Collection Sécurité nucléaire de l'AIEA – N° 8

Guide d'application

Mesures de prévention et de protection contre les menaces internes

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.

MESURES DE PRÉVENTION ET DE PROTECTION CONTRE LES MENACES INTERNES

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
FIDJI
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
RWANDA
SAINT-SIÈGE
SÉNÉGAL
SERBIE
SEYCHELLES
SIERRA LEONE
SINGAPOUR
SLOVAQUIE
SLOVÉNIE
SOUDAN
SRI LANKA
SUÈDE
SUISSE
TADJIKISTAN
TCHAD
THAÏLANDE
TOGO
TRINITÉ-ET-TOBAGO
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 Nº 8

MESURES DE PRÉVENTION ET DE PROTECTION CONTRE LES MENACES INTERNES

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
Novembre 2012
STI/PUB/1359

MESURES DE PRÉVENTION
ET DE PROTECTION CONTRE LES
MENACES INTERNES
AIEA, VIENNE, 2012
STI/PUB/1359
ISBN 978–92–0–236710–4
ISSN 1816–9317

AVANT-PROPOS

En application de la résolution GC(46)/RES/13 de la Conférence générale de l'AIEA du 20 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 et des installations nucléaires, la comptabilisation des matières nucléaires, la détection et l'intervention en cas de trafic de matières nucléaires et autres matières radioactives, la sécurité des sources radioactives, la sécurité du transport de matières nucléaires et autres matières radioactives, les interventions d'urgence et leur préparation dans les États Membres et à l'AIEA, et la promotion de l'acceptation et de l'application par les États des 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 des autres matières radioactives, ainsi que des installations connexes, de garantir la sécurité de ces matières lors de leur transport, et de lutter contre le trafic illicite et les mouvements fortuits de ces matières.

Les systèmes de protection physique visent à prévenir des conséquences inacceptables résultant d'actes malveillants. Plus les conséquences potentielles sont graves, plus il importe d'avoir un degré de confiance élevé dans l'efficacité de la protection physique, comme elle a été planifiée.

Si elles font l'objet d'actes malveillants, les matières et les installations nucléaires risquent d'être à l'origine de diverses conséquences radiologiques et de prolifération inacceptables. La nécessité d'un degré de confiance élevé dans l'efficacité de la protection physique a été reconnue depuis longtemps par tous ceux qui sont concernés par les matières et les installations nucléaires. Le niveau de confiance maximum dans la protection physique exige une étroite corrélation entre les mesures de protection et la menace. Cette approche est fermement ancrée dans le principe fondamental selon lequel la protection physique des actifs nucléaires relevant de la compétence juridictionnelle d'un État devrait être basée sur l'évaluation par l'État de la menace pesant sur ces actifs.

Bien comprendre la menace permet d'établir une description détaillée des agresseurs potentiels, qu'ils soient « externes » ou « internes ».

En particulier, les menaces internes constituent un problème unique pour un système de protection physique. Un agresseur interne pourrait mettre à profit ses droits d'accès, associés à son autorité et à sa connaissance de l'installation, pour contourner les dispositifs de protection physique ou d'autres dispositions telles que les mesures de sûreté, les mesures de comptabilité et de contrôle des matières, et les mesures et procédures d'exploitation. Par ailleurs, en tant que personnes de confiance disposant d'un accès, les agresseurs internes ont la

possibilité d'employer des méthodes de « fraude » inaccessibles aux agresseurs externes face aux dispositifs de protection et de contrôle d'accès. Les agresseurs internes ont plus de possibilités de choisir la cible la plus vulnérable et le moment le plus opportun pour commettre l'acte malveillant.

Un certain nombre de publications de l'AIEA traitent de la protection physique contre l'enlèvement non autorisé de matières nucléaires et contre le sabotage de matières et d'installations nucléaires. Elles contiennent des recommandations générales sur la conception et l'évaluation des mesures de protection, et sont principalement axées sur la prévention des menaces externes.

Afin d'élaborer un ensemble complet d'orientations, il a été décidé d'établir un guide traitant spécifiquement des agresseurs internes. En conséquence, la présente publication donne des orientations générales concernant la prévention et la protection contre les menaces internes. Elle indique comment mettre en œuvre les recommandations du document INFCIRC/225/Rev.4 et devrait être utilisée conjointement avec les documents IAEA-TECDOC-967 (Rev. 1) et IAEA-TECDOC-1276, ainsi qu'avec les autres publications de la collection Sécurité nucléaire de l'AIEA.

TABLE DES MATIÈRES

1. INTRODUCTION

1.1. CONTEXTE

Un certain nombre de publications de l'AIEA traitent de la protection physique contre l'enlèvement non autorisé de matières nucléaires et contre le sabotage de matières et d'installations nucléaires.

La Convention sur la protection physique des matières nucléaires (CPPMN) [1] contient des dispositions générales pour la protection physique des matières nucléaires et des dispositions spécifiques pour la protection de ces matières lors de transports internationaux. L'amendement de la CPPMN [2] adopté par la conférence diplomatique des États parties à la CPPMN par consensus le 8 juillet 2005 est soumis à ratification, acceptation ou approbation. Il couvre les dispositions portant sur la protection physique des matières nucléaires en cours d'utilisation, d'entreposage et de transport sur le territoire national, ainsi que sur la protection des matières et des installations nucléaires contre le sabotage. Il reflète par ailleurs les « Objectifs et principes fondamentaux de la protection physique » [3].

Le document intitulé « Objectifs et principes fondamentaux de la protection physique » (GOV/ 2001/41) [3] contient quatre objectifs généraux et 12 principes essentiels à l'élaboration d'un système exhaustif de protection physique.

Le document INFCIRC/225/Rev.4 [4], intitulé « Protection physique des matières et installations nucléaires » contient des recommandations et d'autres orientations à l'intention des autorités nationales compétentes quant à la manière de mettre en œuvre les dispositions nationales en cohérence avec ces recommandations. Ce document est complété par le document IAEA-TECDOC-967 (Rev.1), Orientations et considérations concernant l'application du document INFCIRC/225/Rev.4 [5].

Le manuel sur la protection physique des matières et installations nucléaires (IAEA-TECDOC-1276) [6] donne aux exploitants d'installations des conseils pratiques sur la conception d'un système de protection physique, sur l'éventail des mesures et des équipements par type d'installation, et sur les fonctions d'intervention et les orientations permettant à l'exploitant d'évaluer l'efficacité du système de protection physique existant ; cependant, ce manuel ne traite des menaces internes que dans une mesure limitée.

1.2. PROBLÈMES LIÉS À L'AGRESSEUR INTERNE

Le terme « agresseur » désigne toute personne qui commet ou tente de commettre un acte malveillant. L'agresseur peut être interne ou externe. L'expression « agresseur interne » désigne un agresseur disposant d'une autorisation d'accès à une installation nucléaire, à une opération de transport ou à des informations sensibles. L'expression « agresseur externe » désigne un agresseur autre qu'un agresseur interne.

Un système de protection physique est conçu et évalué en fonction des menaces présentées à la fois par les agresseurs externes et par les agresseurs internes. Les agresseurs internes constituent un problème unique. Ils pourraient tirer profit de leur accès (droit ou possibilité d'obtenir l'accès), associé à leur autorité (pouvoir ou droit d'imposer l'obéissance) et à leur connaissance de l'installation (familiarité ou connaissances acquises lors des formations ou grâce à l'expérience), pour contourner les éléments dédiés de protection physique ou d'autres dispositions telles que les mesures de comptabilité et de contrôle des matières nucléaires (CCMN), ainsi que les mesures et les procédures d'exploitation.

Par ailleurs, en tant que personnes disposant d'un droit d'accès et en situation de confiance, les agresseurs internes pourraient employer des procédés de fraude inaccessibles aux agresseurs externes. Les agresseurs internes ont davantage d'occasions (c'est-à-dire des conditions plus favorables) de sélectionner la cible la plus vulnérable et le moment le plus opportun pour commettre ou tenter de commettre un acte malveillant. Ils ont la possibilité de prolonger l'acte malveillant sur une longue période afin de maximiser la probabilité de réussite. Cela pourrait inclure par exemple la manipulation frauduleuse des équipements de sûreté en vue de préparer une tentative ou un acte de sabotage, ou la falsification des relevés comptables afin de procéder, à plusieurs reprises, au vol de petites quantités de matières nucléaires.

Le présent guide fournit des orientations sur la manière d'appliquer les recommandations établies dans le document INFCIRC/225/Rev.4 [4] – ci-après référencé INFCIRC/225 – et traite expressément des agresseurs internes. Il devrait être utilisé en association avec les documents IAEA-TECDOC-967 (Rev.1) [5] et IAEA-TECDOC-1276 [6].

1.3. OBJET ET CHAMP D'APPLICATION

Le présent guide a pour objet d'énoncer des orientations générales à lintention des autorités compétentes et des exploitants[1] concernant la prévention et la protection contre les menaces internes. Les menaces pesant sur les installations nucléaires peuvent impliquer des agresseurs externes, des agresseurs internes voire la collusion des deux.

Le terme « menace » désigne une cause probable de dommage aux personnes, aux biens ou à l'environnement du fait d'une ou de plusieurs personnes ayant les motivations, l'intention et la capacité de commettre un acte malveillant. Les agresseurs internes constituent une menace sérieuse pour une installation, car ils peuvent exploiter leur droit d'accès, leur autorité et leurs connaissances pour tromper la confiance d'autrui et contourner les mesures de sécurité.

Un agresseur interne peut être présent à n'importe quel poste dans une installation, du simple employé au poste le plus élevé de la hiérarchie. L'analyse détaillée des menaces internes est, par nature, spécifique à chaque installation du fait de la grande diversité des installations à protéger (réacteurs de recherche, centrales nucléaires et autres installations du cycle du combustible nucléaire, par exemple). En raison de la nature spécifique de la menace interne, liée à l'installation, aucun document général tel que le document INFCIRC/225 n'inclut d'orientations à ce sujet.

Le champ d'application du présent guide – conformément au document INFCIRC/225 – couvre l'enlèvement non autorisé de matières nucléaires et le sabotage de matières et d'installations nucléaires. Le présent guide s'applique à tout type d'installations nucléaires, notamment aux centrales nucléaires, aux réacteurs de recherche et aux autres installations du cycle du combustible nucléaire (telles que les usines d'enrichissement, les usines de retraitement, les installations de fabrication de combustible et les installations d'entreposage), qu'elles soient en service, à l'arrêt ou en cours de démantèlement.

Le présent guide devrait être pris en compte lors de la conception, de la construction, de la mise en service et des différentes phases d'exploitation de toute nouvelle installation. Il traite également de l'enlèvement non autorisé des matières nucléaires et des actes de sabotage lors du transport des matières nucléaires. Les orientations et les mesures présentées peuvent également être mises en œuvre dans le

[1] Le terme « exploitant » désigne une entité (personne physique ou morale) autorisée à procéder à l'exploitation d'une installation nucléaire ou radiologique ou à utiliser, entreposer ou transporter des matières nucléaires et/ou radioactives. Une telle entité est normalement en possession d'une licence ou de tout autre document d'autorisation délivré par une autorité compétente, ou travaille pour le compte d'une entité détentrice d'une telle autorisation.

cadre de la protection physique d'autres matières, dont les sources radioactives ou les déchets radioactifs.

La terminologie employée dans le présent guide est conforme aux définitions établies dans la CPPMN et son amendement de 2005 [1, 2] et/ou au Glossaire des garanties de l'AIEA [7].

2. IDENTIFICATION DES MENACES INTERNES POTENTIELLES

La présente section contient des orientations sur l'identification des menaces internes potentielles au niveau de l'installation. Ces orientations se fondent sur les informations portant sur les agresseurs internes fournies par les documents traitant de la menace de référence ou d'autres documents nationaux, comme une évaluation nationale de la menace, et définissent ensuite les agresseurs internes grâce à un examen rigoureux des caractéristiques du site de l'installation ou de l'opération de transport.

La menace de référence est un outil réglementaire pour la planification, la conception et l'évaluation d'un système de protection physique. L'État devrait analyser les moyens et les caractéristiques des agresseurs internes potentiels et les prendre en compte de façon appropriée dans la menace de référence. Selon l'État concerné, la menace de référence relative aux agresseurs internes peut être détaillée ou pas.

Lorsque la menace de référence n'a pas été élaborée pour certains domaines d'activités nucléaires aux conséquences limitées au plan radiologique et en matière de prolifération, les mesures à adopter pour se protéger des agresseurs internes devraient être basées sur celles proposées à la section 5. Une mise en œuvre correcte de ces mesures devrait fournir une base appropriée permettant de se conformer aux recommandations du document INFCIRC/225.

En plus des informations contenues dans la menace de référence, d'autres informations pour chaque installation ou opération de transport devraient être évaluées ou analysées afin de décrire individuellement chaque employé ou type d'agresseur interne sur la base des niveaux d'accès, de l'autorité sur autrui et des connaissances de l'exploitation de l'installation, des dispositions en matière de transport et d'autres capacités générales donnant la possibilité de commettre ou tenter de commettre des actes malveillants.

Les agresseurs internes peuvent avoir différentes motivations et peuvent être passifs ou actifs, non violents ou violents (figure 1). Le terme « motivation » désigne les mobiles qui poussent un agresseur à commettre ou tenter de

commettre un acte malveillant. La motivation peut comprendre des facteurs idéologiques, personnels, financiers et psychologiques, ainsi que d'autres mobiles comme la coercition. Les agresseurs internes pourraient agir indépendamment ou en collusion avec d'autres personnes. Ils pourraient devenir malveillants sur une simple impulsion, ou agir de manière préméditée et parfaitement préparée, en fonction de leur motivation.

Une personne pourrait être forcée à devenir agresseur interne par coercition, ou suite à une pression sur les membres de sa famille.

Les agresseurs internes passifs sont non violents et limitent leur participation à la fourniture d'informations susceptibles d'aider des agresseurs à commettre ou tenter de commettre un acte malveillant.

Les agresseurs internes actifs sont disposés à fournir des informations et exécuter des actions, et peuvent être violents ou non violents. Ils sont prêts à ouvrir des portes ou des serrures, fournir une aide pratique et contribuer à neutraliser les forces d'intervention. Les agresseurs internes actifs non violents ne souhaitent pas être identifiés ou courir le risque d'être confrontés aux forces d'intervention et peuvent limiter leurs activités à la manipulation frauduleuse des systèmes de comptabilité et de contrôle des matières, ainsi que des systèmes de sûreté et de sécurité. Les agresseurs internes actifs violents peuvent utiliser la force sans se préoccuper de savoir si cela accroît leurs chances de réussite ; ils peuvent agir de manière rationnelle ou irrationnelle.

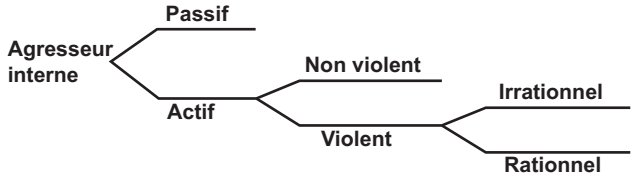

FIG. 1. Catégories d'agresseurs internes.

Il faut au moins prendre en considération les facteurs suivants :

a) Les agresseurs internes peuvent occuper n'importe quel poste dans une organisation (par exemple expérimentateur, concepteur de système de protection physique, agent de sécurité, manutentionnaire, commis, gardien, spécialiste des garanties, technicien d'exploitation et de maintenance ou cadre de direction). D'autres ne sont pas directement employés par l'exploitant, mais disposent également d'un accès (fournisseurs, personnel des services d'urgence, y compris les pompiers et les secouristes de première intervention, entrepreneurs, sous-traitants et inspecteurs des organismes de réglementation) et devraient aussi être pris en considération.

b) Les agresseurs internes peuvent disposer :

i) de l'accès à une partie ou à la totalité de l'installation, des systèmes, de l'équipement ou des outils ;

ii) de l'autorité sur l'exploitation ou le personnel ;

iii) de connaissances de l'aménagement de l'installation, des dispositions en matière de transport et/ou des processus de transport, de la protection physique, des systèmes de sûreté et d'autres informations sensibles ;

iv) des compétences techniques et de l'expérience ;

v) de l'autorité pour se procurer des outils, des équipements, des armes ou des explosifs et des capacités pour les utiliser.

Les agresseurs internes peuvent par conséquent avoir l'occasion de commettre un acte malveillant dans les conditions normales d'exploitation d'une installation, lors de la maintenance, du transport de matières nucléaires ou d'une situation d'urgence, et ils peuvent choisir le moment le plus opportun pour l'accomplir.

En plus des agresseurs internes potentiels identifiés grâce à leur capacité inhérente d'obtenir une autorisation d'accès, les personnes qui n'ont aucun accès à une installation ou à une opération de transport, mais qui détiennent suffisamment de connaissances et/ou d'autorité pour commettre un acte malveillant (par ex. un dirigeant d'entreprise qui délivre un faux bon de livraison pour un emplacement externe) devraient faire l'objet d'une attention particulière. Ces scénarios peuvent aussi être pris en compte par une évaluation de vulnérabilité réalisée à propos des agresseurs externes.

3. SITUATIONS À PRENDRE EN COMPTE DANS L'ANALYSE DES MENACES INTERNES

Certaines situations survenant dans des installations nucléaires peuvent être favorables ou propices aux menaces internes.

Certaines situations dans une installation ou lors d'un transport, y compris celles liées au personnel, aux questions en rapport avec l'emploi telles que les évaluations du comportement professionnel, les politiques de relations professionnelles et une absence de culture de sécurité, de sensibilisation à la sécurité et de programmes de fiabilité, peuvent constituer un terrain favorable ou propice aux tentatives des agresseurs internes de commettre des actes malveillants.

Les situations temporaires, comme les opérations de maintenance, peuvent conduire à une augmentation importante du nombre d'autorisations d'accès délivrées, par exemple aux entreprises sous-traitantes.

Les situations à l'extérieur de l'installation ou à proximité des itinéraires de transport, y compris l'attitude générale des populations, dans un environnement urbain ou rural, ainsi que la présence de groupes hostiles organisés, peuvent également être favorables aux agresseurs internes. Tout groupe mécontent de la population, et les diverses animosités sociales et politiques devraient être pris en considération. Une attention particulière devrait être accordée aux éventuels liens existants entre ces groupes et les personnes possédant une expérience de l'exploitation de l'installation ou détenant une autorisation d'accès à l'installation nucléaire.

L'exploitant devra être conscient de ces situations lors de l'analyse des menaces internes.

4. IDENTIFICATION DE LA CIBLE

La présente section a pour objet de fournir des orientations générales pour l'identification des cibles potentielles d'un enlèvement non autorisé de matières nucléaires et d'un sabotage, en insistant sur les cibles attrayantes pour les agresseurs internes. D'autres publications de l'AIEA, telles que la référence [4], fournissent des orientations plus détaillées concernant l'identification des cibles.

4.1. GÉNÉRALITÉS

L'identification des cibles est une évaluation qui définit ce qui doit être protégé a priori, y compris les matières nucléaires, les zones associées, les bâtiments et équipements, les composants, les systèmes et les fonctions, sans tenir compte de la difficulté à assurer cette protection.

Une importance particulière devrait être accordée à :

a) l'analyse de la sûreté et à l'analyse associée d'identification de zone vitale, à l'aide de la référence [4], paragraphe 7.1.5, comme point de départ de l'identification de cibles de sabotage potentielles ;
b) la catégorisation des matières nucléaires telle qu'elle est appliquée à la protection physique des matières nucléaires (INFCIR/225), afin d'identifier les cibles potentielles d'enlèvement non autorisé [4] ;
c) la menace de référence ou tout autre document national, comme l'évaluation nationale de la menace, qui fournit des informations ou des critères permettant de définir les cibles potentielles.

Les cibles des agresseurs internes diffèrent quelque peu de celles des agresseurs externes. Ainsi, les agresseurs internes pourraient voler, sur une longue période, de petites quantités de matières nucléaires sur plusieurs sites, où les quantités de matières ne sont pas intéressantes pour un agresseur externe. De plus, dans certains cas, la séquence d'actes malveillants d'un agresseur interne conduisant à un sabotage peut être indépendante de toute contrainte de temps, ce qui n'est pas le cas pour un agresseur externe.

Une analyse devrait être réalisée en vue de classer les cibles identifiées en fonction de la gravité des conséquences. Ce classement fournira la base destinée à la mise en œuvre de mesures graduelles de prévention et de protection.

4.2. CIBLES DE SABOTAGE

Les niveaux de conséquences radiologiques inacceptables sont établis par l'État ou l'autorité compétente concernée et peuvent varier d'un État à l'autre. Il est souhaitable que, lors de la spécification des niveaux de conséquences radiologiques utilisés pour les incidents d'origine malveillante, les critères de sûreté soient pris en compte. Cependant, les niveaux inacceptables de conséquences radiologiques d'actes malveillants pourraient différer de ceux pris en compte dans l'analyse de la sûreté de l'installation et peuvent nécessiter d'être classés à des niveaux supérieurs ou inférieurs à ceux de l'analyse de la sûreté.

La phase d'identification des cibles de sabotage dans une installation débute par l'utilisation du rapport de sûreté, y compris l'analyse probabiliste de sûreté pour les événements externes si celle-ci existe, et d'autres sources susceptibles de contribuer à l'identification de séquences accidentelles potentielles qui pourraient avoir des conséquences radiologiques significatives pour les travailleurs, le public et l'environnement. Une séquence accidentelle est une série d'événements résultant d'un ou plusieurs événements initiateurs (erreur humaine ou défaillance d'un ou de plusieurs composants ou fonctions) qui placent l'installation en situation dégradée malgré les dispositifs de sauvegarde et d'atténuation installés.

Toutefois, comme le sabotage n'est pas inclus dans une analyse probabiliste de sûreté, il faut en tenir compte car d'autres événements susceptibles de résulter d'un acte malveillant peuvent également entraîner des conséquences radiologiques importantes. Par exemple, dans certains cas la défaillance simultanée des composants redondants d'un système lié à la sûreté n'est pas considérée comme probable dans une analyse probabiliste de sûreté. Néanmoins, une telle défaillance pourrait vraisemblablement être provoquée par un acte de sabotage et entraîner des conséquences radiologiques. Les composants, systèmes

et fonctions dont la perte ou la défaillance due à un acte malveillant pourrait avoir de graves conséquences devraient être identifiés.

Cette approche permet de recenser les éléments les plus sensibles dans l'installation (composants, systèmes ou fonctions) ainsi que leurs emplacements.

4.3. CIBLES D'UN ENLÈVEMENT NON AUTORISÉ

L'identification des cibles potentielles d'un enlèvement non autorisé de matières nucléaires devrait prendre en compte :

a) l'enlèvement non autorisé et répété de petites quantités de matières nucléaires lors de plusieurs événements (vols sur la durée) ; et
b) l'enlèvement non autorisé d'une grande quantité de matières nucléaires lors d'un seul événement (vol brusque).

Pour prendre en considération ces deux types de vol, il faudrait tenir compte de l'ensemble du stock de matières nucléaires d'une installation ou d'une opération de transport. L'inventaire devrait indiquer la quantité, la forme, le type, l'emplacement et l'état de toutes les matières nucléaires de l'installation ou de l'opération de transport.

Les cibles d'un vol devraient être identifiées grâce aux informations ou aux critères contenus dans le document national. Ces cibles peuvent aussi être classées dans l'une des trois catégories (I, II et III) du tableau de catégorisation des matières nucléaires figurant dans la CPPMN [1] et dans l'INFCIRC/225 [4]. Ce classement devrait être basé sur le risque que les matières nucléaires soient utilisées pour un dispositif nucléaire explosif, qui dépend lui-même : du type de matière (plutonium ou uranium, par exemple) ; de la composition isotopique, c'est-à-dire de la teneur en isotopes fissiles ; de la forme physique et chimique ; du degré de dilution ; de l'intensité de rayonnement ; et de la quantité. De plus, lors de l'identification des cibles d'enlèvement non autorisé de matières nucléaires par des agresseurs internes, il faudrait envisager la possibilité qu'un agresseur rassemble, à partir de plusieurs sites contenant des matières de catégorie inférieure, l'équivalent d'une certaine quantité de matières de catégorie supérieure.

5. MESURES CONTRE DES AGRESSEURS INTERNES POTENTIELS

La présente section décrit une approche visant à contrer la menace interne et recommande quelques mesures spécifiques de prévention et de protection.

5.1. APPROCHE GÉNÉRALE

L'expression « mesures de prévention » désigne des mesures destinées à exclure ou supprimer les menaces internes potentielles, ou à réduire au maximum les occasions de menace, ou à empêcher l'exécution d'un acte malveillant. L'expression « mesures de protection » désigne les mesures visant à détecter, retarder et contrer les actes malveillants et à en atténuer ou réduire au maximum les conséquences. Les mesures de protection devraient être coordonnées avec les plans d'intervention d'urgence généraux conformément aux procédures convenues. Les plans d'intervention d'urgence devraient également inclure des dispositions concernant la récupération en cas d'enlèvement non autorisé de matières nucléaires. Les mesures de prévention et de protection devraient apporter une solution de défense en profondeur et être totalement intégrées à un programme de sécurité bien établi. L'approche à adopter pour empêcher les actes malveillants commis par des agresseurs internes et s'en protéger est décrite à la figure 2.

La figure 2 présente les étapes indiquées ci-après, représentées par les flèches entre les cases, et décrit l'approche de prévention et de protection contre les agresseurs internes potentiels identifiés à la section 2.

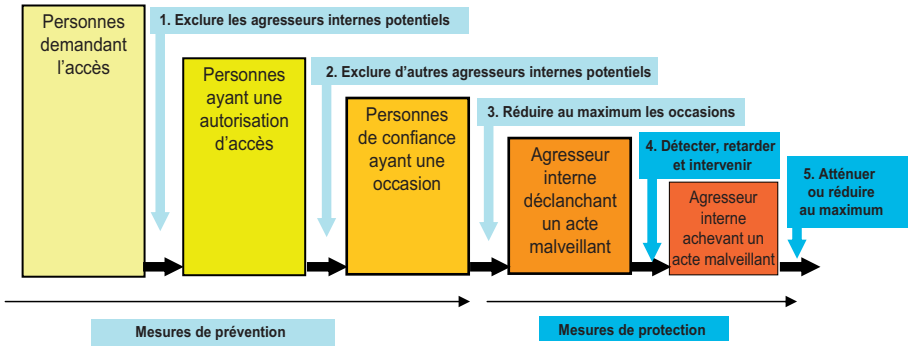

FIG. 2. Approche de prévention et de protection contre les actes malveillants commis par des agresseurs internes.

Prévention :

1) Exclure les agresseurs internes potentiels en identifiant un comportement ou des caractéristiques indésirables, indices éventuels d'une motivation, avant d'accorder une autorisation d'accès ;
2) Exclure d'autres agresseurs internes potentiels en identifiant un comportement ou des caractéristiques indésirables, indices éventuels d'une motivation, après avoir accordé une autorisation d'accès ;
3) Réduire au maximum les occasions d'actes malveillants en limitant l'accès, l'autorité et les connaissances, et par d'autres mesures.

Protection :

4) Détecter et retarder les actes malveillants et intervenir si nécessaire ;
5) Atténuer ou réduire au maximum les conséquences.

De nombreuses mesures énumérées aux sections 5.3 et 5.4 peuvent être considérées à la fois comme des mesures de prévention et de protection. La liste proposée ne devrait être considérée que comme une suggestion. Il est recommandé que chaque mesure proposée soit analysée et mise en œuvre en fonction de ses caractéristiques en matière de prévention ou de protection.

5.2. ÉLABORATION D'UNE APPROCHE EXHAUSTIVE

L'approche exhaustive consiste à mettre en place plusieurs lignes de défense, incluant à la fois les aspects administratifs (procédures, instructions, sanctions administratives, règles de contrôle de l'accès, règles de confidentialité) et les aspects techniques (systèmes de protection multiples dotés de dispositifs de détection et de retardement), que les agresseurs internes auraient à surmonter ou à contourner afin d'atteindre leurs objectifs.

L'application de mesures de prévention et de protection pour contrer la menace interne s'avère généralement beaucoup plus difficile que celle de mesures visant à contrer la menace externe, du fait des droits d'accès, des connaissances, de l'autorité et des attributs des agresseurs internes (tels que définis à la section 2). Ainsi, bien que déjà pris en compte en partie dans le cas de la menace externe, tous les éléments susceptibles de fournir une protection contre la menace interne devraient être analysés. Ces éléments incluent les capacités de détection, de retardement, d'intervention et d'atténuation des dispositifs de sûreté, de radioprotection et de CCMN. Leurs effets synergiques devraient être établis et expressément intégrés dans l'approche exhaustive.

Aux fins de la sûreté nucléaire, certains critères de conception tels que la redondance ou la diversité des systèmes et des équipements importants pour la sûreté, ou les critères d'aménagement tels que la séparation ou l'isolement physique ou géographique de ces systèmes ou de ces équipements, sont introduits dans la phase de conception de l'installation ou du colis de transport. Ces dispositions peuvent améliorer la protection contre le sabotage, car elles exigent de la part d'un agresseur interne davantage de préparation, de moyens et de temps pour commettre un acte malveillant. En conséquence, elles pourraient être d'une grande efficacité pour ce qui est de décourager, d'empêcher ou de retarder les actes de sabotage commis par des agresseurs internes, ou d'en atténuer ou réduire au maximum les conséquences radiologiques.

Les mesures de radioprotection, telles que la limitation de l'accès à des zones spécifiques, et les dispositifs de radioprotection, pourraient contribuer à la fois à décourager et à empêcher tout enlèvement non autorisé ou tout acte de sabotage par des agresseurs internes.

Les dispositifs de CCMN sont conçus pour permettre un inventaire rigoureux de toutes les matières nucléaires et pour consigner toute alerte si le bilan matières présente un écart. Ils permettent aussi aux exploitants : a) de connaître avec exactitude la quantité et le type de toutes les entrées et sorties de matières nucléaires de leurs installations ; b) de connaître en permanence l'emplacement, l'utilisation, les mouvements et la transformation des matières nucléaires ; et c) de détecter toute anomalie concernant la gestion des matières nucléaires. Le système de comptabilisation des matières nucléaires devrait être capable de détecter les transferts non autorisés au sein d'une installation, ou l'enlèvement non autorisé et répété de petites quantités de matières nucléaires d'une installation, qui pourraient échapper au système de protection physique. La détection d'anomalies devrait s'appuyer, en particulier, sur l'utilisation de scellés, de dispositifs d'indication de fraude et d'un système comptable informatisé. L'analyse du système de CCMN est indispensable afin d'en comprendre les limites et les vulnérabilités.

5.3. MESURES DE PRÉVENTION

Les mesures de prévention ont pour objectif d'exclure des agresseurs potentiels et de réduire au maximum la probabilité d'acte malveillant commis par des agresseurs internes. Les mesures suivantes sont recommandées en tant que mesures de prévention :

a) Contrôle d'identité. Les contrôles d'identité[2] authentifient l'identité d'une personne. Ils confirment que le nom et les données personnelles de l'individu en question sont exacts.

b) Enquête de sécurité. Les enquêtes de sécurité[2] consistent en des évaluations initiales et continues de l'intégrité, de l'honnêteté et de la fiabilité d'une personne lors des contrôles préalables à l'embauche et des contrôles en cours d'emploi qui visent à détecter des motivations ou des comportements donnant à penser qu'une personne peut devenir un agresseur interne. Ces contrôles tentent de repérer des facteurs de motivation tels que cupidité, facteurs financiers, idéologiques ou psychologiques, désir de vengeance (dû à un sentiment d'injustice, par exemple), dépendance physique (drogues, alcool ou sexe, par exemple) et facteurs faisant qu'une personne pourrait être contrainte par des agresseurs externes. De tels facteurs pourraient être révélés par un examen du casier judiciaire, des références, des antécédents professionnels, de la situation financière, du dossier médical, du dossier/des tests psychologique(s). Des contrôles périodiques devraient être réalisés en cours d'activité, car certaines de ces conditions peuvent ne pas être apparentes ou évoluer avec le temps. Ces examens sont particulièrement intéressants dans le cas d'employés intérimaires susceptibles de se trouver à proximité des cibles sensibles du fait de leurs tâches. Le niveau des enquêtes de sécurité devrait être gradué en fonction du niveau d'accès de la personne concernée (par ex. l'accès aux matières de catégorie III nécessitera les contrôles de niveau minimum, et l'accès aux matières de catégorie I ou aux zones vitales nécessitera les contrôles de niveau maximum). Ces procédures devraient être définies conformément aux actions décrites aux sections 2 à 4 du présent guide, qui présentent la démarche de collecte de ces informations.

c) Accompagnement et surveillance des travailleurs occasionnels et des visiteurs. Les travailleurs occasionnels, tels que ceux affectés à des tâches de maintenance, de service ou de construction, viennent souvent d'entreprises externes ou de sous-traitants. Les travailleurs occasionnels et les visiteurs peuvent ne pas avoir fait l'objet d'enquêtes de sécurité préalablement à l'autorisation d'accès. L'accompagnement de ces personnes est un moyen de s'assurer qu'elles se trouvent au bon endroit et qu'elles réalisent leurs tâches correctement. Pour être efficace, l'accompagnateur devrait connaître les activités assignées à ces personnes,

[2] Les lois nationales peuvent restreindre le champ d'action ou la réalisation des contrôles d'identité et des enquêtes de sécurité dans un État. Les dispositions du présent guide d'application sont sans préjudice des droits des personnes, y compris le droit à un procès équitable, en vertu de la législation nationale et/ou internationale.

y compris l'accès à des emplacements spécifiques, et les actions qui leur sont interdites. De plus, des patrouilles de surveillance peuvent décourager ou détecter toute tentative de ces personnes de commettre des actes malveillants.

d) Sensibilisation à la sécurité. La mise en œuvre d'un solide programme de sensibilisation à la sécurité destiné au personnel et aux sous-traitants contribue à entretenir une culture de sécurité au sein de l'organisation. Un solide programme de sensibilisation à la sécurité nécessite l'existence de politiques de sécurité claires, la mise en place de pratiques de sécurité et des activités de formation continue. Le programme de formation a pour objet d'établir un environnement dans lequel tous les employés sont attentifs aux politiques et aux procédures de sécurité, afin qu'ils soient en mesure de détecter et de signaler tout comportement ou acte inapproprié. Chaque personne, quel que soit son poste ou sa fonction, devrait être consciente des menaces et des conséquences potentielles d'actes malveillants, et de son propre rôle dans la réduction des risques et la mise en place d'un environnement de sécurité global et efficace. Les programmes de sensibilisation à la sécurité devraient aussi comporter des mesures visant à réduire les risques de chantage, de coercition, d'extorsion ou de toute autre menace sur les employés et leurs familles, et devraient encourager le signalement de telles coercitions ou tentatives au responsable de la sécurité. Enfin, les programmes de sensibilisation à la sécurité devraient être élaborés en coordination avec les programmes de sensibilisation à la sûreté en vue d'établir une culture de sûreté et une culture de sécurité efficaces et complémentaires.

e) Confidentialité (sécurité des informations). Les informations concernant les mesures de sécurité ou les cibles sensibles (emplacement du stock de matières nucléaires, plans du site ou schémas spécifiques d'équipements, de systèmes ou de dispositifs représentant les caractéristiques de conception de cibles spécifiques, combinaisons de serrures, mots de passe et modèles de clés, par exemple) pourraient permettre aux agresseurs internes de réussir à commettre un acte malveillant. Ces informations devraient rester confidentielles et seules les personnes ayant besoin de les connaître devraient y avoir accès. De plus, les informations ayant trait aux vulnérabilités potentielles des systèmes de protection physique devraient être hautement protégées et compartimentées, car elles pourraient faciliter l'enlèvement non autorisé de matières nucléaires ou l'accomplissement d'un sabotage. La compartimentation désigne l'action de diviser les informations en différentes parties contrôlées séparément afin d'empêcher les agresseurs internes de rassembler les informations nécessaires à l'accomplissement d'un acte malveillant. Une attention particulière devrait

être accordée aux informations électroniques. Garantir la confidentialité signifie que pour procéder à l'enlèvement non autorisé de matières nucléaires ou pour accomplir un sabotage, les agresseurs internes auraient à déployer des efforts supplémentaires, qui pourraient les conduire à renoncer ou à être détectés.

f) Assurance de la qualité. Une politique et des programmes d'assurance de la qualité devraient être établis et mis en œuvre pour garantir que les exigences spécifiées pour toutes les activités importantes pour la prévention et la protection contre les menaces internes sont respectées. Cela s'applique non seulement à la prévention, mais également aux autres fonctions primaires.

g) Satisfaction des employés. On ne peut présumer qu'une personne, du simple fait de son statut d'employé ou de sous-traitant, ne puisse pas ressentir une certaine insatisfaction. Par conséquent, la qualité des relations parmi les travailleurs et entre l'encadrement et les travailleurs devrait faire l'objet d'une attention particulière et être intégrée à la culture de sécurité. Les cadres devraient être entraînés à identifier et signaler tout problème concernant le comportement d'un employé vis-à-vis, par exemple, d'un cadre supérieur, d'un responsable de la sécurité ou d'un conseiller en ressources humaines. La mise en œuvre d'une politique d'évolution de carrière visant à former tous les employés au poste immédiatement supérieur dans l'organisation contribuera à créer un vivier d'experts susceptibles de remplacer un employé quittant l'organisation, même avec un prévis de courte durée, et contribuera également à l'assurance de la qualité.

h) Compartimentation physique des zones. Compartimenter l'accès à l'installation grâce à des mesures de contrôle d'accès réduit au maximum les occasions de sabotage ou d'enlèvement non autorisé de matières nucléaires par des agresseurs internes en rendant plus difficile l'obtention de données portant sur la sécurité, les cibles et les capacités totales requises pour l'accomplissement d'un acte malveillant. Tout devrait être fait pour garantir qu'une seule personne n'ait pas toutes les autorisations d'accès qui lui permettraient de commettre un acte malveillant. La portée de la compartimentation des zones doit correspondre aux risques potentiels ; en conséquence, les cibles les plus sensibles devraient être situées dans des zones hautement protégées, tandis que les cibles moins sensibles pourraient être situées dans des zones moins bien protégées. Des règles sur le besoin d'accéder, similaires à celles sur le besoin de connaître s'appliquant aux documents et aux informations sensibles, devraient être appliquées aux zones compartimentées. Le fait de limiter de manière stricte le nombre de personnes ayant accès à une zone sensible, ainsi que le nombre de

personnes habilitées à délivrer les autorisations d'accès aux zones sensibles, peut réduire les occasions pour les agresseurs internes. Durant la phase de conception, une attention particulière devrait être accordée à limiter le plus possible les accès inutiles aux zones protégées.

i) Compartimentation des activités. La compartimentation des activités limitera l'aptitude des agresseurs internes à obtenir l'ensemble des moyens nécessaires à l'accomplissement d'un acte malveillant. Lesdits moyens pourraient inclure la possibilité d'utiliser des outils et des équipements spéciaux requis pour l'exploitation ou pour la manipulation des matières. Le transfert d'outils, de matériels et d'équipements entre les zones devrait être formalisé et impliquer plusieurs personnes afin de réduire au maximum les occasions d'enlèvement non autorisé de matières nucléaires par des agresseurs internes.

j) Sanctions (sanctions disciplinaires et poursuites). Il est essentiel que les agresseurs internes potentiels soient conscients qu'une violation délibérée des lois et règlements ou des instructions de l'exploitant peut être sévèrement sanctionnée. La certitude de sanctions disciplinaires et de poursuites peut dissuader les agresseurs internes de commettre des actes malveillants. De plus, l'obligation faite aux exploitants d'informer les autorités compétentes de tout acte ou tentative d'acte malveillant fournirait, après une analyse appropriée, une base de retour d'expérience vers les autres exploitants et répondrait à un éventuel besoin d'actualisation des prescriptions réglementaires.

5.4. MESURES DE PROTECTION

Les mesures de protection ont pour objet de détecter et retarder les actes malveillants, et d'intervenir si un tel acte est commis, et d'en atténuer ou d'en réduire au maximum les conséquences. Lors de la conception et de la mise en œuvre des mesures de protection, il faudrait s'efforcer de garantir que lesdites mesures aient un impact minimal sur les systèmes de radioprotection, de sûreté ou d'intervention d'urgence. En cas de conflit, il est primordial de trouver une solution permettant de réduire au maximum le risque pour les travailleurs et le public. Les mesures ci-après sont recommandées en tant que mesures de protection.

5.4.1. Détection

Les actes malveillants peuvent être repérés grâce aux détecteurs de sécurité, à la surveillance du personnel et/ou au suivi des processus d'exploitation. Dans le

cas d'agresseurs externes, on met l'accent sur la détection du franchissement des barrières successives. La détection des actes malveillants commis par des agresseurs internes est plus difficile. Les agresseurs internes peuvent être capables de contourner de nombreuses mesures de détection, en raison de leur droit d'accès ou d'autres moyens à leur disposition. Les mesures de protection visant les agresseurs internes devraient par conséquent être axées sur la détection à la fois lors de l'accomplissement des actes et lors des activités préparatoires (non autorisées) comme la manipulation des équipements de sûreté ou la falsification des dossiers de CCMN. La détection d'agresseurs internes peut donc intervenir bien plus tard dans la séquence d'incident que celle des agresseurs externes.

Pour être efficace, la détection doit faire l'objet d'une évaluation. Il peut s'avérer difficile d'évaluer correctement et rapidement la nature d'un acte commis par un agresseur interne. Cette difficulté peut considérablement affaiblir la capacité de réagir en temps opportun.

Puisque la détection d'actes malveillants commis par des agresseurs internes dépend beaucoup de l'observation et de la surveillance, le fait de retarder davantage les actions d'un agresseur interne peut augmenter la probabilité de détection ; en conséquence, renforcer une barrière physique ou accroître la complexité d'exécution d'un acte malveillant peuvent fournir des possibilités supplémentaires de détection ou même dissuader les agresseurs internes de tenter de commettre l'acte malveillant.

Les mesures de surveillance visent à garantir que les activités de tout employé habilité sont surveillées en permanence par au moins un autre employé expérimenté et habilité, afin que tout acte non autorisé de l'un d'entre eux puisse être immédiatement détecté et signalé (« règle des deux personnes »). Cette méthode de détection peut s'avérer être un moyen rapide pour à la fois déclencher et évaluer une alarme. La surveillance peut être assurée par des collègues, des responsables ou un système de vidéosurveillance en circuit fermé. Dans le cas d'un acte malveillant, les enregistrements vidéo peuvent être utiles pour constituer une liste de suspects potentiels. En fait, sans surveillance, l'évaluation d'actes malveillants en temps utile peut se révéler difficile. Une méthode susceptible d'être utilisée pour détecter les agresseurs internes est la surveillance des postes de travail pour vérifier si des activités non autorisées sont effectuées. Cette méthode serait utile dans les cas où une personne effectuerait l'entretien incomplet d'un équipement, ou utiliserait une certaine quantité de matières nucléaires pour réaliser une tâche alors qu'une quantité différente serait consignée.

La règle des deux personnes requiert au minimum deux personnes expérimentées pour une surveillance mutuelle dans une zone sensible. Selon cette procédure de base, au moins deux personnes doivent être présentes dans une zone

sensible pour que chacune vérifie que toutes les actions sont réalisées conformément aux autorisations. Chacune des deux personnes concernées devrait être techniquement qualifiée pour détecter immédiatement des activités non autorisées. Par ailleurs, des moyens devraient être mis à disposition pour signaler immédiatement tout soupçon d'acte malveillant ou d'activité suspecte. Si l'enquête ultérieure montre qu'il n'y a eu aucun acte malveillant, il est important qu'aucune sanction ne soit prise contre l'une ou l'autre des parties en raison de cette fausse alarme, sinon les collaborateurs hésiteront à signaler les comportements suspects. Cela devrait être souligné lors de la formation de sensibilisation à la sécurité. Pour une plus grande efficacité, les deux personnes doivent être visibles l'une de l'autre en permanence, et doivent tout savoir des activités autorisées de l'autre personne. Idéalement, la règle des deux personnes voudrait que l'on affecte deux personnes compétentes à la réalisation de la tâche d'une seule personne. Cette règle est efficace tant que les deux personnes ne deviennent pas mutuellement complaisantes du fait d'une amitié ou d'une collaboration de longue date. Chaque fois que possible, les responsables devraient veiller à ce que les membres de ces équipes de deux personnes alternent. Imposer la règle des deux personnes pour l'accès aux zones sensibles constitue un élément dissuasif et peut contribuer aux actions de détection. De plus, la règle des deux personnes peut aider à protéger les détecteurs contre une manipulation frauduleuse par des agresseurs internes.

Le contrôle d'accès est utilisé pour ne permettre que des entrées ou des sorties autorisées, et pour empêcher ou détecter toute entrée ou sortie non autorisée. Le contrôle d'accès consiste en une identification des personnes au moyen de dispositifs d'identification (un ou plusieurs badges ou clés), d'un code d'accès (combinaison de serrure ou numéro d'identifiant personnel) et/ou d'un identifiant personnel (données biométriques). Le contrôle d'accès devrait également s'appliquer aux véhicules. De plus, le contrôle d'accès peut être utilisé pour déterminer les périodes de présence des personnes dans différentes zones. S'ils sont correctement tenus, les registres de contrôle d'accès peuvent être utilisés lors d'une enquête portant sur un acte malveillant pour établir une liste de suspects potentiels. Des critères spécifiques devraient être définis avant d'autoriser l'accès à une zone sensible (tels que le besoin de réaliser une tâche, le besoin d'être escorté, le besoin de connaître et le niveau de fiabilité). Les personnes autorisées à accéder à une zone sensible devraient satisfaire à ces critères. L'équipement utilisé pour fabriquer les badges et les systèmes d'attribution des accès devraient être protégés afin d'éviter une attribution d'accès non autorisée. En outre, les systèmes d'accès devraient être périodiquement vérifiés pour en garantir l'efficacité.

Le suivi des mouvements et la localisation du personnel au sein de l'installation contribuent à la protection contre la violation des règles d'accès et à

la fourniture d'informations utiles après qu'un incident a eu lieu. La technologie existante permet de suivre chaque employé dans l'ensemble de l'installation grâce à l'enregistrement des lieux et des zones visités chaque jour par l'employé, et des heures auxquelles chaque lieu a été visité. Savoir qu'une installation dispose d'un système de suivi peut dissuader un employé de se livrer à des activités non autorisées. Les enregistrements de suivi peuvent être utilisés lors d'une enquête portant sur un acte malveillant afin d'établir une première liste de suspects.

Les agresseurs internes peuvent avoir besoin d'outils, de matériels et d'armes qui ne sont pas disponibles ou pas autorisés dans l'installation pour exécuter un acte malveillant. Des contrôles devraient donc être effectués pour empêcher et détecter l'introduction d'articles illicites dans les zones sensibles. Les articles illicites peuvent comprendre des outils et des matériels non autorisés, des matériaux de protection contre les rayonnements, des armes et des explosifs, car ceux-ci pourraient être utilisés pour forcer un accès ou endommager des éléments sensibles, ainsi que pour voler des matières nucléaires. La rigueur des fouilles devrait être proportionnelle au degré de sensibilité de la zone, et les fouilles menées à proximité de la cible devraient également être plus rigoureuses.

Les méthodes de détection d'articles illicites incluent la fouille manuelle du personnel, des colis et des véhicules, l'utilisation de détecteurs de métaux, d'appareils à rayons X et de détecteurs de rayonnements, ainsi que l'utilisation de chiens et de détecteurs d'explosifs. Ces méthodes devraient prendre en compte les caractéristiques de l'installation et des menaces contre lesquelles une protection est nécessaire. En spécifiant les lieux où les fouilles doivent être menées, il faudrait veiller à ce que celles-ci ne soient pas effectuées si loin des zones sensibles, qu'il serait aisé de contourner. Par exemple, les agresseurs internes pourraient contourner les contrôles situés en limite de zone protégée en lançant les articles illicites par-dessus la clôture de la zone protégée pour les récupérer plus tard. Puisqu'il est plus difficile de fouiller les véhicules que le personnel, il est plus avantageux de limiter au maximum le nombre de véhicules autorisés à accéder aux zones sensibles.

Pour certains types de matières nucléaires, les détecteurs de rayonnements devraient être utilisés pour en détecter l'enlèvement non autorisé sur des personnes, dans des colis ou des véhicules quittant une zone protégée. Les détecteurs de rayonnements pourraient être placés aux sorties des piétons parallèlement aux détecteurs de métaux pour en renforcer l'efficacité, puisque des matériaux faisant écran peuvent être utilisés pour enlever des matières nucléaires d'une installation nucléaire. Les fouilles manuelles peuvent également être utilisées pour contrôler la sortie de personnes et de matières d'une zone. Des fouilles aléatoires peuvent être effectuées pour décourager l'enlèvement non autorisé de matières nucléaires. La sortie devrait être verrouillée par

déclenchement d'une alarme de sécurité, si cette mesure ne porte pas atteinte aux règles de sûreté. Une attention particulière devrait être accordée aux modalités d'évacuation d'urgence, y compris aux exercices, afin d'empêcher l'enlèvement non autorisé de matières nucléaires. La fouille approfondie d'un véhicule de transport, préalablement au chargement et à l'expédition, devrait être effectuée avec un soin particulier afin de s'assurer que les personnes chargées de réaliser la fouille ne puissent introduire des articles susceptibles de permettre l'accomplissement d'un acte malveillant.

La surveillance du fonctionnement normal des processus ou des activités peut être utilisée pour surveiller une zone, pour détecter une action non autorisée ou pour fournir une évaluation rapide des alarmes. Les paramètres d'exploitation d'une installation nucléaire (températures, pressions, flux, rayonnements, etc.) sont vérifiés en permanence pour s'assurer qu'ils demeurent dans les limites d'exploitation. Une alarme devrait être déclenchée quand l'un de ces paramètres dépasse un seuil spécifié. Puisque le sabotage peut provoquer une anomalie des paramètres d'exploitation, la surveillance de ces derniers peut contribuer à la détection d'actes malveillants.

Il est essentiel qu'une procédure de signalement d'alarmes soit mise en place entre le personnel d'exploitation et le personnel de sécurité se trouvant dans le poste central de sécurité. Le déclenchement d'une alarme devrait être communiqué avant même que le personnel d'exploitation en évalue l'origine (malveillante ou accidentelle).

Le personnel d'exploitation devrait surveiller les équipements, systèmes ou dispositifs sensibles pour vérifier qu'il n'y a eu aucune manipulation frauduleuse ni interférence ou pour déceler rapidement une telle manipulation ou interférence.

Les essais de routine et les opérations de maintenance ont un impact significatif sur la disponibilité des équipements et la prévention ou la correction d'un défaut ou d'une défaillance susceptible de découler d'un acte malveillant. Ces opérations peuvent se révéler très efficaces pour détecter d'éventuels actes malveillants sur des équipements ou des systèmes liés à la protection de matières nucléaires ou de zones sensibles. Lorsqu'un essai de routine ou une opération de maintenance aboutit à une modification des conditions initiales d'un système, ce dernier doit faire l'objet d'une requalification. Il est recommandé d'effectuer la requalification indépendamment de l'opération (essai ou maintenance) aboutissant à la modification. Cette approche contribue à la fois à la prévention par la dissuasion (par crainte des conséquences) et à la détection.

Un moyen d'atténuer les conséquences d'un acte malveillant est de pouvoir remplacer rapidement des pièces endommagées. Pour y parvenir il est prudent de protéger les pièces de rechange pour qu'il soit difficile de détruire ou de détériorer à la fois les pièces en service et les pièces de rechange des équipements vitaux. La protection peut être assurée, par exemple, par des barrières, par le

stockage de la pièce de rechange à bonne distance de la pièce en service et par de fréquents contrôles du lieu de stockage.

Les inspections et les audits, en particulier s'ils sont inopinés, pourraient être un moyen efficace de prévention et de protection contre l'enlèvement non autorisé de matières nucléaires et contre le sabotage. Ils permettent de détecter un équipement endommagé ou des conditions anormales et peuvent ainsi apporter aux exploitants, à l'autorité compétente ou à l'État la garantie que les mesures de prévention et de protection sont mises en œuvre avec efficacité.

5.4.2. Retardement

Le retardement est mis en œuvre par le personnel, les procédures ou les barrières physiques qui augmentent la durée de la tâche d'un agresseur. La plupart des barrières sont conçues pour retarder la pénétration dans une zone, plutôt que pour retarder l'accomplissement d'actes malveillants, et n'ont par conséquent qu'un impact limité sur les agresseurs internes. Il est toutefois possible d'élaborer des barrières pour retarder des actes malveillants à proximité d'équipements ou de matières. Ainsi, le verrouillage d'un équipement, tel qu'une vanne ou un tableau de distribution, retarde les agresseurs internes dans leur tentative de sabotage. Les barrières situées à proximité d'un équipement ou de matières sont particulièrement efficaces lorsque la zone est sous surveillance permanente.

Pour les agresseurs internes qui n'ont pas accès à certaines zones ou à certaines matières, l'installation de barrières qu'un agresseur ne pourrait surmonter sans matériel introduit en fraude ou sans compétences hautement spécialisées renforce la prévention par la dissuasion et accroît la probabilité de détection. L'accumulation de multiples barrières physiques ou procédurales variées positionnées le long de tous les itinéraires potentiels d'un agresseur interne compliquera la progression de ce dernier, qui devra mettre en œuvre des outils et des compétences variés. L'amélioration d'une barrière pour contraindre les agresseurs internes à utiliser un plus grand nombre d'outils complexes multiplie les besoins en ressources, en logistique, en formation et en compétences. Les ressources complexes peuvent ne pas être disponibles dans l'installation et devoir être introduites sur le site par les agresseurs internes. Retarder l'acte malveillant de cette manière pourrait conduire à la détection et à la mise en échec d'agresseurs internes.

Les actions de retardement peuvent également être mises en œuvre par un personnel de sécurité spécialement formé, tel que les gardiens. Dans certains cas, contourner la présence d'un tel personnel peut entraîner un retard important, en particulier pour les agresseurs internes ne disposant que de ressources limitées.

Du fait de la conception des systèmes de sûreté qui procure un certain niveau d'autoprotection, telle que la redondance des équipements, la mise à l'arrêt automatique des équipements et la fermeture automatique des vannes, la tâche d'un agresseur interne peut être rendue plus difficile si ce dernier est obligé de neutraliser de multiples fonctions et équipements redondants et dispersés. Ces dispositions peuvent retarder l'exécution d'un acte malveillant et le faire échouer.

5.4.3. Intervention

L'intervention en cas d'acte malveillant commis par un agresseur interne peut être réalisée à la fois par le personnel d'exploitation et par le personnel de sécurité. Typiquement, le personnel d'exploitation intervient pour contrer un acte malveillant ou en réduire au maximum les conséquences et le personnel de sécurité intervient contre les agresseurs internes eux-mêmes.

L'analyse classique de l'intervention face aux menaces externes compare le temps de réaction avec le temps requis pour la séquence d'actes nécessaires à l'accomplissement d'une action malveillante, pour les agresseurs externes. L'hypothèse implicite, dans une analyse de la menace externe, est que l'agresseur externe sera facilement identifié n'importe où sur le site. Aucune de ces assertions ne se vérifie pour les agresseurs internes puisqu'un acte malveillant commis par un agresseur interne peut consister en plusieurs actes séparés à la fois dans le temps et dans l'espace. Il peut s'avérer difficile d'appréhender les agresseurs internes parmi les employés, à moins qu'ils ne soient identifiés lors de la détection.

Comme indiqué précédemment, un agresseur interne n'aurait pas nécessairement besoin de réaliser tous ses actes dans un ordre déterminé, ni en succession rapide. Un agresseur interne peut commettre des actes isolés, puis attendre de voir s'ils sont détectés. La nature discontinue des actes que les agresseurs internes peuvent tenter d'accomplir peut sérieusement compliquer l'intervention de sécurité requise pour les identifier et les appréhender. En conséquence, l'enquête jouera un rôle plus important dans l'intervention face aux menaces internes. Par ailleurs, il pourrait être nécessaire que des spécialistes de l'exploitation contribuent à l'enquête afin de prédire, d'après l'événement anormal, quels autres actes malveillants sont susceptibles d'être commis.

Chaque employé ou sous-traitant se trouvant sur le site de l'installation devrait non seulement être préparé à détecter les actes malveillants, mais aussi être formé à réagir de manière appropriée pour se protéger et protéger l'installation, et savoir que la première action à mener après avoir détecté un événement est de donner l'alerte conformément à un ensemble précis de procédures. Les procédures en question devraient faire partie du programme de sensibilisation à la sécurité.

Il est essentiel de garder à l'esprit que toute personne participant à une intervention peut elle-même être un agresseur interne, et les procédures d'intervention devraient par conséquent être élaborées en tenant compte de cette hypothèse. Par exemple, un agresseur interne infiltré dans l'équipe d'intervention peut utiliser un exercice d'urgence, simuler une urgence ou créer une urgence réelle en vue de dissimuler un acte malveillant.

5.4.4. Plans d'intervention d'urgence

Les plans d'intervention d'urgence devraient être élaborés en vue de récupérer des matières nucléaires volées et d'atténuer ou de réduire au maximum les conséquences radiologiques d'un sabotage. Généralement, ces plans ne font pas la différence entre agresseurs internes et externes. Il faudrait prendre en compte le fait que les agresseurs internes peuvent être membres de l'équipe d'intervention d'urgence et désorganiser les efforts de récupération ou d'atténuation.

Les plans d'urgence destinés à la récupération ou à l'atténuation devraient être préparés pour neutraliser de manière efficace les conséquences d'un sabotage ou d'un enlèvement non autorisé. Ils devraient décrire les communications, les dispositions concernant la récupération et l'atténuation, et les contremesures immédiates à mettre en œuvre en cas d'enlèvement non autorisé de matières nucléaires ou de sabotage.

Ces plans devraient prévoir la formation des gardiens et des forces d'intervention aux actions qu'ils devraient mener en cas d'acte malveillant. De plus, d'autres membres du personnel de l'installation ou du personnel de transport devraient être formés et préparés à agir en totale coordination avec les gardiens, les forces d'intervention et les équipes d'intervention d'urgence pour la mise en œuvre des plans d'urgence.

Pour garantir qu'aucune matière nucléaire ne soit enlevée sans autorisation, les plans d'urgence devraient spécifier les procédures permettant de vérifier rapidement que toutes les matières nucléaires sont toujours présentes dans l'installation ou le moyen de transport. Les procédures de CCMN devraient permettre de vérifier à la fois la présence et la qualité des matières nucléaires afin de s'assurer qu'il n'y a eu aucune substitution par des matières inertes ou factices. Ces dispositions pourraient être complétées par des actions prises au niveau national en vue de fournir des informations et une assistance technique permettant de localiser et de récupérer toute matière nucléaire manquante, si nécessaire.

Les plans d'urgence devraient garantir la coordination et contenir les protocoles des interfaces opérationnelles entre les exploitants et les autorités locales, régionales et nationales. Les plans d'urgence concernant les actes

malveillants devraient être conçus et coordonnés conformément aux dispositions générales des interventions d'urgence. Ces plans d'urgence devraient, en particulier, être élaborés et mis en œuvre conformément aux prescriptions internationales en matière de préparation et de conduite des interventions en cas d'urgence nucléaire ou radiologique [8, 9].

6. ÉVALUATION DES MESURES DE PRÉVENTION ET DE PROTECTION

6.1. OBJECTIFS ET VUE D'ENSEMBLE DU PROCESSUS D'ÉVALUATION

La présente section donne des orientations sur le processus d'évaluation du risque en rapport avec les cibles qui ont été identifiées. Ce processus d'évaluation est un élément clé de l'évaluation du risque destinée à repérer les vulnérabilités des systèmes face aux menaces internes. Le résultat du processus d'évaluation est une évaluation de l'efficacité des mesures de prévention et de protection pour ce qui est de neutraliser les éventuelles actions d'agresseurs internes qui pourraient aboutir à un enlèvement non autorisé de matières nucléaires ou à un sabotage.

Les résultats de l'évaluation de l'efficacité de ces mesures devraient être comparés aux critères d'acceptation précédemment établis. Les critères d'acceptation sont généralement définis par l'État ou l'autorité compétente et sont basés sur les conséquences potentielles d'une action malveillante et sa probabilité de réussite. Si l'évaluation indique que les mesures de prévention et de protection ne satisfont pas aux critères d'acceptation, des améliorations devraient être mises en œuvre.

De plus, une attention particulière devrait être accordée :

a) À la facilité relative d'accomplissement d'un acte malveillant. Un scénario pour lequel les conséquences sont jugées acceptables mais qui est relativement facile à mettre en oeuvre peut s'avérer inacceptable (par ex. modifications non autorisées d'un seuil d'un processus ou du réglage d'un circuit) et peut nécessiter une action corrective.
b) Au niveau de risque. Le risque peut être jugé acceptable, mais être proche du seuil à partir duquel le niveau de risque n'est plus acceptable. Une telle situation ne devrait pas être ignorée et une gestion prudente peut exiger des mesures de protection supplémentaires.

L'efficacité des mesures de protection et de prévention devrait être réévaluée périodiquement, notamment à chaque fois qu'il y a des changements en matière de menace de référence, de mesures de prévention et de protection ou de conditions d'exploitation.

Les orientations ci-après traitent à la fois des mesures de prévention et des mesures de protection, et le processus d'évaluation devrait également concerner les deux types de mesures afin de garantir que les mesures de sécurité sont efficaces.

6.2. ÉVALUATION DES MESURES DE PRÉVENTION

Une évaluation rigoureuse des étapes 1 et 2 (exclusion d'agresseurs internes potentiels) décrites à la section 5.1 est difficile, comme avec toutes les mesures de prévention, mais les mesures appliquées (comme les enquêtes de sécurité avant et pendant l'emploi) sont considérées comme efficaces pour ce qui est de réduire – sans pour autant éliminer totalement – l'éventualité d'agresseurs internes. Ces mesures sont des précautions raisonnables et prudentes même si leur effet ne peut pas être quantitativement évalué.

Cependant, l'efficacité de la mise en œuvre des mesures de prévention peut être vérifiée et des critères peuvent être spécifiés et analysés afin de garantir que ces mesures sont appliquées comme prévu. Ainsi, il est possible d'analyser le nombre de refus d'accès au site d'une installation, le nombre de personnes n'ayant plus accès à un site après la fin d'un contrat de travail, et le nombre d'incidents signalés.

L'étape 3 (réduction des occasions) de l'approche de prévention et de protection contre les actes malveillants commis par des agresseurs internes (décrite à la section 5.1) consiste à limiter les occasions qu'aurait un agresseur interne d'obtenir l'accès, l'autorité ou les connaissances nécessaires pour réussir à commettre un acte malveillant entraînant des conséquences radiologiques inacceptables. La mesure dans laquelle ces occasions sont limitées et la façon dont elles le sont constituent des éléments importants pour orienter l'élaboration de scénarios crédibles. En outre, il faudra donc procéder à un réexamen systématique pour déterminer quelles mesures de prévention, telles que celles proposées à la section 5.3, sont en place et correctement appliquées.

6.3. ÉVALUATION DES MESURES DE PROTECTION

Les mesures utilisées pour détecter et retarder les actes malveillants, et intervenir si nécessaire, peuvent être quantitativement analysées. La probabilité

de détection et la rapidité de l'intervention sont souvent quantifiables et constituent donc la base d'une analyse de l'efficacité des mesures de protection.

Le processus présenté reconnaît la valeur des étapes 1, 2 et 3 (voir la section 5.1) et encourage leur application prudente, mais l'accent est mis sur l'évaluation de l'efficacité des mesures de protection pour contrer un acte malveillant. L'approche comprend l'élaboration de scénarios crédibles d'agressions internes, y compris le cas échéant de scénarios de collusion avec des agresseurs externes, puis l'évaluation de l'efficacité du système de protection contre ceux-ci.

L'élaboration de scénarios crédibles consiste à identifier la combinaison d'événements nécessaires à l'accomplissement de l'acte malveillant. En ce qui concerne le sabotage, il faudrait tenir compte des actions qui doivent être effectuées pour déclencher une séquence aboutissant à des conséquences radiologiques inacceptables. Les scénarios de sabotage devraient inclure les attaques menées contre des cibles uniques aussi bien que contre des cibles multiples. En ce qui concerne l'enlèvement non autorisé de matières nucléaires, les actions qui doivent être menées successivement afin d'enlever des matières nucléaires d'une installation devraient être identifiées. Les scénarios impliquant l'enlèvement non autorisé de matières nucléaires devraient inclure les situations dans lesquelles les agresseurs internes quittent directement l'installation avec des matières nucléaires ou cachent des matières sur le site de l'installation, et procèdent à leur enlèvement ultérieur dans des circonstances plus favorables. Il faudrait prendre en compte aussi bien les vols étalés dans le temps que les vols commis en une seule fois.

Afin d'élaborer des scénarios détaillés, il faudrait prendre en compte l'association des cibles identifiées (section 4) avec des groupes d'agresseurs internes définis (section 2). Compte tenu de la menace de référence, les tâches à réaliser par un agresseur interne devraient être définies dans des termes spécifiques, par exemple en tant qu'ensemble d'actions requises en vue d'atteindre l'objectif. Cet ensemble devrait inclure à la fois les actions générales et les zones où elles sont exécutées. Les actions peuvent se produire le long d'itinéraires dans l'installation. Tous les éléments de protection que pourraient rencontrer les agresseurs internes le long de chacun de ces itinéraires, ou au cours de ces ensembles d'actions, devraient être également définis. Les itinéraires, les ensembles d'actions le long des itinéraires et les éléments de protection rencontrés devraient tous être pris en considération. Puisque les agresseurs internes peuvent exécuter les actions requises pour l'acte malveillant sur une période prolongée, et peuvent ne pas suivre une séquence prévisible, le concept d'itinéraire peut ne pas être toujours pertinent.

Il faudrait évaluer l'efficacité des éléments de protection contre les diverses stratégies susceptibles d'être utilisées par les agresseurs internes. Ces stratégies sont élaborées en prenant en compte l'accès, l'autorité et les connaissances des

agresseurs internes pour contourner les dispositifs de détection et de retardement. Il est possible d'élaborer un scénario crédible en associant les éléments de protection et les stratégies des agresseurs internes, pour un ensemble d'actions de ces agresseurs. Il convient de noter que les itinéraires empruntés pour introduire des articles illicites dans une installation, ou pour procéder à un enlèvement non autorisé de matières nucléaires d'une installation, peuvent être différents des itinéraires empruntés par les agresseurs internes.

Une fois qu'un scénario détaillé d'agression interne a été élaboré, l'efficacité des mesures de protection est évaluée en analysant l'impact cumulé des mesures de détection, d'évaluation et de retardement, et en superposant les mesures d'intervention et d'atténuation et le scénario d'agression interne. L'efficacité de l'intervention dépendra à la fois de l'efficacité de l'interruption de l'acte malveillant et de l'efficacité de la prévention des conséquences. L'évaluation devrait tenir compte des efforts que pourraient faire les agresseurs internes pour réduire l'efficacité de l'intervention.

Le processus d'évaluation devrait être répété pour chaque scénario crédible. Les conclusions concernant l'efficacité des mesures de protection devraient refléter les résultats de l'ensemble de ces évaluations.

Après évaluation des mesures de protection, les résultats peuvent être combinés pour donner un aperçu global du statut de la protection dans le cadre de l'installation ou de l'opération de transport.

L'analyse des scénarios met en lumière les améliorations pouvant être apportées aux mesures de protection. Les scénarios devraient être hiérarchisés en compilant l'efficacité du système de protection pour chaque paire cible/agresseur interne, puis en appliquant des critères prédéterminés pour établir les priorités pour chaque scénario correspondant à une paire cible/agresseur interne. Les critères de hiérarchisation devraient être basés à la fois sur l'efficacité du système pour le scénario en question et sur les conséquences potentielles en cas de réussite de l'acte malveillant. Par exemple, les scénarios combinant un système peu efficace et des conséquences élevées devraient être hautement prioritaires, tandis que les scénarios combinant un système efficace et des faibles conséquences seraient nettement moins prioritaires. Les scénarios ayant le rang de priorité le plus élevé devraient être évalués en premier lieu, afin de déterminer les améliorations du système qui en augmenteraient l'efficacité. Les scénarios devraient être analysés en détail pour définir les améliorations possibles. Il faudrait recenser les actions face auxquelles les dispositifs de détection, d'évaluation et de retardement ont été inefficaces ou peu efficaces. Les scénarios dans lesquels l'intervention se révèlerait lente ou inefficace devraient être évalués afin de définir des améliorations potentielles. Les solutions possibles pour ces situations pourraient aller de modifications des procédures à des modifications des équipements.

Pour la conception de ces améliorations, il conviendrait de s'assurer que les améliorations introduites au titre de certains scénarios ne dégradent pas les performances du système de protection avec d'autres scénarios et n'ont pas d'effets inacceptables sur les systèmes d'exploitation et de sûreté. Les améliorations proposées devraient être introduites, et une autre analyse devrait être réalisée pour mesurer le degré d'amélioration obtenu. Il se peut qu'il faille répéter ce processus à plusieurs reprises avant que des solutions satisfaisantes et acceptables ne soient formulées, et les recommandations d'améliorations devraient s'appuyer sur des démonstrations d'efficacité documentées.

RÉFÉRENCES

[1] Convention sur la protection physique des matières nucléaires, INFCIRC/274/Rev.1, AIEA, Vienne (1980).

[2] Sécurité nucléaire – mesures de protection contre le terrorisme nucléaire, Amendement de la Convention sur la protection physique des matières nucléaires, Rapport du Directeur général, GOV/INF/2005/10-GC(49)/INF/6, AIEA, Vienne (2005).

[3] Objectifs et principes fondamentaux de la protection physique, GOV/2001/41, AIEA, Vienne (2001).

[4] La protection physique des matières et installations nucléaires, INFCIRC/225/Rev.4, AIEA, Vienne (2000).

[5] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Orientations et considérations concernant l'application du document INFCIRC/225/Rev.4, La protection physique des matières et installations nucléaires, IAEA-TECDOC-967 (Rev.1)/F, AIEA, Vienne (2002).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Handbook on the Physical Protection of Nuclear Material and Facilities, IAEA-TECDOC-1276, IAEA, Vienna (2002).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safeguards Glossary: 2001 Edition, International Nuclear Verification Series No. 3, IAEA, Vienna (2002).

[8] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Préparation et intervention en cas de situation d'urgence nucléaire ou radiologique, collection Normes de sûreté n° GS-R-2, AIEA, Vienne (2004).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Arrangements for Preparedness for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-G-2.1, IAEA, Vienna (2007).

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, 1-9-18, Kaigan, Minato-ku, Tokyo, 105-0022
Téléphone : +81 3 6367 6079 • Télécopie : +81 3 6367 6207
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

12-44342

Le présent guide d'application expose une méthodologie détaillée d'élaboration de mesures de prévention et de protection contre les menaces internes dans les installations nucléaires et durant le transport de matières nucléaires de tous types. Les agresseurs internes, qui connaissent intimement le fonctionnement des systèmes de sécurité, représentent un défi unique pour l'établissement de systèmes efficaces de contrôle des matières nucléaires. Ils ont en général des droits d'accès qui, associés à leur autorité et à leur connaissance des installations, font qu'ils ont davantage d'occasions qu'un agresseur externe de contourner les dispositifs de protection physique ou d'autres dispositions comme les systèmes de sûreté ou les procédures d'exploitation. En outre, les agresseurs internes, en tant que personnes de confiance, peuvent utiliser des méthodes de fraude inaccessibles aux agresseurs externes. La présente publication donne des orientations et propose des mesures pour réduire ces risques et d'autres liés aux agresseurs internes.

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE
ISBN 978–92–0–236710–4
ISSN 1816–9317