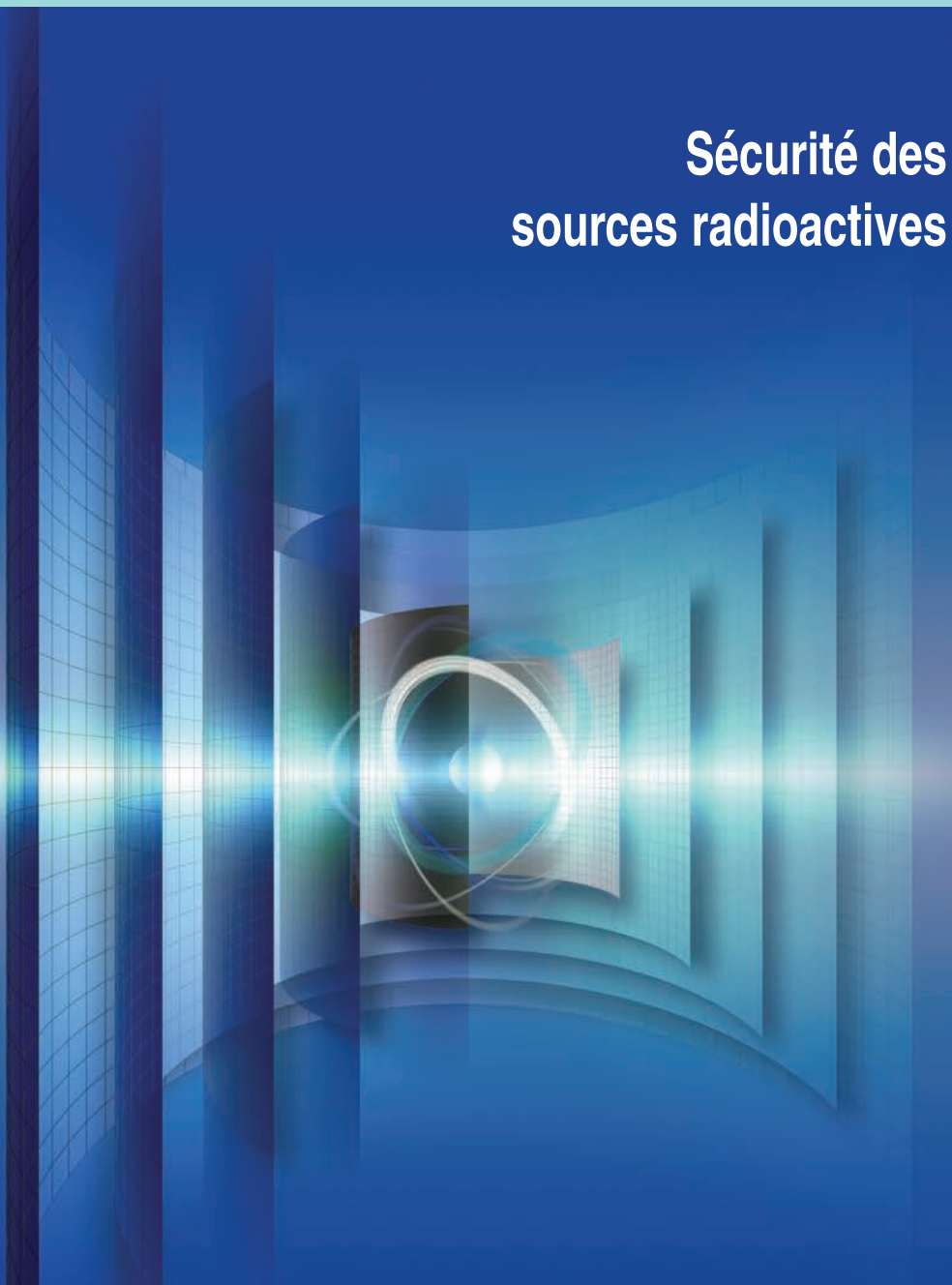
Collection Sécurité nucléaire de l'AIEA – Nº 11

Guide d'application

Sécurité des sources radioactives



IAEA
Agence internationale de l'énergie atomique

LA COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA

Les publications de la **collection Sécurité nucléaire de l'AIEA** traitent des mesures à prendre (prévention, détection, intervention) contre le vol, le sabotage et la cession illégale de matières nucléaires et de sources radioactives et des installations connexes, l'accès non autorisé à ces matières, sources et installations et les autres actes malveillants dont elles peuvent faire l'objet. Ces publications sont conformes aux instruments internationaux relatifs à la sécurité nucléaire, notamment la Convention sur la protection physique des matières nucléaires telle qu'amendée, le Code de conduite sur la sûreté et la sécurité des sources radioactives, les résolutions 1373 et 1540 du Conseil de sécurité de l'ONU et la Convention internationale pour la répression des actes de terrorisme nucléaire, 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 énoncent les objectifs, les concepts et les principes de la sécurité nucléaire et servent de base pour l'élaboration de recommandations en matière de sécurité.
- Les **Recommandations**, qui présentent les pratiques exemplaires que les États Membres devraient adopter pour la mise en œuvre des Fondements de la sécurité nucléaire.
- Les **Guides d'application,** qui complètent les Recommandations dans certains grands domaines et proposent des mesures pour en assurer la mise en œuvre.
- Les **Orientations techniques**, comprenant les **Manuels de référence**, qui présentent des mesures détaillées et/ou donnent des conseils pour la mise en œuvre des Guides d'application dans des domaines ou des activités spécifiques, les **Guides de formation**, qui présentent les programmes et/ou les manuels des cours de formation de l'AIEA dans le domaine de la sécurité nucléaire, et les **Guides des services,** qui donnent des indications concernant la conduite et la portée des missions consultatives de l'AIEA sur la sécurité nucléaire.

RÉDACTION ET EXAMEN

Des experts internationaux aident le Secrétariat de l'AIEA à élaborer ces publications. Pour l'élaboration des Fondements de la sécurité nucléaire, des Recommandations et des Guides d'application, l'AIEA organise des réunions techniques à participation non limitée afin que les États Membres intéressés et les organisations internationales compétentes puissent examiner comme il se doit les projets de texte. En outre, pour faire en sorte que ces projets soient examinés de façon approfondie et largement acceptés au niveau international, le Secrétariat les soumet aux États Membres, qui disposent de 120 jours pour les examiner officiellement, ce qui leur donne la possibilité d'exprimer pleinement leurs vues avant que le texte soit publié.

Les publications de la catégorie Orientations techniques sont élaborées en consultation étroite avec des experts internationaux. Il n'est pas nécessaire d'organiser des réunions techniques, mais on peut le faire lorsque cela est jugé nécessaire pour recueillir un large éventail de points de vue.

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 spécifiques 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.

SÉCURITÉ DES SOURCES RADIOACTIVES

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

AFGHANISTAN, RÉP. ISLAMIQUE D'
AFRIQUE DU SUD
ALBANIE
ALGÉRIE
ALLEMAGNE
ANGOLA
ARABIE SAOUDITE
ARGENTINE
ARMÉNIE
AUSTRALIE
AUTRICHE
AZERBAÏDJAN
BAHREÏN
BANGLADESH
BÉLARUS
BELGIQUE
BELIZE
BÉNIN
BOLIVIE
BOSNIE-HERZÉGOVINE
BOTSWANA
BRÉSIL
BULGARIE
BURKINA FASO
BURUNDI
CAMBODGE
CAMEROUN
CANADA
CHILI
CHINE
CHYPRE
COLOMBIE
CONGO
CORÉE, RÉPUBLIQUE DE
COSTA RICA
CÔTE D'IVOIRE
CROATIE
CUBA
DANEMARK
DOMINIQUE
ÉGYPTE
EL SALVADOR
ÉMIRATS ARABES UNIS
ÉQUATEUR
ÉRYTHRÉE
ESPAGNE
ESTONIE
ÉTATS-UNIS D'AMÉRIQUE
ÉTHIOPIE
FÉDÉRATION DE RUSSIE
FINLANDE
FRANCE
GABON
GÉORGIE
GHANA
GRÈCE
GUATEMALA
HAÏTI
HONDURAS
HONGRIE
ÎLES MARSHALL
INDE
INDONÉSIE
IRAN, RÉP. ISLAMIQUE D'
IRAQ
IRLANDE
ISLANDE
ISRAËL
ITALIE
JAMAÏQUE
JAPON
JORDANIE
KAZAKHSTAN
KENYA
KIRGHIZISTAN
KOWEÏT
LESOTHO
LETTONIE
L'EX-RÉPUBLIQUE YOUGOSLAVE DE MACÉDOINE
LIBAN
LIBÉRIA
LIBYE
LIECHTENSTEIN
LITUANIE
LUXEMBOURG
MADAGASCAR
MALAISIE
MALAWI
MALI
MALTE
MAROC
MAURICE
MAURITANIE, RÉP. ISLAMIQUE DE
MEXIQUE
MONACO
MONGOLIE
MONTÉNÉGRO
MOZAMBIQUE
MYANMAR
NAMIBIE
NÉPAL
NICARAGUA
NIGER
NIGERIA
NORVÈGE
NOUVELLE-ZÉLANDE
OMAN
OUGANDA
OUZBÉKISTAN
PAKISTAN
PALAOS
PANAMA
PAPOUASIE-NOUVELLE-GUINÉE
PARAGUAY
PAYS-BAS
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
SAINT-SIÈGE
SÉNÉGAL
SERBIE
SEYCHELLES
SIERRA LEONE
SINGAPOUR
SLOVAQUIE
SLOVÉNIE
SOUDAN
SRI LANKA
SUÈDE
SUISSE
TADJIKISTAN
TCHAD
THAÏLANDE
TUNISIE
TURQUIE
UKRAINE
URUGUAY
VENEZUELA, RÉP. BOLIVARIENNE DU
VIETNAM
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 N° 11

SÉCURITÉ DES SOURCES RADIOACTIVES

GUIDE D'APPLICATION

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE, 2012

DROIT D'AUTEUR

Unité de la promotion et de la vente, Section d'édition
Agence internationale de l'énergie atomique
Centre international de Vienne
B.P. 100
1400 Vienne, Autriche
télécopie : +43 1 2600 29302
téléphone : +43 1 2600 22417
courriel : sales.publications@iaea.org
http://www.iaea.org/books

Imprimé par l'AIEA en Autriche
Août 2012

SÉCURITÉ DES
SOURCES RADIOACTIVES
AIEA, VIENNE, 2012
STI/PUB/1387
ISBN 978–92–0–232910–2
ISSN 1816–9317

AVANT-PROPOS

En application d'une résolution de la Conférence générale de l'AIEA de septembre 2002, l'AIEA a adopté une approche intégrée de la protection contre le terrorisme nucléaire. Cette approche coordonne ses activités concernant la protection physique des matières nucléaires et des installations nucléaires, la comptabilisation des matières nucléaires, la détection et l'intervention en cas de trafic des matières nucléaires et autres matières radioactives, la sécurité des sources radioactives, la sécurité du transport des matières nucléaires et autres matières radioactives, les interventions d'urgence et les mesures de préparation aux situations d'urgence en place dans les États Membres et à l'AIEA, et la promotion de l'adhésion des États aux instruments internationaux pertinents. L'AIEA aide en outre à déterminer les menaces et la vulnérabilité des matières nucléaires et autres matières radioactives du point de vue de la sécurité. Toutefois, les États ont la responsabilité d'assurer la protection physique des matières nucléaires et autres matières radioactives, ainsi que des installations connexes, de garantir la sécurité de ces matières, notamment en cours de transport, et de lutter contre le trafic illicite et les mouvements fortuits de ces matières.

Les sources radioactives procurent d'énormes avantages à l'humanité, principalement grâce à leur utilisation en agriculture, dans l'industrie, en médecine, et dans la recherche, et la grande majorité d'entre elles sont utilisées dans des environnements réglementés. Toutefois, on a perdu le contrôle d'une petite fraction de ces sources, ce qui a parfois entraîné des accidents, dont certains avec de sérieuses conséquences.

À l'heure actuelle, on est de plus en plus préoccupé par le fait que des groupes terroristes ou criminels pourraient avoir accès à des sources radioactives de haute activité et les utiliser de manière malveillante. En conséquence, la tendance mondiale est le renforcement du contrôle, de la comptabilisation et de la sécurité des sources radioactives pour prévenir leur utilisation malveillante et les conséquences connexes possibles.

La Code de conduite sur la sûreté et la sécurité des sources radioactives est un exemple de cette tendance mondiale. On l'a révisé en 2003 pour y inclure des principes de sécurité renforcés, y compris des recommandations appelant chaque État à définir sa menace nationale et à évaluer sa vulnérabilité par rapport à cette menace pour les diverses sources présentes sur son territoire. En outre, plusieurs conférences internationales importantes ont été convoquées sur cette question et ont conclu que la sécurité des sources radioactives devait être une priorité mondiale et qu'il fallait accroître les efforts pour lutter contre le trafic illicite de ces sources.

La présente publication donne des orientations que peuvent utiliser les organismes de réglementation lors de l'élaboration des prescriptions de sécurité des sources radioactives.

Elle fait partie de la collection Sécurité nucléaire de l'AIEA, et sa préparation a nécessité de vastes consultations avec les États Membres, y compris une réunion technique à participation non limitée tenue à Vienne en mai 2006. Dernière étape de ce processus, le projet de document a été envoyé à tous les États Membres pour recueillir d'autres observations et suggestions avant sa publication.

TABLE DES MATIÈRES

1. INTRODUCTION 1

1.1. Contexte 1
1.2. Objectif 1
1.3. Champ d'application 2

2. RESPONSABILITÉS DE L'ÉTAT ET DE L'EXPLOITANT 3

2.1. Introduction 3
2.2. État 3
2.3. Exploitants 4

3. CONCEPTS DE SÉCURITÉ 5

3.1. Introduction 5
3.2. Culture de sécurité 6
3.3. Objet d'un système de sécurité 7
3.4. Fonctions de sécurité 8
3.5. Conception et évaluation des systèmes de sécurité 9
3.6. Intégration des mesures de sûreté et des mesures de sécurité 10
3.7. Approche graduée de la sécurité 10
3.8. Compréhension et prise en compte du contexte de la menace . . . 11
3.8.1. Évaluation de la menace nationale 11
3.8.2. Menace de référence 13
3.8.3. Menaces d'origine interne 13
3.8.4. Menace accrue 14
3.9. Évaluation de la vulnérabilité 14

4. ÉTABLISSEMENT D'UN PROGRAMME RÉGLEMENTAIRE POUR LA SÉCURITÉ DES SOURCES RADIOACTIVES 14

4.1. Étape 1 : Établir des niveaux de sécurité gradués avec des buts et des objectifs pour chaque niveau 16
4.2. Étape 2 : Déterminer le niveau de sécurité applicable à une source donnée 18
4.2.1. Catégorisation des sources radioactives 18
4.2.2. Affectation des niveaux de sécurité 23

4.2.3. Autres considérations pour l'affectation des niveaux de sécurité 25
4.3. Étape 3 : Sélectionner et mettre en œuvre une approche de réglementation 26
4.3.1. Approche basée sur les prescriptions 28
4.3.2. Approche basée sur les résultats. 51
4.3.3. Approche combinée 53

APPENDICE I: DESCRIPTION DES MESURES DE SÉCURITÉ 55

APPENDICE II: EXEMPLES DE TENEUR D'UN PLAN DE SÉCURITÉ 60

APPENDICE III: DESCRIPTION D'UNE ÉVALUATION DE LA VULNÉRABILITÉ 62

APPENDICE IV: EXEMPLES DE MESURES DE SÉCURITÉ INDICATIVES APPLICABLES À CERTAINES INSTALLATIONS ET ACTIVITÉS 63

RÉFÉRENCES 69
DÉFINITIONS 71

1. INTRODUCTION

1.1. CONTEXTE

La présente publication énonce des orientations pour la mise en œuvre de mesures de sécurité concernant les sources radioactives. Elle donne aussi des conseils sur la mise en œuvre des dispositions de sécurité du Code de conduite sur la sûreté et la sécurité des sources radioactives [1] (ci-après dénommé « Code de conduite ») (voir la partie Définitions pour les explications des termes figurant dans la présente publication).

Le présent Guide d'application, bien qu'il remplace le document intitulé Radioactive Sources — Interim guidance for comment (IAEA-TECDOC-1355) [2], tient compte de l'approche générale de la sécurité établie dans cette publication et que certains États pourraient avoir utilisée comme référence dans la conception de leurs régimes de sécurité actuels. La présente publication, qui a été harmonisée avec la publication de l'AIEA intitulée Catégorisation des sources radioactives [3], propose une approche graduée de la sécurité basée sur des niveaux de sécurité et les fonctions de sécurité suivantes : dissuasion, détection, retardement, intervention et gestion de la sécurité.

Elle devrait se lire en liaison avec les publications suivantes : Code de conduite [1], Catégorisation des sources radioactives [3], Sûreté des générateurs de rayonnements et des sources radioactives scellées [4], Normes fondamentales internationales de protection contre les rayonnements ionisants et de sûreté des sources de rayonnements [5], et Principes fondamentaux de sûreté [6].

Enfin, le présent guide reconnaît la nécessité d'un équilibre entre la sécurité de la gestion des sources et l'utilisation sûre de ces sources par le personnel autorisé. Étant donné que les sources radioactives sont un outil intégré et essentiel des industries des soins de santé, de la fabrication, de la recherche et du contrôle de la qualité, il faut s'assurer que leurs nombreuses utilisations bénéfiques ne soient pas inutilement entravées. Le défi pour l'organisme de réglementation, les utilisateurs et les autres parties prenantes est de trouver le point d'équilibre approprié.

1.2. OBJECTIF

La présente publication est destinée à être utilisée par les États dans la formulation de leurs politiques de sécurité des sources radioactives et par les organismes de réglementation dans l'élaboration de prescriptions réglementaires conformes au Code de conduite. Elle aidera aussi les États parties à s'acquitter de certaines obligations dans le cadre de la Convention internationale pour la

répression des actes de terrorisme nucléaire [7]. Elle pourrait aussi s'avérer utile aux exploitants gérant des sources radioactives dans l'élaboration de programmes de sécurité.

1.3. CHAMP D'APPLICATION

La présente publication comprend des orientations et des mesures recommandées pour la prévention et la détection d'actes malveillants mettant en jeu des sources radioactives et pour l'intervention en cas de tels actes. Elle aidera aussi à prévenir la perte du contrôle de ces sources. Elle ne s'applique pas aux matières nucléaires telles que définies dans la Convention sur la protection physique des matières nucléaires et son amendement [8], à l'exception de celles contenant du plutonium 239.

Bien que le présent guide n'examine pas spécifiquement la question de la sécurité des matières radioactives non scellées, un État pourrait choisir d'appliquer les concepts et les mesures de sécurité qui y sont exposés à de telles matières.

La présente publication recommande l'application de mesures de sécurité aux sources radioactives en cours de fabrication, d'utilisation, et d'entreposage de courte ou de longue durée (voir la partie Définitions).

Le présent guide recommande que les mesures de sécurité soient appliquées sur une base graduée, en tenant compte de l'évaluation actuelle de la menace, de l'attractivité relative de la source et des conséquences potentielles de l'utilisation malveillante. On atteint le niveau de sécurité requis en combinant dissuasion, détection, retardement, intervention et gestion de la sécurité.

Les États pourraient décider que les risques pour certaines ou la totalité des sources sont plus ou moins élevés que la base d'élaboration du présent guide. Dans ces cas, les État devront faire montre de souplesse pour moduler les mesures de sécurité dont ils ont besoin par rapport à celles recommandées ici. Ce faisant, ils devront rester autant que possible dans le cadre de la structure générale du présent guide.

Celui-ci ne présente pas de recommandations sur la préparation et la conduite des interventions d'urgence, ni sur la remédiation des zones contaminées. Ces orientations figurent dans d'autres publications de l'AIEA [5, 9, 10]. Les orientations ayant trait à la protection des personnes contre les rayonnements après une attaque sont énoncées par la Commission internationale de protection radiologique [11].

Enfin, la présente publication n'examine pas la question des matières radioactives, y compris les sources radioactives, en cours de transport. Ces orientations, notamment pour les expéditeurs tiers, sont énoncées dans la référence [12].

2. RESPONSABILITÉS DE L'ÉTAT ET DE L'EXPLOITANT

2.1. INTRODUCTION

Le Code de conduite [1] établit que la sûreté et la sécurité des sources radioactives d'un État se fondent sur un système national de contrôle réglementaire efficace. La présente section donne d'autres orientations sur les responsabilités de l'État et de l'exploitant pour ce qui est de la sécurité des sources radioactives.

2.2. ÉTAT

Chaque État devra définir la menace nationale (voir la section 3.8.1). Ce processus doit commencer par une évaluation de celle-ci, qui consiste en une analyse établissant — au niveau national — les motivations, intentions et capacités crédibles d'agresseurs potentiels susceptibles de provoquer des dommages en se livrant au sabotage d'une installation ou à l'enlèvement non autorisé d'une source radioactive à des fins malveillantes. Les orientations en la matière sont traitées en détail dans la réf. [13].

Chaque État devra prendre les mesures appropriées pour faire en sorte que les sources radioactives qui se trouvent sur son territoire, ou sous sa juridiction ou son contrôle, soient sécurisées durant leur vie utile et au terme de celle-ci. Parmi ces mesures figurent la promotion d'une culture de sécurité pour les sources radioactives et la formation théorique et pratique adéquate du personnel des organismes de réglementation et des exploitants.

Pour encadrer la sécurité des sources radioactives, les États devront avoir une infrastructure législative et réglementaire nationale efficace en place qui :

— Prescrit des responsabilités gouvernementales et les attribue aux organismes pertinents, dont un organisme de réglementation indépendant, pour l'établissement, l'application et le maintien d'un régime qui assure la sécurité des sources radioactives ;
— Établit des prescriptions de sécurité pour les sources radioactives et comprend un système d'évaluation, d'octroi de licences et de coercition ou d'autres procédures de délivrance d'autorisations ;
— Confère aux exploitants la responsabilité première de la sécurité des sources radioactives ;
— Prévoit des mesures destinées à réduire la probabilité de tentatives d'actes malveillants ;

— Prévoit des mesures atténuant/réduisant au minimum les conséquences d'actes malveillants mettant en jeu des sources radioactives ;
— Établit des infractions punissables couvrant les actes malveillants mettant en jeu des sources radioactives ;

La mise en place et la gestion de l'infrastructure législative et réglementaire pour la sécurité des sources radioactives reposent sur la coopération efficace entre les divers organismes ayant des responsabilités gouvernementales. Ces derniers incluent le plus souvent l'organisme de réglementation, les services de renseignements, les ministères de l'intérieur, de la défense, du transport et des affaires étrangères d'un État ; les forces de l'ordre ; les douanes et les garde-côtes, ainsi que les autres organismes ayant des responsabilités dans le domaine de la sécurité.

Les États devront veiller à ce que l'organisme de réglementation dispose des ressources suffisantes, en termes de personnel et de financement, pour exercer ses fonctions réglementaires, qui incluent la mise en œuvre d'un programme d'inspection permettant de vérifier que la sécurité des sources radioactives est effectivement garantie. Ce programme d'inspection devrait être appuyé par des procédures écrites et exécuté par un personnel qualifié. La fréquence des inspections devrait dépendre du niveau de sécurité (voir la section 4.1) s'appliquant à la (aux) source(s) radioactive(s) et pourrait être établie compte tenu de la performance antérieure de l'exploitant quant au respect des prescriptions de sécurité. L'inspection des mesures de sécurité appliquées par un exploitant peut être effectuée à l'occasion des inspections de vérification de la conformité aux autres prescriptions réglementaires, concernant par exemple la sûreté, ou dans le cadre d'inspections indépendantes.

2.3. EXPLOITANTS

Les exploitants, en tant qu'entités autorisées, devraient avoir comme responsabilité première d'appliquer et de maintenir les mesures de sécurité qui s'appliquent aux sources radioactives conformément aux prescriptions nationales. Les exploitants peuvent, selon les prescriptions réglementaires des États, nommer ou engager par contrat une tierce partie pour exécuter les mesures et les tâches ayant trait à la sécurité des sources radioactives, même si l'exploitant autorisé devrait conserver la responsabilité capitale d'assurer le respect de la réglementation et l'efficacité des mesures et des tâches. De plus, les exploitants devraient veiller à ce que leur personnel et leurs sous-traitants soient correctement formés et respectent les prescriptions réglementaires, qui devraient inclure la fiabilité.

Les exploitants devraient vérifier, à intervalles définis, que les sources se trouvent à leur emplacement autorisé. Toute absence ou anomalie devrait sans délai faire l'objet d'une enquête et être signalée à l'organisme de réglementation. Des processus devraient être en place pour que les sources de catégories 1, 2 et 3 (voir la section 4.2.1) pour lesquelles les exploitants ont une autorisation puissent être identifiées et localisées.

Lorsque les organismes de réglementation en font la demande, les exploitants devraient procéder à des évaluations de la vulnérabilité (voir la partie Définitions) de leurs sources radioactives sur la base de la menace actuelle évaluée.

Les exploitants devraient promouvoir une culture de sécurité (voir la section 3.2) et établir un système de gestion en rapport avec les niveaux de sécurité (voir la section 4.1) pour veiller à ce que :

— Des politiques et procédures accordant à la sécurité un haut niveau de priorité soient établies ;
— Les problèmes de sécurité soient rapidement identifiés et corrigés d'une manière tenant compte de leur importance ;
— Les responsabilités de chacun en matière de sécurité soient clairement définies et que tous soient dûment formés, qualifiés et jugés dignes de confiance ;
— Les lignes hiérarchiques pour les décisions en matière de sécurité soient clairement définies ;
— Des dispositions organisationnelles et des lignes de communication soient établies pour permettre la bonne circulation des informations relatives à la sécurité dans toute l'organisation ;
— Les informations sensibles soient identifiées et protégées conformément à la réglementation nationale ;
— Les sources radioactives soient gérées, lorsque l'organisme de réglementation en fait la demande, conformément à un plan de sécurité (voir la partie Définitions).

3. CONCEPTS DE SÉCURITÉ

3.1. INTRODUCTION

La présente section expose les principes fondamentaux applicables à la sécurité des sources radioactives établis dans le Code de conduite [1] puis développe les concepts de sécurité, notamment les fonctions de sécurité de base

que sont la dissuasion, la détection, le retardement, l'intervention et la gestion de la sécurité (tableau 1).

3.2. CULTURE DE SÉCURITÉ

Une culture de sécurité dynamique et efficace devrait exister à tous les niveaux du personnel et de la direction des organismes exploitants.

TABLEAU 1. PRINCIPES TIRÉS DU CODE DE CONDUITE SUR LA SÉCURITÉ DES SOURCES RADIOACTIVES

Le Code de conduite établit les principes fondamentaux applicables à la sécurité des sources radioactives, dont plusieurs rentrent dans le cadre de la présente publication. En vertu de ces principes, chaque État doit :

- Prendre les mesures appropriées qui sont nécessaires pour faire en sorte que les sources radioactives soient « **sécurisées durant leur vie utile et au terme de celle-ci** » (paragraphe 7) ;
- « [I]nsister auprès des concepteurs, des fabricants (aussi bien ceux qui fabriquent les sources radioactives que ceux qui fabriquent les dispositifs auxquels ces dernières sont incorporées), des fournisseurs, des utilisateurs et de ceux qui gèrent les sources retirées du service sur **leurs responsabilités en ce qui concerne la sûreté et la sécurité des sources radioactives** » (paragraphe 15) ;
- « [D]éfinir la **menace nationale** et **évaluer sa vulnérabilité** par rapport à cette dernière pour les diverses sources utilisées sur son territoire en prenant en compte la possibilité d'une perte de contrôle d'une ou de plusieurs sources radioactives ou d'acte malveillant à l'encontre de telles sources » (paragraphe 16) ;
- Avoir établi une législation et une réglementation prévoyant des « prescriptions applicables aux **mesures de sécurité destinées à décourager, détecter et retarder** l'accès non autorisé à des sources radioactives, ou leur vol, leur perte, ou bien leur utilisation ou leur enlèvement non autorisés à tous les stades de la gestion » (paragraphe 19) ;
- Faire en sorte que « l'organisme de réglementation créé par sa législation soit habilité […] à assortir les autorisations qu'il délivre de conditions claires et sans ambiguïté, notamment de conditions concernant : […] viii) les mesures pour déterminer, le cas échéant, si les personnes participant à la gestion des sources radioactives sont **habilitées** à le faire ; et ix) la **confidentialité des informations** relatives à la sécurité des sources » (paragraphe 20) ;
- Faire en sorte que son organisme de réglementation soit habilité à **exiger un plan de sécurité ou une analyse de la situation en la matière, selon le cas, et favoriser l'instauration d'une culture de sécurité** chez toutes les personnes et dans tous les organismes qui s'occupent de la gestion des sources radioactives (paragraphes 20 et 22).

La culture de sécurité se caractérise par des croyances, des attitudes, des comportements et des systèmes de gestion qui, bien agencés, accroissent l'efficacité de la sécurité.

Elle se fonde sur la reconnaissance — par ceux qui interviennent dans la réglementation, la gestion ou la mise en œuvre d'installations ou d'activités mettant en jeu des sources radioactives, ou même par ceux sur lesquels ces activités pourraient avoir des incidences — qu'une menace crédible existe et que la sécurité est importante.

Les lecteurs du présent guide devraient aussi consulter la publication intitulée Culture de sécurité nucléaire [14], qui décrit les concepts et les éléments fondamentaux de la culture de sécurité.

La culture de sécurité peut être renforcée par des moyens divers, dont les suivants selon les cas :

— Confier la responsabilité de la sécurité des sources radioactives à un haut responsable tout en veillant à ce que le personnel sache qu'il s'agit d'une responsabilité partagée à tous les niveaux de l'organisation ;
— Documenter les responsabilités juridiques et réglementaires qui s'appliquent à l'exploitant en matière de sécurité et les porter à l'attention des responsables et du personnel concernés, et selon les besoins, de tous les employés et sous-traitants ;
— Assurer la sensibilisation aux menaces et la formation des responsables de la sécurité, du personnel d'intervention et de tout le personnel ayant des responsabilités secondaires en matière de sécurité ;
— Aborder des questions de sécurité dans des cours d'initiation destinés au personnel et aux sous-traitants ;
— Donner des instructions de sécurité et organiser régulièrement des réunions de sensibilisation à la sécurité pour le personnel et les sous-traitants, dispenser une formation et évaluer les enseignements tirés ;
— Effectuer régulièrement des tests de performance et des activités de maintenance préventive.

3.3. OBJET D'UN SYSTÈME DE SÉCURITÉ

Un système de sécurité devrait être conçu par les spécialistes de la sécurité de l'exploitant pour dissuader un agresseur de commettre un acte malveillant ou pour réduire au minimum, au moyen de la détection, du retardement et de l'intervention, la probabilité que l'agresseur parvienne à mener à son terme un tel acte. Celui-ci consisterait en une série d'actions posées par un ou plusieurs agresseurs (menace)

pour avoir accès à une source (cible) afin de commettre un acte de sabotage, ou un autre acte malveillant, ou d'enlever la source sans autorisation.

3.4. FONCTIONS DE SÉCURITÉ

Un système de sécurité destiné à protéger les sources radioactives d'un acte malveillant qu'entend commettre un agresseur devrait être conçu pour remplir les fonctions de sécurité de base que sont la dissuasion, la détection, le retardement, l'intervention et la gestion de la sécurité :

— La ***dissuasion*** consiste à dissuader un agresseur, qui a par ailleurs une motivation à commettre un acte malveillant, de tenter un tel acte. Les mesures dissuasives ont pour effet de le convaincre que cet acte serait trop difficile à réaliser, que sa réussite serait trop incertaine ou que ses conséquences seraient trop désagréables pour lui pour en justifier l'exécution. Les mesures conçues expressément aux fins de la dissuasion consistent donc à faire savoir à l'agresseur qu'il existe des mesures remplissant les autres fonctions de sécurité. Si cette information produit l'effet escompté, le résultat est la dissuasion.

— La ***détection*** est la découverte d'une intrusion, tentée ou effective, qui pourrait avoir comme objectif l'enlèvement non autorisé ou le sabotage d'une source radioactive. Les moyens utilisés à cette fin sont notamment l'observation visuelle, la surveillance vidéo, les capteurs électroniques, les relevés comptables, les scellés et autres dispositifs d'indication de fraude, les systèmes de surveillance des processus et d'autres procédés. Les mesures de détection peuvent en outre être dissuasives si l'agresseur en a connaissance.

— Le ***retardement*** empêche un agresseur de tenter d'obtenir un accès non autorisé ou d'enlever ou de saboter une source radioactive, généralement au moyen de barrières ou d'autres moyens physiques. Une mesure de retardement correspond au temps dont a besoin un agresseur, après la détection, pour enlever ou saboter la source radioactive. Les barrières de retardement peuvent en outre être dissuasives si l'agresseur en a connaissance.

— L'***intervention*** comprend les mesures prises après détection pour faire échouer un agresseur ou pour atténuer les conséquences potentiellement graves. Ces mesures, exécutées en règle générale par le personnel de sécurité ou les forces de l'ordre, et d'autres organismes nationaux, consistent notamment à interrompre et maîtriser l'agresseur au cours de la tentative d'enlèvement non autorisé ou de sabotage, à l'empêcher d'utiliser

la source radioactive pour provoquer des conséquences néfastes, à récupérer celle-ci ou, à défaut, à réduire la gravité des conséquences. La perspective de succès d'une intervention peut aussi être dissuasive.

— La ***gestion de la sécurité*** consiste notamment à assurer des ressources suffisantes (humaines et financières) adéquates pour la sécurité des sources. Elle comprend en outre l'élaboration des procédures, politiques, relevés et plans pour assurer la sécurité des sources et, de manière générale, une culture de sécurité plus efficace. Cette expression inclut en outre la mise au point de procédures visant le traitement approprié des informations sensibles et leur protection contre toute divulgation non autorisée.

3.5. CONCEPTION ET ÉVALUATION DES SYSTÈMES DE SÉCURITÉ

Un système de sécurité bien conçu devrait intégrer des mesures permettant de remplir toutes les cinq fonctions de sécurité, de manière à protéger efficacement la cible de la menace, conformément aux principes de sécurité suivants :

La *dissuasion n'est pas mesurable* : elle a pour objectif de dissuader un agresseur de tenter un acte malveillant. Ainsi, l'impact des mesures de dissuasion ne peut être quantifié. La conception d'un système de sécurité ne devrait donc pas reposer entièrement sur la dissuasion.

La détection précède le retardement : le retardement a pour fonction de laisser au personnel d'intervention suffisamment de temps pour se déployer et interrompre ou intercepter la tentative de l'agresseur de mener à son terme un acte malveillant. La détection doit donc précéder le retardement. Si un agresseur peut franchir les barrières et autres obstacles avant d'atteindre les détecteurs d'intrusion ou d'autres moyens de détection, il aura accompli le plus difficile avant d'être détecté et pourrait bien réussir à enlever ou à saboter la source radioactive avant l'arrivée du personnel d'intervention. Dans ce cas, les barrières ne sont plus un moyen de retardement mais tout au plus une mesure de dissuasion.

La détection appelle une évaluation : la plupart des moyens de détection donne des indices indirects d'actes malveillants potentiels tels que des tentatives d'accès non autorisé, d'enlèvement ou de sabotage d'une source radioactive. Le seul indice direct est l'observation directe par le personnel. Par conséquent, lorsqu'une alerte ou tout autre indice indirect se déclenche, il y a toujours un certain degré d'incertitude quant à sa cause. La détection devrait donc toujours être complétée par une évaluation visant à déterminer la cause de l'alerte. L'évaluation de celle-ci requiert une observation ou un jugement humains par le déploiement de personnel d'intervention pour en rechercher la cause à l'aide de systèmes de télévision en circuit fermé commandé à distance ou de moyens semblables. Parfois, les agresseurs peuvent essayer de profiter du laps de temps

entre la détection et l'évaluation pour dissimuler leur dessein malveillant. Une évaluation immédiate est donc l'objectif de tout système de sécurité.

La durée du retardement dépasse celles de l'évaluation et de l'intervention réunies : un système de sécurité est efficace s'il détecte une tentative d'acte malveillant et que celle-ci est correctement évaluée suffisamment rapidement pour les mesures de retardement et pour permettre au personnel d'intervention d'interrompre et de stopper l'agresseur avant qu'il ne mène l'acte à son terme ou d'engager sans délai des mesures visant à atténuer les conséquences potentiellement graves. Ce rapport entre les fonctions de détection, de retardement et d'intervention est appelé *détection en temps voulu*.

La protection équilibrée : concept des fonctions de sécurité équivalentes (dissuasion, détection, retardement, intervention et gestion de la sécurité) assurant une protection adéquate contre toutes les menaces à tous les niveaux d'accès possibles. Autrement dit, les durées de retardement à tous les niveaux d'accès, les mesures de détection associées à chaque aspect de la détection et les mesures d'intervention qui en résultent fournissent la protection nécessaire pour empêcher le succès d'un acte.

La défense en profondeur : concept mettant en jeu plusieurs niveaux et modalités de protection (qu'ils soient structurels ou techniques, concernant le personnel ou organisationnels) que doit surmonter ou contourner un agresseur pour atteindre ses objectifs.

3.6. INTÉGRATION DES MESURES DE SÛRETÉ ET DES MESURES DE SÉCURITÉ

Les mesures de sûreté et les mesures de sécurité ont pour objectif commun de protéger les vies et la santé humaines ainsi que l'environnement. Ces mesures devraient être conçues et mises en œuvre de manière intégrée de sorte que les mesures de sécurité ne portent pas préjudice à la sûreté et que les mesures de sûreté ne portent pas préjudice à la sécurité. Lors de l'application des recommandations figurant dans le présent guide, les concepteurs des systèmes de sécurité devraient consulter des experts de la sûreté qualifiés pour s'assurer que les mesures de sécurité ne portent pas préjudice à la sûreté des personnes ni à la protection de l'environnement.

3.7. APPROCHE GRADUÉE DE LA SÉCURITÉ

Les prescriptions de sécurité devraient être basées sur une approche graduée tenant compte de l'évaluation actuelle de la menace, de l'attractivité

relative d'une source radioactive, de la nature de la source et des conséquences qui pourraient résulter de son enlèvement non autorisé ou de son sabotage. Cette approche graduée garantit que les sources à haut risque bénéficient du niveau de sécurité le plus élevé.

3.8. COMPRÉHENSION ET PRISE EN COMPTE DU CONTEXTE DE LA MENACE

La conception et l'évaluation d'un système de sécurité devraient tenir compte de l'évaluation actuelle de la menace nationale et pourraient comprendre la définition et l'application d'une menace de référence (voir la partie Définitions).

3.8.1. Évaluation de la menace nationale

Le Code de conduite dispose :

> « Chaque État devrait définir la menace nationale et évaluer sa vulnérabilité par rapport à cette dernière pour les diverses sources utilisées sur son territoire en prenant en compte la possibilité d'une perte de contrôle d'une ou de plusieurs sources radioactives ou d'acte malveillant à l'encontre de telles sources ».

Pour respecter ce principe, l'État devrait commencer par évaluer la menace nationale, soit une analyse consignant par écrit — au niveau national — les motivations, intentions et capacités crédibles d'agresseurs potentiels susceptibles de provoquer des dommages en se livrant au sabotage d'une installation ou à l'enlèvement non autorisé d'une source radioactive à des fins malveillantes. Cette évaluation est généralement réalisée par les services de renseignements de l'État, souvent avec le concours d'organismes comme les ministères de l'intérieur, de la défense, des transports et des affaires étrangères ; les forces de l'ordre ; les douanes et les garde-côtes ; et d'autres organismes ayant des responsabilités en matière de sécurité, y compris éventuellement l'organisme de réglementation. S'il n'a jamais participé à cette évaluation auparavant, celui-ci devrait être informé de la menace telle qu'elle est actuellement évaluée par les organismes nationaux compétents afin d'en tenir compte dans l'élaboration de son programme réglementaire pour la sécurité des sources radioactives.

Le processus d'évaluation est un raisonnement déductif. À partir de ce que l'on sait, on émet un avis sur la manière dont un groupe d'agresseurs ou un agresseur pourrait se comporter à l'avenir. Cela pourrait concerner, par exemple, des événements passés et des capacités connues d'attaque des types d'installations

où des sources radioactives sont entreposées ou utilisées. L'évaluation de la menace devrait au moins couvrir, pour chaque agresseur d'origine interne ou externe, les moyens et caractéristiques suivants :

— *Motivation*. Politique, financière, idéologique, personnelle
— *Niveau d'engagement*. Indifférence de l'agresseur à l'égard de sa santé, de sa sûreté, de son bien-être et de sa survie.
— *Intentions*. Sabotage de matières (enlèvement non autorisé) ou d'installations, panique et perturbations au sein de la population, instabilité politique, nombreux morts et blessés.
— *Taille du groupe*. Force d'attaque, coordination, appui.
— *Armes*. Types, nombre, disponibilité, armes improvisées.
— *Outils*. Mécaniques, thermiques, manuels, électriques, électroniques, électromagnétiques, appareils de communication..
— *Modes de transport*. Publics, privés, terrestres, maritimes, aériens, types, nombre, disponibilité.
— *Compétences techniques*. Ingénierie, utilisation d'explosifs et de produits chimiques, expérience paramilitaire, capacités de communication.
— *Cybercompétences*. Utilisation d'ordinateurs et de systèmes de contrôle automatisés pour appuyer directement des attaques physiques, rassembler des renseignements, mener des cyberattaques, recueillir des fonds, etc.
— *Connaissances*. Cibles, plans et procédures de site, mesures de sécurité, procédures de sûreté et de radioprotection, opérations, utilisation possible de matières nucléaires ou d'autres matières radioactives.
— *Financement*. Source, montant, disponibilité.
— *Questions concernant les agresseurs d'origine interne*. Collusion, passifs/actifs, violents/non violents, nombre
— *Structure d'appui*. Sympathisants locaux, organisation d'appui, logistique.
— *Tactique*. Secrètes ou manifestes.

Une fois qu'il aura évalué sa menace nationale, l'État devra décider d'une base pour établir les réglementations relatives à la sécurité des sources radioactives. Une approche consiste à les élaborer en se fondant sur l'évaluation de la menace nationale, tandis qu'une autre consiste à les établir sur la base de la menace de référence (voir ci-dessous), en se servant de l'évaluation de la menace nationale. Lors du choix d'une base de réglementation, l'État devra prendre en compte plusieurs facteurs, y compris la gravité des conséquences liées aux actes malveillants mettant en jeu des sources radioactives dans l'État, la détermination par l'État de la capacité d'établir des systèmes de protection efficaces grâce à chacune de ces approches et la capacité de l'organisme de réglementation de mettre en œuvre les différentes approches.

Il convient de noter que tous les États n'ont pas besoin de recourir à une approche fondée sur la menace de référence pour leur système de réglementation. Cependant, si un État n'utilise pas cette approche, il devra tout de même procéder à une évaluation de la menace nationale et la tenir à jour.

3.8.2. Menace de référence

La menace de référence, définie au niveau de l'État, est un outil qui aide à déterminer les prescriptions en matière de performance pour la conception de systèmes de protection physique de certains types d'installations. Elle est aussi utilisée par les exploitants et les autorités nationales pour évaluer l'efficacité des systèmes à contrer des agresseurs en mesurant la performance de ces systèmes au regard des capacités des agresseurs décrits dans la menace, et en effectuant des évaluations de la vulnérabilité. Une menace de référence est une description détaillée des motivations, intentions et capacités des agresseurs potentiels en fonction desquels les systèmes de protection sont conçus et évalués. Les capacités de l'agresseur — qu'il soit d'origine interne ou externe — aident à déterminer les prescriptions en matière de détection, de retardement et d'intervention nécessaires pour qu'un système de protection physique soit efficace contre une menace de référence.

La définition d'une menace de référence sera propre à chaque État du fait des différences sociales, culturelles et géopolitiques. Comme dans le cas de l'évaluation de la menace nationale, la définition d'une menace de référence requiert en principe les efforts combinés des autorités nationales, comme les services de renseignements et de sécurité, les forces de l'ordre et les organismes de réglementation, ainsi que des exploitants. La menace de référence devra éventuellement être réexaminée de temps en temps à la lumière des nouvelles informations fournies par les organismes nationaux. On trouvera de plus amples informations sur le processus d'établissement de la menace de référence dans la réf. [13].

3.8.3. Menaces d'origine interne

Il convient d'accorder une attention particulière aux menaces d'origine interne lors de la conception d'un système de sécurité. Ces menaces peuvent émaner d'une ou plusieurs personnes ayant légitimement accès à une installation et connaissant bien les activités ou les emplacements des sources. Il peut s'agir d'employés ou de sous-traitants qui pourraient enlever des sources radioactives ou soustraire des informations à des fins malveillantes, ou de se livrer à des actes de sabotage dans les locaux. En outre, des personnes peuvent chercher un emploi dans une installation dans l'intention de commettre des actes malveillants et aider

des agresseurs d'origine externe à enlever des sources ou à exécuter des actes malveillants. Les menaces d'origine interne et les contre-mesures appropriées recommandées sont expliquées plus en détail dans la réf. [15].

3.8.4. Menace accrue

Un système de sécurité devrait permettre de contrer efficacement la menace présente évaluée. Il faudrait toutefois prévoir des dispositions permettant de renforcer temporairement le niveau de sécurité en cas de menace accrue. Ces dispositions devraient comprendre l'introduction de mesures de sécurité supplémentaires ou la limitation de l'accessibilité des sources radioactives.

3.9. ÉVALUATION DE LA VULNÉRABILITÉ

L'évaluation de la vulnérabilité, aussi appelée expertise de sécurité ou évaluation de la sécurité, est une méthode utilisée pour évaluer les systèmes de sécurité de protection. C'est une évaluation systématique de l'efficacité d'un système de sécurité pour la protection contre une menace évaluée (ou une menace de référence, le cas échéant). Elle peut être de nature spécifique ou générale, réalisée au niveau local par l'exploitant ou par l'État/l'organisme de réglementation et être utilisée pour aider l'État/l'organisme de réglementation à élaborer des réglementations ou pour démontrer que l'exploitant se conforme aux règlements. L'appendice III donne de plus amples informations sur la manière d'effectuer une évaluation de la vulnérabilité.

4. ÉTABLISSEMENT D'UN PROGRAMME RÉGLEMENTAIRE POUR LA SÉCURITÉ DES SOURCES RADIOACTIVES

Les dispositions du Code de conduite relatives à la sécurité des sources radioactives ont été renforcées par l'introduction de mesures visant à réduire la probabilité d'actes malveillants. En outre, le Code dispose spécifiquement que les États devraient tenir dûment compte des sources radioactives qu'ils jugent susceptibles d'avoir des conséquences inacceptables si elles sont utilisées à des fins malveillantes. Au cas où un tel événement se produirait, des prescriptions et des orientations concernant la préparation et la conduite des interventions

d'urgence et la remédiation des zones contaminées sont disponibles dans des publications de l'AIEA [5, 9, 10]. Les orientations ayant trait à la protection des personnes contre les rayonnements après une attaque radiologique sont énoncées par la Commission internationale de protection radiologique [11].

Ces actes malveillants et leurs éventuelles conséquences pourraient comprendre :

— Le placement délibéré d'une source endommagée ou non protégée dans un lieu public ;
— La dispersion délibérée de matières radioactives pour causer des effets sanitaires nocifs (par l'utilisation, par exemple, d'un engin à dispersion de radioactivité (EDR)) ;
— Le recours à un EDR pour contaminer des sols, des bâtiments et des infrastructures, avec comme conséquence l'interdiction totale de l'accès à ces zones compte tenu des critères de radioprotection, de l'incidence économique et du coût de l'assainissement et de la reconstruction.

De nombreux États ont déjà un programme réglementaire en place qui couvre des activités telles que l'autorisation, l'examen et l'évaluation, l'inspection et la coercition [16]. La présente section donne aux organismes de réglementation des orientations sur la manière d'élaborer ou d'améliorer des programmes réglementaires pour assurer la sécurité des sources radioactives afin de réduire la probabilité d'actes malveillants mettant en jeu ces sources. Les mesures de sûreté et de sécurité devraient être conçues et mises en œuvre de manière intégrée pour ne pas se porter mutuellement préjudice.

L'élaboration d'un tel programme réglementaire pour la sécurité des sources radioactives par l'organisme de réglementation comprend trois étapes principales :

— **Étape 1** : Établir des niveaux de sécurité gradués avec des buts et des objectifs pour chaque niveau (voir la section 4.1).
— **Étape 2** : Déterminer le niveau de sécurité applicable à une source donnée (voir la section 4.2).
— **Étape 3** : Choisir et mettre en œuvre une approche réglementaire (basée sur les prescriptions, les résultats ou les deux) pour guider les exploitants dans la conception, l'application et l'évaluation des mesures de sécurité afin de répondre aux objectifs de sécurité énoncés dans le tableau 1 (voir la section 4.3).

4.1. ÉTAPE 1 : ÉTABLIR DES NIVEAUX DE SÉCURITÉ GRADUÉS AVEC DES BUTS ET DES OBJECTIFS POUR CHAQUE NIVEAU

Les sources radioactives ont des caractéristiques très variées (telles que l'activité) qui les rendent intéressantes à divers degrés aux yeux des agresseurs. Il convient de recourir, à l'aide d'une approche graduée, à des mesures de sécurité efficaces tout aussi variées pour garantir que ces sources sont convenablement protégées. Le concept de niveaux de sécurité permet d'assurer des capacités de sécurité adéquates sans imposer de mesures excessivement restrictives. Trois niveaux de sécurité (A, B et C) ont été établis pour permettre de définir précisément la performance du système de sécurité de manière graduée. Le niveau A correspond au degré de sécurité le plus élevé et les deux autres à des degrés progressivement décroissants.

À chaque niveau de sécurité correspond un but. Celui-ci définit le résultat général que le système de sécurité devrait être en mesure d'obtenir pour un niveau de sécurité donné. Voici les buts qui ont été définis :

— **Niveau de sécurité A** : *empêcher* l'enlèvement non autorisé d'une source.
— **Niveau de sécurité B** : *réduire au minimum la probabilité* d'un enlèvement non autorisé d'une source.
— **Niveau de sécurité C** : *réduire la probabilité* d'un enlèvement non autorisé d'une source.

Les actes malveillants peuvent consister soit en un enlèvement non autorisé d'une source soit en un acte de sabotage. Si les buts de sécurité ne concernent que l'enlèvement non autorisé, leur réalisation permettra de réduire les chances de succès d'un acte de sabotage. Les systèmes de sécurité qui atteignent les buts énumérés ci-dessus donneront une certaine capacité (quoique limitée) de détecter un acte de sabotage et d'intervenir.

Afin de satisfaire aux *buts*, il faut atteindre un niveau de performance adéquat pour chacune des *fonctions* de sécurité : dissuasion, détection, retardement, intervention et gestion de la sécurité. Ce niveau de performance est défini comme un ensemble d'*objectifs* pour chacune des fonctions. Ces objectifs indiquent le résultat souhaité de la combinaison des *mesures* appliquées pour les atteindre. La dissuasion est une fonction de sécurité difficile à quantifier. On ne lui a donc affecté aucun ensemble d'objectifs et de mesures de sécurité dans la présente publication.

Les niveaux de sécurité et les objectifs de sécurité correspondants sont résumés dans le tableau 2.

TABLEAU 2. NIVEAUX DE SÉCURITÉ ET OBJECTIFS DE SÉCURITÉ

Fonctions de sécurité	Objectifs de sécurité		
	Niveau de sécurité A But : empêcher l'enlèvement non autorisé[a]	Niveau de sécurité B But : réduire au minimum la probabilité d'un enlèvement non autorisé[a]	Niveau de sécurité C réduire la probabilité d'un enlèvement non autorisé[a]
Détection	Assurer la détection immédiate de tout accès non autorisé à la zone sécurisée/ l'emplacement de la source		
	Assurer la détection immédiate de toute tentative d'enlèvement non autorisé de la source, y compris par un agresseur d'origine interne	Assurer la détection de toute tentative d'enlèvement non autorisé de la source	Assurer la détection de tout enlèvement non autorisé de la source
	Fournir immédiatement une évaluation de la détection		
	Assurer immédiatement la communication avec le personnel d'intervention		
	Fournir un moyen de détecter une perte de source par le biais de la vérification		
Retardement	Assurer un retardement suffisant après la détection pour permettre au personnel d'intervention d'interrompre un enlèvement non autorisé	Assurer un retardement pour réduire le plus possible la probabilité d'un enlèvement non autorisé	Assurer un retardement pour réduire la probabilité d'un enlèvement non autorisé
Intervention	En cas d'alarme évaluée, assurer une intervention immédiate avec suffisamment de ressources pour interrompre et empêcher l'enlèvement non autorisé	Déclencher immédiatement l'intervention pour interrompre l'enlèvement non autorisé	Mettre en œuvre les mesures appropriées en cas d'enlèvement non autorisé d'une source
Gestion de la sécurité	Assurer des contrôles de l'accès à l'emplacement de la source pour limiter efficacement l'accès aux seules personnes autorisées		
	S'assurer que les personnes autorisées sont dignes de confiance		
	Déterminer et protéger les informations sensibles		
	Prévoir un plan de sécurité		
	Assurer une capacité de gérer les événements de sécurité couverts par le plan d'intervention spécialisé sur la sécurité (voir la partie Définitions)		
	Mettre en place un système de notification d'événements de sécurité		

[a] La réalisation de ces buts permettra également de réduire les chances de succès d'un acte de sabotage.

Lorsqu'un objectif correspond à deux ou plusieurs niveaux de sécurité dans le tableau 2, il est censé être atteint de manière plus rigoureuse au niveau de sécurité plus élevé.

4.2. ÉTAPE 2 : DÉTERMINER LE NIVEAU DE SÉCURITÉ APPLICABLE À UNE SOURCE DONNÉE

Pour spécifier un niveau de sécurité approprié pour une source, il faudrait tenir compte des dommages potentiels qu'elle peut causer si elle est utilisée dans un acte malveillant. Ces dommages potentiels guideront alors le processus d'affectation d'un niveau de sécurité approprié à la source. Ce processus comprend les étapes suivantes :

— La catégorisation des sources basée sur les dommages potentiels qu'elles peuvent causer si elles sont utilisées à des fins malveillantes (y compris le regroupement de sources dans un lieu donné comme approprié) (voir la section 4.2.1) ;
— L'affectation d'un niveau de sécurité approprié à chaque catégorie (voir la section 4.2.2).

4.2.1. Catégorisation des sources radioactives

Le Code de conduite s'applique à toutes les sources radioactives qui peuvent présenter un risque important pour les personnes, la société et l'environnement, c'est-à-dire les sources des catégories 1 à 3. Des mesures de sécurité appropriées devraient être appliquées pour réduire la probabilité d'actes malveillants mettant en jeu ces sources.

La catégorisation des sources utilisée dans le Code de conduite est basée sur le concept de « sources dangereuses », lesquelles sont quantifiées en termes de valeurs D [17]. Ce concept est examiné plus en détail dans la publication de l'AIEA Catégorisation des sources radioactives [3]. La présente publication donne un système de catégorisation recommandé, en particulier pour les sources utilisées dans l'industrie, en médecine, en agriculture, et dans la recherche et l'enseignement. Ce système peut aussi être appliqué aux sources, selon que de besoin, dans le contexte national, dans le cadre de programmes militaires ou de défense. La catégorisation, qui fournit une base harmonisée au plan international pour la prise de décisions en fonction des risques, est fondée sur une méthode logique et transparente suffisamment souple pour pouvoir être appliquée dans des circonstances très variées. Les décisions peuvent être prises en fonction des

risques grâce à une approche graduée du contrôle réglementaire des sources radioactives aux fins de la sûreté et de la sécurité.

Compte tenu de l'importance primordiale de la santé humaine, le système de catégorisation est essentiellement basé sur les effets déterministes potentiels des sources sur la santé. La valeur D est l'activité spécifique du radionucléide d'une source qui, si elle n'est pas sous contrôle, pourrait causer des effets déterministes graves pour une série de scénarios comprenant à la fois une exposition externe à une source non protégée et une exposition fortuite interne à la suite d'une dispersion (par exemple par un incendie ou une explosion) de la source.

L'activité de la matière radioactive (A) des sources varie sur de nombreux ordres de grandeur ; les valeurs D sont donc utilisées pour normaliser la gamme d'activités et permettre d'avoir une référence en vue de comparer les risques. Pour ce faire, il faudrait diviser l'activité A de la source (en TBq) par la valeur D pour le radionucléide pertinent.

Il conviendrait de noter qu'une quantité de matière inférieure à celle correspondant à la valeur D peut être dangereuse [17]. Ce peut être le cas avec une administration malveillante de matières radioactives non scellées à un individu.

Les seuils de radioactivité pour les radionucléides mentionnés dans le Code de conduite pour les sources des catégories 1 à 3 sont indiqués dans le tableau 3. Pour les radionucléides ne figurant pas dans ce tableau, voir les réf. [3, 17].

Dans certaines situations, il pourrait s'avérer approprié de catégoriser une source sur la base du seul rapport A/D, par exemple lorsque l'utilisation prévue de la source est inconnue ou n'est pas confirmée. Toutefois, lorsque les circonstances de l'utilisation de la source sont connues, l'organisme de réglementation pourrait faire preuve de discernement pour modifier la catégorisation initiale en se servant des autres informations relatives à la source ou à son utilisation. Dans certaines circonstances, on pourrait s'accommoder d'affecter une catégorie sur la base de l'utilisation prévue de la source (voir le tableau 4).

Le système de catégorisation comprend cinq catégories, comme indiqué au tableau 4. Ce nombre de catégories devrait suffire pour permettre d'appliquer pratiquement le système sans précision inutile. Dans le cadre de ce système de catégorisation, les sources de catégorie 1 sont considérées comme étant les plus « dangereuses » car elles peuvent constituer un risque très élevé pour la santé humaine si elles ne sont pas gérées de manière sûre et sécurisée. Une exposition de seulement quelques minutes à une source de catégorie 1 non protégée peut être fatale. En bas de l'échelle du système de catégorisation se trouvent les sources de catégorie 5, les moins dangereuses. Toutefois, même ces sources peuvent donner lieu à des doses supérieures aux limites de doses si elles ne sont pas correctement

TABLEAU 3. ACTIVITÉS CORRESPONDANT AUX SEUILS DES CATÉGORIES

Radionucléide	Catégorie1 1000 × D		Catégorie 2 10 × D		Catégorie 3 D	
	(TBq)	(Ci)[a]	(TBq)	(Ci)[a]	(TBq)	(Ci)[a]
Am-241	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Am-241/Be	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Cf-252	2.E+01	5.E+02	2.E-01	5.E-00	2.E-02	5.E-01
Cm-244	5.E+01	1.E+03	5.E-01	1.E+01	5.E-02	1.E+00
Co-60	3.E+01	8.E+02	3.E-01	8.E+00	3.E-02	8.E-01
Cs-137	1.E+02	3.E+03	1.E+00	3.E+01	1.E-01	3.E+00
Gd-153	1.E+03	3.E+04	1.E+01	3.E+02	1.E+00	3.E+01
Ir-192	8.E+01	2.E+03	8.E-01	2.E+01	8.E-02	2.E+00
Pm-147	4.E+04	1.E+06	4.E+02	1.E+04	4.E+01	1.E+03
Pu-238	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Pu-239[b]/Be	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Ra-226	4.E+01	1.E+03	4.E-01	1.E+01	4.E-02	1.E+00
Se-75	2.E+02	5.E+03	2.E+00	5.E+01	2.E-01	5.E+00
Sr-90 (Y-90)	1.E+03	3.E+04	1.E+01	3.E+02	1.E+00	3.E+01
Tm-170	2.E+04	5.E+05	2.E+02	5.E+03	2.E+01	5.E+02
Yb-169	3.E+02	8.E+03	3.E+00	8.E+01	3.E-01	8.E+00
Au-198*	2.E+02	5.E+03	2.E+00	5.E+01	2.E-01	5.E+00
Cd-109*	2.E+04	5.E+05	2.E+02	5.E+03	2.E+01	5.E+02
Co-57*	7.E+02	2.E+04	7.E+00	2.E+02	7.E-01	2.E+01
Fe-55*	8.E+05	2.E+07	8.E+03	2.E+05	8.E+02	2.E+04
Ge-68*	7.E+02	2.E+04	7.E+00	2.E+02	7.E-01	2.E+01
Ni-63*	6.E+04	2.E+06	6.E+02	2.E+04	6.E+01	2.E+03
Pd-103*	9.E+04	2.E+06	9.E+02	2.E+04	9.E+01	2.E+03
Po-210*	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Ru-106 (Rh-106)*	3.E+02	8.E+03	3.E+00	8.E+01	3.E-01	8.E+00
Tl-204*	2.E+04	5.E+05	2.E+02	5.E+03	2.E+01	5.E+02

[a] Les principales valeurs à utiliser sont données en TBq. Les valeurs en curies sont données à des fins pratiques et sont arrondies après conversion.

[b] Il faudra prendre en considération les questions de criticité et de garanties pour les multiples de D.

* Étant donné qu'il est très peu probable que ces radionucléides soient utilisés dans des sources radioactives à un niveau d'activité qui amènerait à les classer dans les catégories 1, 2 ou 3, ils ne seront donc régis ni par les dispositions du paragraphe du Code consacré aux registres nationaux, ni par celles des paragraphes traitant du contrôle des importations et des exportations

TABLEAU 4. CATÉGORIES POUR LES SOURCES COMMUNÉMENT UTILISÉES

Catégoie	Source[a]	A/D[b]
1	Générateurs thermoélectriques à radio-isotopes (GTR) Irradiateurs Sources de téléthérapie Sources fixes en téléthérapie multifaisceaux (scalpel gamma)	$A/D \geq 1000$
2	Sources de gammagraphie industrielle Sources de curiethérapie à débit de dose élevé/moyen	$1000 > A/D \geq 10$
3	Jauges industrielles fixes comprenant des sources de haute activité[c] Sondes de diagraphie	$10 > A/D \geq 1$
4	Curiethérapie à faible débit de dose (sauf plaques ophtalmiques et implants permanents) Jauges industrielles ne comprenant pas de sources de haute activité Ostéodensitomètres Éliminateurs de charges statiques	$1 > A/D \geq 0{,}01$
5	Sources de curiethérapie à faible débit de dose : plaques ophtalmiques et implants permanents Dispositifs à fluorescence X Dispositifs à capture d'électrons Sources de spectrométrie Mössbauer Sources de référence pour la tomographie à émission de positons (PET)	$0{,}01 > A/D$ et A > niveaux d'exemption[d]

[a] Des facteurs autres que le seul rapport A/D ont été pris en considération pour l'affectation de ces sources à une catégorie (voir réf. [3], annexe I).

[b] Cette colonne peut être utilisée pour déterminer la catégorie d'une source uniquement sur la base du rapport A/D. Cela peut être approprié, par exemple si les installations et les activités ne sont pas connues ou indiquées, si les sources ont une courte période et/ou ne sont pas scellées, ou si les sources sont regroupées (voir réf. [3], paragraphe 3.5)

[c] Des exemples sont donnés dans la réf. [3], annexe I.

[d] Les niveaux d'exemption sont indiqués à l'appendice I de la réf. [5].

contrôlées. Elles devraient donc être soumises à un contrôle réglementaire approprié. Il faudrait éviter de subdiviser les catégories car cela aboutirait à un degré de précision inutile et pourrait porter préjudice à l'harmonisation internationale.

4.2.1.1. Sources non recensées

En ce qui concerne les sources non recensées dans le tableau 4, l'organisme de réglementation peut leur attribuer une catégorie sur la base du rapport *A/D*.

4.2.1.2. Radionucléides à courte période

Dans le cadre de certaines activités, comme en médecine nucléaire, les radionucléides à courte période sont utilisés dans un type de source non scellée. Des exemples de telles applications comprennent les isotopes ^{99m}Tc en radiodiagnostic et ^{131}I en radiothérapie. Dans ces situations, les principes du système de catégorisation pourraient s'appliquer afin de déterminer une catégorie pour la source. Ces situations devraient être examinées au cas par cas.

4.2.1.3. Sources radioactives non scellées

L'organisme de réglementation peut affecter une catégorie aux sources radioactives non scellées sur la base du rapport *A/D.*

4.2.1.4. Décroissance radioactive

Si l'activité d'une source décroît à un niveau inférieur au seuil approprié figurant dans le tableau 3 ou en-deçà de celui normalement utilisé (tel qu'indiqué dans le tableau 4), l'organisme de réglementation peut autoriser l'exploitant à catégoriser à nouveau la source sur la base du rapport A/D.

4.2.1.5. Regroupement de sources

Il y aura des situations dans lesquelles les sources radioactives seront très près les unes des autres, comme dans les processus de fabrication (par exemple dans la même salle ou le même bâtiment) ou dans des installations d'entreposage (par exemple dans la même enceinte). Dans ces circonstances, l'organisme de réglementation peut souhaiter regrouper l'activité des sources pour déterminer une catégorisation propre à une situation aux fins de la mise en œuvre des mesures de contrôle réglementaire. Dans ce type de situation, il conviendrait de diviser la somme des activités du radionucléide par la valeur D appropriée et de comparer le rapport A/D calculé aux rapports A/D indiqués dans le tableau 2, ce qui permet de catégoriser la série de sources sur la base de l'activité. Si des sources contenant divers radionucléides sont regroupées, alors il faudrait utiliser la somme des rapports A/D pour déterminer la catégorie conformément à la formule :

$$\text{A/D total} = \sum_n \frac{\sum_i A_{i,n}}{D_n}$$

où :

$A_{i,n}$ = activité de chaque source i de radionucléide n.
D_n = valeur D pour le radionucléide n.

De plus amples informations sur le regroupement des sources radioactives figurent dans la réf. [3].

4.2.2. Affectation des niveaux de sécurité

Comme arrangement par défaut, l'organisme de réglementation pourrait utiliser les catégories énumérées ci-dessus pour affecter le niveau de sécurité applicable à une source donnée.

Les mesures de sécurité pour les sources de catégorie 1 devraient répondre aux objectifs du niveau de sécurité A, celles des sources de catégorie 2 aux objectifs du niveau de sécurité B, et celles des sources de catégorie 3 aux objectifs du niveau de sécurité C.

Les Normes fondamentales internationales de protection contre les rayonnements ionisants et de sûreté des sources de rayonnements (paragraphe 2.34 [5]) présentent des prescriptions générales pour la sécurité des sources radioactives. Dans le cadre du présent guide, on considère que ces mesures de contrôle assurent un niveau de sécurité suffisant pour les sources radioactives des catégories 4 et 5, mais qu'il faudrait appliquer les mesures renforcées qui y sont indiquées aux sources radioactives des catégories 1, 2 et 3 pour réduire la probabilité d'actes malveillants mettant en jeu ces sources. En outre, l'organisme de réglementation pourrait, compte tenu de la menace nationale, souhaiter renforcer la sécurité des sources des catégories 4 et 5 dans des circonstances appropriées. Cette approche est récapitulée dans le tableau 5.

Même si cette approche peut être vue comme une méthode par défaut, l'utilisation malveillante des sources radioactives pourrait ne pas nécessairement mettre en jeu des sources classées dans la plus haute catégorie de ce système de catégorisation. Par exemple, la plupart des sources de catégorie 1 seront protégées et gardées dans des dispositifs ou des installations fixes. Toute tentative d'enlèvement de la source demandera du temps et pourrait exposer les agresseurs à un niveau de rayonnements sensiblement nuisible. Il est donc possible que les agresseurs se concentreront sur les sources d'une catégorie plus faible, moins dangereuse à manipuler, portable, et plus facile à dissimuler.

TABLEAU 5. NIVEAUX DE SÉCURITÉ PAR DEFAUT RECOMMANDÉS POUR LES SOURCES COMMUNÉMENT UTILISÉES

Catégorie	Source	A/D	Niveau de sécurité
1	GTR Irradiateurs Sources de téléthérapie Sources fixes en téléthérapie multifaisceaux (scalpel gamma)	A/D $\geq$ 1000	A
2	Sources de gammagraphie industrielle Sources de curiethérapie à débit de dose élevé/moyen	1000 > A/D $\geq$ 10	B
3	Jauges industrielles fixes comprenant des sources de haute activité? Sondes de diagraphie	10 > A/D $\geq$ 1	C
4	Curiethérapie à faible débit de dose ? (sauf plaques ophtalmiques et implants permanents) Jauges industrielles ne comprenant pas de sources de haute activité Ostéodensitomètres Éliminateurs de charges statiques	1 > A/D $\geq$ 0,01	Appliquer les mesures figurant dans les Normes internationales de sûreté [5]
5	Sources de curiethérapie à faible débit de dose : plaques ophtalmiques et implants permanents Dispositifs à fluorescence X Dispositifs à capture d'électrons Sources de spectrométrie Mössbauer Sources de référence pour la tomographie à émission de positons (PET)	0,01 > A/D et A > niveau d'exemption	

La catégorisation des sources radioactives vise à fournir une base acceptable au plan international pour la prise de décisions en fonction des risques, y compris des mesures visant à réduire la probabilité d'actes malveillants. Toutefois, les conséquences socio-économiques des actes malveillants ont été exclues des critères de catégorisation car il n'y a aucune méthodologie permettant de quantifier et de comparer ces conséquences, en particulier sur une base internationale.

4.2.3. Autres considérations pour l'affectation des niveaux de sécurité

L'annexe I du Code de conduite indique que les États devraient tenir dûment compte des sources radioactives qu'ils jugent susceptibles d'avoir des conséquences inacceptables si elles sont utilisées à des fins malveillantes.

Même si certains des facteurs ci-dessous sont pris en compte dans les réf. [3, 17], l'organisme de réglementation doit accorder une attention particulière à ces facteurs et ces considérations lors de l'affectation des niveaux de sécurité aux sources radioactives. Ces facteurs représentent des variables qui sont propres à la source ainsi qu'à la façon dont elle est utilisée et à l'endroit où elle est employée — et ceux-ci peuvent influer sur le niveau de sécurité approprié pour une source ou une installation donnée.

4.2.3.1. Attractivité des sources

Outre l'activité de la source, d'autres facteurs pourraient rendre certaines sources plus attrayantes pour les actes malveillants. Ces facteurs comprennent :

— La forme chimique et physique de la matière radioactive contenue dans la source, qui pourrait faciliter sa dispersion et donc la rendre plus attrayante pour un agresseur.
— La nature du rejet radioactif. Certains radionucléides produisent des doses plus élevées par unité d'incorporation que d'autres, notamment les émetteurs alpha. Les sources contenant ces radionucléides pourraient être plus attrayantes pour utilisation dans un ERD.
— La facilité de manipulation. Les sources faciles à manipuler ou facilement accessibles pourraient être plus attrayantes car ce serait moins probable que l'agresseur reçoive une dose de rayonnements élevée et la source est plus facile à déplacer. Un exemple de ce type de source est une source placée dans un dispositif portable à autoprotection.
— La concentration. Des sources multiples ou de grandes quantités de matières radioactives concentrées en un endroit pourraient attirer un agresseur car s'il arrive à pénétrer le système de sécurité, il pourrait enlever ou saboter suffisamment de matières pour provoquer de très sérieuses conséquences.
— La valeur économique perçue de la source ou de son contenant.

L'organisme de réglementation pourrait envisager de tenir compte de l'attractivité des sources pour déterminer le niveau de sécurité à affecter à la source et les mesures de sécurité appliquées à ce niveau de sécurité.

4.2.3.2. Sources entreposées

Les sources radioactives entreposées devraient être protégées conformément aux mesures recommandées dans la présente publication ainsi qu'à la catégorisation de la source et au niveau de sécurité qui lui est appliqué.

4.2.3.3. Vulnérabilité et niveau de la menace

Le niveau de la menace nationale et toute augmentation de ce niveau pourraient nécessiter une évaluation du niveau de sécurité affecté à la source, en tenant compte des autres caractéristiques de la source (attractivité, vulnérabilité par exemple). Une autre solution serait aussi de renforcer les mesures de sécurité spécifiques concernant un niveau de sécurité donné.

4.2.3.4. Sources mobiles, portables et utilisées dans des zones éloignées

Les sources utilisées sur le terrain (par exemple en radiographie et en diagraphie) sont habituellement contenues dans des dispositifs conçus pour être portables, et sont fréquemment transportés entre les lieux de travail. La facilité de manipulation de ces dispositifs et leur présence dans des véhicules en dehors des installations sécurisées les rend attrayants pour des enlèvements non autorisés.

Étant donné que les mesures de sécurité ayant trait aux sources fixes pourraient ne pas être applicables dans la pratique à des sources utilisées sur le terrain, il faudrait recourir à d'autres mesures pour atteindre les objectifs de sécurité. Veuillez consulter les mesures de détection et de retardement pour les niveaux de sécurité B et C (section 4.3.1), ainsi que les autres mesures de sécurité indicatives ayant trait aux sources mobiles figurant dans l'appendice IV.

Les sources utilisées dans les zones éloignées pourraient être enlevées par des individus non autorisés et transportées en dehors de la zone avant qu'une intervention efficace ne soit possible.

L'organisme de réglementation pourrait envisager de tenir compte de la mobilité, de la portabilité et de la localisation de la source pour affecter un niveau de sécurité ou envisager des mesures supplémentaires dans le cadre du niveau de sécurité affecté pour contrebalancer ces conditions.

4.3. ÉTAPE 3 : SÉLECTIONNER ET METTRE EN ŒUVRE UNE APPROCHE DE RÉGLEMENTATION

L'organisme de réglementation dispose de trois approches différentes pour donner aux exploitants des orientations sur la manière de démontrer qu'ils se

conforment aux objectifs de sécurité énoncés dans le tableau 2. Il devrait en choisir une ou plusieurs compte tenu de ses propres capacités et ressources, de celles des exploitants qu'il réglemente et des diverses sources à protéger :

— L'*approche basée sur les prescriptions* établit des mesures de sécurité spécifiques déterminées par l'organisme de réglementation pour atteindre les objectifs de sécurité correspondant à chaque niveau de sécurité. Les orientations données dans la présente section définissent un ensemble de mesures pour chaque niveau, que l'organisme de réglementation peut adopter comme prescriptions en l'absence d'une menace de référence. L'organisme de réglementation peut aussi utiliser les mesures de sécurité énoncées dans le présent guide comme point de départ, mais en les adaptant aux circonstances nationales. L'approche basée sur les prescriptions est particulièrement appropriée lorsque la combinaison de la menace et des conséquences potentielles est faible ou lorsqu'il n'est pas possible de réaliser une évaluation détaillée de la menace. Elle présente l'avantage d'être simple à mettre en œuvre, à la fois pour l'organisme de réglementation et pour l'exploitant, et facilite les inspections et les vérifications. Son inconvénient tient à sa souplesse relativement limitée pour tenir compte des circonstances réelles. Par exemple, l'expérience montre qu'un exploitant peut se conformer aux mesures prescrites, sans pour autant atteindre l'objectif du système de sécurité consistant à protéger les cibles contre une menace réelle ou définie. S'il utilise cette approche, l'organisme de réglementation doit donc s'assurer que des inspections ou des évaluations de la sécurité sont réalisées en vue d'évaluer l'efficacité globale du système de sécurité de l'installation à atteindre les buts et les objectifs de sécurité applicables au niveau de sécurité (voir la section 4.3.1).
— L'*approche basée sur les résultats* permet à l'organisme de réglementation de donner une marge de manœuvre à l'exploitant, lequel peut proposer une combinaison particulière des mesures de sécurité à utiliser pour satisfaire aux objectifs de sécurité énoncés dans le tableau 2. Les mesures de sécurité proposées devraient reposer sur une évaluation de la vulnérabilité, tenant compte des informations fournies par l'organisme de réglementation et basée sur une évaluation de la menace nationale et, le cas échéant, sur une menace de référence. Les avantages de cette approche sont qu'elle reconnaît qu'un système de sécurité efficace peut être composé de nombreuses combinaisons de mesures de sécurité et que les conditions propres à chaque exploitant peuvent être uniques. Sa condition préalable est que l'exploitant et l'organisme de réglementation doivent avoir des niveaux relativement élevés de compétences spécialisées en matière de sécurité (voir la section 4.3.2).

— L'*approche combinée* intègre des éléments de l'approche basée sur les prescriptions et de l'approche basée sur les résultats. Il existe de nombreuses versions possibles de cette approche. Par exemple, l'organisme de réglementation peut adopter un ensemble de mesures de sécurité parmi lesquelles l'exploitant peut choisir, tout en demandant à ce dernier de démontrer que le système de sécurité dans son ensemble répond aux objectifs de sécurité applicables. Il peut aussi recourir à une approche basée sur les résultats pour les sources radioactives dont une utilisation malveillante pourrait avoir les conséquences les plus graves, et à une approche basée sur les prescriptions pour celles dont les risques sont plus faibles. Il est aussi possible de compléter un ensemble de prescriptions par des prescriptions axées sur les résultats traitant de questions spécifiques. Le principal avantage de l'approche combinée est sa souplesse (voir la section 4.3.3).

Le reste de la présente section contient des orientations à l'intention des organismes de réglementation sur l'utilisation de chacune de ces approches.

4.3.1. Approche basée sur les prescriptions

L'organisme de réglementation peut choisir de préciser les mesures de sécurité que les exploitants sont tenus d'appliquer pour satisfaire aux objectifs de sécurité énoncés dans le tableau 2. Les tableaux 6, 7 et 8 indiquent les mesures de sécurité visant à atteindre les objectifs de sécurité des niveaux A, B et C, respectivement. Ils comprennent des mesures de sécurité pour les sources en cours d'utilisation ou d'entreposage. Ces mesures sont examinées en détail après chaque tableau correspondant. Elles peuvent varier selon qu'une source donnée est en cours d'utilisation ou d'entreposage, ou est mobile ou portable. L'appendice I donne de plus amples informations sur certaines de ces mesures. Des exemples de mesures de sécurité indicatives pouvant être appliquées à certaines installations et activités figurent à l'appendice IV.

Introduction de mesures correspondant au niveau de sécurité A

Le but du niveau de sécurité A est d'**empêcher l'enlèvement non autorisé** de sources radioactives. En cas de tentative d'accès non autorisé ou d'enlèvement non autorisé, la détection et l'évaluation doivent être suffisamment rapides pour que le personnel d'intervention ait assez de temps et de ressources pour interrompre l'agresseur et empêcher l'enlèvement de la source. Les mesures suivantes sont recommandées pour atteindre ce but.

TABLEAU 6. MESURES RECOMMANDÉES POUR LE NIVEAU DE SÉCURITÉ A
(*but : empêcher l'enlèvement non autorisé*)

Fonction de sécurité	Objectif de sécurité	Mesures de sécurité
Détection	Assurer la détection immédiate de tout accès non autorisé à la zone sécurisée/l'emplacement de la source.	Système électronique de détection des intrusions et/ou surveillance continue par le personnel de l'exploitant.
	Assurer la détection immédiate de toute tentative d'enlèvement non autorisé de la source, y compris par un agresseur d'origine interne.	Matériel électronique de détection des manipulations frauduleuses et/ou surveillance continue par le personnel de l'exploitant.
	Fournir immédiatement une évaluation de la détection.	Télésurveillance de la télévision en circuit fermé ou évaluation à distance par le personnel de l'exploitant ou le personnel d'intervention.
	Assurer immédiatement la communication avec le personnel d'intervention.	Moyens de communication rapides, fiables et divers tels que téléphones fixes, téléphones portables, téléavertisseurs et radios.
	Permettre de détecter une perte par le biais de la vérification.	Vérification quotidienne à l'aide de contrôles physiques, de la télévision en circuit fermé, de dispositifs d'indication de fraude, etc.
Retardement	Assurer un retardement suffisant après la détection pour permettre au personnel d'intervention d'interrompre l'enlèvement non autorisé.	Système composé d'au moins deux niveaux de barrières (par ex. murs, cages) qui, ensemble, assurent un retardement suffisant pour permettre au personnel d'intervention d'agir.
Intervention	En cas d'alarme évaluée, assurer une intervention immédiate avec suffisamment de ressources pour interrompre et empêcher l'enlèvement non autorisé.	Capacité d'intervention immédiate avec les effectifs, le matériel et la formation nécessaires à l'interception.

TABLEAU 6. MESURES RECOMMANDÉES POUR LE NIVEAU DE SÉCURITÉ A (suite)
(*but : empêcher l'enlèvement non autorisé*)

Fonction de sécurité	Objectif de sécurité	Mesures de sécurité
Gestion de la sécurité	Assurer les contrôles de l'accès à l'emplacement de la source limitant efficacement l'accès aux seules personnes autorisées.	Identification et vérification au moyen par exemple de dispositifs de déverrouillage par lecture de carte magnétique et numéro d'identification personnel, ou de clés et de contrôle des clés.
	S'assurer que les personnes autorisées sont dignes de confiance.	Vérifications des antécédents de tous les membres du personnel autorisés à avoir accès sans escorte à l'emplacement de la source et à accéder à des informations sensibles.
	Déterminer et protéger les informations sensibles.	Procédures pour déterminer les informations sensibles et les protéger contre toute divulgation non autorisée.
	Prévoir un plan de sécurité.	Plan de sécurité conforme aux prescriptions réglementaires et permettant d'intervenir lorsque les niveaux de menace augmentent.
	Assurer une capacité de gérer les événements de sécurité couverts par les plans d'intervention spécialisés sur la sécurité.	Procédures d'intervention pour les scénarios relatifs à la sécurité.
	Mettre en place un système de notification d'événements de sécurité.	Procédures de notification en temps voulu d'événements de sécurité.

Détection

Objectif de sécurité : Assurer la détection immédiate de tout accès non autorisé à la zone sécurisée/l'emplacement de la source.

Mesures de sécurité : Système électronique de détection des intrusions et/ou surveillance continue par le personnel de l'exploitant.

Des capteurs électroniques reliés à une alarme ou une surveillance visuelle continue par le personnel de l'exploitant indiquent tout accès non autorisé à la zone sécurisée (voir la section « Retardement » ci-dessous) ou à l'emplacement

de la source. Il faudrait veiller à ce que les mesures de détection des intrusions ne puissent être contournées. Pour les sources en cours d'utilisation, de telles mesures devraient permettre de détecter l'accès non autorisé à la zone sécurisée où les sources sont utilisées. Pour les sources entreposées, elles devraient permettre de détecter l'accès non autorisé à la pièce verrouillée ou à tout autre emplacement où ces sources se trouvent. En ce qui concerne les sources mobiles ou portables en cours d'utilisation, la surveillance visuelle continue peut être le seul moyen possible pour détecter immédiatement les intrusions.

Objectif de sécurité : Assurer la détection immédiate de toute tentative d'enlèvement non autorisé de la source (par ex. par un agresseur d'origine interne).

Mesures de sécurité : Matériel électronique de détection des manipulations frauduleuses et/ou surveillance continue par le personnel de l'exploitant.

Des capteurs électroniques reliés à une alarme ou une surveillance visuelle continue par le personnel de l'exploitant indiquent toute tentative d'enlèvement non autorisé d'une source. Il faudrait veiller à ce que les mesures de détection des manipulations frauduleuses ne puissent être contournées. Pour les sources mobiles en cours d'utilisation, la surveillance visuelle continue peut être le seul moyen possible pour détecter une tentative d'enlèvement non autorisé. Il convient toutefois de noter que, si on choisit la surveillance continue comme mesure de sécurité, la surveillance visuelle continue peut nécessiter l'observation permanente d'au moins *deux* personnes pour faire échec à un scénario d'agression d'origine interne.

Objectif de sécurité : Fournir immédiatement une évaluation de la détection.

Mesures de sécurité : Télésurveillance de la télévision en circuit fermé ou évaluation à distance par le personnel de l'exploitant / le personnel d'intervention.

Dès qu'une alarme de détection d'intrusion ou de manipulation frauduleuse se déclenche, il faudrait en évaluer immédiatement la cause. Cette évaluation peut être réalisée par le personnel de l'exploitant à l'emplacement de la source, par le biais de la télévision en circuit fermé ou par des personnes immédiatement déployées pour chercher la cause de l'alarme. Pour les sources mobiles ou portables en cours d'utilisation, et dans d'autres cas où la détection des intrusions et des manipulations frauduleuses est assurée par une surveillance visuelle

continue du personnel de l'exploitant, ce dernier devrait faire l'évaluation en même temps que la détection en maintenant la source sous surveillance visuelle continue.

Objectif de sécurité : Assurer immédiatement la communication avec le personnel d'intervention.

Mesures de sécurité : Moyens de communication rapides, fiables et divers tels que téléphones fixes, téléphones portables, téléavertisseurs et radios.

Si l'évaluation confirme qu'il y a eu accès non autorisé ou tentative d'enlèvement non autorisé, le personnel de l'exploitant devrait en informer immédiatement le personnel d'intervention par divers (au moins deux) moyens de communication, tels que téléphones fixes, composeurs automatiques, téléphones portables, radios et téléavertisseurs.

Objectif de sécurité : Fournir un moyen de détecter une perte par le biais de la vérification.

Mesures de sécurité : Vérification quotidienne à l'aide de contrôles physiques, de la télévision en circuit fermé, de dispositifs d'indication de fraude, etc.

La vérification quotidienne devrait comprendre des mesures visant à garantir que les sources sont présentes et n'ont pas fait l'objet de manipulations frauduleuses. Ces mesures pourraient comprendre des contrôles physiques pour s'assurer que la source est à son emplacement, l'observation à distance par télévision en circuit fermé, la vérification des scellés ou d'autres dispositifs de détection des manipulations frauduleuses, ainsi que des mesures des rayonnements ou d'autres phénomènes physiques donnant l'assurance de la présence de la source. Pour les sources en cours d'utilisation, il peut s'avérer suffisant de vérifier que le dispositif est fonctionnel.

Retardement

Objectif de sécurité : Assurer un retardement suffisant après la détection pour permettre au personnel d'intervention d'interrompre l'enlèvement non autorisé.

Mesures de sécurité : Système composé d'au moins deux niveaux de barrières (par ex. murs, cages) qui, ensemble, assurent un retardement suffisant pour permettre au personnel d'intervention d'agir.

Un système équilibré comprenant au moins deux barrières devrait séparer la source du personnel non autorisé et assurer un retardement suffisant après la détection pour permettre au personnel d'intervention d'agir avant que l'agresseur ne puisse enlever la source. Pour les sources en cours d'utilisation, ces mesures peuvent comprendre un dispositif verrouillé dans une zone sécurisée pour le séparer du personnel non autorisé. Pour les sources entreposées, elles peuvent comprendre un conteneur verrouillé et fixe ou un dispositif contenant la source dans une salle d'entreposage verrouillée, séparant ainsi le conteneur du personnel non autorisé. S'agissant des sources mobiles en cours d'utilisation, une surveillance visuelle continue du personnel de l'exploitant peut remplacer l'un des niveaux de barrières ou les deux.

Intervention

Objectif de sécurité : En cas d'alarme évaluée, assurer une intervention immédiate avec suffisamment de ressources pour interrompre et empêcher l'enlèvement non autorisé

Mesures de sécurité : Capacité d'intervention immédiate avec les effectifs, le matériel et la formation nécessaires à l'interception.

L'exploitant devrait établir des protocoles pour assurer le déploiement immédiat et rapide du personnel d'intervention en cas d'alarme. L'intervention devrait être à la fois immédiate et adéquate. *Immédiate* signifie que les intervenants arrivent, une fois la notification reçue, dans un délai inférieur à celui requis pour violer les barrières et réaliser les tâches nécessaires à l'enlèvement de la source. *Adéquate* signifie que la taille de l'équipe d'intervention et ses moyens sont suffisants pour lui permettre de maîtriser l'agresseur. L'intervention peut être menée par des forces de sécurité directement employées, une équipe de sécurité tierce, la police locale ou la gendarmerie nationale.

Gestion de la sécurité

Objectif de sécurité : Assurer des contrôles de l'accès à l'emplacement de la source pour le limiter efficacement aux seules personnes autorisées.

Mesures de sécurité : Identification et vérification contrôlées, par exemple, à l'aide de systèmes de verrouillage activés par lecteurs de carte magnétique et numéro d'identification personnel, ou par clés et contrôle de clés.

Le contrôle d'accès vise à limiter aux personnes autorisées l'accès à l'emplacement de la source, en général en leur permettant de désactiver temporairement des barrières physiques, comme une porte verrouillée (mesures de retardement), après vérification de leur identité et autorisation d'accès. (Dans le contexte de l'exposition médicale, les patients n'ont pas besoin d'être « autorisés » car ils sont accompagnés jusqu'à la source et sont sous la surveillance constante du personnel médical).

L'identité et l'autorisation d'une personne souhaitant obtenir un accès peuvent être vérifiées notamment par :

— Un numéro d'identification personnel (NIP) pour activer le dispositif de contrôle d'une porte ;
— Un système de badges pouvant aussi activer un lecteur électronique ;
— Un système d'échange de badges à un point de contrôle d'accès ;
— Des informations biométriques pour activer le dispositif de contrôle d'une porte.

Après vérification de l'autorisation d'accès de la personne, le système permet à celle-ci d'accéder à la zone sécurisée ou à l'emplacement de la source, en ouvrant un verrou par exemple. Au moins deux mesures de vérification devraient être combinées, comme l'utilisation d'une carte magnétique et d'un NIP ; ou l'utilisation d'une carte magnétique et d'une clé contrôlée ; ou un NIP et un mot de passe informatique ; ou l'utilisation d'une clé contrôlée et la vérification visuelle de l'identité par d'autres membres du personnel autorisé. Pour les sources en cours d'utilisation, ces mesures devraient permettre de contrôler l'accès à la zone où elles sont utilisées. Pour les sources entreposées, elles devraient permettre de contrôler l'accès à la pièce verrouillée ou à tout autre emplacement où elles sont entreposées. Quant aux sources mobiles en cours d'utilisation, une surveillance visuelle continue de plusieurs membres du personnel de l'exploitant peut remplacer le contrôle d'accès.

Objectif de sécurité : S'assurer que les personnes autorisées sont dignes de confiance.

Mesures de sécurité : Vérifications des antécédents de tous les membres du personnel autorisés à avoir accès sans escorte à

l'emplacement de la source et à accéder à des informations sensibles.

Il faut vérifier qu'une personne est digne de confiance au moyen d'une évaluation satisfaisante de ses antécédents avant de l'autoriser à accéder sans escorte à des sources radioactives, à des emplacements où celles-ci sont utilisées ou entreposées, ou à toute information sensible connexe. La nature et l'ampleur des vérifications d'antécédents devraient être proportionnées au niveau de sécurité de la source radioactive et conformes à la réglementation de l'État ou aux dispositions énoncées par l'organisme de réglementation. Ces vérifications devraient au moins comprendre la confirmation d'identité et la vérification des références afin de déterminer l'intégrité, le caractère et la fiabilité de chaque personne. Ce processus devrait être examiné périodiquement et faire l'objet d'une attention continue des superviseurs et responsables afin de s'assurer que le personnel à tous les niveaux continue d'agir de manière responsable et fiable et que toute crainte à cet égard est portée à la connaissance de l'autorité pertinente.

Objectif de sécurité : Déterminer et protéger les informations sensibles.

Mesures de sécurité : Procédures pour déterminer les informations sensibles et les protéger contre toute divulgation non autorisée.

Il faut non seulement assurer la sécurité des sources radioactives mais aussi protéger les informations connexes, notamment les documents, données sur les systèmes informatiques et autres supports pouvant être utilisés pour connaître en détail :

— L'emplacement précis et le stock de sources ;
— Le plan de sécurité qui s'applique et les dispositions de sécurité détaillées ;
— Les systèmes de sécurité (alarme anti-intrusion, par exemple), notamment leur performance et leurs schémas d'installation ;
— Les faiblesses temporaires ou à plus long terme du programme de sécurité ;
— Les dispositions prises ayant trait au personnel de sécurité et les moyens d'intervention en cas d'événements ou d'alertes ;
— Les dates, les itinéraires et le mode d'expédition ou de transfert des sources prévus ;
— Les plans d'intervention spécialisés et les mesures d'intervention pour la sécurité.

Les orientations règlementaires devraient également prévoir :

— Le contrôle, le dépôt, la préparation, l'identification, le marquage et la transmission des documents ou de la correspondance contenant les informations sensibles ;
— Les méthodes recommandées de destruction des documents contenant des informations sensibles ;
— Les dispositions relatives au déclassement et à la gestion des documents lorsqu'ils sont trop anciens ou lorsqu'ils ne sont plus sensibles.

Objectif de sécurité : Prévoir un plan de sécurité.

Mesures de sécurité : Plan de sécurité conforme aux prescriptions réglementaires et permettant d'intervenir en cas de menace accrue.

Un plan de sécurité devrait être élaboré pour chaque installation par son exploitant. L'appendice II donne des exemples de contenu des plans de sécurité. Ces derniers peuvent être autorisés par l'organisme de réglementation et revus à des intervalles déterminés au cours du processus d'inspection pour veiller à ce qu'ils tiennent compte du système de sécurité appliqué. Ils peuvent être différents pour les sources mobiles et portables ou pour les sources entreposées entre des périodes d'utilisation. La plupart des plans contiennent généralement des informations sensibles sur les dispositions de sécurité de protection et devraient donc être gérés en conséquence. Les plans de sécurité devraient en outre permettre de passer efficacement et rapidement à un plus haut niveau de sécurité si la menace contre la sécurité augmente.

Objectif de sécurité : Assurer les moyens de gérer les événements de sécurité couverts par les plans d'intervention spécialisés pour la sécurité

Mesures de sécurité : Procédures d'intervention pour les scénarios relatifs à la sécurité

Dans chaque installation, des plans d'intervention spécialisés pour la sécurité devraient être dressés pour un ensemble d'événements, incluant :

— Une présomption ou une menace d'acte malveillant ;
— Une manifestation publique pouvant menacer la sécurité des sources ;
— L'intrusion d'une ou plusieurs personnes non autorisées dans la zone sécurisée. Cela peut aller d'une simple entrée non autorisée à une attaque délibérée par des individus cherchant à enlever des sources radioactives ou à leur porter atteinte.

L'exploitant devrait mettre au point des scénarios raisonnablement prévisibles incluant ces événements et des procédures pour y faire face. Les plans d'intervention spécialisés pour la sécurité devraient être partagés avec les autorités appropriées et faire l'objet d'exercices à intervalles réguliers.

Objectif de sécurité : Mettre en place un système de notification d'événements de sécurité.

Mesures de sécurité : Procédures de notification en temps voulu d'événements de sécurité.

L'exploitant devrait mettre au point des procédures de notification des événements de sécurité à l'organisme de réglementation, aux premiers intervenants et aux autres acteurs concernés dans un délai prescrit par l'organisme de réglementation et tenant compte de l'importance de l'événement sur le plan de la sécurité. Les événements à signaler peuvent comprendre :

— Les écarts dans les données comptables ;
— Le vol présumé ou effectif d'une source radioactive ;
— L'intrusion non autorisée dans une installation ou une zone d'entreposage de sources ;
— La découverte d'un dispositif explosif présumé ou avéré à l'intérieur ou à proximité d'une installation ou d'un entrepôt ;
— La perte de contrôle d'une source radioactive ;
— L'accès non autorisé à une source ou l'utilisation non autorisée d'une source ;
— Les autres actes malveillants menaçant des activités autorisées ;
— Des activités de surveillance ou des événements suspects pouvant indiquer qu'un acte de sabotage, une intrusion ou l'enlèvement d'une source est en préparation ;
— La défaillance ou la perte de systèmes de sécurité essentiels à la protection des sources radioactives.

TABLEAU 7. MESURES RECOMMANDÉES POUR LE NIVEAU DE SÉCURITÉ B

(but : réduire au minimum la probabilité d'un enlèvement non autorisé)

Fonction de sécurité	Objectif de sécurité	Mesures de sécurité
Détection	Assurer la détection immédiate de tout accès non autorisé à la zone sécurisée/l'emplacement de la source.	Matériel électronique de détection des intrusions et/ou surveillance continue par le personnel de l'exploitant
	Assurer la détection de toute tentative d'enlèvement non autorisé de la source	Matériel de détection des manipulations frauduleuses et/ou vérifications périodiques par le personnel de l'exploitant
	Fournir immédiatement une évaluation de la détection	Télésurveillance par télévision en circuit fermé ou évaluation par le personnel de l'exploitant/d'intervention
	Assurer immédiatement la communication avec le personnel d'intervention	Moyens de communication rapides et fiables tels que téléphones fixes, téléphones portables, téléavertisseurs et radios.
	Fournir un moyen de détecter une perte par le biais de la vérification	Vérification hebdomadaire à l'aide de contrôles physiques, de matériel de détection des manipulations frauduleuses, etc.
Retardement	Assurer un retardement pour réduire le plus possible la probabilité d'un enlèvement non autorisé	Système de deux niveaux de barrières (par exemple, murs, cages)
Intervention	Déclencher immédiatement l'intervention pour interrompre un enlèvement non autorisé	Matériel et procédures pour déclencher immédiatement une intervention
Gestion de la sécurité	Assurer des contrôles de l'accès à l'emplacement de la source limitant efficacement l'accès aux seules personnes autorisées	Une mesure d'identification
	S'assurer que les personnes autorisées sont dignes de confiance	Vérifications des antécédents de tout le personnel autorisé à avoir accès sans escorte à l'emplacement de la source et à accéder à des informations sensibles

TABLEAU 7. MESURES RECOMMANDÉES POUR LE NIVEAU DE SÉCURITÉ B (suite)
(but : réduire au minimum la probabilité d'un enlèvement non autorisé)

Fonction de sécurité	Objectif de sécurité	Mesures de sécurité
Gestion de la sécurité	Déterminer et protéger les informations sensibles	Procédures pour déterminer les informations sensibles et les protéger contre toute divulgation non autorisée.
	Prévoir un plan de sécurité	Plan de sécurité conforme aux prescriptions réglementaires et permettant d'intervenir lorsque les niveaux de menace augmentent.
	Assurer une capacité de gérer les événements de sécurité couverts par les plans d'intervention spécialisés pour la sécurité	Procédures d'intervention pour les scénarios relatifs à la sécurité
	Mettre en place un système de notification d'événements de sécurité	Procédures de notification en temps voulu d'événements de sécurité

Introduction de mesures correspondant au niveau de sécurité B

Le niveau de sécurité B a pour but de **réduire au minimum la probabilité d'enlèvement non autorisé** de sources radioactives. En cas de tentative d'accès ou d'enlèvement non autorisé, l'intervention doit être déclenchée immédiatement après détection et évaluation de l'intrusion, mais il n'est pas nécessaire qu'elle ait lieu à temps suffisant pour empêcher l'enlèvement de la source. Les mesures ci-dessous sont recommandées pour atteindre ce but.

Détection

Objectif de sécurité : Assurer la détection immédiate de tout accès non autorisé à la zone sécurisée/l'emplacement de la source.

Mesures de sécurité : Matériel électronique de détection des intrusions et/ou surveillance continue par le personnel de l'exploitant

Des capteurs électroniques reliés à une alarme ou une surveillance visuelle continue par le personnel de l'exploitant indiquent tout accès non autorisé à la zone sécurisée (voir la section « Retardement » ci-dessous) ou à l'emplacement de la source. Il faudrait veiller à ce que les mesures de détection des intrusions ne

puissent être contournées. Pour les sources en cours d'utilisation, de telles mesures devraient permettre de détecter l'accès non autorisé à la zone sécurisée où les sources sont utilisées. Pour les sources entreposées, elles devraient permettre de détecter l'accès non autorisé à la pièce verrouillée ou à tout autre emplacement où ces sources sont entreposées. En ce qui concerne les sources mobiles ou portables en cours d'utilisation, la surveillance visuelle continue peut être le seul moyen possible pour détecter les intrusions.

Objectif de sécurité : Assurer la détection de toute tentative d'enlèvement non autorisé de la source.

Mesures de sécurité : Matériel de détection des manipulations frauduleuses et/ou vérifications périodiques par le personnel de l'exploitant.

Le matériel de détection des manipulations frauduleuses ou la surveillance visuelle par le personnel de l'exploitant pendant les vérifications périodiques permettent d'indiquer s'il y a tentative d'enlèvement non autorisé d'une source. Il faudrait veiller à ce que les mesures de détection des manipulations frauduleuses ne puissent être contournées, ce que l'utilisation de matériel électronique de détection de ces manipulations peut faciliter. Pour les sources mobiles ou portables en cours d'utilisation, la surveillance visuelle continue peut être le seul moyen possible pour détecter une tentative d'enlèvement non autorisé.

Objectif de sécurité : Fournir immédiatement une évaluation de la détection.

Mesures de sécurité : Télésurveillance par télévision en circuit fermé ou évaluation par le personnel de l'exploitant/d'intervention.

Dès qu'une alarme de détection d'intrusion se déclenche, il faudrait en évaluer immédiatement la cause. Cette évaluation peut être réalisée par le personnel de l'exploitant à l'emplacement de la source, par le biais de la télévision en circuit fermé ou par des personnes immédiatement déployées pour chercher la cause de l'alarme. Pour les sources mobiles ou portables en cours d'utilisation, et dans d'autres cas où la détection des intrusions et des manipulations frauduleuses est assurée par une surveillance visuelle continue du personnel de l'exploitant, ce dernier devrait faire l'évaluation en même temps que la détection en maintenant la source sous surveillance visuelle continue.

Objectif de sécurité : Assurer immédiatement la communication avec le personnel d'intervention.

Mesures de sécurité : Moyens de communication rapides et fiables tels que téléphones fixes, téléphones portables, téléavertisseurs et radios.

Si l'évaluation confirme qu'il y a eu accès non autorisé ou tentative d'enlèvement non autorisé, le personnel de l'exploitant devrait en informer immédiatement le personnel d'intervention par des moyens de communication fiables tels que téléphones fixes, composeurs automatiques, téléphones portables, radios ou téléavertisseurs.

Objectif de sécurité : Fournir un moyen de détecter une perte par le biais de la vérification.

Mesures de sécurité : Vérification hebdomadaire à l'aide de contrôles physiques, de matériel de détection des manipulations frauduleuses, etc.

La vérification hebdomadaire comprend des mesures visant à garantir que les sources sont présentes et n'ont pas fait l'objet de manipulations frauduleuses. Ces mesures pourraient inclure des contrôles physiques pour s'assurer que la source est à son emplacement, la vérification des scellés ou d'autres dispositifs de détection des manipulations frauduleuses, ainsi que des mesures des rayonnements ou d'autres phénomènes physiques dans l'assurance de la présence de la source. Pour les sources en cours d'utilisation, il peut s'avérer suffisant de vérifier que le dispositif est fonctionnel.

Retardement

Objectif de sécurité : Assurer un retardement pour réduire au minimum la probabilité d'un enlèvement non autorisé.

Mesures de sécurité : Système de deux niveaux de barrières (par exemple, murs, cages).

Un système équilibré de deux barrières devrait séparer la source du personnel non autorisé. Pour les sources en cours d'utilisation, ces mesures peuvent comprendre un dispositif verrouillé situé dans une zone sécurisée le séparant du personnel non autorisé. Pour les sources entreposées, elles peuvent comprendre un conteneur verrouillé et fixe ou un dispositif contenant la source et une salle d'entreposage verrouillée, séparant le conteneur du personnel non autorisé. Quant aux sources mobiles ou portables en cours d'utilisation, une surveillance visuelle continue du personnel de l'exploitant peut remplacer les barrières.

Intervention

Objectif de sécurité : Assurer le déclenchement immédiat de l'intervention pour interrompre l'enlèvement non autorisé.

Mesures de sécurité : Matériel et procédures pour déclencher immédiatement une intervention.

L'exploitant devrait établir des protocoles pour assurer le déploiement immédiat et rapide du personnel d'intervention en cas d'alarme afin d'interrompre l'agression. L'intervention peut être menée par des forces de sécurité directement employées, une équipe de sécurité tierce, la police locale ou la gendarmerie nationale. Elle devrait être coordonnée avec les autorités locales pour atténuer les conséquences potentielles.

Gestion de la sécurité

Objectif de sécurité : Assurer des contrôles de l'accès à l'emplacement de la source pour limiter efficacement l'accès aux seules personnes autorisées.

Mesures de sécurité : Une mesure d'identification.

Le contrôle d'accès vise à limiter aux personnes autorisées l'accès à l'emplacement de la source, en général en leur permettant de les désactiver temporairement des barrières physiques, comme des portes verrouillées (mesures de retardement), après vérification de leur identité et autorisation d'accès (dans le contexte de l'exposition médicale, les patients n'ont pas besoin d'être « autorisés »).

L'identité et l'autorisation d'une personne souhaitant obtenir un accès peuvent être vérifiées notamment par :

— Un numéro d'identification personnel (NIP) pour activer le lecteur de contrôle d'une porte ;
— Un système de badges pouvant aussi activer un lecteur électronique ;
— Un dispositif d'échange de badges à un point de contrôle d'accès ;
— Des informations biométriques pour activer le dispositif de contrôle d'une porte.

Après vérification de l'autorisation d'accès de la personne, le système permet à celle-ci d'accéder à la zone sécurisée ou à l'emplacement de la source,

par ouverture d'un verrou par exemple. Au moins une mesure d'identification devrait être requise, comme l'utilisation d'une carte magnétique, d'un NIP, d'un mot de passe informatique, d'une clé contrôlée ou de la vérification visuelle de l'identité par d'autres membres du personnel autorisé. Pour les sources en cours d'utilisation, les mesures devraient permettre de contrôler l'accès à la zone où elles sont utilisées. Pour les sources entreposées, elles devraient permettre de contrôler l'accès à la pièce verrouillée ou à tout autre emplacement où elles sont entreposées. Quant aux sources mobiles ou portables en cours d'utilisation, une surveillance visuelle continue du personnel de l'exploitant peut remplacer le contrôle d'accès.

Objectif de sécurité : S'assurer que les personnes autorisées sont dignes de confiance.

Mesures de sécurité : Vérifications des antécédents de tout le personnel autorisé à avoir accès sans escorte à l'emplacement de la source et à accéder à des informations sensibles.

Il faut vérifier qu'une personne est digne de confiance au moyen d'une évaluation satisfaisante de ses antécédents avant de l'autoriser à accéder sans escorte à des sources radioactives, à des emplacements où celles-ci sont utilisées ou entreposées, ou à toute information sensible connexe. La nature et l'ampleur des vérifications d'antécédents devraient être proportionnées au niveau de sécurité de la source radioactive et conformes à la réglementation de l'État ou aux dispositions énoncées par l'organisme de réglementation. Ces vérifications devraient au moins comprendre la confirmation d'identité et la vérification des références afin de déterminer l'intégrité, le caractère et la fiabilité de chaque personne. Ce processus devrait être examiné périodiquement et faire l'objet d'une attention continue des superviseurs et responsables afin de s'assurer que le personnel à tous les niveaux continue d'agir de manière responsable et fiable et que toute crainte à cet égard est portée à la connaissance de l'autorité pertinente.

Objectif de sécurité : Déterminer et protéger les informations sensibles.

Mesures de sécurité : Procédures pour déterminer les informations sensibles et les protéger contre toute divulgation non autorisée.

Le système de sécurité devrait non seulement assurer la sécurité des sources radioactives mais aussi protéger les informations connexes, notamment les documents, données sur les systèmes informatiques et autres supports pouvant être utilisés pour connaître en détail :

— L'emplacement précis et le stock de sources ;
— Le plan de sécurité qui s'applique et les dispositions de sécurité détaillées ;
— Les systèmes de sécurité (alarme anti-intrusion, par exemple), notamment leur performance et leurs schémas d'installation ;
— Les faiblesses temporaires ou à plus long terme du programme de sécurité ;
— Les dispositions ayant trait au personnel de sécurité et les moyens d'intervention en cas d'événement ou d'alerte ;
— Les dates, les itinéraires et les modes d'expédition ou de transfert des sources prévus ;
— Les plans d'intervention spécialisés et les mesures d'intervention pour la sécurité.

Les orientations règlementaires devraient également prévoir :

— Le contrôle, le dépôt, la préparation, l'identification, le marquage et la transmission des documents ou de la correspondance contenant les informations sensibles ;
— Les méthodes recommandées de destruction des documents contenant des informations sensibles ;
— Les dispositions relatives au déclassement et à la gestion des documents lorsqu'ils sont trop anciens ou lorsqu'ils ne sont plus sensibles.

Objectif de sécurité : Prévoir un plan de sécurité.

Mesures de sécurité : Plan de sécurité conforme aux prescriptions réglementaires et permettant d'intervenir en cas de menace accrue.

Un plan de sécurité devrait être élaboré pour chaque installation par son exploitant. L'appendice II donne des exemples de contenu d'un plan de sécurité. Les plans de sécurité peuvent être approuvés par l'organisme de réglementation et revus à des intervalles déterminés au cours du processus d'inspection pour veiller à ce qu'ils tiennent compte du système de sécurité appliqué. Ils peuvent être différents pour les sources mobiles et portables ou pour les sources entreposées pendant les périodes d'utilisation. La plupart des plans contiennent généralement des informations sensibles sur les dispositions de sécurité de protection et devraient donc être gérés en conséquence. Le plan de sécurité devrait en outre permettre de passer efficacement et rapidement à un plus haut niveau de sécurité, si la menace contre la sécurité augmente.

Objectif de sécurité : Assurer les moyens de gérer les événements de sécurité couverts par les plans d'intervention spécialisés pour la sécurité.

Mesures de sécurité : Procédures d'intervention pour les scénarios relatifs à la sécurité.

Dans chaque installation, des plans d'intervention spécialisés devraient être dressés pour un ensemble d'événements, incluant :

— Une présomption ou une menace d'acte malveillant ;
— Une manifestation publique pouvant menacer la sécurité des sources ;
— L'intrusion d'une ou plusieurs personnes non autorisées dans la zone sécurisée. Cela peut aller d'une simple entrée non autorisée à une attaque délibérée par des individus cherchant à enlever des sources radioactives ou à leur porter atteinte.

L'exploitant devrait mettre au point des scénarios raisonnablement prévisibles incluant ces événements et des procédures pour y faire face. Les plans d'intervention spécialisés devraient être partagés avec les autorités appropriées et faire l'objet d'exercices à intervalles réguliers.

Objectif de sécurité : Mettre en place un système de notification d'événements de sécurité.

Mesures de sécurité : Procédures de notification en temps voulu d'événements de sécurité.

L'exploitant devrait mettre au point des procédures de notification des événements de sécurité à l'organisme de réglementation, aux premiers intervenants et aux autres acteurs concernés dans un délai prescrit par l'organisme de réglementation et tenant compte de l'importance de l'événement sur le plan de la sécurité. Les événements à signaler peuvent être notamment comprendre :

— Les écarts dans les données comptables ;
— Le vol présumé ou effectif d'une source radioactive ;
— L'intrusion non autorisée dans une installation ou une zone d'entreposage de sources ;
— La découverte d'un dispositif explosif présumé ou avéré à l'intérieur ou à proximité d'une installation ou d'un entrepôt ;
— La perte de contrôle d'une source radioactive ;

TABLEAU 8. MESURES RECOMMANDÉES POUR LE NIVEAU DE SÉCURITÉ C
(but : réduire au minimum la probabilité d'un enlèvement non autorisé)

Fonction de sécurité	Objectif de sécurité	Mesures de sécurité
Détection	Assurer la détection de tout enlèvement non autorisé de la source.	Matériel de détection des manipulations frauduleuses et/ou vérifications périodiques par le personnel de l'exploitant.
	Fournir immédiatement une évaluation de la détection.	Évaluation par le personnel de l'exploitant/d'intervention.
	Fournir un moyen de détecter une perte par le biais de la vérification.	Vérification mensuelle à l'aide de contrôles physiques, de dispositifs d'indication de fraude ou d'autres contrôles confirmant la présence de la source.
Retardement	Assurer un retardement pour réduire la probabilité d'un enlèvement non autorisé d'une source.	Une barrière (par exemple, cage, enveloppe de protection) ou observation par le personnel de l'exploitant.
Intervention	Mettre en œuvre les mesures voulues en cas d'enlèvement non autorisé d'une source.	Procédures pour déterminer les mesures nécessaires conformes aux plans d'intervention spécialisés.
Gestion de la sécurité	Assurer des contrôles de l'accès à l'emplacement de la source pour le limiter efficacement aux seules personnes autorisées.	Une mesure d'identification.
	S'assurer que les personnes autorisées sont dignes de confiance.	Méthodes appropriées pour déterminer que les personnes autorisées à avoir accès sans escorte aux sources radioactives et à accéder à des informations sensibles sont dignes de confiance.
	Déterminer et protéger les informations sensibles.	Procédures pour déterminer les informations sensibles et les protéger contre toute divulgation non autorisée.
	Prévoir un plan de sécurité.	Documentation sur les dispositions de sécurité et les procédures de référence.
	Assurer un moyen de gérer les événements de sécurité couverts par les plans d'intervention spécialisés pour la sécurité.	Procédures d'intervention pour les scénarios relatifs à la sécurité.
	Mettre en place un système de notification d'événements de sécurité.	Procédures de notification en temps voulu d'événements de sécurité.

— L'accès non autorisé à une source ou l'utilisation non autorisée d'une source ;
— Les autres actes malveillants menaçant des activités autorisées ;
— Des activités de surveillance ou des événements suspects pouvant indiquer qu'un acte de sabotage, une intrusion ou l'enlèvement d'une source est en préparation ;
— La défaillance ou la perte de systèmes de sécurité essentiels à la protection des sources radioactives.

Introduction de mesures correspondant au niveau de sécurité C

Le niveau de sécurité C a pour but de **réduire la probabilité d'un enlèvement non autorisé** de sources radioactives. Les mesures ci-dessous sont recommandées pour atteindre ce but :

Détection

Objectif de sécurité : Assurer la détection de tout enlèvement non autorisé de la source.

Mesures de sécurité : Matériel de détection des manipulations frauduleuses et/ou vérifications périodiques par le personnel de l'exploitant.

Les exploitants devraient vérifier la présence des sources. Les mesures pourraient inclure des contrôles physiques pour s'assurer que la source est à sa place, la vérification des scellés ou d'autres dispositifs d'indication de fraude, ainsi que des mesures des rayonnements ou d'autres phénomènes physiques donnant l'assurance de la présence de la source. Pour les sources en cours d'utilisation, il peut s'avérer suffisant de vérifier que le dispositif est fonctionnel.

Objectif de sécurité : Fournir immédiatement une évaluation de la détection.

Mesures de sécurité : Évaluation par le personnel de l'exploitant ou d'intervention.

Lorsque des activités de détection des manipulations frauduleuses ou un contrôle physique indiquent une possible disparition d'une source, une évaluation de la situation devrait être immédiatement réalisée pour déterminer si un enlèvement non autorisé a effectivement eu lieu.

Objectif de sécurité : Fournir un moyen de détecter une perte par le biais de la vérification.

Mesures de sécurité : Vérification mensuelle à l'aide de contrôles physiques, de dispositifs d'indication de fraude, etc.

La vérification mensuelle comprend des mesures visant à garantir que les sources sont présentes et n'ont pas fait l'objet de manipulations frauduleuses. Ces mesures pourraient inclure des contrôles physiques pour s'assurer que la source est à sa place, la vérification des scellés ou d'autres dispositifs d'indication de fraude, ainsi que des mesures des rayonnements ou d'autres phénomènes physiques donnant l'assurance de la présence de la source. Pour les sources en cours d'utilisation, il peut s'avérer suffisant de vérifier que le dispositif est fonctionnel.

Retardement

Objectif de sécurité : Assurer un retardement pour réduire la probabilité d'un enlèvement non autorisé d'une source.

Mesures de sécurité : Une barrière (par exemple, cage, enveloppe de protection) ou observation par le personnel de l'exploitant.

Au moins une barrière physique devrait séparer la source du personnel non autorisé. Pour les sources en cours d'utilisation, les mesures peuvent comprendre une enveloppe de protection de la source ou l'utilisation de celle-ci dans une zone sécurisée. Pour les sources entreposées, elles peuvent comprendre un conteneur verrouillé et fixe, un dispositif contenant la source ou une salle d'entreposage verrouillée pour séparer le conteneur du personnel non autorisé. Quant aux sources mobiles ou portables en cours d'utilisation, une surveillance visuelle continue par le personnel de l'exploitant peut remplacer les barrières.

Intervention

Objectif de sécurité : Mettre en œuvre les mesures appropriées en cas d'enlèvement non autorisé d'une source.

Mesures de sécurité : Procédures pour déterminer les mesures nécessaires conformément aux plans d'intervention spécialisés.

Les procédures réglementaires devraient garantir que toute présomption d'enlèvement non autorisé ou de perte d'une source est évaluée et, si confirmée, signalée sans délai à l'autorité compétente. Cela devrait être suivi d'efforts pour localiser et récupérer la source ainsi que pour déterminer les circonstances qui ont conduit à l'événement.

Gestion de la sécurité

Objectif de sécurité : Assurer des contrôles de l'accès à l'emplacement de la source pour le limiter efficacement aux seules personnes autorisées.

Mesures de sécurité : Une mesure d'identification.

Le contrôle d'accès vise à limiter aux personnes autorisées l'accès à l'emplacement de la source, en général en leur permettant de désactiver temporairement les barrières physiques, comme des portes verrouillées (mesures de retardement), après vérification de leur identité et autorisation d'accès. (Dans le contexte de l'exposition médicale, les patients n'ont pas besoin d'être « autorisés »).

L'identité et l'autorisation d'une personne souhaitant obtenir un accès peuvent être vérifiées notamment par :

— Un numéro d'identification personnel (NIP) pour activer le lecteur de contrôle d'une porte ;
— Un système de badges pouvant aussi activer un lecteur électronique ;
— Un système d'échange de badges à un point de contrôle d'accès ;
— Des informations biométriques pour activer le dispositif de contrôle d'une porte.

Après vérification de l'autorisation d'accès d'une personne, le système permet à celle-ci d'accéder à la zone sécurisée ou à l'emplacement de la source, en ouvrant un verrou par exemple. Au moins une mesure d'identification devrait être requise, comme l'utilisation d'une carte magnétique, d'un NIP, d'un mot de passe informatique, d'une clé contrôlée ou de la vérification visuelle de l'identité par d'autres membres autorisés du personnel. Pour les sources en cours d'utilisation, ces mesures devraient permettre de contrôler l'accès à la zone où elles sont utilisées. Pour les sources entreposées, elles devraient permettre de contrôler l'accès à la pièce verrouillée ou à tout autre lieu d'entreposage. Quant aux sources mobiles ou portables en cours d'utilisation, une surveillance visuelle continue du personnel de l'exploitant peut remplacer le contrôle d'accès.

Objectif de sécurité : S'assurer que les personnes autorisées sont dignes de confiance.

Mesures de sécurité : Méthodes appropriées pour déterminer que les personnes autorisées à avoir accès sans escorte aux sources radioactives et à accéder à des informations sensibles sont dignes de confiance.

Il faut vérifier qu'une personne est digne de confiance au moyen d'une évaluation satisfaisante de ses antécédents avant de l'autoriser à accéder sans escorte à des sources radioactives, à des emplacements où celles-ci sont utilisées ou entreposées, ou à toute information sensible connexe. La nature et l'ampleur des vérifications d'antécédents devraient être proportionnées au niveau de sécurité de la source radioactive et conformes aux normes de l'État ou aux dispositions énoncées par l'organisme de réglementation.

Objectif de sécurité : Déterminer et protéger les informations sensibles.

Mesures de sécurité : Procédures pour déterminer les informations sensibles et les protéger contre toute divulgation non autorisée.

Les dispositions réglementaires devraient prévoir que l'exploitant évalue la fiabilité des personnes ayant accès à des informations relatives à la sécurité ou à des sources radioactives. À moins d'être déclarées dignes de confiance, elles ne devraient pas être autorisées à y accéder sans escorte.

Objectif de sécurité : Prévoir un plan de sécurité.

Mesures de sécurité : Documentation sur les dispositions de sécurité et les procédures de référence.

Les dispositions de sécurité et les procédures de référence devraient être adoptées sous la forme d'un plan de sécurité. L'appendice II donne des exemples de contenu d'un tel plan.

Objectif de sécurité : Assurer les moyens de gérer les événements de sécurité couverts par les plans d'intervention spécialisés pour la sécurité.

Mesures de sécurité : Procédures d'intervention pour les scénarios relatifs à la sécurité.

Les dispositions de sécurité devraient inclure des procédures d'enquête et de notification pour tout accès non autorisé ou tout enlèvement de source.

Objectif de sécurité : Mettre en place un système de notification d'événements de sécurité.

Mesures de sécurité : Procédures de notification en temps voulu d'événements de sécurité.

L'exploitant devrait mettre au point des procédures de notification des événements de sécurité à l'organisme de réglementation, aux premiers intervenants et aux autres acteurs concernés dans un délai prescrit par l'organisme de réglementation et tenant compte de l'importance de l'événement sur le plan de la sécurité. Les événements à signaler peuvent comprendre :

— les écarts dans les données comptables ;
— le vol présumé ou effectif d'une source radioactive ;
— l'intrusion non autorisée dans une installation ou dans une zone d'entreposage de sources ;
— la découverte d'un dispositif explosif présumé ou avéré à l'intérieur ou à proximité d'une installation ou d'un entrepôt ;
— la perte de contrôle d'une source radioactive ;
— l'accès non autorisé à une source ou l'utilisation non autorisée d'une source ;
— les autres actes malveillants menaçant des activités autorisées ;
— des activités de surveillance ou des événements suspects pouvant indiquer qu'un acte de sabotage, une intrusion ou l'enlèvement d'une source est en préparation ;
— la défaillance ou la perte de systèmes de sécurité essentiels à la protection des sources radioactives ;

4.3.2. Approche basée sur les résultats.

L'organisme de réglementation peut décider de prescrire l'utilisation pour les exploitants d'une approche basée sur les résultats pour répondre aux objectifs de sécurité applicables. En général, l'approche que choisira un État dépendra des compétences spécialisées en matière de sécurité dont disposent l'organisme de réglementation et l'exploitant. L'approche basée sur les résultats fonctionnera de manière optimale si les exploitants ont des conseillers de haut niveau et des compétences spécialisées pour concevoir et appliquer les mesures nécessaires et ont toujours fait preuve de cohérence et respecté celles-ci par le passé. L'organisme de

réglementation devrait s'assurer que les mesures approuvées sont clairement documentées, par exemple dans un plan de sécurité, et évaluées à intervalles appropriés.

Pour suivre l'approche basée sur les résultats, un État devra s'appuyer sur l'évaluation de la menace nationale et pourra en outre déterminer, le cas échéant, une menace de référence. L'organisme de réglementation devrait en outre préciser un objectif de sécurité pour les classes de sources auxquelles s'appliquera l'approche basée sur les résultats. En général, ces objectifs de sécurité devraient être formulés en fonction du niveau d'efficacité du système requis, comme indiqué à la section 3.

Un système de sécurité répondant aux objectifs de sécurité applicables devrait alors être mis au point à partir d'une évaluation de la vulnérabilité à la menace de référence applicable ou à la menace évaluée. Selon les circonstances, cette évaluation peut être réalisée par l'organisme de réglementation ou par l'exploitant grâce à l'approche décrite à la section 3 ou à une autre méthode que l'organisme de réglementation aura déterminée. Les résultats de l'évaluation de la vulnérabilité ou de cette méthode seront en outre utilisés pour montrer que le système de sécurité issu de ce processus répond de fait aux objectifs de sécurité applicables.

L'ensemble de mesures de sécurité mises au point à l'aide de l'approche basée sur les résultats ne correspondra pas nécessairement à celles qui seraient recommandées par l'approche basée sur les prescriptions pour chacune des sources, et qui sont présentées dans les tableaux 6 à 8. Même si elles comprendront les mesures couvrant les fonctions de sécurité de *détection*, de *retardement* et d'*intervention* figurant dans le tableau 2, les combinaisons spécifiques des mesures peuvent dépendre de l'analyse de la situation faite dans l'évaluation de la vulnérabilité. L'application de l'approche basée sur les résultats conduit généralement à un ensemble de mesures de sécurité plus adaptées et plus efficientes que celles qu'on peut obtenir à l'aide de l'approche basée sur les prescriptions. L'approche basée sur les résultats ne se prête pas à une analyse statistique de la *dissuasion* ou de la *gestion de la sécurité*, même si ces fonctions font partie intégrante du programme. Elle devrait donc prescrire, entre autres, des mesures de dissuasion et de gestion de la sécurité pouvant s'appliquer au niveau de sécurité de la source ou des sources concernée(s), comme indiqué dans la documentation sur l'approche basée sur les prescriptions. L'approche basée sur les résultats devrait tenir compte de l'interaction systématique entre détection, retardement et intervention pour déterminer l'efficacité globale du système par rapport à la menace évaluée.

L'efficacité du système est la mesure clé de l'approche basée sur les résultats. Pour concevoir un système de sécurité à l'aide de cette approche, on prend comme hypothèse que toutes les mesures de dissuasion échouent et qu'il y

a tentative d'acte malveillant. Le système de sécurité devrait donc être conçu, compte tenu de la menace évaluée, pour atteindre le niveau d'efficacité requis afin d'empêcher que l'acte malveillant présumé ne se produise.

4.3.3. Approche combinée

De nombreux États peuvent souhaiter combiner des aspects de l'approche basée sur les prescriptions et de l'approche basée sur les résultats pour appliquer des mesures de sécurité qui répondent aux objectifs de sécurité énoncés ci-dessus. Par exemple, un État pourrait utiliser l'approche basée sur les prescriptions pour les sources radioactives dont l'utilisation malveillante aurait de moindres conséquences mais appliquer l'approche basée sur les résultats pour les sources les plus dangereuses. Pour la plupart de celles-ci, cet État conduirait une évaluation de la menace nationale et définirait une menace de référence. L'exploitant serait donc chargé d'appliquer les mesures de sécurité appropriées pour répondre à un ensemble d'objectifs de sécurité définis selon les fonctions de sécurité que sont la *dissuasion*, la *détection*, le *retardement*, l'*intervention* et la *gestion de la sécurité*.

Appendice I

DESCRIPTION DES MESURES DE SÉCURITÉ

Les mesures de sécurité recommandées, dont certaines sont mentionnées à la section 4, sont décrites ci-dessous.

Étant donné que les normes nationales varient, la présente publication ne donne pas de conseils détaillés en ce qui concerne les spécifications pour les équipements de sécurité ou les caractéristiques physiques. Toutefois, l'orientation générale est que la conception et la fiabilité des mesures de sécurité doivent être adaptées à la menace telle qu'identifiée par l'évaluation de la menace ou définie dans la menace de référence. Cela suppose généralement le recours à des équipements et technologies de haute qualité, éprouvés et satisfaisant aux normes de qualité nationales ou internationales.

I.1. CONTRÔLE DE L'ACCÈS

Le contrôle de l'accès peut se faire aux points d'entrée par le personnel de l'exploitant, l'utilisation de lecteurs électroniques ou des mesures de contrôle des clés. La technologie des systèmes automatisés de contrôle de l'accès est disponible sous diverses formes, allant des simples dispositifs mécaniques à bouton-poussoir aux lecteurs plus sophistiqués qui répondent à des badges de proximité ou à des caractéristiques biométriques individuelles. Utilisés avec un tourniquet, ces systèmes peuvent aussi intégrer des contrôles visant à empêcher les pratiques comme des utilisations identiques consécutives du même badge et la pénétration dans le sillage de quelqu'un. Dans la plupart des cas, il faudrait vérifier l'utilisation d'un badge par le biais d'un NIP saisi dans le lecteur ; dans les situations à haut risque, un point d'entrée équipé d'un système automatisé de contrôle de l'accès devrait être surveillé par un garde clairement visible. Un facteur essentiel est que les futurs exploitants spécifient un système automatisé de contrôle de l'accès viable, satisfaisant aux prescriptions et pour lequel les compétences sont disponibles localement chez un fabricant ou un installateur. Il importe en outre de limiter l'accès aux ordinateurs et aux logiciels de gestion de ce système pour empêcher toute manipulation non autorisée des bases de données. Lorsque des dispositifs de verrouillage et des clés classiques sont utilisés comme moyen de contrôle, ces dispositifs devraient être de bonne qualité et les procédures de gestion des clés devraient être conçues pour empêcher tout accès non autorisé ou tout préjudice.

I.2. CAGES

Des cages ou des conteneurs métalliques peuvent aussi être utilisés pour séparer et sécuriser des sources en créant un niveau de protection supplémentaire, par exemple pour garder temporairement des sources dans une zone de réception et d'envoi. Ailleurs, les modalités d'entreposage pourraient mettre en jeu des cages dans une zone définie, fermée, sous contrôle et supervision.

I.3. SURVEILLANCE PAR TÉLÉVISION EN CIRCUIT FERMÉ

La télévision en circuit fermé est un outil utile qui permet au personnel de sécurité de surveiller les accès externes et les zones où des sources radioactives sont entreposées. Il est possible d'associer les caméras à un système de détection des intrusions pour obtenir des images déclenchées par les événements. Cependant, la performance des caméras et des détecteurs de la télévision en circuit fermé devrait être régulièrement évaluée pour assurer leur pleine efficacité et garantir qu'ils continuent de fournir des images de bonne qualité. Les systèmes devraient en outre être appuyés par une capacité d'intervention pour permettre d'analyser les événements et les indications d'alarme déclenchés par la technologie.

I.4. COMMUNICATION

Le personnel de sécurité à tous les niveaux devrait disposer de moyens de communication efficaces et fiables. Ceux-ci devraient notamment permettre la communication entre les patrouilles, les postes fixes et le centre de notification ou de contrôle local, ainsi qu'avec les organismes extérieurs chargés d'intervenir rapidement en cas d'événements de sécurité.

I.5. CLÔTURES ET PORTES

Le type de clôture utilisé sur un périmètre devrait être adapté à la menace, à la nature des sources protégées et à la catégorie du site dans son ensemble. Il existe différents types de clôtures allant de celles qui sont à peine plus que de simples démarcations à celles, plus robustes, qui peuvent être équipées d'un système périmétrique de détection et d'évaluation des intrusions ou de panneaux électrifiés. Les clôtures doivent être vérifiées régulièrement pour s'assurer que la structure est en bon état et qu'elle n'a pas été manipulée de manière illicite ni

endommagée. Les portes des clôtures devraient être construites conformément à une norme comparable à celle des clôtures et sécurisées à l'aide de dispositifs de verrouillage de bonne qualité.

I.6. SYSTÈMES DE DÉTECTION DES INTRUSIONS

Ces systèmes sont un moyen utile pour assurer la sécurité d'une zone non occupée. Lorsqu'il y a lieu, cette technologie peut être étendue à la zone extérieure d'un établissement grâce à un système périmétrique de détection et d'évaluation des intrusions. Tous les systèmes de détection des intrusions devraient être appuyés par une capacité d'intervention pour permettre d'analyser les événements ou les conditions d'alarme. Les alarmes peuvent retentir à distance à un point de contrôle de sécurité ou localement par le biais d'un émetteur à volume élevé. La télévision en circuit fermé peut se révéler utile pour réaliser des vérifications initiales d'événements survenus dans un secteur ou une zone équipé(e) d'alarmes, mais devrait normalement être appuyée par une patrouille effectuant des contrôles visuels ou des investigations.

I.7. PROCÉDURES DE CONTRÔLE DES CLÉS

Les clés qui permettent d'accéder à des sources radioactives devraient être contrôlées et sécurisées. Il peut s'agir de clés d'accès à des cages, des portes, des conteneurs d'entreposage ou des dispositifs blindés dans lesquels des sources sont utilisées. Des niveaux de contrôle analogues devraient être appliqués aux doubles et aux clés de réserve.

I.8. DISPOSITIFS DE VERROUILLAGE, CHARNIÈRES ET SYSTÈMES D'INTERVERROUILLAGE DES PORTES

Les dispositifs de verrouillage utilisés pour protéger les sources radioactives devraient être de bonne qualité, avec des caractéristiques résistant à une attaque en force. Il en va de même pour les charnières des portes. Les clés devraient être protégées comme indiqué ci-dessus dans les procédures de contrôle des clés. Dans les locaux, les portes équipées de systèmes d'interverrouillage qui satisfont aux prescriptions de sécurité peuvent répondre aux besoins de sécurité en contrôlant le mouvement des employés et en permettant au personnel de surveiller l'accès à l'installation.

I.9. CONTENEURS VERROUILLÉS ET BLINDÉS

Des dispositifs de blindage fixes contenant des sources radioactives peuvent assurer une protection et retarder toute tentative de manipulation illicite des sources. Toutefois, en l'absence du personnel, la zone devrait être protégée par un système d'alarme anti-intrusion pour alerter le personnel d'intervention ou de sécurité de la nécessité de déterminer les circonstances d'une intrusion.

I.10. MAINTENANCE ET ESSAIS DEs TECHNOLOGIEs DE SÉCURITÉ

Les technologies de sécurité devraient être largement utilisées pour signaler rapidement l'entrée d'un agresseur sur le site ou dans la zone sécurisée. Par conséquent, les systèmes de détection des intrusions utilisés pour protéger les sources radioactives devraient non seulement être correctement spécifiés, mais aussi être soumis à des essais de fonctionnement lors de l'installation, entretenus à intervalles réguliers par des personnes compétentes et testés à des intervalles définis par l'organisme de réglementation.

I.11. SYSTÈME DE BADGES

Un système de badges est un moyen efficace et efficient pour donner une première indication du droit d'une personne de se trouver dans des locaux ou dans une zone sécurisée. Les badges devraient néanmoins être vérifiés à l'entrée de l'installation et portés de manière visible par leurs détenteurs pour confirmer le droit de ces derniers de se trouver dans les locaux et faciliter l'identification. Des technologies intégrées peuvent aussi permettre d'utiliser les badges en combinaison avec des systèmes de contrôle de l'accès.

I.12. ASSURANCE DE LA QUALITÉ

Des dispositions et procédures de sécurité devraient être élaborées, documentées et maintenues conformément aux normes d'assurance de la qualité recommandées, telles que l'enregistrement de l'approbation officielle ; la gestion des versions ; les examens périodiques et planifiés ; l'essai des dispositions et des procédures ; et l'intégration des enseignements tirés dans les procédures.

I.13. SÉCURITÉ ET ÉCLAIRAGE DES ZONES

L'éclairage efficace des zones peut largement contribuer à la protection physique. Dans les situations à risque de sécurité élevé, des configurations d'éclairage spéciales peuvent s'avérer nécessaires. Toutefois, l'éclairage extérieur et public — installé à d'autres fins — peut souvent illuminer pour dissuader des agresseurs et aider le personnel d'intervention en patrouille.

I.14. PORTES ET BLOCS DE PORTES SPÉCIALEMENT SÉCURISÉS

Dans certaines installations contenant des sources radioactives, il peut être approprié d'équiper les zones d'entreposage de portes et d'encadrements de porte spécialement sécurisés, capables de résister à une attaque en force. Cela peut être utile pour les zones régulièrement laissées sans surveillance.

I.15. ALIMENTATION DE SECOURS

Les salles de contrôle de la sécurité et les systèmes de sécurité devraient pouvoir rester opérationnels en cas de baisse de tension ou de perte totale de l'approvisionnement principal en électricité. Cette capacité peut être assurée par le biais d'un système d'alimentation sans coupure et d'un générateur de secours qui démarre automatiquement lorsqu'une fluctuation des niveaux d'électricité est détectée. La batterie de secours n'a qu'une durée limitée et devrait donc être considérée uniquement comme une source d'alimentation de secours à court terme.

I.16. MURS

À moins qu'ils ne soient déjà en place, les murs constituent un moyen coûteux d'établir les limites d'un périmètre. Ils présentent aussi l'inconvénient d'empêcher le personnel d'intervention de regarder au-delà de la zone protégée.

Appendice II

EXEMPLES DE TENEUR D'UN PLAN DE SÉCURITÉ

Un plan de sécurité devrait inclure toutes les informations nécessaires pour décrire l'approche et le système de sécurité utilisés pour la protection de la source ou des sources. Le niveau de détail et de développement de ces informations devrait être proportionné au niveau de sécurité de la source ou de sources couvertes par le plan. Les points suivants devraient généralement être inclus :

— Description de la source, de sa catégorie et de son utilisation.
— Description du milieu, du bâtiment et/ou de l'installation où la source est utilisée ou entreposée, et selon le cas, plan de l'installation et du système de sécurité.
— Emplacement du bâtiment ou de l'installation par rapport aux zones accessibles au public.
— Procédures de sécurité locales.
— Objectifs du plan de sécurité pour l'installation ou le bâtiment spécifique, indiquant notamment :
  • la préoccupation à laquelle il faut répondre : enlèvement non autorisé, destruction ou utilisation malveillante ;
  • le type de contrôle requis pour empêcher des conséquences indésirables, y compris les équipements auxiliaires qui peuvent s'avérer nécessaires ;
  • les équipements ou les installations qui seront sécurisés.
— Mesures de sécurité à adopter, comme :
  • les mesures destinées à sécuriser, assurer la surveillance, contrôler l'accès, détecter, retarder, intervenir et communiquer ;
  • les caractéristiques de conception pour l'évaluation de la qualité des mesures requises contre la menace supposée.
— Mesures administratives à prendre, notamment sur :
  • les rôles et les responsabilités en matière de sécurité des dirigeants, du personnel et des autres acteurs ;
  • les opérations courantes et non courantes, comme la comptabilisation de la source ou des sources ;
  • l'entretien et les essais du matériel ;
  • la détermination du niveau de confiance du personnel ;
  • l'application de la sécurité de l'information ;
  • les méthodes applicables pour l'autorisation d'accès ;
  • les aspects du plan d'urgence relatifs à la sécurité, y compris la notification d'événements ;

- la formation ;
- les procédures de contrôle des clés.

— Procédures pour faire face à un niveau de menace accru.
— Processus d'évaluation périodique de l'efficacité du plan et mise à jour en conséquence.
— Toute mesure compensatoire qui pourrait être nécessaire.
— Références aux règlements et aux normes existants.

Appendice III

DESCRIPTION D'UNE ÉVALUATION DE LA VULNÉRABILITÉ

L'évaluation de la vulnérabilité, encore appelée expertise de sécurité ou évaluation de la sécurité, est une méthode d'évaluation des systèmes de sécurité de protection. C'est une évaluation systématique de l'efficacité d'un système de sécurité de protection contre une menace évaluée (ou une menace de référence, le cas échéant). Elle peut être de nature spécifique ou générale, réalisée au niveau local par l'exploitant ou par l'État/l'organisme de réglementation et utilisée pour aider l'État/l'organisme de réglementation à élaborer des règlements ou pour démontrer le respect de ces derniers par l'exploitant. Les évaluations de la vulnérabilité devraient être réalisées par un personnel formé. Les principaux éléments de ces évaluations sont les suivants :

— Établissement d'un inventaire des sources radioactives et des informations associées, en tenant compte de leur catégorie, forme, emplacement et environnement physique. Ce processus devrait également inclure les sources retirées du service ;
— Évaluation des conséquences potentielles liées à l'enlèvement non autorisé et à l'utilisation malveillante de la source ou d'un acte de sabotage commis dans l'installation ;
— Prise en compte de l'évaluation de la menace nationale (ou de la menace de référence, le cas échéant) ainsi que toute autre considération locale ;
— Détermination des mesures de sécurité existantes et évaluation de l'efficacité attendue du système de sécurité pour la protection contre les attaques liées aux menaces supposées (et/ou à la menace de référence, le cas échéant) ; et
— Définition des mesures de sécurité supplémentaires qui pourraient s'avérer nécessaires pour assurer un niveau de protection acceptable et adapté.

L'évaluation de la vulnérabilité devrait être effectuée par des experts techniques connaissant bien l'installation concernée, en particulier ses impératifs techniques et commerciaux, les niveaux de sécurité existants et les aspects de sûreté qui pourraient accroître le niveau de protection globale.

Appendice IV

EXEMPLES DE MESURES DE SÉCURITÉ INDICATIVES APPLICABLES À CERTAINES INSTALLATIONS ET ACTIVITÉS

Le présent appendice est destiné à appuyer la section 4 en illustrant à l'intention de l'organisme de réglementation la mise en œuvre pratique des mesures de sécurité pour un ensemble d'installations et d'activités pertinentes, incluant les opérations mobiles à mener lorsque les mesures concernant une installation fixe ne sont pas applicables. Étant donné que les évaluations de la menace nationale seront différentes les unes des autres, il faudra adapter les mesures de sécurité comme il se doit.

Fonction de sécurité	Grande installation fixe Niveau de sécurité A (ex. : irradiateur industriel)	Petite installation fixe Niveau de sécurité B (par ex. : petite entreprise de radiographie)	Petite installation fixe Niveau de sécurité C (par ex. : petite chaîne de traitement)	Ajustements pour les utilisations mobiles Niveau de sécurité B (cas spécial) (par ex. : radiographie mobile)
DÉTECTION	Détection immédiate de tout accès non autorisé à la zone sécurisée/ l'emplacement de la source. *Système de détection et d'évaluation périmétriques des intrusions et système de protection locale contre les intrusions ou surveillance continue par le personnel de l'exploitant.*	Détection immédiate de tout accès non autorisé à la zone sécurisée/l'emplacement de la source. *Système de détection et d'évaluation périmétriques des intrusions ou système de protection locale contre les intrusions, ou surveillance continue par le personnel de l'exploitant.*		Détection immédiate de tout accès non autorisé à la zone sécurisée/l'emplacement de la source. *Surveillance continue par le personnel de l'exploitant.* *Alarme sur véhicule lorsque la source est entreposée.*
	Détection immédiate de toute tentative d'enlèvement non autorisé de la source, y compris par un agresseur d'origine interne *Vérification à l'aide des données de contrôle du processus et de systèmes d'interverrouillage lorsque la source est en cours d'utilisation.* *(Alarme d'intrusion locale quand la source est dans une piscine).*	Détection de toute tentative d'enlèvement non autorisé de la source. *Matériel de détection des manipulations frauduleuses ou inspection visuelle.*	Détection d'enlèvement non autorisé d'une source. *Détection à l'aide des données de contrôle du processus et d'une maintenance régulière.*	Détection de toute tentative d'enlèvement non autorisé de la source. *Matériel de détection des manipulations frauduleuses, alarme sur véhicule ou inspection visuelle.*
	Évaluation immédiate de la détection. *Télésurveillance des alarmes/télévisions en circuit fermé (par le personnel de l'exploitant ou la police locale).* *Patrouille de sécurité.*	Évaluation immédiate de la détection. *Télésurveillance des alarmes ou télévisions en circuit fermé (par le personnel de l'exploitant ou la police locale).*	Évaluation immédiate de la détection. *Inspection visuelle*	Évaluation immédiate de la détection. *Personnel de l'exploitant.* *(Personnel du client si c'est sur le terrain).*

Fonction de sécurité	Grande installation fixe Niveau de sécurité A (ex. : irradiateur industriel)	Petite installation fixe Niveau de sécurité B (par ex. : petite entreprise de radiographie)	Petite installation fixe Niveau de sécurité C (par ex. : petite chaîne de traitement)	Ajustements pour les utilisations mobiles Niveau de sécurité B (cas spécial) (par ex. : radiographie mobile)
DÉTECTION	Communication immédiate avec le personnel d'intervention. *Ligne fixe et :* *Radio mobile privée ou* *Téléphone cellulaire ou* *Téléavertisseur.*	Communication immédiate avec le personnel d'intervention. *Ligne fixe.* *Téléphone cellulaire.*		Communication immédiate avec le personnel d'intervention. *Téléphone cellulaire et/ou radio mobile privée.* *(Ligne fixe si c'est sur le terrain).*
	Moyen de détection d'une perte de source par la vérification. *Vérification à l'aide des données de contrôle du processus et de systèmes d'interverrouillage lorsque la source est en cours d'utilisation.* *(Alarme d'intrusion locale lorsque la source est dans une piscine).*	Moyen de détection d'une perte de source par la vérification. *Vérification à l'aide d'instruments de sûreté.*	Moyen de détection d'une perte de source par la vérification. *Vérification à l'aide des données du contrôle de processus et des instruments de sûreté pour la source entreposée.*	Moyen de détection d'une perte de source par la vérification. *Vérification à l'aide d'instruments de sûreté et inspection visuelle.*
RETARDEMENT	Retardement suffisant après la détection pour permettre au personnel d'intervention d'interrompre l'enlèvement non autorisé. *Mur extérieur.* *Verrous sur le tableau de contrôle du processus/systèmes d'interverrouillage.* *Entreposage sous clé des outils utilisés dans le processus (ou placement hors site).* *Dernière porte de sécurité et bloc de portes.*	Retardement pour réduire le plus possible la probabilité d'un enlèvement non autorisé. *Mur extérieur.* *Verrous sur la cellule de radiographie/* *systèmes d'interverrouillage.* *Entreposage sous clé des outils.* *Porte de sécurité et bloc de portes.* *Hors horaires : enceinte ou entrepôt sécurisé pour abriter la source.*	Retardement pour réduire la probabilité d'enlèvement non autorisé. *Barrière : cage ou abri et fixages sécurisés.*	Retardement pour réduire au minimum la probabilité d'un enlèvement non autorisé. *Surveillance continue par le personnel de l'exploitant.* *Verrous sur le conteneur de la source.* *Conteneur de source fixé au véhicule.* *Entreposage sous clé des outils.* *Hors horaires : véhicule verrouillé et muni d'une alarme.*

Fonction de sécurité	Grande installation fixe Niveau de sécurité A (ex. : irradiateur industriel)	Petite installation fixe Niveau de sécurité B (par ex. : petite entreprise de radiographie)	Petite installation fixe Niveau de sécurité C (par ex. : petite chaîne de traitement)	Ajustements pour les utilisations mobiles Niveau de sécurité B (cas spécial) (par ex. : radiographie mobile)
INTERVENTION	Intervention immédiate après évaluation de l'alarme, avec suffisamment de ressources pour interrompre et empêcher l'enlèvement non autorisé. *Personnel de l'exploitant.* *Intervention de la police.*	Déclenchement immédiat de l'intervention aux fins de l'interruption. *Personnel de l'exploitant.* *Intervention de la police.*	Mesures appropriées en cas d'enlèvement non autorisé d'une source. *Personnel de l'exploitant.* *Intervention de la police.*	Déclenchement immédiat de l'intervention aux fins de l'interruption. *Personnel de l'exploitant.* *Intervention de la police.*
GESTION DE LA SÉCURITÉ	Contrôles de l'accès à l'emplacement de la source pour limiter efficacement aux seules personnes autorisées. *Système de badges ou identification et vérification par reconnaissance du personnel de l'exploitant.*	Contrôles de l'accès à l'emplacement de la source pour limiter efficacement aux seules personnes autorisées. *Reconnaissance par le personnel de l'exploitant.* *Verrous aux spécifications adaptées.* *Gestion des clés (coffre, procédure, etc.)*	Contrôles de l'accès à l'emplacement de la source pour limiter efficacement aux seules personnes autorisées. *Une barrière : cage ou enveloppe de protection et fixages sécurisés.*	Contrôles de l'accès à l'emplacement de la source pour limiter efficacement aux seules personnes autorisées. *Reconnaissance par le personnel de l'exploitant.* *Verrous pour véhicules aux spécifications adaptées.* *Clés gardées par le personnel autorisé.*
	Mesures pour vérifier que les personnes autorisées sont dignes de confiance. *Vérification périodique des antécédents du personnel de l'exploitant conformément à la politique nationale.*	Mesures pour vérifier que les personnes autorisées sont dignes de confiance. *Vérification périodique des antécédents du personnel de l'exploitant conformément à la politique nationale.*	Mesures pour vérifier que les personnes autorisées sont dignes de confiance. *Vérification périodique des antécédents du personnel de l'exploitant s'occupant de gérer la source, conformément à la politique nationale.*	Mesures pour vérifier que les personnes autorisées sont dignes de confiance. *Vérification périodique des antécédents du personnel de l'exploitant conformément à la politique nationale.*

Fonction de sécurité	Grande installation fixe Niveau de sécurité A (ex. : irradiateur industriel)	Petite installation fixe Niveau de sécurité B (par ex. : petite entreprise de radiographie)	Petite installation fixe Niveau de sécurité C (par ex. : petite chaîne de traitement)	Ajustements pour les utilisations mobiles Niveau de sécurité B (cas spécial) (par ex. : radiographie mobile)
GESTION DE LA SÉCURITÉ	Détermination et protection des informations sensibles. Promotion de la culture de sécurité. *Initiation appropriée du personnel.* *Rôles et responsabilités.* *Stock protégé.* *Plan de sécurité.* *Procédures de gestion de la sécurité.* *Conteneurs de sécurité.*	Détermination et protection des informations sensibles. Promotion de la culture de sécurité. *Initiation appropriée du personnel.* *Rôles et responsabilités.* *Stock protégé.* *Plan de sécurité.* *Procédures de gestion de la sécurité.* *Conteneurs de sécurité.*	Détermination et protection des informations sensibles. Promotion de la culture de sécurité. *Initiation appropriée du personnel.* *Rôles et responsabilités.* *Stock protégé.* *Plan de sécurité.* *Procédures de gestion de la sécurité.* *Conteneurs de sécurité (enceinte verrouillée).*	Détermination et protection des informations sensibles. Promotion de la culture de sécurité. *Initiation appropriée du personnel.* *Rôles et responsabilités.* *Stock protégé (dans le secteur d'attache).* *Plan de sécurité.* *Procédures de gestion de la sécurité.* *Conteneurs de sécurité (dans le secteur d'attache).*
	Plan de sécurité. *Plan de sécurité conforme à l'appendice II.*	Plan de sécurité. *Plan de sécurité conforme à l'appendice II.*	Plan de sécurité. *Dispositions de sécurité conformes à l'appendice II.*	Plan de sécurité. *Plan de sécurité conforme à l'appendice II.*

Fonction de sécurité	Grande installation fixe Niveau de sécurité A (ex. : irradiateur industriel)	Petite installation fixe Niveau de sécurité B (par ex. : petite entreprise de radiographie)	Petite installation fixe Niveau de sécurité C (par ex. : petite chaîne de traitement)	Ajustements pour les utilisations mobiles Niveau de sécurité B (cas spécial) (par ex. : radiographie mobile)
GESTION DE LA SÉCURITÉ	Moyen de gestion des événements de sécurité couverts par les plans d'intervention spécialisés pour la sécurité. *Initiation/formation/sensibilisation du personnel.* *Plan d'intervention spécialisé sur la sécurité (dans le cadre du plan de sécurité).* *Séances d'information en retour sur les enseignements tirés.* *Exercices occasionnels, dans le cadre du plan d'intervention spécialisé sur la sécurité.* *Examen du plan d'intervention spécialisé sur la sécurité.*	Moyen de gestion des événements de sécurité couverts par les plans d'intervention spécialisés pour la sécurité. *Initiation/formation/sensibilisation du personnel.* *Plan d'intervention spécialisé sur la sécurité (dans le cadre du plan de sécurité).* *Séances d'information en retour sur les enseignements tirés.* *Preuve de contacts périodiques avec la police locale.* *Examen du plan d'intervention spécialisé sur la sécurité.*	Moyen de gestion des événements de sécurité couverts par les plans d'intervention spécialisés pour la sécurité. *Initiation/formation/sensibilisation du personnel.* *Plan d'intervention spécialisé sur la sécurité (dans le cadre du plan de sécurité).* *Examen du plan d'intervention spécialisé sur la sécurité pour les périodes de maintenance et annuellement pour les opérations.*	Moyen de gestion des événements de sécurité couverts par les plans d'intervention spécialisés pour la sécurité. *Initiation/formation/sensibilisation du personnel.* *Plan d'intervention spécialisé sur la sécurité (dans le cadre du plan de sécurité).* *Séances d'information en retour sur les enseignements tirés.* *Preuve de contacts avec la police locale à chaque visite.* *Examen du plan d'intervention spécialisé sur la sécurité.*
	Système de notification d'événements de sécurité. *Responsabilités identifiées en matière de notification (dans le plan de sécurité).* *Rapports verbaux immédiats induisant des rapports de suivi écrits prévus dans le plan de sécurité.* *Clarté vérifiable sur l'itinéraire de notification.*	Système de notification d'événements de sécurité. *Responsabilités identifiées en matière de notification (dans le plan de sécurité).* *Rapports verbaux immédiats induisant des rapports de suivi écrits prévus dans le plan de sécurité.* *Clarté vérifiable sur l'itinéraire de notification.*	Système de notification d'événements de sécurité. *Responsabilités identifiées en matière de notification (dans le plan de sécurité).* *Rapports verbaux immédiats induisant des rapports de suivi écrits prévus dans le plan de sécurité.* *Clarté vérifiable sur l'itinéraire de notification.*	Système de notification d'événements de sécurité. *Responsabilités identifiées en matière de notification (dans le plan de sécurité).* *Rapports verbaux immédiats induisant des rapports de suivi écrits prévus dans le plan de sécurité.* *Clarté vérifiable sur l'itinéraire de notification.*

RÉFÉRENCES

[1] AGENCE INTERNATIONALE DE L'ENERGIE ATOMIQUE, Code de conduite sur la sûreté et la sécurité des sources radioactives, IAEA/CODEOC/2004, AIEA, Vienne (2004).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Sources (Interim Guidance for Comment), IAEA-TECDOC-1355, IAEA, Vienna (2003).

[3] AGENCE INTERNATIONALE DE L'ENERGIE ATOMIQUE, Catégorisation des sources radioactives, collection Normes de sûreté n° RS-G-1.9, AIEA, Vienne (2011).

[4] AGENCE INTERNATIONALE DE L'ENERGIE ATOMIQUE, Sûreté des générateurs de rayonnements et des sources radioactives scellées, collection Normes de sûreté n° RS-G-1.10, AIEA, Vienne (2008).

[5] AGENCE DE L'OCDE POUR L'ÉNERGIE NUCLÉAIRE, AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, ORGANISATION DES NATIONS UNIES POUR L'ALIMENTATION ET L'AGRICULTURE, ORGANISATION INTERNATIONALE DU TRAVAIL, ORGANISATION MONDIALE DE LA SANTÉ, ORGANISATION PANAMÉRICAINE DE LA SANTÉ, Normes fondamentales internationales de protection contre les rayonnements ionisants et de sûreté des sources de rayonnements, collection Sécurité n° 115, AIEA, Vienne (1997).

[6] AGENCE DE L'OCDE POUR L'ÉNERGIE NUCLÉAIRE, AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, COMMUNAUTÉ EUROPÉENNE DE L'ÉNERGIE ATOMIQUE, ORGANISATION DES NATIONS UNIES POUR L'ALIMENTATION ET L'AGRICULTURE, ORGANISATION INTERNATIONALE DU TRAVAIL, ORGANISATION MARITIME INTERNATIONALE, ORGANISATION MONDIALE DE LA SANTÉ, ORGANISATION PANAMÉRICAINE DE LA SANTÉ, PROGRAMME DES NATIONS UNIES POUR L'ENVIRONNEMENT, Principes fondamentaux de sûreté, collection Normes de sûreté n° SF-1, AIEA, Vienne (2007).

[7] Convention internationale pour la répression des actes de terrorisme nucléaire, Nations Unies (2005).

[8] Convention sur la protection physique des matières nucléaires, INFCIRC/274/Rev.1, AIEA, Vienne (1980) ; Amendement de la Convention sur la protection physique des matières nucléaires, GOV/INF/2005/10-GC(49)/INF/6, AIEA, Vienne (2005).

[9] AGENCE INTERNATIONALE DE L'ENERGIE ATOMIQUE, Préparation et intervention en cas de situation d'urgence nucléaire ou radiologique, collection Normes de sûreté no GS-R-2, AIEA, Vienne (2004).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Remediation of Areas Contaminated by Past Activities and Accidents Safety Requirement, IAEA Safety Standards Series No. WS-R-3, IAEA, Vienna (2003).

[11] INTERNATIONAL COMMISSION ON RADIOLOGICAL PROTECTION, Protecting People against Radiation Exposure in the Event of A Radiological Attack Publication 96, Pergamon Press, Oxford (2005).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Security in the Transport of Radioactive Material, IAEA Nuclear Security Series No. 9, IAEA, Vienna (2008).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).
[14] AGENCE INTERNATIONALE DE L'ENERGIE ATOMIQUE, Culture de sécurité nucléaire, collection Sécurité nucléaire de l'AIEA no 7, AIEA, Vienne (2009).
[15] INTERNATIONAL ATOMIC ENERGY AGENCY Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).
[16] AGENCE INTERNATIONALE DE L'ENERGIE ATOMIQUE, Infrastructure législative et gouvernementale pour la sûreté nucléaire, la sûreté radiologique, la sûreté des déchets radioactifs et la sûreté du transport, collection Normes de sûreté n° GS-R-1'AIEA, Vienne (2004).
[17] AGENCE INTERNATIONALE DE L'ENERGIE ATOMIQUE, Quantités dangereuses de matières radioactives (valeurs D), EPR-D-Values 2006, collection Préparation et conduite des interventions d'urgence, AIEA, Vienne (2012).
[18] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Glossaire de sûreté de l'AIEA, Terminologie employée en sûreté nucléaire et en radioprotection, Édition 2007, AIEA, Vienne (2007), http://www-ns.iaea.org/standards/safety-glossary.html.
[19] La protection physique des matières et installations nucléaires, INFCIRC/225/Rev.4, AIEA, Vienne (2000).

DÉFINITIONS

acte malveillant. Acte ou activité illicite accompli ou menée intentionnellement sans justification ou prétexte légal (tel que la contrebande), ou acte ou activité visant à tuer ou blesser des personnes, ou à causer un dommage matériel à des personnes (tel que le vol) ou un dommage à des biens ou à l'environnement (définition adoptée du document GOV/2002/10).

autorisation. Permission accordée dans un document par un organisme de réglementation à une personne qui a déposé une demande en vue de gérer une source radioactive. L'autorisation peut revêtir la forme d'un enregistrement, d'une licence ou d'autres mesures de contrôle juridique efficaces qui satisfont aux objectifs du Code de conduite (définition adoptée de la Réf. [1]).

culture de sécurité. Caractéristiques et attitudes qui, dans les organismes et chez les personnes, font que les questions relatives à la sécurité bénéficient de l'attention qu'elles méritent en raison de leur importance (définition adoptée de la Réf. [1]).

enlèvement non autorisé. Vol ou obtention par d'autres moyens illicites de sources radioactives (définition adaptée de la Réf. [19]).

entreposage. Conservation de sources radioactives dans une installation qui pourvoit à leur confinement avec intention de les récupérer (définition adoptée de la Réf. [1]).

évaluation de la menace. Analyse qui établit les motivations, intentions et capacités crédibles d'agresseurs potentiels susceptibles d'être à l'origine de conséquences négatives pour des matières nucléaires en cours d'utilisation, d'entreposage ou de transport ou pour des installations associées (définition adoptée de la Réf. [12]).

évaluation de la vulnérabilité. Processus permettant d'évaluer et de documenter les caractéristiques et l'efficacité de l'ensemble du système de sécurité dans une installation donnée.

exploitant. Tout organisme ou toute personne qui a demandé ou obtenu une autorisation et/ou qui est responsable de la sûreté nucléaire, de la sûreté radiologique, de la sûreté des déchets radioactifs ou de la sûreté du transport

lors de l'exécution d'activités ou en ce qui concerne toute installation nucléaire ou source de rayonnements ionisants. Il peut s'agir notamment de particuliers, d'organismes publics, d'expéditeurs ou de transporteurs, de titulaires d'autorisation, d'hôpitaux, de travailleurs indépendants, etc. (définition adoptée de la Réf. [18]).

menace de référence. Exposé détaillé des motifs, des intentions et des capacités d'agresseurs potentiels sur la base desquels sont conçus et évalués les systèmes de protection (définition adoptée de la Réf. [13]).

organisme de réglementation. Entité ou organisation ou réseau d'entités ou d'organisations investie(s) par le gouvernement d'un État des pouvoirs juridiques nécessaires pour exercer le contrôle réglementaire des sources radioactives, y compris la délivrance des autorisations, et donc réglementer un ou plusieurs aspects de la sûreté ou de la sécurité de ces sources (définition adoptée de la Réf. [1]).

plan de sécurité. Document - établi par l'exploitant et devant éventuellement être revu par l'organisme de réglementation pour examen - qui présente une description détaillée des dispositions de sécurité en place dans une installation.

plan d'intervention spécialisé sur la sécurité. Partie du plan de sécurité ou document indépendant qui détermine les événements de sécurité raisonnablement prévisibles, indique les mesures initiales prévues (y compris l'alerte des autorités compétentes) et attribue des responsabilités au personnel de l'exploitant et au personnel d'intervention appropriés.

sabotage. Endommagement délibéré ; le sabotage dans ce contexte est l'endommagement délibéré d'une source radioactive en cours d'utilisation, d'entreposage ou de transport, ou d'une installation associée. Un acte délibéré dirigé contre une source radioactive en cours d'utilisation, d'entreposage ou de transport pourrait, directement ou indirectement, porter atteinte à la santé ou à la sûreté du personnel ou du public, ou à l'environnement, en provoquant une exposition à des rayonnements ou un relâchement de matières radioactives (définition adaptée de la Réf. [19]).

sécurité (nucléaire). Prévention, détection et intervention en cas de vol, de sabotage, d'accès non autorisé, de cession illégale ou d'autres actes malveillants mettant en jeu des matières nucléaires et autres matières radioactives ou les installations associées (définition adoptée de la Réf. [12]).

source radioactive. Matière radioactive qui est enfermée d'une manière permanente dans une capsule ou fixée sous forme solide et qui n'est pas exemptée du contrôle réglementaire. Ce terme englobe également toute matière radioactive rejetée si la source radioactive fuit ou est brisée, mais pas les matières enfermées aux fins de stockage définitif, ni les matières nucléaires faisant partie du cycle du combustible nucléaire de réacteurs de recherche et de puissance (définition adoptée de la Réf. [1]).

source retirée du service. Source radioactive qui n'est plus utilisée et n'est plus destinée à l'être dans le cadre des installations et des activités pour lesquelles une autorisation a été octroyée (définition adoptée de la Réf. [18]).

IAEA
Agence internationale de l'énergie atomique

Lieux de vente des publications de l'AIEA

Dans les pays suivants, vous pouvez vous procurer les publications de l'AIEA chez nos dépositaires ci-dessous ou auprès de grandes librairies. Le paiement peut être effectué en monnaie locale ou avec des coupons Unesco.

ALLEMAGNE
UNO-Verlag, Vertriebs- und Verlags GmbH, Am Hofgarten 10, 53113 Bonn
Téléphone : + 49 228 94 90 20 • Télécopie : +49 228 94 90 20 ou +49 228 94 90 222
Courriel : bestellung@uno-verlag.de • Site web : http://www.uno-verlag.de

AUSTRALIE
DA Information Services, 648 Whitehorse Road, MITCHAM 3132
Téléphone : +61 3 9210 7777 • Télécopie : +61 3 9210 7788
Courriel : service@dadirect.com.au • Site web : http://www.dadirect.com.au

BELGIQUE
Jean de Lannoy, 202 avenue du Roi, 1190 Bruxelles
Téléphone : +32 2 538 43 08 • Télécopie : +32 2 538 08 41
Courriel : jean.de.lannoy@infoboard.be • Site web : http://www.jean-de-lannoy.be

CANADA
Bernan Associates, 4501 Forbes Blvd, Suite 200, Lanham, MD 20706-4346, États-Unis d'Amérique
Téléphone : 1-800-865-3457 • Télécopie : 1-800-865-3450
Courriel : customercare@bernan.com • Site web : http://www.bernan.com

Renouf Publishing Company Ltd., 1-5369 Canotek Rd., Ottawa, Ontario, K1J 9J3
Téléphone : +613 745 2665 • Télécopie : +613 745 7660
Courriel : order.dept@renoufbooks.com • Site web : http://www.renoufbooks.com

CHINE
Publications de l'AIEA en chinois : China Nuclear Energy Industry Corporation, Translation Section, P.O. Box 2103, Beijing

CORÉE, RÉPUBLIQUE DE
KINS Inc., Information Business Dept. Samho Bldg. 2nd Floor, 275-1 Yang Jae-dong SeoCho-G, Seoul 137-130
Téléphone : +02 589 1740 • Télécopie : +02 589 1746 • Site web : http://www.kins.re.kr

ESPAGNE
Díaz de Santos, S.A., c/Juan Bravo, 3A, 28006 Madrid
Téléphone : +34 91 781 94 80 • Télécopie : +34 91 575 55 63
Courriel : compras@diazdesantos.es, carmela@diazdesantos.es, barcelona@diazdesantos.es, julio@diazdesantos.es • Site web : http://www.diazdesantos.es

ÉTATS-UNIS D'AMÉRIQUE
Bernan Associates, 4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4346
Téléphone : 1-800-865-3457 • Télécopie : 1-800-865-3450
Courriel : customercare@bernan.com • Site web : http://www.bernan.com

Renouf Publishing Company Ltd., 812 Proctor Ave., Ogdensburg, NY, 13669
Téléphone : +888 551 7470 (nº vert) • Télécopie : +888 568 8546 (nº vert)
Courriel : order.dept@renoufbooks.com • Site web : http://www.renoufbooks.com

FINLANDE
Akateeminen Kirjakauppa, PO BOX 128 (Keskuskatu 1), 00101 Helsinki
Téléphone : +358 9 121 41 • Télécopie : +358 9 121 4450
Courriel : akatilaus@akateeminen.com • Site web : http://www.akateeminen.com

FRANCE
Form-Edit, 5 rue Janssen, B.P. 25, 75921 Paris Cedex 19
Téléphone : +33 1 42 01 49 49 • Télécopie : +33 1 42 01 90 90
Courriel : formedit@formedit.fr • Site web : http://www. formedit.fr

Lavoisier SAS, 145 rue de Provigny, 94236 Cachan Cedex
Téléphone : + 33 1 47 40 67 02 • Télécopie : +33 1 47 40 67 02
Courriel : romuald.verrier@lavoisier.fr • Site web : http://www.lavoisier.fr

HONGRIE
Librotrade Ltd., Book Import, P.O. Box 126, 1656 Budapest
Téléphone : +36 1 257 7777 • Télécopie : +36 1 257 7472 • Courriel : books@librotrade.hu

INDE
Allied Publishers Group, 1st Floor, Dubash House, 15, J. N. Heredia Marg, Ballard Estate, Mumbai 400 001
Téléphone : +91 22 22617926/27 • Télécopie : +91 22 22617928
Courriel : alliedpl@vsnl.com • Site web : http://www.alliedpublishers.com

Bookwell, 2/72, Nirankari Colony, Delhi 110009
Téléphone : +91 11 23268786, +91 11 23257264 • Télécopie : +91 11 23281315
Courriel : bookwell@vsnl.net

ITALIE
Libreria Scientifica Dott. Lucio di Biasio « AEIOU », Via Coronelli 6, 20146 Milan
Téléphone : +39 02 48 95 45 52 ou 48 95 45 62 • Télécopie : +39 02 48 95 45 48
Courriel : info@libreriaaeiou.eu • Site web : www.libreriaaeiou.eu

JAPON
Maruzen Company, Ltd., 13-6 Nihonbashi, 3 chome, Chuo-ku, Tokyo 103-0027
Téléphone : +81 3 3275 8582 • Télécopie : +81 3 3275 9072
Courriel : journal@maruzen.co.jp • Site web : http://www.maruzen.co.jp

NOUVELLE-ZÉLANDE
DA Information Services, 648 Whitehorse Road, Mitcham Victoria 3132, Australie
Téléphone : +61 3 9210 7777 • Télécopie : +61 3 9210 7788
Courriel : service@dadirect.com.au • Site web : http://www.dadirect.com.au

ORGANISATION DES NATIONS UNIES
Dépt. I004, Bureau DC2-0853, First Avenue at 46th Street, New York, N.Y. 10017, États-Unis d'Amérique
(ONU) Téléphone : +800 253-9646 ou +212 963-8302 • Télécopie : +212 963-3489
Courriel : publications@un.org • Site web : http://www.un.org

PAYS-BAS
De Lindeboom Internationale Publicaties B.V., M.A. de Ruyterstraat 20A, 7482 BZ Haaksbergen
Téléphone : +31 (0) 53 5740004 • Télécopie : +31 (0) 53 5729296
Courriel : books@delindeboom.com • Site web : http://www.delindeboom.com

Martinus Nijhoff International, Koraalrood 50, P.O. Box 1853, 2700 CZ Zoetermeer
Téléphone : +31 793 684 400 • Télécopie : +31 793 615 698
Courriel : info@nijhoff.nl • Site web : http://www.nijhoff.nl

Swets and Zeitlinger b.v., P.O. Box 830, 2160 SZ Lisse
Téléphone : +31 252 435 111 • Télécopie : +31 252 415 888
Courriel : infoho@swets.nl • Site web : http://www.swets.nl

RÉPUBLIQUE TCHÈQUE
Suweco CZ, S.R.O., Klecakova 347, 180 21 Prague 9
Téléphone : +420 26603 5364 • Télécopie : +420 28482 1646
Courriel : nakup@suweco.cz • Site web : http://www.suweco.cz

ROYAUME-UNI
The Stationery Office Ltd, International Sales Agency, P.O. Box 29, Norwich, NR3 1 GN
Téléphone (commandes) : +44 870 600 5552 • (demandes de renseignements) : +44 207 873 8372 •
Télécopie : +44 207 873 8203
Courriel (commandes) : book.orders@tso.co.uk • (demandes de renseignements) : book.enquiries@tso.co.uk •
Site web : http://www.tso.co.uk

Commandes en ligne
DELTA Int. Book Wholesalers Ltd., 39 Alexandra Road, Addlestone, Surrey, KT15 2PQ
Courriel : info@profbooks.com • Site web : http://www.profbooks.com

Ouvrages sur l'environnement
Earthprint Ltd., P.O. Box 119, Stevenage SG1 4TP
Téléphone : +44 1438748111 • Télécopie : +44 1438748844
Courriel : orders@earthprint.com • Site web : http://www.earthprint.com

SLOVÉNIE
Cankarjeva Zalozba d.d., Kopitarjeva 2, 1512 Ljubljana
Téléphone : +386 1 432 31 44 • Télécopie : +386 1 230 14 35
Courriel : import.books@cankarjeva-z.si • Site web : http://www.cankarjeva-z.si/uvoz

Les commandes et demandes d'information peuvent aussi être adressées directement à :

Unité de la promotion et de la vente, Agence internationale de l'énergie atomique
Centre international de Vienne, B.P. 100, 1400 Vienne (Autriche)
Téléphone : +43 1 2600 22529 (ou 22530) • Télécopie : +43 1 2600 29302
Courriel : sales.publications@iaea.org • Site web : http://www.iaea.org/books

12-14902

Le présent rapport comprend des orientations et des mesures recommandées pour la prévention et la détection d'actes malveillants mettant en jeu des sources radioactives et pour l'intervention en cas de tels actes. Il vise à prévenir la perte du contrôle de ces sources. Il recommande en outre l'application de mesures de sécurité aux sources radioactives en cours de fabrication, d'utilisation, et d'entreposage de courte ou de longue durée. Le présent guide d'application recommande que les mesures de sécurité soient appliquées sur une base graduée, en tenant compte de l'évaluation actuelle de la menace, de l'attractivité relative de la source et des conséquences potentielles de l'utilisation malveillante. On atteint le niveau de sécurité requis en combinant dissuasion, détection, retardement, intervention et gestion de la sécurité.

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE
ISBN 978–92–0–232910–2
ISSN 1816–9317