces scénarios.

10.25. Pour analyser la menace d'un agresseur interne agissant seul, des experts mettent au point des scénarios dans lesquels cet agresseur exploite les avantages que lui procurent l'accès, l'autorité et les connaissances dont il dispose. Si l'évaluation de la menace ou la menace de référence l'exige, il faudrait également mettre au point des scénarios faisant intervenir plusieurs agresseurs internes. La mise au point de scénarios impliquant un agresseur interne devrait tenir compte de la possibilité de le voir exploiter les faiblesses des mesures administratives ou

techniques de surveillance, de confinement et de contrôle. On pourrait estimer l'efficacité du SPP face à ces menaces en ayant recours à des experts, en procédant à des analyses des chemins empruntés par des agresseurs internes (incorporant les données tirées des essais de performance des systèmes de contrôle d'accès, de confinement et de surveillance) ou en effectuant des exercices sur table.

10.26. La collusion d'agresseurs internes avec des agresseurs externes peut amener les premiers à appuyer directement ou indirectement la réussite d'un enlèvement non autorisé ou d'un acte de sabotage. Pour analyser ces éventualités, on met au point des scénarios représentant l'agresseur externe et impliquant l'utilisation de l'accès, de l'autorité et des connaissances d'un agresseur interne appuyant activement l'attaque. Ces scénarios d'attaque sont ensuite évalués comme indiqué précédemment à l'aide d'essais de performance, d'analyses des chemins et d'analyses de neutralisation.

ANALYSE DE SCÉNARIOS

10.27. L'analyse de scénarios consiste à créer un ensemble représentatif de scénarios d'agression détaillés, en déterminant la réponse qui serait apportée à chacun d'entre eux sur la base des plans de sécurité de l'installation, de ses procédures et du déploiement tactique des forces d'intervention, et à réaliser une simulation aussi réaliste que possible des interactions entre les agresseurs et le SPP.

10.28. Cette analyse est une technique d'évaluation de l'efficacité d'un SPP qui consiste à postuler des scénarios d'attaque et à déterminer P_E directement sans calculer P_I dans une analyse et P_N dans une autre. Les chemins pouvant être empruntés par un agresseur devraient être choisis de manière à tirer profit d'éventuelles vulnérabilités du SPP, ce qu'un agresseur réel serait censé faire. Il s'agit donc de recenser les mesures du SPP qui pourraient être neutralisées du fait des caractéristiques de leur mise en place ou de leurs procédures opérationnelles. Il faudrait prendre en considération d'éventuelles méthodes de neutralisation des capteurs, barrières et systèmes de communication, ainsi que des possibilités de détournement ou d'élimination d'une partie de la force d'intervention. Les outils pouvant être utilisés dans une analyse de scénarios sont notamment les exercices sur table, les simulations de combats sur ordinateur et les exercices d'attaque simulée.

10.29. Les résultats de l'analyse de scénario peuvent servir à calculer une valeur de P_N dans l'équation (1) ou à estimer directement P_E si l'attaque est détectée à un emplacement où la probabilité de détection est raisonnablement élevée.

11. SYSTÈMES DE GESTION POUR LA SÉCURITÉ NUCLÉAIRE

11.1. Dans une installation nucléaire, la gestion consiste à exercer des fonctions telles que la planification, l'organisation, la constitution des effectifs, la direction des opérations, ainsi que le contrôle, la surveillance et l'évaluation du travail et l'évaluation des résultats. Les systèmes de gestion sont les méthodes, processus et outils que les responsables d'une installation nucléaire utilisent pour créer un cadre permettant de mener les activités de manière sûre et sécurisée tout en veillant à ce que les objectifs de l'exploitant soient atteints dans le respect du cadre juridique et réglementaire national.

11.2. Étant donné que les systèmes de gestion utilisés dans toutes les activités d'une installation nucléaire sont basés sur des concepts et principes communs, leur intégration dans un cadre général améliore l'efficience et l'efficacité et permet à l'exploitant :

a) d'établir et d'appliquer des politiques, processus et procédures cohérents pour satisfaire aux prescriptions de l'autorité compétente et de l'exploitant ;
b) d'améliorer l'efficience globale en éliminant les doubles emplois ;
c) de faciliter l'amélioration continue des systèmes de gestion ;
d) de favoriser le changement et d'encourager l'innovation en créant un cadre pour l'amélioration continue et les gains de performance sur la base de l'expérience acquise dans chaque discipline ;
e) de gérer efficacement le changement, de façon à maintenir ou améliorer la sécurité ;
f) de prendre des décisions qui répondent le mieux aux besoins généraux de l'installation d'une manière cohérente et disciplinée ;
g) de rassembler les compétences des différentes disciplines pour analyser les prescriptions divergentes et trouver les solutions permettant de tenir compte de toutes les prescriptions ;
h) d'empêcher la réduction des risques dans une discipline, telle que la sûreté, d'augmenter les risques ou d'en créer de nouveaux dans une autre, telle que la protection physique ;
i) de veiller à ce que la protection physique n'affecte pas indûment les opérations de l'installation.

11.3. Un système de gestion intégré incorpore la gestion de tous les aspects d'une installation nucléaire dans un système cohérent, en appliquant les principes et processus essentiels de gestion à chaque discipline (p. ex. la protection physique,

la comptabilité et le contrôle des matières nucléaires, la sûreté et les opérations). Le système de gestion devrait englober les activités qui ont une incidence sur la performance d'exploitation ou la conformité en matière de réglementation. Un système de gestion intégré fournit un cadre unique aux arrangements et processus qui permettent de prendre en compte tous les objectifs de l'exploitant de l'installation, notamment la sûreté, la santé, l'impact environnemental, la sécurité nucléaire, la qualité et la gestion de l'économie et de l'information. Le système de gestion intégré fait également une place à la coordination des éléments tels que la structure organisationnelle, la prise de décisions stratégiques, l'allocation des ressources et les processus de contrôle et d'examen de la performance. L'ensemble des processus et des documents qui les décrivent devraient être intégrés dans un cadre unique. Il faudrait veiller à ce que les informations sensibles en rapport avec le SPP et toutes les autres informations sensibles soient protégées comme il convient et ne soient partagées que sur la base du principe du besoin de savoir.

11.4. Les exploitants d'installations nucléaires devraient utiliser un système de gestion intégré pour toutes les phases de la durée de vie de l'installation et, en ce qui concerne une installation nouvelle, le système de gestion devrait être intégré à un stade précoce à toutes les activités [17]. Si un système de gestion intégré n'existe pas encore dans une installation nucléaire, il peut être mis en place en intégrant les systèmes de gestion existants, notamment la gestion de la qualité, dans un système unique. Les orientations données dans la présente section supposent qu'un système de gestion intégré existe dans une installation nucléaire.

11.5. Les fonctions et responsabilités relatives à la protection physique, et à l'assurance de la qualité de cette protection, devraient être définies dans le cadre du système de gestion [2]. Les exploitants devraient, dans le cadre de leur système de gestion, adopter une approche intégrée et coordonnée de l'examen de tous les changements qu'il est proposé d'apporter aux dispositions relatives à la protection physique, ce avant la mise en œuvre de ces changements, de façon qu'ils n'aient pas d'incidences imprévues sur la sûreté. On trouvera d'autres informations sur l'application d'un système de gestion intégré aux installations nucléaires dans les références [25 à 27]. La référence [2] énonce que les exploitants devraient respecter le cadre juridique et réglementaire national, être responsables au premier chef de la mise en œuvre du SPP, encourager l'adoption d'une solide culture de sécurité nucléaire et coopérer avec les autres entités publiques ayant des responsabilités dans le domaine de la protection physique, comme les forces d'intervention

hors site. Dans la publication nº 7 de la collection Sécurité nucléaire de l'AIEA, *Culture de sécurité nucléaire* [28], il est indiqué ce qui suit :

> « La qualité de la direction, les attentes, la communication des exigences et des critères fixés pour l'exécution des tâches, la formation, l'existence de procédures écrites et les systèmes d'information sont au nombre des facteurs qui influent sur la performance du personnel. »

APPLICATION DES SYSTÈMES DE GESTION AU SYSTÈME DE PROTECTION PHYSIQUE

11.6. Les responsables d'une installation nucléaire utilisent un système de gestion intégré pour suivre et contrôler toutes les activités qui y sont menées, notamment le SPP. Aux fins de la présente publication, l'expression « fonctionnement d'un SPP » s'entend de toutes les activités associées au SPP, y compris la maintenance et les essais. L'application du système de gestion contribue à faire en sorte que le SPP reste conforme à ses spécifications de conception d'origine et évolue selon que de besoin en fonction des modifications apportées aux prescriptions.

11.7. Dans une installation nucléaire, un système de gestion intégré peut être appliqué au SPP au moyen d'une série d'éléments : la gestion des prescriptions ; la direction et le contrôle des activités ; la gestion des ressources, et les activités d'assurance (voir la figure 44).

11.8. Certaines des fonctions exercées dans une installation nucléaire peuvent l'être par d'autres organismes, auquel cas le système de gestion de l'installation pourrait ne pas s'appliquer à toutes les fonctions du SPP. Par exemple, l'intervention à mener dans une installation nucléaire peut être assurée par la police ou les forces armées nationales, auquel cas l'exploitant a la responsabilité du fonctionnement des composants du SPP relatifs à la détection et au retardement et pourrait mettre en œuvre les processus généraux d'assurance de la qualité qui font partie du système de gestion de l'installation. La police ou les forces armées nationales mettront en œuvre leurs propres procédures d'assurance de la qualité pour leurs activités. Si une installation ne dispose pas d'un système de gestion intégré, l'exploitant devrait s'efforcer d'intégrer la protection physique aux autres disciplines, telles que les opérations de l'installation, la comptabilité et le contrôle des matières nucléaires et la sûreté, s'agissant en particulier des activités communes, telles que l'assurance de la qualité. L'exploitant devrait entretenir des rapports étroits avec toutes les entités nationales et autres associées à toutes les

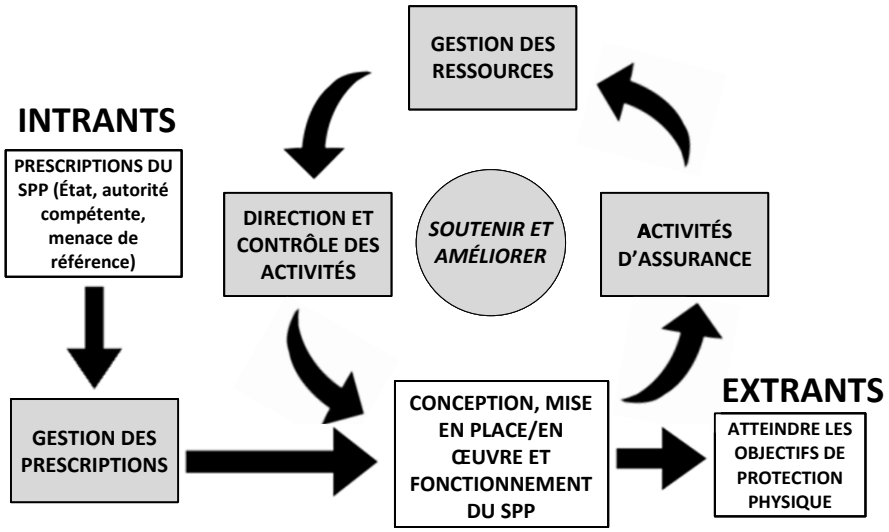


FIG. 44. Le système de gestion appliqué au système de protection physique

phases de conception, d'élaboration et de mise en place des mesures de protection physique et au fonctionnement du SPP.

GESTION DES PRESCRIPTIONS

11.9. La conception d'un SPP devrait répondre à un ensemble d'objectifs fixés par l'État et par son autorité compétente. Ces objectifs pourraient être exprimés sous la forme de prescriptions normatives, de prescriptions de performance ou d'une combinaison des deux, utilisées dans la conception du SPP pour élaborer des spécifications. Une fois que la conception du SPP est achevée, approuvée et installée, les spécifications de conception forment la base des activités de vérification destinées à s'assurer que le SPP continue de satisfaire aux prescriptions de fonctionnement le concernant. Les méthodes et outils de gestion des prescriptions se déclinent habituellement en quatre phases :

1) recueillir les prescriptions des parties prenantes ;
2) analyser les prescriptions ;
3) vérifier les prescriptions ;
4) étayer par des documents la traçabilité des prescriptions.

11.10. Ces phases peuvent être menées successivement au fur et à mesure du déroulement du processus ou, dans certains cas, en parallèle. Les normes industrielles fournissent d'autres informations sur la manière de rassembler les exigences des parties prenantes et d'analyser les prescriptions (voir la référence [29]).

Recueillir les prescriptions des parties prenantes

11.11. La première phase du processus consiste à recenser les prescriptions applicables de toutes les parties prenantes. Elles pourraient comprendre les prescriptions de l'État et de l'autorité compétente, ainsi que les prescriptions opérationnelles ou de sûreté. Pendant la conception, ces prescriptions des parties prenantes serviront à élaborer des prescriptions supplémentaires dérivées qui seront utilisées pour définir les spécifications de conception.

Analyser les prescriptions

11.12. Une fois que toutes les prescriptions des parties prenantes ont été recueillies, il s'agit de les analyser pour s'assurer de leur clarté, recenser les prescriptions divergentes et transformer les prescriptions en prescriptions dérivées pour le SPP et en spécifications de conception pour le fonctionnement et la maintenance du système, à l'aide d'une approche de gestion du risque. Les parties prenantes applicables devraient être en mesure de comprendre comment les prescriptions dérivées reflètent leurs prescriptions.

11.13. Les exemples ci-après montrent comment les prescriptions dérivées peuvent être élaborées (*souligné dans l'original*) :

a) Recommandation (par. 4.39 de la référence [1]) : « Les *zones intérieures* devraient retarder l'accès non autorisé afin de permettre une intervention rapide et adaptée face à un *enlèvement non autorisé*. » Il faudrait obtenir de la partie prenante concernée (p. ex. l'autorité compétente) ou retenir comme hypothèses des informations supplémentaires afin d'élaborer des spécifications de conception : par exemple, la recommandation ne précise pas la durée de retardement pour la barrière des zones intérieures, le temps d'intervention pour les forces d'intervention ou les capacités qu'un agresseur pourrait utiliser pour neutraliser la barrière. Si les capacités de celui-ci telles qu'elles sont définies dans l'évaluation de la menace ou la menace de référence autorisent l'utilisation d'explosifs pour neutraliser une barrière, par exemple, celle-ci devrait être plus solide que si les capacités en question sont présumées limitées à l'utilisation d'outils manuels. L'analyse

pourrait déboucher sur des critères de conception dérivés selon lesquels le mur de la zone intérieure retardera d'au moins 30 minutes l'entrée forcée.

b) Recommandation (par. 4.42 de la référence [1]) : « Seules les personnes autorisées devraient avoir accès à la *zone intérieure*. » Il est ainsi recommandé à l'exploitant d'élaborer, avant que le SPP ne devienne opérationnel, des plans, processus et procédures qui définissent :
   i) les titulaires de postes ou catégories de personnel devant avoir accès à la zone intérieure pour s'acquitter des fonctions qui leur sont attribuées ;
   ii) les modalités de contrôle du processus d'approbation de l'accès à la zone intérieure pour les personnes autorisées ;
   iii) le processus permettant à une personne autorisée d'accéder à la zone intérieure ;
   iv) la formation à la sécurité requise avant que le personnel puisse avoir accès à la zone intérieure.

11.14. L'analyse de gestion des prescriptions devrait repérer les éventuelles incompatibilités entre les recommandations relatives à la protection physique et les prescriptions de sûreté. Par exemple, le paragraphe 4.40 de la référence [1] énonce que « le nombre de points d'accès aux *zones intérieures* devrait être limité au strict minimum (un seul point d'accès serait l'idéal) ». Toutefois, une prescription de sûreté pourrait imposer de prévoir une issue de secours à 25 mètres au plus de tout endroit d'une zone dangereuse. Par ailleurs, des prescriptions opérationnelles pourraient amener à créer des points d'accès à certains endroits de la zone intérieure afin de rationaliser les mouvements de matières nucléaires entre d'autres zones intérieures et de réduire le temps de traitement. Le fait de n'avoir qu'un seul point d'accès serait, dans certains cas, incompatible avec les prescriptions opérationnelles et les prescriptions de sûreté. Il conviendrait de lever ces incompatibilités pendant la phase d'analyse de manière à trouver un juste équilibre entre les différents critères possibles.

11.15. Le processus d'analyse des prescriptions est mené parallèlement au processus de conception du SPP, afin que les prescriptions deviennent des prescriptions dérivées officielles et des spécifications de conception pour le fonctionnement et la maintenance du système.

Vérifier les prescriptions

11.16. Durant la mise en place et l'application des mesures de protection physique, les prescriptions des parties prenantes et les prescriptions dérivées serviront de base aux activités de vérification. La vérification des prescriptions

vise à faire en sorte qu'il soit satisfait aux spécifications de conception et à toutes les prescriptions de fonctionnement et de maintenance du SPP (et, de ce fait, aux prescriptions des parties prenantes).

11.17. La vérification pourrait comprendre des essais de performance, des évaluations, des inspections, des audits ou autres moyens de donner l'assurance que les prescriptions officiellement établies sont respectées. De plus, les activités de vérification peuvent être menées aux niveaux des composants, des sous-systèmes ou du SPP.

Étayer par des documents la traçabilité des prescriptions

11.18. La gestion des prescriptions consiste notamment à attester la manière dont chaque prescription d'une partie prenante trouve son origine dans les prescriptions concernant le SPP et, au-delà, dans les spécifications de conception, de mise en place et d'application des mesures de protection physique et de leur utilisation.

11.19. Le fait d'étayer cette traçabilité par des documents apporte la preuve qu'il a été satisfait à la prescription et permet de déterminer les plans, processus et procédures et la formation à modifier en cas de modification de cette prescription. Il est courant, pour les systèmes simples, de créer une matrice de traçabilité où sont énumérés chaque prescription et tous les plans, processus et procédures associés, et où sont consignées les mesures utilisées pour satisfaire à une prescription donnée. Pour les systèmes plus complexes, il devient impossible de réaliser des matrices de traçabilité et des outils plus formels sont utilisés.

11.20. Par exemple, il pourrait exister une prescription réglementaire selon laquelle le personnel devrait suivre tous les six mois un certain type de formation à la sécurité pour être autorisé à accéder à une zone intérieure. Cette prescription figure dans le plan de sécurité de l'installation. Une matrice de traçabilité concernant cette prescription pourrait être utilisée comme suit :

a) Un plan de formation, accompagné de plans de séance de formation, est élaboré à l'intention du personnel de sécurité auquel est dispensée une formation à la fréquence spécifiée.
b) On établit un processus selon lequel les responsables doivent veiller à ce que la formation du personnel devant avoir accès à la zone intérieure soit planifiée et à ce qu'il suive cette formation avant de pouvoir y accéder et à la fréquence requise par la suite, et doivent enregistrer le fait que la formation de chaque membre du personnel concerné a été menée à bonne

fin et adresser une copie du registre au personnel de sécurité désigné chaque fois qu'une formation est achevée.

c) Le personnel de sécurité établit et gère une liste du personnel autorisé à accéder à la zone intérieure, où figurent le nom de chaque membre du personnel, le service où il travaille, la ou les dates de la formation suivie et la date de la prochaine remise à niveau obligatoire. La liste est mise à jour une fois par mois : le personnel de sécurité recense tous les membres du personnel figurant sur la liste qui devront suivre une formation de remise à niveau au cours du mois suivant et en informe les services concernés. Il fournit au point de contrôle de l'accès une liste des membres du personnel qui ont suivi la formation entre deux mises à jour mensuelles.

d) Des procédures sont définies pour permettre aux gardiens en poste aux points de contrôle de l'accès à la zone intérieure de vérifier que les personnes concernées figurent bien sur la liste à jour et que leur formation est à jour avant de les laisser accéder à cette zone.

11.21. Dans cet exemple, la prescription d'une partie prenante unique est prise en compte dans le plan de sécurité, un plan de formation, des plans de séances de formation, des registres et des procédures. Une matrice de traçabilité énumérerait tous ces éléments, de sorte que lorsqu'un changement intervient, tel que celui de la fréquence de la formation requise, tous les plans, processus, procédures et registres peuvent être mis à jour compte tenu de la nouvelle prescription.

DIRECTION ET CONTRÔLE DES ACTIVITÉS

11.22. La direction des activités de gestion du SPP comprend notamment la détermination des fonctions à exercer, l'élaboration des politiques de sécurité, la mise en place d'une structure organisationnelle permettant d'exercer ces fonctions, la définition des rôles, des responsabilités et des aspects liés à l'obligation de rendre des comptes, la fixation d'objectifs stratégiques et tactiques et l'établissement de critères de performance pour le SPP.

11.23. La détermination des fonctions à remplir pour concevoir, mettre en place et maintenir un SPP suppose une bonne compréhension des fonctions techniques, administratives et d'appui permettant d'effectuer les tâches nécessaires. Certaines de ces fonctions peuvent être remplies par le personnel de sécurité de l'installation et d'autres pourraient l'être par d'autres services. Ainsi :

a) La phase de conception d'un SPP pourrait faire intervenir les spécialistes de la sécurité, un concepteur, le personnel responsable de l'infrastructure

de l'installation, le personnel d'exploitation, les gardiens et les forces d'intervention, les spécialistes de la sûreté, le personnel d'appui informatique et les spécialistes du budget.

b) La mise en place des installations, barrières et autres systèmes du SPP fait intervenir le personnel chargé de la construction et de l'infrastructure.

c) Le fonctionnement d'un SPP est assuré par le personnel chargé de faire fonctionner les mesures du SPP et d'en assurer la maintenance, le personnel d'encadrement et les autres membres du personnel de sécurité qui exercent des fonctions telles que la formation, l'évaluation, les essais de performance, l'assurance de la qualité, les habilitations de sécurité, la gestion des dossiers, la sécurité de l'information, la sécurité informatique, l'administration, la budgétisation, les achats et la gestion des contrats.

11.24. Une politique selon laquelle les hauts responsables de l'installation expriment leur volonté d'en garantir la protection physique est nécessaire. Cette politique de sécurité devrait de préférence être publiée directement par les hauts responsables afin de faire apparaître clairement son importance et de démontrer leur engagement en faveur de la protection physique. Les membres du personnel de l'installation doivent comprendre que le respect de cette politique est attendu de la part de chacun d'entre eux. Cette politique souligne que la direction de l'installation a la haute main sur les questions de protection physique dans tous les domaines, notamment le SPP.

11.25. Pour établir une structure organisationnelle permettant de gérer efficacement un SPP, il importe de définir le cadre de fonctionnement du service de protection physique. La structure organisationnelle la mieux adaptée à la protection physique d'une installation donnée dépend de nombreux facteurs, comme la structure organisationnelle générale, le type d'installation nucléaire, les lois et prescriptions nationales et les normes culturelles. Toutefois, il s'agit de mettre en place une structure organisationnelle qui prévoie une gestion efficace des activités de conception, d'installation et d'exploitation d'un SPP. La définition de la structure organisationnelle d'un service de protection physique doit prendre en compte certaines considérations communes, qui sont notamment les suivantes :

a) Veiller à ce que la chaîne de commandement soit clairement définie en mettant en place une ligne hiérarchique ininterrompue entre le responsable de la protection physique et les membres du personnel remplissant des fonctions en rapport avec le SPP.

b) Déterminer les « sphères de direction » (nombre de subordonnés sous les ordres d'un responsable ou d'un supérieur hiérarchique) appropriées. Selon la nature et la complexité des activités menées, la sphère de direction peut

être ajustée de sorte que le personnel et les activités puissent être gérés efficacement.

c) Déterminer les modalités de la prise des décisions au sein de l'organisation et identifier la personne qui, dans la chaîne de commandement, a la responsabilité de prendre ces décisions. Si les décisions sont prises par une seule personne à l'échelon le plus élevé de la chaîne de commandement, on parle de modèle de prise de décisions centralisée. Le niveau approprié de prise de décisions est déterminé par des facteurs tels que les incidences potentielles d'une décision sur les autres organisations et les risques et les coûts associés à chaque option.

d) Répartir les activités ou tâches entre les postes (division du travail). Certains postes dont les titulaires font fonctionner un SPP nécessitent une formation spécialisée, comme dans le cas d'un serrurier ou d'un armurier, et certains autres nécessitent des compétences générales, comme dans le cas d'un planificateur de la sécurité chargé d'établir les plans et procédures de sécurité liés au SPP.

e) Formaliser les fonctions à l'intérieur de la structure organisationnelle de sécurité. On peut prendre comme critère la mesure dans laquelle certaines tâches ou activités ne demandent que de se conformer aux processus et procédures établis tandis que d'autres peuvent exiger la prise de mesures discrétionnaires.

f) Regrouper des fonctions pour aider à coordonner les activités et tâches communes. Certains organismes de sécurité se sont dotés d'un groupe technique de la sécurité à même de remplir toutes les fonctions permettant de maintenir un SPP en état de fonctionner car il comprend notamment des ingénieurs, des concepteurs, des techniciens, des spécialistes des réseaux, des spécialistes des essais de performance et des manœuvres. Dans d'autres cas, un groupe technique de la sécurité peut remplir certaines des fonctions tout en faisant appel, si c'est nécessaire pour une activité spécifique, au personnel d'autres services, par exemple aux spécialistes des réseaux du service informatique.

11.26. Pour mettre en place une structure de gestion de la protection physique efficace, il est important de définir les rôles et les responsabilités des services et du personnel. Tous les membres du personnel de l'installation doivent bien comprendre leurs propres rôles et responsabilités et ceux des personnes avec lesquelles ils doivent être en relation pour obtenir les résultats souhaités. C'est ainsi que tous les responsables doivent comprendre la responsabilité qui leur est déléguée en matière de protection physique des cibles situées dans leurs zones respectives, s'agissant notamment des systèmes d'information et informatiques et des tâches d'appui, telles que celles qui concernent la constitution des effectifs et la

formation du personnel, ainsi que la mise en œuvre d'une politique d'habilitation. Il incombe également aux responsables de veiller à ce que leurs subordonnés comprennent leur responsabilité en matière de protection physique et appliquent, aux termes de leur contrat d'emploi, les prescriptions et procédures établies en la matière, et à ce que leur travail fasse l'objet d'un contrôle approprié.

11.27. Pour définir des critères de performance concernant le SPP, il importe d'élaborer des prescriptions ou attentes en la matière qui devraient être respectées par le SPP dans son ensemble ou par chacun de ses composants. Les critères de performance devraient être spécifiques, mesurables, atteignables, réalistes et assortis d'un délai. Ils peuvent prendre en compte un grand nombre de facteurs, parmi lesquels les composants qualité, quantité ou temps, qui définissent la qualité et la précision du travail accompli ou l'efficacité de son résultat. Un exemple d'indicateur de performance quantitatif pour un SPP est la capacité de faire passer 100 personnes par heure par un point de contrôle de l'accès à une installation nucléaire. Le fait pour les gardiens de réagir en moins de cinq minutes à une alarme déclenchée sur le périmètre est un exemple d'indicateur de performance temporel.

11.28. Il est suggéré que les responsables fixent des objectifs de protection physique mesurables. Tous les responsables cherchent activement des informations sur la performance en matière de protection physique dans leur domaine de responsabilité en mettant en place une surveillance appropriée et, conformément aux politiques de sécurité des informations, partagent ces informations au sein de l'organisation, montrant ainsi leur détermination à s'engager dans une démarche d'amélioration continue. Les indicateurs de performance et les données de référence ne devraient encourager ni comportements négatifs ni autosatisfaction. Tout système de récompense devrait être structuré de manière à ne pas susciter de comportements indésirables. Par exemple, si une installation a pour objectif l'absence totale d'incidents de sécurité, le personnel pourrait être réticent à signaler des incidents de ce type.

11.29. Le contrôle du travail implique une action de supervision et de planification s'exerçant grâce à la mise en place d'un cadre de conduite des activités, ainsi que la garantie que la conception ou le fonctionnement du SPP ne sera modifié que d'une manière délibérée, contrôlée et intégrée.

11.30. Les responsables doivent faire en sorte que les activités de protection physique soient menées comme il convient en planifiant, assignant et supervisant les activités associées au SPP. Les responsables peuvent imprimer une dynamique en donnant personnellement l'exemple d'une détermination à accorder systématiquement aux activités de protection physique l'attention prioritaire

qu'elles exigent. Toutes les activités doivent être correctement planifiées de façon à atteindre leurs objectifs et à ne pas compromettre la protection physique. Il importe de planifier aussi bien les tâches courantes que les tâches exceptionnelles ou les événements anormaux, comme les exercices, la maintenance, la modification et le remplacement des équipements, les pannes, les pertes d'alimentation, la défaillance des mesures de protection physique et les événements de sécurité nucléaire, afin que l'intégrité du SPP soit maintenue en toutes circonstances. Il faudra planifier des mesures compensatoires pour certaines tâches exceptionnelles ou certains événements anormaux.

11.31. Pour que les modifications de la conception ou du fonctionnement du SPP se fassent d'une manière délibérée, contrôlée et intégrée, il est nécessaire d'appliquer des programmes de gestion et de contrôle des modifications de la configuration concernant la gestion du SPP. La gestion de la configuration devrait faire partie intégrante du programme de pérennisation de l'exploitant et documenter les éléments physiques ainsi que les aspects de procédure et de formation du SPP de l'organisme exploitant, notamment les systèmes et logiciels informatiques pertinents. Elle fournit un référentiel pour les documents de conception, les procédures opérationnelles standard et les directives régissant le système. Elle comprend également des processus de coordination des modifications des systèmes ou des opérations d'une installation qui pourraient avoir une incidence sur l'efficacité du SPP. De plus, la référence [2] indique que la gestion de la configuration pourrait être l'un des contrôles de gestion utilisés pour régler les questions liées à l'interface entre sûreté et sécurité pendant la conception, la construction, le fonctionnement normal, les événements de sécurité nucléaire, les situations d'urgence et le déclassement.

11.32. La gestion de la configuration permet l'élaboration, l'évaluation, l'approbation, la mise en œuvre, la vérification et la documentation appropriées des modifications apportées à un SPP. L'accès immédiat à ces informations peut aider l'exploitant à se remettre rapidement d'une défaillance de matériel ou de logiciel et à assurer le fonctionnement prévu de l'équipement lors de sa remise en service. En outre, l'accès à des dossiers exacts concernant la formation, les procédures, la maintenance et la logistique permet à l'exploitant de vérifier que ces aspects importants d'un SPP sont bien mis en œuvre. L'exploitant devrait :

a) s'assurer que les implications des modifications du SPP soumis à la gestion de la configuration sont examinées avant la mise en œuvre et bien étayées ;
b) veiller à ce que les informations relatives à cette gestion soient exactes, disponibles en temps voulu et protégées de manière appropriée ;

c) appliquer la gestion de la configuration pour documenter la configuration physique, la mise en œuvre des procédures et les dossiers relatifs à la formation du personnel de son SPP.

11.33. Les orientations de l'AIEA soulignent l'importance des programmes de gestion concernant la gestion de la configuration du SPP [2]. D'autres orientations indiquent des moyens d'appliquer la gestion de la configuration au regroupement de tous les documents relatifs à la sécurité pertinents (p. ex., les documents de conception, les procédures opérationnelles standard et les documents directeurs) et à la prise de décisions éclairées (p. ex. en matière de coordination des modifications) [26].

11.34. La gestion des modifications peut garantir que toute modification importante qu'il est proposé d'apporter à l'installation nucléaire – par tout service pour quelque raison que ce soit, et qu'elle soit de nature structurelle, procédurale ou organisationnelle, et qu'elle soit temporaire ou permanente – est analysée au regard de ses incidences sur la protection physique. Aucune réduction de l'efficacité de la protection physique n'est acceptable, même pour une courte période, sans qu'elle soit dûment justifiée et approuvée. Le système de gestion des modifications peut également servir à empêcher toute modification importante du SPP proposée de compromettre d'autres systèmes, tels que les systèmes de comptabilité et de contrôle des matières nucléaires et le système de sûreté.

11.35. Il faudrait de préférence qu'un responsable approuve chaque modification et que celle-ci soit également approuvée par les personnes dont le domaine de responsabilité est concerné. Il conviendrait d'accorder une attention particulière à ce processus d'examen et d'approbation lorsque la modification a des incidences sur les domaines de responsabilité de différentes parties de l'organisme. L'organisme de sécurité doit recevoir la preuve que la modification satisfait aux prescriptions de protection physique.

11.36. La mise en œuvre de la modification doit faire l'objet d'une surveillance adéquate afin que l'on puisse signaler rapidement tout effet négatif sur l'efficacité du SPP et, de ce fait, disposer de suffisamment de temps pour prendre toute mesure corrective nécessaire. Les activités planifiées susceptibles de nuire à la protection physique sont notamment les suivantes :

a) activités qui pourraient entraîner une perte de l'alimentation électrique primaire pour les équipements de protection physique ;
b) placement de véhicules ou d'équipements lourds, ou mise au point ou en place de mesures de protection physique ou de barrières qui pourraient

bloquer les capacités de détection ou d'évaluation, réduire le retardement ou allonger les durées d'intervention ;

c) activités de construction qui enlèvent ou dégradent les barrières physiques, permettant de ce fait d'éviter les contrôles de l'accès.

11.37. Dans le cas où l'installation nucléaire serait mitoyenne d'une autre installation nucléaire existante ou prévue, des arrangements devraient être pris, selon que de besoin, pour que ses activités prévues ne diminuent pas l'efficacité du plan de sécurité ou du SPP de l'installation adjacente.

GESTION DES RESSOURCES

11.38. La gestion des ressources couvre notamment les aspects suivants : programmes de formation et de qualification ; sélection du personnel appelé à remplir les fonctions d'appui à la conception, à la mise en place et à l'application des mesures de protection physique, et au fonctionnement du SPP ; achat de biens et de services, et mise en place d'un environnement de travail productif.

11.39. La sélection du personnel s'entend du processus méthodique mené pour choisir le personnel appelé à exercer les fonctions liées au SPP et trouver les personnes possédant les connaissances, les compétences, les capacités et les autres caractéristiques leur permettant d'apporter la contribution la plus précieuse à l'organisme. Dans une installation nucléaire, les processus de gestion des ressources humaines s'inscrivent dans le cadre du système de gestion intégré, et il incombe aux responsables de la protection physique de s'employer à recruter et à conserver les meilleurs agents disponibles dans les limites du système. La sélection du personnel impose également de veiller à ce que ses membres aient les qualifications nécessaires pour s'acquitter de leurs fonctions, et ils font l'objet d'un contrôle d'habilitation avant de se voir attribuer des postes pour lesquels un contrôle de ce type est exigé.

11.40. La protection physique ne peut être efficace que si le personnel possède les connaissances et les compétences nécessaires pour s'acquitter de ses fonctions conformément aux normes souhaitées. Les responsables doivent s'assurer que leurs agents non seulement suivent une formation à la sécurité adaptée à leurs responsabilités, mais aussi sont conscients des menaces et au fait des autres questions liées à une solide culture de sécurité nucléaire [28].

11.41. L'achat de biens et de services est essentiel pour soutenir un SPP efficace. À cet égard, les aspects particulièrement importants à prendre en considération

sont notamment l'achat pour le SPP d'équipements à des vendeurs reconnus et la garantie que les pièces de rechange seront disponibles pendant la durée de vie prévue des équipements, l'essai et l'évaluation de nouveaux composants avant leur achat pour s'assurer qu'ils peuvent être intégrés dans les composants du SPP existants et sont compatibles avec ces derniers, et l'évaluation des risques éventuels de sécurité liés à la chaîne d'approvisionnement. L'exploitant reste responsable de la protection physique lorsqu'il a recours aux services de prestataires ou achète des biens et services quels qu'ils soient. Les exploitants doivent rester compétents pour préciser la portée et la qualité requises d'un produit ou service et, ultérieurement, déterminer si ce produit ou service satisfait aux prescriptions et spécifications relatives aux équipements de protection physique. Le système de gestion peut comprendre des dispositions concernant :

a) la qualification des vendeurs, des sous-traitants et des fournisseurs de biens et de services ;
b) la sélection des vendeurs, des sous-traitants et des fournisseurs sur la base de l'efficacité de leurs systèmes de gestion et de leur performance ;
c) la vérification que les vendeurs, les sous-traitants et les fournisseurs comprennent et respectent les prescriptions de protection physique (s'agissant notamment de la sécurité des informations sensibles) concernant les biens et services qu'ils fournissent ;
d) l'approbation préalable par l'exploitant de tout contrat de sous-traitance passé avec le vendeur, le sous-traitant ou le fournisseur ;
e) la spécification des conditions contractuelles, notamment les prescriptions de protection physique ;
f) la fourniture, le cas échéant, de conseils, d'informations et d'une formation aux vendeurs, sous-traitants et fournisseurs et à leur personnel ;
g) l'évaluation périodique des systèmes de gestion, notamment des dispositions prises en matière de protection physique, des vendeurs, des sous-traitants et des fournisseurs et de leur performance, à l'aide d'une approche graduée ;
h) la vérification que les biens et services fournis respectent les spécifications de protection physique de l'installation et sont authentiques.

11.42. Le cadre de travail physique et psychologique influe largement sur la façon dont le personnel s'acquitte de ses tâches et se conforme aux prescriptions de protection physique. Il importe que les procédures de protection physique ne soient pas considérées comme une charge excessive ou inutile. Les responsables peuvent associer le personnel à l'examen des guides et procédures de protection physique pour s'assurer qu'il comprend les documents et leur raison d'être et peut faire des suggestions pour les rendre plus efficaces.

ACTIVITÉS D'ASSURANCE

11.43. Les activités d'assurance comprennent la mise en œuvre de l'assurance de la qualité et l'exécution de programmes d'assurance. Un programme d'assurance de la qualité garantit que le SPP fonctionne comme prévu et satisfait aux prescriptions réglementaires et de performance. Un programme d'assurance met en place des activités d'évaluation et d'essais suffisamment rigoureuses pour garantir que les mesures du SPP sont à tout moment opérationnelles, fonctionnent comme prévu et interagissent de façon à repérer toute agression et à y réagir avant qu'un acte malveillant n'ait pu être accompli.

11.44. L'assurance de la qualité est une composante de la gestion de la qualité (qui devrait elle-même faire partie du système de gestion intégré) qui s'attache à donner l'assurance que les prescriptions de qualité seront respectées. Un système de gestion de la qualité est un ensemble de processus opérationnels qui mettent l'accent sur l'application de la politique et des objectifs de qualité afin de satisfaire aux prescriptions réglementaires.

11.45. Le programme d'assurance prend en compte le résultat des inspections effectuées par l'autorité compétente et les résultats des autoévaluations internes dans le cadre d'une approche globale afin de garantir le maintien de l'efficacité du SPP. Les activités d'évaluation devraient être graduées et adaptées aux actifs se trouvant à un emplacement donné et aux mesures qui constituent le SPP global d'une installation nucléaire. Il conviendrait d'accorder une attention particulière à l'établissement de calendriers pour les activités d'assurance, en planifiant les modalités d'utilisation des résultats de ces activités et en définissant les mesures, notamment les mesures compensatoires, qui devraient être prises si ces activités font apparaître une dégradation inacceptable de l'efficacité du SPP. Un programme d'autoévaluation (ou d'examen interne) devrait normalement utiliser un large éventail d'évaluations, d'analyses des causes profondes, d'indicateurs de performance, d'enseignements tirés et de programmes de suivi des mesures correctives.

11.46. Les activités d'assurance consistent notamment en évaluations régulièrement menées pour garantir la capacité de l'exploitant de maintenir le SPP en état de fonctionnement en recensant les points forts et les domaines où des améliorations sont nécessaires. La rigueur de ces évaluations devrait être basée sur une approche graduée, selon le type de matières nucléaires ou d'installation nucléaire, la nature des opérations et les mesures qui constituent le SPP. La section 9 donne des informations supplémentaires sur les activités d'assurance.

DURABILITÉ ET AMÉLIORATION CONTINUE

11.47. La durabilité s'entend du maintien de la performance des personnes, des procédures et des équipements. Elle consiste à contrôler la performance et à motiver et à imprimer une dynamique pour créer une organisation qui soit toujours efficace et ne cesse de s'améliorer. Elle comporte des programmes de maintenance et d'essais visant à permettre aux systèmes du SPP de continuer à fonctionner comme prévu, ainsi que l'instauration d'une solide culture de sécurité nucléaire, telle qu'elle est décrite dans la publication n° 30-G de la collection Sécurité nucléaire de l'AIEA, intitulée *Maintien d'un régime de sécurité nucléaire* [30].

11.48. Pour maintenir efficacement un SPP, il importe de maintenir non seulement la technologie, mais aussi les personnes qui l'utilisent. Les responsables doivent faire savoir au personnel ce que l'on attend de lui et lui indiquer les objectifs de l'organisation, les pratiques qui seront récompensées et les actes qui seront sanctionnés. Tous les employés et décideurs doivent faire connaître à l'ensemble de l'organisation les réalisations que l'on attend d'eux et les pratiques acceptables à cet égard. Les responsables doivent imprimer une dynamique conforme aux politiques, valeurs et stratégies de l'organisation.

11.49. Le maintien d'une performance élevée n'est possible que si le personnel compétent occupe les postes stratégiques et possède les qualités d'encadrement nécessaires. Cette performance peut être maintenue grâce aux programmes visant à :

a) recruter du personnel possédant les meilleures qualifications ;
b) renforcer les compétences et aptitudes du personnel à la faveur de programmes de formation et de qualification ;
c) saluer et récompenser les bonnes pratiques ;
d) recycler, muter ou licencier les membres du personnel dont le travail ne donne pas satisfaction ;
e) fournir un environnement de travail sûr.

11.50. L'amélioration continue est un processus consistant à définir les améliorations à apporter aux politiques, processus, plans, procédures ou équipements ou au système de gestion au vu des problèmes recensés pendant les activités d'évaluation, telles que les inspections, les autoévaluations ou les essais de performance, les retours d'information du personnel ou les enseignements tirés, ou résultant des modifications apportées aux opérations, à la sûreté ou à d'autres programmes de l'installation nucléaire. Dans la pratique, la performance d'un SPP se rapproche, à un moment donné, de son point le plus élevé, et, après ce point, ne connaît que des améliorations marginales, sauf si un changement

ponctuel (une nouvelle technologie, p. ex.) permet une amélioration importante de l'efficience ou de l'efficacité du SPP. Toutefois, la performance d'un SPP risque toujours de baisser, pour des raisons telles que le vieillissement ou l'obsolescence des équipements, la diminution du soutien financier, la perte de motivation du personnel et l'excès de confiance des responsables.

Appendice

EXEMPLES D'ÉVALUATION DES BESOINS ET D'ANALYSE DES PRESCRIPTIONS POUR LES SYSTÈMES DE DRONES AÉRIENS

A.1. Le présent appendice donne un aperçu détaillé d'une évaluation des besoins et d'une analyse des prescriptions fictives. Dans cet exemple, les responsables de l'installation ont jugé nécessaire d'avoir une meilleure connaissance de la situation et de disposer de moyens flexibles d'évaluation pour couvrir la zone d'accès limité sans exposer les gardes en patrouille aux préjudices que pourraient leur causer les agresseurs. Si possible, il pourrait également être utile d'avertir les agresseurs d'avoir à s'éloigner, là encore sans exposer les gardiens en patrouille.

A.2. Pour ce faire, on peut notamment utiliser un système de drones aériens (SDA). D'autres solutions pourraient consister à installer des caméras dans la zone d'accès limité, soit en en équipant les véhicules de patrouille, soit en les répartissant à plusieurs endroits de cette zone. Les options et les informations prises en compte en ce qui concerne les SDA pourraient être les suivantes :

a) Les SDA peuvent être exploités de plusieurs façons :
   i) Présence permanente d'un SDA non attaché au-dessus de zones protégées pour surveiller en continu (sous réserve des conditions météorologiques) et guider le personnel et le matériel de renseignement, de surveillance et de reconnaissance (p. ex. les caméras et les capteurs) dans les secteurs préoccupants. Ce mode de fonctionnement implique de longs temps de vol (endurance) ou un échange rapide de matériel en service ou hors service pour permettre le rechargement des batteries ou le rechargement en combustible.
   ii) Fonctionnement normal avec câble d'attache pour alimentation électrique et communications. On pourrait concevoir un tel système de façon qu'il puisse être attaché en différents endroits à des moments différents. Par exemple, le câble pourrait être fixé à un véhicule ou un bateau pour des opérations mobiles. Ce mode de fonctionnement pourrait être exploité sur une certaine période (sous réserve de disponibilité), mais les options seraient plus limitées que dans le cas des opérations permanentes d'engins non attachés.
   iii) Déploiement périodique (p. ex. une fois par heure) ou à la demande pour évaluation ou détermination des intentions d'un agresseur identifié.

b) On ne dispose que de très peu d'informations fiables, autres que les revendications du vendeur, pour évaluer la qualité de fonctionnement de ces systèmes sur de longues périodes.
c) Comme il est fréquent que l'exploitation des SDA soit contrôlée par la réglementation aérienne nationale, il importe de tenir compte des limitations d'exploitation d'ordre juridique et politique.

A.3. Supposons, par exemple, qu'un exploitant songe à déployer un SDA à la demande chaque fois qu'il y a des raisons de penser que des agresseurs se trouvent dans la zone d'accès limité. La première chose à faire lorsque l'on envisage d'utiliser un SDA est de déterminer les prescriptions de la partie prenante concernant ce sous-système, à savoir les capacités et fonctions de ce dernier dont elle a besoin, ainsi que les normes de qualité, les essais et l'évaluation, et les essais de performance. Les prescriptions de la partie prenante pourraient être les suivantes :

a) Prescriptions concernant l'efficacité opérationnelle : Par exemple, le SDA doit être capable de déterminer catégoriquement la présence d'un agresseur et de l'affronter dans les 30 secondes qui suivent sa détection aux bornes de la zone d'accès limité. Les SDA doivent être déployables au moins 75 % du temps et pouvoir couvrir 70 % des chemins qu'un agresseur est le plus susceptible d'emprunter à travers la zone d'accès limité.
b) Prescriptions réglementaires : La réglementation aérienne nationale limite les modalités de déploiement d'un SDA par les entités publiques et précise les limites de poids et les limites opérationnelles de l'engin ainsi que les prescriptions relatives à la formation des contrôleurs de vol de SDA. Ces contrôleurs sont limités à 8 heures de temps de vol sur une période de 24 heures. L'autorité compétente pourrait avoir édicté des prescriptions concernant l'opérateur s'il est membre de l'équipe d'intervention.
c) Prescriptions de l'exploitant :
    i) Conformément aux politiques de sûreté de l'exploitant, tout sous-système de protection physique doit fonctionner dans le respect d'un plan de sûreté protégeant à la fois le personnel de l'installation et le public.
    ii) Documentation requise, notamment les plans d'essais de réception, les plans de maintenance et les plans de formation des contrôleurs de SDA et du personnel chargé de la maintenance.
d) Estimation des coûts : Le coût n'est pas plafonné à l'avance, mais il est nécessaire d'estimer les coûts initiaux et les coûts d'exploitation du déploiement d'un SDA de sorte que les responsables puissent décider s'il

convient d'étudier plus avant l'utilisation d'un système de ce type et d'en entreprendre la conception.

e) Maturité requise du système : Il s'impose de bien cerner la nature des risques que pose l'exploitation d'un SDA et les avantages que peut procurer son utilisation.

A.4. Il s'agit ensuite de déterminer le concept d'opérations (c'est-à-dire le mode de fonctionnement du système du point de vue de l'exploitant), notamment les besoins des utilisateurs et les buts et caractéristiques du système. Le concept d'opérations d'un SDA pourrait comprendre les éléments suivants :

1) Les agresseurs potentiels seraient observés à l'intérieur de la zone d'accès limité à l'aide d'imageurs thermiques ou par des patrouilles munies de jumelles.
2) Les patrouilles motorisées et les patrouilles fluviales opérant dans la zone d'accès limité seraient averties que des véhicules ou personnes éventuellement non autorisés sont présents dans cette zone ou le long des berges dont l'accès est interdit au public.
3) L'opérateur du PCS donnerait alors à l'un des véhicules ou bateaux de patrouille l'ordre de lancer un SDA. Le personnel à bord du véhicule ou du bateau déterminerait si son SDA est opérationnel et se trouve dans un endroit où il pourrait être lancé, et si les conditions météorologiques sont favorables à ce lancement. Si tel n'est pas le cas, il en informerait le PCS, qui pourrait demander à d'autres patrouilles si elles sont en mesure de lancer un SDA.
4) Le PCS pourrait aussi contrôler le SDA pour qu'il se rapproche suffisamment du véhicule ou de l'agresseur afin de déterminer s'il est armé, si le véhicule est blindé ou s'il transporte des objets suspects. Si c'est le cas, le PCS notifierait par radio l'intrusion aux gardiens et aux forces d'intervention.
5) S'il s'avère impossible de déterminer ce qui précède, le SDA se rapprocherait suffisamment des agresseurs pour leur ordonner par haut-parleur de quitter la zone d'accès limité ou les berges dont l'accès est interdit au public.

A.5. Les prescriptions de la partie prenante et le concept d'opérations pourraient déboucher sur des prescriptions dérivées, telles que les prescriptions fictives ci-après :

a) Les actions prévues dans les phases 1 à 4 du concept d'opérations présentées au paragraphe A.4 doivent être accomplies dans les 30 secondes qui suivent la détection d'un agresseur potentiel aux bornes de la zone d'accès limité. Les vitesses et descriptions qui pourraient être présumées en ce qui concerne

les véhicules ou bateaux des agresseurs seront précisées sur la base de l'évaluation de la menace ou de la menace de référence. Il pourra être nécessaire de recueillir des données de performance pour créer un calendrier des phases du concept d'opérations. Ce calendrier peut ensuite servir à vérifier que les prescriptions de la partie prenante seraient respectées face à des agresseurs éventuels.

b) Le SDA devrait pouvoir être déployé 75 % du temps, compte tenu des contraintes imposées par les conditions météorologiques et la fiabilité du système. Pour déterminer le pourcentage de temps effectif de lancement d'un SDA, on prendra en considération les spécifications du vendeur concernant le poids, les dimensions et la vitesse de l'engin, ainsi que les données historiques sur les conditions météorologiques, telles que la pluie, la neige, la grêle, les vents forts et les rafales de vent.

c) Comme le SDA doit pouvoir être déployé 75 % du temps, il convient de pouvoir disposer de certains moyens de détection et de suivi nocturnes d'agresseurs. En l'état actuel de la technologie, ces moyens semblent devoir être fournis par l'imagerie thermique, les radars ou les systèmes de détection et de télémétrie par la lumière (LIDAR).

d) Il faudra indiquer, pour la zone d'accès limité et sur les berges, les zones d'interdiction de survol ou zones interdites où il n'est pas possible d'utiliser un SDA. Ces zones permettront de définir les parties de la zone de l'installation dont le survol est autorisé et les altitudes auxquelles l'utilisation d'un SDA est permise.

e) Il faudra définir des politiques et des procédures visant à empêcher le lancement ou l'utilisation d'un SDA à l'intérieur des zones interdites et à le faire atterrir en toute sécurité en cas de dysfonctionnement ou de perte de contrôle.

f) Le personnel concerné devra être formé à l'accomplissement des actions prévues dans toutes les phases du concept d'opérations. Il s'agit de l'opérateur du PCS, du personnel à bord des véhicules et bateaux de patrouille et du personnel de maintenance.

g) L'estimation des coûts sera basée sur la nécessité de disposer d'un nombre suffisant de SDA à déployer 75 % du temps pour couvrir 70 % des chemins qu'un agresseur est le plus susceptible d'emprunter à travers la zone d'accès limité.

h) Certaines hypothèses devront être posées quant aux avertisseurs sonores ou lumineux dont il conviendra de disposer pour éloigner les agresseurs des bornes de la zone d'accès limité, notamment dans différentes conditions météorologiques.

i) Afin de satisfaire aux prescriptions concernant la maturité requise du système, seuls les modèles de SDA qui auront été utilisés dans une

installation nucléaire pendant au moins un an seront évalués en vue d'une utilisation éventuelle.

RÉFÉRENCES

[1] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Recommandations de sécurité nucléaire sur la protection physique des matières nucléaires et des installations nucléaires (INFCIRC/225/Révision 5), nº 13 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2011).

[2] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Protection physique des matières nucléaires et des installations nucléaires (Guide d'application de la publication INFCIRC/225/Révision 5), nº 27-G de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2019).

[3] Convention sur la protection physique des matières nucléaires (INFCIRC/274/Rev.1), AIEA, Vienne (1980).

[4] Amendement de la Convention sur la protection physique des matières nucléaires (INFCIRC/274/Rev.1/Mod.1), AIEA, Vienne (2016).

[5] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Établissement de l'infrastructure de sécurité nucléaire pour un programme électronucléaire, nº 19 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2018).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Developing Regulations and Associated Administrative Measures for Nuclear Security, IAEA Nuclear Security Series No. 29-G, IAEA, Vienna (2018).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (2021).

[8] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Utilisation de la comptabilité et du contrôle des matières nucléaires à des fins de sécurité nucléaire dans les installations, nº 25-G de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2018).

[9] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Mise en place d'un système de contrôle des matières nucléaires, à des fins de sécurité nucléaire, encadrant leur utilisation, leur entreposage et leur déplacement dans les installations, nº 32-T de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2024).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8-G (Rev. 1), IAEA, Vienna (2020).

[11] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Sécurité des matières nucléaires en cours de transport, nº 26-G de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2019).

[12] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Sécurité des matières radioactives en cours de transport, nº 9-G (Rev.1) de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2022).

[13] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Évaluation de la menace contre la sécurité nucléaire nationale, menaces de référence et énoncés de la menace représentative, nº 10-G (Rev. 1) de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2022).
[14] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Systems and Software Engineering: System Life Cycle Processes, ISO/IEC/IEEE 15288:2015, ISO, Geneva (2015).
[15] INTERNATIONAL COUNCIL ON SYSTEMS ENGINEERING, Systems Engineering Handbook: A Guide for System Life Cycle Process and Activities, 4th edn, Wiley, Hoboken, NJ (2015).
[16] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Identification des zones vitales des installations nucléaires, nº 16 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2015).
[17] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, La sécurité tout au long de la durée de vie d'une installation nucléaire, nº 35-G de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2021).
[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, IAEA Nuclear Security Series No. 4, IAEA, Vienna (2007).
[19] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Sécurité de l'information nucléaire, nº 23-G de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2017).
[20] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Sécurité informatique pour la sécurité nucléaire, nº 42-G de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2022).
[21] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Sécurité informatique des systèmes de contrôle-commande dans les installations nucléaires, nº 33-T de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2023).
[22] AMERICAN NATIONAL STANDARDS INSTITUTE, INTERNATIONAL SOCIETY FOR AUTOMATION, Management of Alarm Systems for the Process Industries, ANSI/ISA-18.2-2016, ISA, Research Triangle, NC (2016).
[23] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Élaboration d'un plan d'intervention spécialisé en sécurité nucléaire pour les installations nucléaires, nº 39-T de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2023).
[24] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Safety of X Ray Generators and Other Radiation Sources Used for Inspection Purposes and for Non-medical Human Imaging, IAEA Safety Standards Series No. SSG-55, IAEA, Vienna (2020).
[25] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-G-3.1, IAEA, Vienna (2006).

[26] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Nuclear Installations, IAEA Safety Standards Series No. GS-G-3.5, IAEA, Vienna (2009).
[27] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Management for Research Reactors and Related Facilities, IAEA, Vienna (2016).
[28] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Culture de sécurité nucléaire, nº 7 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2009).
[29] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Systems and Software Engineering: Life Cycle Processes — Requirements Engineering, ISO/IEC/IEEE 29148:2018, ISO, Geneva (2018).
[30] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Maintien d'un régime de sécurité nucléaire, nº 30-G de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2020).

ABRÉVIATIONS

NIP	numéro d'identification personnel
PCS	poste central de sécurité
SDA	système de drones aériens
SPP	système de protection physique

OÙ COMMANDER ?

Vous pouvez vous procurer les publications de l'AIEA destinées à la vente chez notre principal distributeur ou dans les grandes librairies. Les publications non destinées à la vente doivent être commandées directement à l'AIEA.

Commande de publications destinées à la vente

Veuillez-vous adresser à votre libraire préféré ou à notre principal distributeur :

Eurospan
1 Bedford Row
London WC1R 4BU
Royaume-Uni

Commandes commerciales et renseignements :
Tél. : +44 (0)1235 465576
Mél. : trade.orders@marston.co.uk

Commandes individuelles :
Tél. : +44 (0)1235 465577
Mél. : direct.orders@marston.co.uk
www.eurospanbookstore.com/iaea

Pour plus d'informations :
Tél. : +44 (0)207 240 0856
Mél. : info@eurospan.co.uk
www.eurospan.co.uk

Les commandes de publications destinées ou non à la vente peuvent être adressées directement à :

Section d'édition
Agence internationale de l'énergie atomique
Centre international de Vienne
B.P. 100
1400 Vienne (Autriche)
Tél. : +43 1 2600 22529 ou 22530
Mél. : sales.publications@iaea.org
www.iaea.org/publications

La présente publication est destinée à fournir aux États, aux autorités compétentes et aux exploitants des orientations exhaustives et détaillées pour les aider à mettre en œuvre les recommandations et orientations de l'AIEA concernant un système de protection physique (SPP) efficace des matières nucléaires en cours d'utilisation et en entreposage et des installations nucléaires. Elle fournit de plus amples précisions techniques sur la manière de concevoir et d'évaluer un SPP en ce qui concerne le choix et l'intégration des mesures de protection physique appropriées et efficaces.

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE