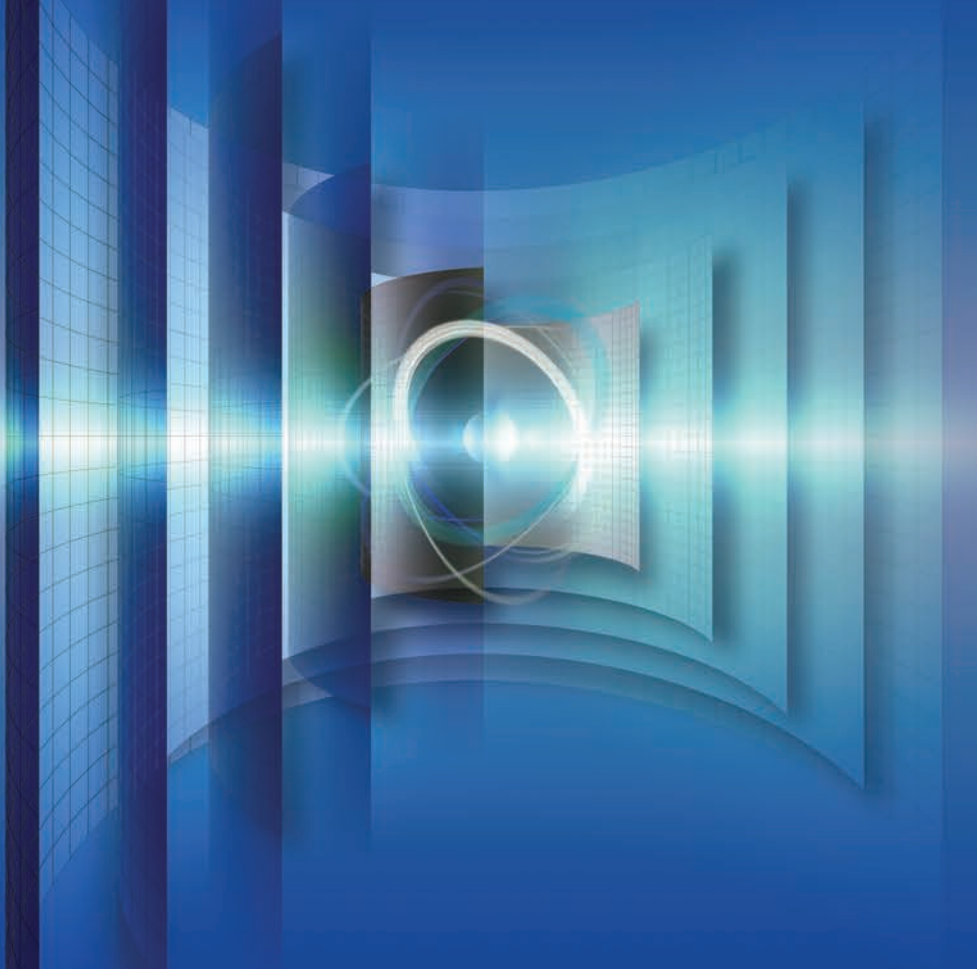
Collection Sécurité nucléaire de l'AIEA Nº 8-G (Rev. 1)

Guide d'application

Mesures de prévention et de protection contre les menaces internes



IAEA
Agence internationale de l'énergie atomique

COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA

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

CATÉGORIES DANS LA COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA

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

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

RÉDACTION ET EXAMEN

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

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

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

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

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

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
AFRIQUE DU SUD
ALBANIE
ALGÉRIE
ALLEMAGNE
ANGOLA
ANTIGUA-ET-BARBUDA
ARABIE SAOUDITE
ARGENTINE
ARMÉNIE
AUSTRALIE
AUTRICHE
AZERBAÏDJAN
BAHAMAS
BAHREÏN
BANGLADESH
BARBADE
BÉLARUS
BELGIQUE
BELIZE
BÉNIN
BOLIVIE, ÉTAT PLURINATIONAL DE
BOSNIE-HERZÉGOVINE
BOTSWANA
BRÉSIL
BRUNÉI DARUSSALAM
BULGARIE
BURKINA FASO
BURUNDI
CAMBODGE
CAMEROUN
CANADA
CHILI
CHINE
CHYPRE
COLOMBIE
COMORES
CONGO
CORÉE, RÉPUBLIQUE DE
COSTA RICA
CÔTE D'IVOIRE
CROATIE
CUBA
DANEMARK
DJIBOUTI
DOMINIQUE
ÉGYPTE
EL SALVADOR
ÉMIRATS ARABES UNIS
ÉQUATEUR
ÉRYTHRÉE
ESPAGNE
ESTONIE
ESWATINI
ÉTATS-UNIS D'AMÉRIQUE
ÉTHIOPIE
FÉDÉRATION DE RUSSIE
FIDJI
FINLANDE
FRANCE
GABON
GÉORGIE
GHANA
GRÈCE
GRENADE
GUATEMALA
GUYANA
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
LIBAN
LIBÉRIA
LIBYE
LIECHTENSTEIN
LITUANIE
LUXEMBOURG
MACÉDOINE DU NORD
MADAGASCAR
MALAISIE
MALAWI
MALI
MALTE
MAROC
MAURICE
MAURITANIE
MEXIQUE
MONACO
MONGOLIE
MONTÉNÉGRO
MOZAMBIQUE
MYANMAR
NAMIBIE
NÉPAL
NICARAGUA
NIGER
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
SAINTE-LUCIE
SAINT-MARIN
SAINT-SIÈGE
SAINT-VINCENT-ET-LES-GRENADINES
SAMOA
SÉNÉGAL
SERBIE
SEYCHELLES
SIERRA LEONE
SINGAPOUR
SLOVAQUIE
SLOVÉNIE
SOUDAN
SRI LANKA
SUÈDE
SUISSE
TADJIKISTAN
TCHAD
THAÏLANDE
TOGO
TRINITÉ-ET-TOBAGO
TUNISIE
TURKMÉNISTAN
TURQUIE
UKRAINE
URUGUAY
VANUATU
VENEZUELA, RÉP. BOLIVARIENNE DU
VIET NAM
YÉMEN
ZAMBIE
ZIMBABWE

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

COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA – Nº 8-G
(Rev. 1)

MESURES DE PRÉVENTION ET DE PROTECTION CONTRE LES MENACES INTERNES

GUIDE D'APPLICATION

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE, 2021

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 26007 22529
Téléphone : +43 1 2600 22417
Courriel : sales.publications@iaea.org
https://www.iaea.org/fr/publications

Imprimé par l'AIEA en Autriche
Décembre 2021
STI/PUB1858

MESURES DE PRÉVENTION ET DE PROTECTION
CONTRE LES MENACES INTERNES
AIEA, VIENNE, 2021
STI/PUB1858
ISBN 978-92-0-214421-7 (imprimé) | ISBN 978-92-0-214521-4 (pdf)
ISSN 2520-6931

AVANT-PROPOS

Aux termes de son Statut, l'AIEA a pour principal objectif « de hâter et d'accroître la contribution de l'énergie atomique à la paix, la santé et la prospérité dans le monde entier ». Ses travaux consistent, d'une part, à prévenir la prolifération des armes nucléaires et, d'autre part, à veiller à ce que la technologie nucléaire puisse être employée à des fins pacifiques dans des domaines tels que la santé ou l'agriculture. Il est essentiel que l'ensemble des matières nucléaires et des autres matières radioactives, comme des installations qui les abritent, soient gérées de manière sûre et protégées comme il se doit contre les agissements criminels et les actes non autorisés commis de façon délibérée.

Si la sécurité nucléaire relève de la responsabilité individuelle des États, il est vital que ceux-ci travaillent dans le cadre d'une coopération internationale pour mettre en place et maintenir des régimes efficaces de sécurité nucléaire. Le rôle central que joue l'AIEA en favorisant cette coopération et en prêtant assistance aux États est largement reconnu. Il se justifie par le nombre de ses États Membres, le mandat qui lui a été confié, les compétences spécifiques qu'elle détient et la longue expérience qu'elle a acquise en fournissant une assistance technique et des conseils spécialisés et pratiques aux États.

En 2006, l'AIEA a lancé sa collection Sécurité nucléaire dans le but d'aider les États à mettre en place des régimes nationaux de sécurité nucléaire efficaces. Les publications de cette collection renforcent les instruments juridiques internationaux relatifs à la sécurité nucléaire que sont la Convention sur la protection physique des matières nucléaires telle qu'amendée, la Convention internationale pour la répression des actes de terrorisme nucléaire, les résolutions 1373 et 1540 du Conseil de sécurité de l'Organisation des Nations Unies et le Code de conduite sur la sûreté et la sécurité des sources radioactives.

Les orientations sont élaborées avec la participation active d'experts d'États Membres de l'AIEA, de sorte qu'elles sont l'expression d'un consensus sur les bonnes pratiques en matière de sécurité nucléaire. Le Comité des orientations sur la sécurité nucléaire de l'AIEA, créé en mars 2012 et constitué de représentants des États Membres, examine et approuve les projets de publications de la collection Sécurité nucléaire lors de leur élaboration.

L'AIEA continuera à travailler avec ses États Membres afin de veiller à ce que les applications pacifiques de la technologie nucléaire contribuent à la santé, au bien-être et à la prospérité des populations dans le monde entier.

NOTE DE L'ÉDITEUR

La présente publication ne traite pas des questions de la responsabilité, juridique ou autre, résultant d'actes ou omissions imputables à une quelconque personne.

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

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

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

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

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

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

TABLE DES MATIÈRES

1. INTRODUCTION

CONTEXTE

1.1. La collection Sécurité nucléaire de l'AIEA donne aux États des orientations destinées à les aider à mettre en œuvre, à examiner et, le cas échéant, à renforcer un régime national de sécurité nucléaire. Elle leur donne aussi des orientations concernant le respect des obligations et des engagements contractés dans le cadre d'instruments internationaux juridiquement et non juridiquement contraignants. La publication de la catégorie Fondements de la sécurité nucléaire (nº 20 de la collection Sécurité nucléaire de l'AIEA [1]) expose l'objectif et les éléments essentiels de l'ensemble du régime de sécurité nucléaire. Les publications contenant des recommandations indiquent ce dont un régime de sécurité nucléaire doit tenir compte pour assurer la protection physique des matières nucléaires et des installations nucléaires [2], des matières radioactives et des installations associées [3], ainsi que des matières nucléaires et autres matières radioactives non soumises à un contrôle réglementaire [4]. Ces publications, comme nombre d'autres dans la collection Sécurité nucléaire de l'AIEA (réf. [5 à 12]), font état des menaces particulières que pourraient représenter les initiés, ainsi que de la nécessité de mettre en place des mesures spécifiques contre les menaces internes et de les évaluer.

1.2. La présente publication est une version mise à jour de la publication intitulée *Mesures de prévention et de protection contre les menaces internes* (nº 8 de la collection Sécurité nucléaire de l'AIEA), publiée par l'AIEA en 2008[1]. La révision a été entreprise afin de mieux aligner ce guide d'application sur les fondements de la sécurité nucléaire et les recommandations publiés après 2008, de faire référence aux autres guides d'application pertinents publiés depuis 2008, et d'ajouter des informations supplémentaires sur certains sujets sur la base de l'expérience d'utilisation de la publication nº 8 de la collection Sécurité nucléaire de l'AIEA par cette dernière et par les États Membres.

[1] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Mesures de prévention et de protection contre les menaces internes, nº 8 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2012).

OBJECTIF

1.3. L'objectif du présent guide d'application est de donner des orientations à jour aux États et à leurs autorités compétentes, aux exploitants[2], aux expéditeurs et aux transporteurs concernant le choix, la mise en place et l'évaluation de mesures de réponse aux menaces internes. Les menaces pour les installations nucléaires peuvent émaner d'agresseurs externes ou internes, ou des deux, en collusion (coopération à des fins illégales ou malveillantes avec un autre agresseur interne ou avec un agresseur externe).

CHAMP D'APPLICATION

1.4. La présente publication couvre la prévention de l'enlèvement non autorisé de matières nucléaires et du sabotage de matières et d'installations nucléaires par des initiés, ainsi que la protection contre de tels actes. Elle concerne les installations nucléaires de tout type — notamment les centrales nucléaires, les réacteurs de recherche et les autres installations du cycle du combustible nucléaire (p. ex. usines d'enrichissement, usines de retraitement, usines de fabrication de combustible, installations d'entreposage) —, qu'elles soient à l'étape de conception ou de remaniement, en construction, en service, en exploitation, à l'arrêt ou en cours de déclassement.

1.5. Les orientations figurant dans cette publication sur les menaces internes peuvent aussi s'appliquer à : la prévention de l'enlèvement non autorisé et du sabotage de matières radioactives et d'installations associées et à la protection contre de tels actes [3] ; la sécurisation des matières nucléaires et des matières radioactives pendant le transport [6 et 13] ; et la prévention et la détection des matières nucléaires et autres matières radioactives non soumises au contrôle réglementaire ainsi que l'intervention en pareil cas [4]. Ces orientations peuvent aussi être suivies pour sécuriser les informations relatives à une installation détenues ou obtenues par d'autres parties prenantes, notamment l'autorité compétente [8].

[2] Le terme « exploitant » désigne une entité (personne ou organisme) autorisée à exploiter une installation nucléaire ou radiologique ou à utiliser, entreposer ou transporter des matières nucléaires et/ou des matières radioactives. Normalement, une telle entité serait titulaire d'une licence ou d'un autre document d'autorisation délivré par une autorité compétente, ou serait un sous-traitant d'un titulaire d'une telle autorisation.

1.6. Dans le cadre de la présente publication, l'accès des initiés à une installation comprend l'accès physique aux emplacements et aux matières, l'accès interne ou l'accès à distance autorisé aux ordinateurs ou au réseau, et l'accès à des informations sensibles concernant l'installation.

1.7. Bien que cette publication ne porte pas sur les considérations de sûreté, les mesures de prévention et de protection décrites devraient être mises en œuvre d'une manière équilibrée et compatible avec les considérations de sûreté, et compte tenu de la radioprotection des travailleurs. Les mesures de sécurité et les mesures de sûreté devraient être conçues et appliquées de façon intégrée afin de créer une synergie entre ces deux domaines et de façon telle que les mesures de sécurité ne compromettent pas la sûreté et que les mesures de sûreté ne compromettent pas la sécurité [1].

STRUCTURE

1.8. Après cette introduction, la présente publication comporte quatre sections. La section 2 présente les menaces internes et la façon de catégoriser les initiés. La section 3 recense les cibles et les systèmes des installations devant être protégés contre des actes malveillants susceptibles d'être commis par des initiés. La section 4 traite de la mise en œuvre, à l'échelle de l'installation, de mesures de prévention des menaces internes et de protection contre ces menaces. La section 5 porte sur l'évaluation des mesures décrites à la section 4.

2. IDENTIFICATION DES MENACES INTERNES

2.1. Le terme « agresseur » désigne toute personne qui commet ou tente de commettre un acte malveillant. Un agresseur peut être un initié ou une personne externe.

2.2. Le terme « initié » est employé pour désigner

> « [t]oute personne bénéficiant d'un accès autorisé à [des matières nucléaires,] des *installations* ou des *activités associées* ou à des *informations* ou des *ressources d'informations sensibles*, qui pourrait commettre un acte criminel ou des actes non autorisés délibérés mettant en jeu ou visant des *matières nucléaires*, d'*autres matières radioactives*, des *installations* ou *activités*

associées, ou d'autres actes que l'État considère comme nuisant à la sécurité nucléaire, ou en faciliter la commission » [1].

Le terme « agresseur externe » désigne un agresseur autre qu'un initié.

ATTRIBUTS DES INITIÉS

2.3. Les initiés possèdent au moins l'un des attributs suivants, qui leur confèrent des avantages par rapport à des agresseurs externes lorsqu'ils tentent de commettre des actes malveillants :

a) Accès : Les initiés bénéficient d'un accès autorisé aux zones, au matériel et aux informations nécessaires à l'exécution de leurs tâches. Cet accès comprend l'accès physique à : des installations nucléaires ; des matières nucléaires et des systèmes, des composants et du matériel associés ; ainsi qu'à des systèmes informatiques. Il comprend également l'accès informatique à distance à une installation, comme l'accès aux systèmes et aux réseaux informatiques qui contrôlent les processus, assurent la sûreté, contiennent des informations sensibles ou contribuent d'une autre manière à la sécurité nucléaire. L'exploitant ne devrait pas permettre l'accès à distance à des systèmes essentiels, comme les systèmes importants pour la sûreté.
b) Autorité : Les initiés sont autorisés à effectuer des opérations dans le cadre des tâches qui leur sont assignées et peuvent aussi être habilités à diriger d'autres employés. Ils peuvent faire usage de cette autorité pour appuyer des actes malveillants, notamment des actes physiques ou informatiques, comme la manipulation de fichiers numériques ou de processus.
c) Connaissances : Les connaissances qu'ont les initiés de l'installation ou des activités ou systèmes associés peuvent être limitées ou spécialisées. Elles peuvent comprendre des connaissances susceptibles de permettre à un initié de contourner ou de neutraliser les systèmes de protection physique et les autres systèmes de l'installation qui contribuent à la sécurité nucléaire, comme les systèmes de sûreté et les systèmes de comptabilité et de contrôle des matières nucléaires, les procédures opérationnelles et les capacités d'intervention.

Ces attributs peuvent aussi comprendre l'accès à des informations sensibles ou à des ressources d'informations sensibles, notamment des informations relatives au transport ou au mouvement de matières nucléaires, ou la connaissance de telles informations ou ressources d'informations [13].

2.4. Un initié peut ne pas posséder ces trois attributs mais avoir quand même la capacité de commettre un acte malveillant. Par exemple, un dirigeant de siège peut avoir un accès physique limité à une installation mais être en mesure de délivrer un faux bon de livraison pour un emplacement externe. Les agresseurs internes peuvent feindre d'avoir une autorité ou des connaissances pour faciliter ou entreprendre un acte malveillant. Un agresseur interne peut agir de façon indépendante ou en collusion avec un autre agresseur interne ou un agresseur externe.

2.5. Compte tenu de leur accès, de leur autorité et de leur connaissances, les initiés peuvent choisir la cible la plus vulnérable et le meilleur moment pour commettre ou tenter de commettre un acte malveillant. Pour maximiser la probabilité de réussite, un agresseur interne peut étaler un acte malveillant sur une longue période de temps. Cette tactique pourrait consister à : a) manipuler frauduleusement le matériel de protection physique ou le matériel de sûreté pour préparer un acte de sabotage, b) falsifier des données afin que l'agresseur interne puisse enlever sans autorisation, de façon répétée et sans être repéré, de petites quantités de matières nucléaires de catégorie inférieure, qui ont une protection moins robuste que les matières nucléaires de catégorie supérieure, ou c) enlever sans autorisation des matières nucléaires dans des quantités inférieures aux seuils de détection des systèmes de mesure. Les agresseurs internes peuvent avoir l'occasion de commettre un acte malveillant lorsqu'une installation est dans des conditions normales ou anormales, notamment pendant la maintenance, ou lors d'un mouvement de matières nucléaires, et peuvent choisir le moment le plus favorable pour le faire [14].

MOTIVATIONS DES INITIÉS

2.6. Les initiés peuvent entreprendre des actes malveillants pour différentes raisons ; leur motivation peut être financière ou idéologique, la revanche, leur ego, la coercition ou une combinaison de ces motivations.

2.7. Un initié peut développer à lui seul une motivation suffisante pour commettre un acte malveillant, notamment à la suite d'un problème de santé mentale. Un initié peut aussi être recruté par un agresseur externe qui cherche à tirer parti du droit d'accès, de l'autorité ou des connaissances de l'initié. Un initié pourrait être contraint de commettre un acte malveillant par coercition (p. ex. par chantage).

2.8. Un initié peut occuper n'importe quel poste au sein d'un organisme, du niveau le plus haut à celui le plus bas. Tout initié, quel que soit son niveau,

pourraient avoir une motivation suffisante pour commettre un acte malveillant. D'autres membres du personnel, qui ne sont pas directement employés par l'exploitant, l'expéditeur ou le transporteur mais qui bénéficient d'un accès autorisé de façon régulière à l'installation ou à ses systèmes (p. ex. vendeurs, premiers intervenants, sous-traitants, inspecteurs d'organismes de réglementation ou autres autorités compétentes) devraient également être considérés comme des menaces internes potentielles.

CATÉGORIES D'INITIÉS

2.9. Un initié involontaire est un initié n'ayant ni l'intention ni la motivation de commettre un acte malveillant qui est exploité à son insu par un agresseur. Par exemple, dans une attaque informatique, un initié involontaire peut ne pas savoir que certaines actions (p. ex. un clic sur un lien malveillant dans un courriel déguisé semblant provenir d'une source fiable) peuvent fournir des informations ou donner un accès authentifié à un agresseur.

2.10. Un agresseur interne est un initié qui commet des actes malveillants sciemment, à dessein et de façon motivée. Un agresseur interne peut être passif ou actif, et un agresseur interne actif peut être violent ou non violent. Cette catégorisation est utile à des fins d'évaluation, comme lors de l'établissement des profils d'agresseurs dans l'évaluation de la menace ou la menace de référence, ou lors de la création de scénarios devant servir à tester les mesures de sécurité nucléaire dans le cadre d'un processus d'évaluation du système de sécurité nucléaire.

2.11. Un agresseur interne passif aide un autre agresseur en fournissant des informations devant servir à commettre un acte malveillant. Un agresseur interne passif ne participerait pas à l'acte malveillant d'une autre manière et cesserait probablement d'y participer s'il y avait une forte probabilité qu'il soit identifié.

2.12. Un agresseur interne actif non violent a recours à la dissimulation ou à la tromperie pour faciliter ou commettre un acte malveillant, et peut communiquer des informations à un autre agresseur. Par exemple, un agresseur interne actif non violent peut tenter de voler des matières nucléaires de façon soudaine ou étalée dans le temps, ou aider des agresseurs externes à commettre un acte malveillant en désactivant ou en ignorant les alarmes, ou en ouvrant des portes. Un agresseur interne actif non violent mettrait probablement fin à l'acte malveillant s'il y avait une forte probabilité qu'il soit identifié (autrement dit ce type d'agresseur

interne pourrait risquer d'être découvert mais ne se risquerait probablement pas à être identifié).

2.13. Un agresseur interne actif violent est semblable à un agresseur interne actif non violent, mais est prêt à recourir à la force physique contre le personnel pour faciliter ou commettre un acte malveillant. Suivant les circonstances, un agresseur interne non violent peut devenir violent.

IDENTIFICATION DE MENACES INTERNES POTENTIELLES

2.14. Les orientations figurant dans cette section peuvent aider l'exploitant à identifier les menaces internes potentielles et devraient être utilisées conjointement avec d'autres processus d'identification des menaces internes, comme l'élaboration de scénarios plausibles dans le cadre de l'évaluation du système de sécurité nucléaire.

2.15. Dans la référence [2], il est recommandé ceci : « [l]es autorités nationales compétentes devraient définir, à partir de diverses sources d'information crédibles, la *menace* et les moyens associés sous forme d'une *évaluation de la menace* et, s'il y a lieu, d'une *menace de référence* »[3]. L'État devrait prendre en considération les attributs, les motivations et les catégories des initiés, et décrire toute menace interne crédible dans l'évaluation nationale de la menace ou la menace de référence.

2.16. L'évaluation de la menace et du risque peut aussi aider à identifier les menaces internes potentielles. Outre les informations générales concernant les menaces internes figurant dans l'évaluation nationale de la menace ou la menace de référence, les informations relatives à la menace locale concernant la zone située autour d'une installation donnée devraient être prises en considération dans l'évaluation propre à l'installation. Ces informations peuvent mettre en évidence des conditions utiles (p. ex. niveaux de criminalité) ou des situations hors de l'installation (p. ex. attitude générale de la communauté, présence de groupes hostiles organisés) qui pourraient être propices à des agresseurs internes.

2.17. Il est également possible d'identifier des menaces internes potentielles en déterminant quels initiés ont un accès autorisé, à distance ou sur le site, aux

---

[3] On entend par menace de référence les « moyens et caractéristiques d'*agresseurs* potentiels *d'origine interne* et/ou externes visant à un *enlèvement non autorisé* ou à un *sabotage* en fonction desquels un *système de protection physique* est conçu et évalué » [2].

systèmes de l'installation par l'intermédiaire de réseaux informatiques. Les systèmes d'installations modernes, notamment ceux qui contribuent à la sécurité nucléaire, reposent sur des contrôles et des réseaux informatisés. Ces systèmes devraient être protégés contre des attaques informatiques comme il est indiqué dans la référence [7]. Il conviendrait de prendre en considération le personnel ayant accès à ces systèmes lors de l'identification des menaces internes.

3. IDENTIFICATION DES CIBLES

3.1. Comme indiqué dans la référence [15], l'identification des cibles consiste à établir quelles matières et quel matériel doivent être protégés d'un agresseur. Les cibles peuvent être notamment des matières nucléaires, des zones associées, des bâtiments, du matériel, des composants, des informations, des systèmes et des fonctions. Des orientations relatives à l'identification des cibles pour ce qui est des installations et des matières nucléaires et radioactives sont fournies dans les références [2 à 4, 8, 15 et 16].

3.2. Il peut aussi être nécessaire de protéger des biens (p. ex. systèmes de surveillance, portiques de détection) qui ne sont pas identifiés comme étant des cibles mais qui sont essentiels à la protection des cibles recensées. Un agresseur interne pourrait contourner ou dégrader ces biens pour commettre un acte malveillant.

CIBLES D'UN ENLÈVEMENT NON AUTORISÉ

3.3. Les matières nucléaires cibles d'un enlèvement non autorisé peuvent être classées dans l'une des trois catégories existantes (I à III) en fonction de leur attractivité et de leurs caractéristiques, ainsi que des conséquences potentielles de leur utilisation dans un dispositif nucléaire explosif. Cette catégorisation est établie dans le tableau 1 de la référence [2]. L'enlèvement non autorisé de matières nucléaires ou radioactives en vue de la fabrication d'un engin à dispersion de radioactivité devrait aussi être pris en considération [3]. Outre les matières nucléaires et autres matières radioactives, les informations sensibles et les ressources d'informations sensibles peuvent aussi être des cibles de vol.

3.4. Lors de l'identification des cibles potentielles d'un enlèvement non autorisé de matières nucléaires par un agresseur interne, il devrait être tenu compte du fait

qu'un vol peut être commis de façon soudaine ou sur la durée. Un « vol soudain » est l'enlèvement non autorisé d'une cible ou d'une quantité significative de matières nucléaires au cours d'un seul acte. Un « vol sur la durée » est l'enlèvement non autorisé répété de quantités, éventuellement petites, de matières nucléaires d'un seul ou de plusieurs emplacements.

3.5. Un agresseur interne peut commettre un vol sur la durée de matières nucléaires pour ne pas être repéré, en enlevant de façon répétée de petites quantités des matières qui sont inférieures aux limites de détection des systèmes de comptabilité et de contrôle des matières nucléaires et des systèmes de protection physique. Le vol sur la durée peut être commis soit en enlevant les matières nucléaires de l'installation à chaque acquisition ou en accumulant les matières nucléaires à un emplacement caché pour les retirer ensuite, éventuellement de façon soudaine, de l'installation. Lors de l'identification des cibles, il faudrait envisager la possibilité qu'un agresseur interne rassemble, en collectant des quantités suffisantes de matières nucléaires de catégorie inférieure, l'équivalent d'une certaine quantité de matières nucléaires de catégorie supérieure. Des facteurs tels que l'élément, la forme physique des matières, la façon dont elles sont utilisées, la quantité utilisée dans le processus et la quantité entreposée devraient également être pris en considération lors de l'identification des cibles, pour établir si des scénarios de vols sur la durée sont possibles et crédibles. Des considérations similaires devraient être appliquées aux scénarios de vols soudains.

CIBLES DE SABOTAGE

3.6. On détermine les cibles de sabotage d'une installation en analysant la possibilité que le stock et les déchets de matières radioactives de l'installation, notamment les matières nucléaires et les sources radioactives [3], donnent lieu à des conséquences radiologiques inacceptables ou graves. Les références [2 et 15] donnent de plus amples informations sur les mesures de sécurité nucléaire qui devraient être prises pour protéger contre le sabotage ainsi que pour procéder à une analyse des cibles de sabotage.

3.7. Lors du processus d'identification des cibles, il conviendrait de déterminer les combinaisons d'actions (scénarios) possibles qu'un agresseur interne est susceptible d'exécuter pour dégrader les structures, les systèmes et les composants d'une installation et qui pourraient avoir des conséquences radiologiques inacceptables ou graves.

RECENSEMENT DES SYSTÈMES CONTRIBUANT À LA SÉCURITÉ NUCLÉAIRE

3.8. Dans le processus d'identification des cibles, il faudrait tenir compte de tous les systèmes pouvant requérir une protection supplémentaire contre les menaces internes. Les systèmes de protection physique, les systèmes de comptabilité et de contrôle des matières nucléaires, les systèmes de sûreté et les systèmes de contrôle des processus devraient être considérés comme les cibles potentielles d'actes malveillants, notamment de ceux commis par un agresseur interne.

3.9. Un agresseur interne peut bénéficier d'un accès autorisé à l'installation ou à des informations relatives à l'installation et peut attaquer d'autres structures, systèmes ou composants pour perpétrer indirectement une attaque, dissimuler des actes malveillants ou aider un agresseur externe. Suivant l'installation ou l'exploitation, l'agresseur interne peut exploiter les systèmes informatisés (p. ex. utiliser des réseaux bureautiques ou des ordinateurs de communication pour acquérir des informations sensibles).

3.10. La dégradation des systèmes informatisés d'une installation pourrait porter atteinte à la sûreté ou à la sécurité des matières nucléaires, ou entraver l'atténuation d'un accident. L'exploitant devrait évaluer et protéger les systèmes informatisés qui contiennent des informations relatives à la sûreté ou à la sécurité en tenant compte du risque de divulgation de ces informations et des conséquences possibles. L'évaluation devrait viser à identifier les systèmes informatisés essentiels qui pourraient être les plus vulnérables à un acte malveillant et dont la défaillance pourrait entraîner un événement de sécurité nucléaire.

3.11. L'exploitant devrait envisager de dispenser une formation supplémentaire aux employés et aux sous-traitants qui ont accès à des systèmes sensibles pour les sensibiliser à la sécurité. Les agresseurs externes peuvent cibler des initiés ayant accès à une installation, à des informations sensibles, à des ressources d'informations sensibles ou aux réseaux de l'installation pour qu'ils les aident à commettre ou à dissimuler des actes malveillants.

4. MESURES CONTRE LES MENACES INTERNES POTENTIELLES

4.1. Les mesures de sécurité nucléaire appliquées pour protéger contre les menaces internes devraient comprendre des mesures de prévention et des mesures de protection. Le terme « mesures de prévention » désigne des mesures destinées à réduire le nombre d'initiés potentiels avant d'octroyer un droit d'accès aux personnes, afin de réduire au minimum la possibilité qu'un initié entreprenne un acte malveillant si l'accès est octroyé ou d'empêcher un agresseur interne potentiel de commettre un acte malveillant. Le terme « mesures de protection » désigne des mesures destinées à détecter ou à retarder des actes malveillants, à intervenir en cas de tels actes ou à en atténuer les conséquences.

4.2. Les présentes orientations ne couvrent pas toutes les mesures pouvant être prises contre une menace interne. Cependant, l'application de mesures de prévention et de protection peut aider à contrer les menaces internes si celles-ci sont correctement définies, le processus d'identification des cibles est complet et les mesures sont appliquées et évaluées efficacement.

4.3. Les autorités compétentes devraient collecter les informations relatives aux mesures prises contre les menaces internes et les incidents liés à des actes malveillants commis par des agresseurs internes, en vue d'analyser les tendances, les faiblesses et les bonnes pratiques. S'il y a lieu, les informations devraient être communiquées aux organismes internationaux autorisés afin que l'ampleur et la nature des défis en matière de sécurité que posent les agresseurs internes puissent être mieux comprises.

APPROCHE GÉNÉRALE DE LA MISE EN ŒUVRE

4.4. Comme indiqué dans la référence [2], les prescriptions de sécurité nucléaire devraient être établies selon une approche graduée tenant compte de l'évaluation actuelle de la menace, de l'attractivité relative et de la nature des matières, ainsi que des conséquences qui pourraient résulter de l'enlèvement non autorisé de matières nucléaires ou du sabotage de matières nucléaires ou d'installations nucléaires. Des orientations générales sur la mise en œuvre d'une approche graduée visant à protéger les matières nucléaires et les installations contre les menaces internes et externes figurent dans la référence [15].

4.5. L'application de mesures de sécurité nucléaire destinées à protéger contre les menaces internes suppose le choix d'une combinaison de mesures de prévention et de protection[4] et leur mise en œuvre suivant une approche graduée. Il est important que les mesures choisies soient mises en œuvre et évaluées efficacement afin qu'elles aient les effets souhaités. Toutes les mesures ne conviennent pas à toutes les installations ou à toutes les exploitations.

4.6. Plusieurs niveaux de mesures de prévention et de protection devraient être mis en place, conformément au principe de défense en profondeur, de sorte que les agresseurs internes aient à surmonter ou à contourner de multiples niveaux de mesures ou de technologies pour atteindre leurs objectifs. Ces niveaux peuvent comprendre des mesures administratives (p. ex. procédures, instructions, règles de contrôle des accès, règles de confidentialité), des mesures techniques ou une combinaison des deux. Les deux types de mesures devraient concerner les personnes et le matériel.

4.7. L'exploitant devrait établir un plan de sécurité dans le cadre de sa demande de licence, comme il est indiqué dans la référence [2], et veiller à ce qu'y soient décrites les mesures nécessaires pour faire face aux menaces internes, notamment les mesures répondant aux menaces internes à la sécurité de l'information et à la sécurité informatique (p. ex. une cyberattaque menée par un agresseur interne [7 et 8]). L'exploitant devrait tenir compte des menaces internes lors de la conception, de l'évaluation, de la mise en œuvre et de la maintenance des systèmes de sécurité nucléaire au niveau de l'installation.

4.8. Le plan de sécurité devrait prévoir la façon de mettre en œuvre les systèmes de sécurité nucléaire dans l'installation, et recenser les mesures destinées à protéger les cibles identifiées contre les menaces internes. Il devrait comprendre des informations relatives à ces mesures. Par exemple, les mesures techniques peuvent inclure des mesures de confinement et de surveillance visant à détecter et à retarder un agresseur interne, des mesures visant à surveiller et à renforcer les réseaux et les dispositifs associés, et des mesures visant à assurer le contrôle des accès. Les mesures administratives peuvent inclure des procédures, des instructions, des sanctions administratives, la règle des deux personnes, des règles de confidentialité et des vérifications administratives, ainsi que des inspections planifiées, non planifiées ou inopinées de la mise en œuvre des mesures de prévention et de protection. Les inspections devraient être effectuées par l'exploitant ou par des équipes indépendantes. Le plan de sécurité devrait préciser la façon dont les mesures seront évaluées (voir la section 5).

[4] Certaines mesures peuvent avoir des effets à la fois préventifs et protecteurs.

4.9. Il peut être nécessaire de mettre à niveau les systèmes de sécurité des installations en service existantes pour répondre à l'évolution des menaces internes.

MISE EN ŒUVRE DE MESURES CONTRE LES MENACES INTERNES

4.10. Les mesures de prévention et les mesures de protection devraient servir à protéger contre les menaces internes potentielles. Les mesures de prévention peuvent servir à :

a) réduire les menaces internes potentielles avant d'octroyer un accès à des personnes en repérant des comportements ou des caractéristiques indésirables pouvant être le signe d'une motivation ;
b) réduire encore les menaces internes potentielles après qu'un accès a été octroyé à des initiés en repérant des comportements ou des caractéristiques indésirables pouvant être le signe d'une motivation ;
c) réduire au minimum les occasions de commission d'actes malveillants en limitant l'accès, l'autorité et les connaissances des initiés.

Les mesures de protection peuvent servir à :

1) détecter et retarder des actes malveillants, et intervenir face à de tels actes ;
2) atténuer ou réduire le plus possible les conséquences d'un événement de sécurité nucléaire et, le cas échéant, localiser ou récupérer les matières.

La figure 1 montre comment ces étapes peuvent permettre de répondre à des menaces internes.

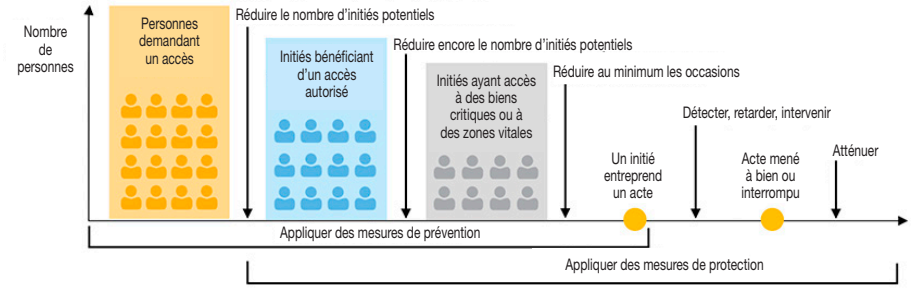


FIG. 1. Étapes de l'application des mesures de prévention et de protection contre les menaces internes potentielles.

4.11. Nombre des mesures énumérées dans les deux sections suivantes peuvent être considérées comme des mesures à la fois de prévention et de protection. Dans le cadre du processus de choix et d'évaluation, il conviendrait d'examiner l'utilité potentielle de chaque mesure proposée tant pour la protection que pour la prévention.

Mise en œuvre de mesures de prévention

4.12. Les mesures de prévention sont destinées à réduire le nombre de menaces internes potentielles et à réduire au minimum la possibilité pour des initiés de commettre un acte malveillant. Elles devraient être appliquées avant l'embauche, pendant la période d'emploi et à l'issue de celle-ci. En outre, elles incluent des mesures d'assurance de la qualité et des mesures de sécurité informatique spécifiques. Les exploitants devraient appliquer les mesures de prévention décrites dans la présente section.

Mesures à appliquer avant l'embauche

4.13. Les personnes qui postulent à un emploi requérant l'accès à une installation devraient faire l'objet d'un contrôle d'identité, d'une vérification des documents personnels et d'enquêtes de sécurité.

4.14. Le contrôle d'identité sert à vérifier que les données personnelles de l'individu concerné sont exactes et authentiques.

4.15. La vérification des documents personnels sert à vérifier l'authenticité du parcours professionnel et de la formation d'un candidat, et à vérifier qu'il possède les compétences que requièrent les tâches à effectuer. La vérification et la validation des documents et des qualifications peut se faire en contactant les employeurs précédents, les établissements d'enseignement et les personnes de référence.

4.16. Les enquêtes de sécurité servent à obtenir une évaluation initiale (lors du processus de recrutement) et des évaluations continues (régulièrement tout au long de la période d'emploi) de l'intégrité, de l'honnêteté et de la fiabilité d'une personne. Dans la référence [2], il est recommandé ceci :

> « En prenant en considération la législation, la réglementation ou les politiques nationales relatives à la vie privée et aux qualifications requises, l'État devrait déterminer la politique d'habilitation des personnes à suivre pour recenser les cas où elle doit être appliquée et la manière dont elle doit l'être, en adoptant une *approche graduée*. »

4.17. Les enquêtes devraient porter sur le respect par la personne des lois ainsi que des règles de l'installation, et tout comportement ou tout facteur de motivation préoccupant. Par exemple, une enquête devrait viser à déceler des facteurs de motivation tels que des problèmes financiers ou des pressions (p. ex. dettes, réductions de salaire), l'adhésion à une idéologie préoccupante, un désir de vengeance (p. ex. le sentiment d'être victime d'une injustice), la dépendance physique (p. ex. drogues, alcool, sexe), un état psychologique ou psychiatrique, une grande insatisfaction dans la vie privée ou professionnelle, ou d'autres facteurs pouvant amener une personne à être contrainte de commettre un acte malveillant. De tels facteurs de motivation peuvent être révélés par un examen du casier judiciaire, des références personnelles et professionnelles, des antécédents professionnels, de la situation financière, des réseaux en ligne et autres réseaux sociaux, du dossier médical ou des rapports d'évaluation professionnelle, ainsi que des informations recueillies auprès de collègues sur les comportements observés.

4.18. Les lois nationales peuvent restreindre l'étendue ou la conduite du contrôle d'identité, de la vérification des documents personnels et des enquêtes de sécurité dans un État.

Mesures à appliquer au cours de la période d'emploi

4.19. Les initiés qui ont fait l'objet des vérifications antérieures à l'emploi et à qui l'on a octroyé un accès autorisé, notamment l'accès à des biens critiques, à des informations sensibles et à des zones vitales, devraient être soumis aux mesures décrites dans les paragraphes qui suivent.

4.20. Des procédures d'accompagnement devraient être élaborées et mises en œuvre. Les personnes pour lesquelles il n'a pas été établi qu'elles présentaient toutes les garanties en matière de sécurité ou dont les tâches ne requièrent pas qu'une enquête de sécurité soit menée (p. ex. les travailleurs occasionnels chargés de travaux de réparation, le personnel administratif, le personnel de maintenance, les travailleurs du bâtiment, les visiteurs) devraient être accompagnées dans les zones vitales ou les zones intérieures par des personnes qui bénéficient d'un accès autorisé et ne sont pas elles-mêmes tenues d'être accompagnées. L'accompagnateur devrait savoir quelles actions sont approuvées, et notamment connaître les zones et les systèmes auxquels la personne accompagnée devrait avoir accès et les activités qu'elle est autorisée à effectuer.

4.21. Les initiés devraient faire régulièrement l'objet d'enquêtes de sécurité au cours de la période d'emploi. Il est possible que certains comportements et certains facteurs de motivation préoccupants n'aient pas été visibles auparavant

ou se soient développés au fil du temps. Par exemple, un contrôle aléatoire destiné à repérer la consommation de drogues ou d'alcool lors d'un service devrait être considéré comme un moyen d'assurer la fiabilité d'un travailleur. L'ampleur des vérifications de sécurité devrait être fonction du niveau d'accès qu'a l'initié à l'installation et à ses biens, ainsi que de son niveau d'autorité. Par exemple, les initiés qui gèrent des réseaux, facilitent l'accès à distance aux ressources d'informations sensibles et travaillent avec des matières nucléaires devraient faire l'objet de vérifications de sécurité plus fréquentes et plus approfondies que ceux qui travaillent dans le domaine des ressources humaines.

4.22. Les employés pour lesquels le résultat de l'enquête de sécurité a changé en raison de circonstances personnelles peuvent voir leur niveau d'accès temporairement rétrogradé ou se voir retirer leurs responsabilités en matière de direction jusqu'à ce qu'ils fassent l'objet d'une nouvelle enquête. Pour maintenir la fiabilité des employés, on peut avoir recours à des programmes de sensibilisation à la sécurité ainsi qu'à la satisfaction des employés et à des récompenses, dont il est question ci-après.

4.23. Les informations sensibles devraient être tenues confidentielles de sorte que seules les personnes qui ont besoin de les connaître soient autorisées à y accéder. L'acquisition d'informations relatives aux cibles sensibles ou concernant les procédures ou les mesures de sécurité (p. ex. l'emplacement du stock de matières nucléaires ou les plans et calendriers de transport) peut aider les agresseurs internes à mener à bien un acte malveillant. Il conviendrait de tenir un registre des personnes ayant accès à des informations sensibles, d'y consigner notamment la date et l'heure auxquelles les informations ont été consultées, et d'empêcher que ce registre puisse être modifié. Les informations relatives aux vulnérabilités potentielles des systèmes de sécurité nucléaire devraient être hautement protégées et compartimentées (comme indiqué au paragraphe 4.30), car elles pourraient faciliter la commission d'un enlèvement non autorisé ou d'un acte de sabotage.

4.24. L'accès aux installations nucléaires, aux matières nucléaires, aux systèmes d'installations nucléaires et aux informations sensibles devrait être contrôlé. Pour l'octroi ou le retrait de l'autorisation d'un tel accès, un processus documenté devrait être établi et appliqué pour toute personne requérant l'accès, à distance ou sur le site, à une installation ou à des opérations y relatives, y compris le transport. Les données personnelles d'un individu pourraient être vérifiées grâce aux documents d'identification délivrés par le gouvernement et à la biométrie (p. ex. rétine, empreintes palmaires, empreintes digitales, reconnaissance faciale). Dans le cadre de ce processus, des règles strictes fondées sur le besoin de connaître et le besoin d'accéder, définies par l'autorité compétente, devraient s'appliquer. Les

personnes devraient être autorisées à accéder sans escorte seulement aux zones dans lesquelles elles ont besoin d'entrer pour effectuer les tâches qui leur sont assignées. Le nombre de personnes bénéficiant d'un accès autorisé à des zones désignées devrait être limité au strict minimum.

4.25. La transformation ou le mouvement de matières nucléaires et d'autres matières radioactives devraient être autorisés au préalable afin de réduire au minimum les occasions d'enlèvement non autorisé de matières et de détecter les activités non autorisées [6 et 13]. Par exemple, l'exploitant de l'installation devrait disposer d'une procédure écrite indiquant qui peut retirer des matières nucléaires d'une casemate d'entreposage en vue de leur transformation, quand les matières peuvent être retirées et comment le retrait devrait être autorisé et consigné. Un calendrier journalier ou hebdomadaire des activités, coordonné et approuvé par le personnel d'exploitation, peut réduire les occasions pour le personnel qui exécute normalement ces activités d'en effectuer d'autres, non autorisées.

4.26. Les zones physiques, les tâches, le temps et les informations devraient être compartimentés afin qu'il soit improbable qu'un initié ait un accès, une autorité et des connaissances suffisants pour mener à bien un acte malveillant. La compartimentation requiert de l'initié un effort accru pour commettre un acte malveillant, et accroît la probabilité qu'un initié doive mener des activités autres que ses activités autorisées habituelles pour mener à bien un acte malveillant.

4.27. L'exploitant de l'installation devrait veiller à ce que les zones physiques soient compartimentées de sorte qu'un initié n'ait pas, à lui seul, accès à tous les systèmes, les composants et le matériel qui lui permettraient de mener à bien un acte malveillant. Le nombre de personnes ayant accès à une quelconque zone requérant une protection devrait être limité. Des règles déterminant quels membres du personnel ont besoin d'accéder à des zones compartimentées devraient être établies et s'appliquer à chaque zone compartimentée. Il conviendrait de réexaminer et de modifier ces règles lorsque les processus ou les configurations au sein de la zone compartimentée sont modifiés. De plus, le nombre de personnes autorisées à accéder à chacune des zones compartimentées devrait être limité au strict minimum. Des inspections et des tests de performance devraient être effectués pour s'assurer que les procédures respectent les règles d'accès.

4.28. La séparation des tâches compartimente les activités des initiés en vue de limiter la possibilité qu'un initié obtienne un accès autorisé, une autorité et des connaissances suffisants pour commettre un acte malveillant. Elle comprend l'application du principe du moindre privilège aux systèmes informatisés,

principe en vertu duquel ne sont accordés à un initié que les privilèges qui sont essentiels à son travail.

4.29. La compartimentation du temps devrait consister à limiter l'accès autorisé lors des différentes périodes d'activité dans une installation (p. ex. heures de travail, maintenance, arrêts, conditions inhabituelles). Par exemple, un initié ne devrait avoir accès à une zone critique que pendant ses tours de service.

4.30. La compartimentation des informations devrait consister à répartir les informations stockées tant sur support papier que sur support électronique en éléments d'information contrôlés de manière séparée, et à appliquer des mesures administratives et techniques pour contrôler l'accès à ces informations. La compartimentation des informations a pour but d'empêcher les initiés de rassembler toutes les informations nécessaires pour tenter de commettre un acte malveillant. Il conviendrait de tenir compte des règles du besoin de connaître du personnel concernant les informations sensibles lors de la compartimentation des informations.

4.31. Des procédures opérationnelles standard devraient être suivies. Il s'agit d'instructions écrites qui régissent des tâches récurrentes conformément à des spécifications approuvées, le but étant d'obtenir un résultat déterminé. Les procédures opérationnelles standard réduisent au minimum les variations et favorisent l'assurance de la qualité grâce à l'application cohérente d'un processus au sein d'un organisme, quels que soient les changements de personnel. Les procédures opérationnelles standard peuvent aider à détecter, et donc à prévenir, un acte malveillant commis par un agresseur interne, car elles fournissent une référence des activités prédéterminées par rapport à laquelle tout écart dans la procédure peut être plus facilement détecté et mis en question.

4.32. Il conviendrait d'élaborer et de mettre en œuvre un programme de sensibilisation à la sécurité à l'intention du personnel et des sous-traitants. Un tel programme contribue à la culture de sécurité nucléaire de l'organisme et peut aider à prévenir les menaces internes si la sensibilisation à la sécurité concernant de telles menaces est intégrée dans la culture de sécurité nucléaire de l'installation. Tous les membres du personnel, quel que soit leur poste ou leur fonction, devraient avoir connaissance des menaces et des conséquences potentielles des actes malveillants, ainsi que de leur rôle s'agissant de réduire le risque qu'un tel acte soit commis. Les programmes de sensibilisation à la sécurité peuvent réduire le risque de chantage, de coercition, d'extorsion ou d'autres menaces dont peuvent faire l'objet les employés et leur famille, et devraient encourager le signalement d'une possible intimidation aux responsables de la sécurité. Leur élaboration

devrait être coordonnée à celle des programmes de sensibilisation à la sûreté afin que soient mises en place une culture de sûreté et une culture de sécurité efficaces et complémentaires.

4.33. Le programme de sensibilisation à la sécurité devrait notamment porter sur des politiques de sécurité claires, l'application de pratiques en matière de sécurité et la formation continue. La formation a pour but de créer un environnement dans lequel tous les employés sont informés des politiques et des procédures de sécurité afin qu'ils soient en mesure d'aider à détecter et à signaler les comportements suspects ou fautifs ainsi que les actes non autorisés. La formation devrait comprendre des méthodes d'évaluation de la sensibilisation à la sécurité et de l'efficacité de la formation, ainsi que des processus d'amélioration continue et de mise à niveau. Elle devrait préparer le personnel à l'éventualité d'un incident physique survenant dans l'installation ou visant ses biens, mais aussi à l'éventualité d'une cyberattaque.

4.34. Il conviendrait d'élaborer et de mettre en place un programme d'aptitude au travail. Les responsables devraient être formés de manière à pouvoir détecter le comportement préoccupant d'un employé et le signaler à la personne appropriée. Il peut être envisagé de mettre en place des programmes d'aptitude au travail pour surveiller régulièrement la santé des employés. L'exploitant de l'installation peut également envisager d'offrir une aide aux employés qui traversent une situation difficile (sur le plan financier, médical ou psychologique, par exemple).

4.35. Les incidents préoccupants du point de vue de la sécurité (c.-à-d. les incidents survenant dans une installation qui supposent des violations ou des irrégularités concernant les politiques, les procédures ou les systèmes de sécurité de l'installation) devraient être signalés et examinés. Le signalement et l'examen des incidents préoccupants du point de vue de la sécurité peuvent aider à élaborer des actions correctives et à prévenir les menaces internes. Un incident causé par un agresseur interne peut être précurseur d'un acte malveillant, et servir soit à préparer cet acte soit à tester la réponse d'un système. Le fait que des enquêtes approfondies soient menées à la suite d'incidents peut dissuader les initiés, et ces enquêtes peuvent permettre d'identifier les membres du personnel susceptibles d'être des agresseurs internes.

4.36. Les employés devraient bénéficier de bonnes conditions de travail, de récompenses et d'une reconnaissance. Ces trois éléments jouent un rôle important dans le maintien et le renforcement du moral et de la loyauté des employés, lesquels contribuent à une culture de sécurité efficace.

4.37. Il conviendrait de faire savoir aux initiés que les violations délibérées des instructions de travail, des règlement ou des lois seront sanctionnées. L'éventualité d'une action disciplinaire ou de poursuites judiciaires peut dissuader les initiés de commettre des actes malveillants. En outre, le fait de demander aux exploitants d'informer l'autorité compétente des tentatives ou des commissions d'actes malveillants peut, une fois celles-ci correctement évaluées, rendre possible l'échange d'informations entre les exploitants, et permettre de rassembler des informations étayant les modifications qu'il convient d'apporter aux prescriptions réglementaires.

Mesures à appliquer à l'issue de la période d'emploi

4.38. L'accès et l'autorité d'une personne, notamment l'accès informatique, devraient être annulés en cas de suppression du poste, ou à l'issue de la période d'emploi ou du contrat de cette personne. Les procédures à suivre en pareil cas devraient être établies et comprendre la suppression du droit d'accès physique à l'installation ; le recours à un accord de non-divulgation pour protéger les informations sensibles ; et le changement des clés de cryptage, des mots de passe et des codes d'accès.

Politique et programmes d'assurance de la qualité

4.39. La politique et les programmes d'assurance de la qualité d'une installation en matière de sécurité nucléaire devraient tenir compte des menaces internes décrites dans l'évaluation de la menace ou la menace de référence. Ainsi qu'il est énoncé au paragraphe 3.52 de la réf. [2] :

> « La politique d'assurance de la qualité et les programmes de protection physique devraient s'assurer qu'un *système de protection physique* est conçu, mis en œuvre, géré et maintenu dans un état lui permettant d'être efficace au regard de l'*évaluation de la menace* ou face à la *menace de référence* et qu'il est conforme à la réglementation de l'État, notamment à ses exigences prescriptives et/ou basées sur la performance. »

4.40. Les programmes d'assurance de la qualité devraient couvrir tous les systèmes d'une installation contribuant à la sécurité nucléaire pour assurer une protection adéquate contre les menaces internes. Aux fins de l'assurance de la qualité, il conviendrait de gérer la configuration des systèmes de sécurité nucléaire pour s'assurer qu'ils continuent de satisfaire aux critères de performance souhaités et pour comprendre toutes les conséquences qui pourraient résulter de changements apportés à ces systèmes, par exemple par un initié.

Mesures relatives aux systèmes informatisés

4.41. Si certaines mesures, comme l'accompagnement, peuvent être efficaces pour limiter l'accès des initiés aux matières nucléaires et radioactives, elles ne confèrent pas une protection suffisante contre les éventuelles menaces internes visant les systèmes informatiques et les réseaux ; une telle protection peut être apportée par des mesures de sécurité de l'information [7 et 8]. Par exemple, des tiers et des vendeurs peuvent bénéficier d'un accès physique sur le site à des informations sensibles et à des ressources d'informations sensibles pendant le développement et la maintenance de systèmes informatiques et de réseaux. S'ils souhaitent conserver un accès à distance pendant toutes les étapes du cycle de vie des systèmes informatiques et des réseaux, cet accès ne devrait être accordé que conformément à l'approche fondée sur les risques [1].

4.42. L'exploitant de l'installation devrait établir et appliquer une politique concernant l'utilisation acceptable des systèmes informatisés. Cette politique peut définir l'utilisation approuvée des systèmes informatisés, exposer les attentes de l'employeur concernant la surveillance de cette utilisation, prévoir une formation et recenser précisément les actions interdites sur les systèmes informatiques. L'exploitant de l'installation devrait également envisager de recourir à des mesures techniques pour faire appliquer ou renforcer la politique relative aux systèmes. Il peut, par exemple, établir une politique concernant les médias sociaux et donner accès à une formation assistée par ordinateur sur l'utilisation des médias sociaux pour réduire le risque que des agresseurs se servent d'employés comme initiés involontaires.

Mise en œuvre de mesures de protection

4.43. Les mesures de protection contre les menaces internes visent à détecter et à retarder un acte malveillant, à y répondre s'il est commis et, éventuellement, à en atténuer les conséquences et à récupérer les matières nucléaires et radioactives. Lors de l'élaboration et de la mise en œuvre de ces mesures, il conviendrait de s'assurer qu'elles créent des conditions favorables à l'exploitation et à la sûreté de l'installation et ne nuisent pas à ces dernières. En cas de conflit, en particulier concernant la sûreté, il conviendrait de trouver une solution qui réduise au minimum le risque global pour les travailleurs et le public et maintienne une sécurité suffisante.

4.44. Les mesures de protection contre les menaces internes devraient être appliquées au moyen d'une approche graduée pour les cibles identifiées. En plus d'assurer la protection contre l'enlèvement non autorisé, ainsi qu'il est énoncé

au paragraphe 5.12 de la référence [2], « [l]'*exploitant* devrait concevoir un *système de protection physique* efficace contre les scénarios de *sabotage* élaborés et conforme au niveau de protection requis pour l'*installation nucléaire* et les *matières nucléaires* ». Certains des scénarios de sabotage devraient impliquer un ou plusieurs agresseurs internes. Les sections qui suivent portent sur les mesures de protection contre les menaces internes qu'il conviendrait d'envisager lors de la conception d'un système de sécurité nucléaire.

Mesures de détection

4.45. La détection des actes malveillants que tentent de commettre des agresseurs externes consiste principalement à détecter le contournement de l'une quelconque des mesures de protection d'une installation. Les initiés, quant à eux, pourraient contourner ou neutraliser certaines mesures de protection physique et mesures de comptabilité et de contrôle des matières nucléaires, compte tenu de leur accès autorisé, de leur autorité et de leurs connaissances. Les exploitants devraient mettre en place, pour ces systèmes, plusieurs mesures de protection différentes afin de détecter les actes malveillants susceptibles d'être commis par un initié et de recueillir les informations nécessaires à une enquête et à une analyse. L'exploitant de l'installation devrait examiner de manière approfondie toutes les informations recueillies grâce à ces mesures de détection. Des signes qui, pris isolément, semblent insignifiants peuvent indiquer un acte malveillant lorsqu'ils sont examinés ensemble.

4.46. Une enquête peut comprendre l'examen des enregistrements vidéo et des données de surveillance du réseau, la vérification des dispositifs indicateurs de manipulation frauduleuse ou des données de mesure liées aux matières nucléaires, l'inspection du journal des accès ou la réalisation d'un inventaire d'urgence. L'enquête et l'analyse du possible acte malveillant devraient être effectuées par du personnel qualifié. Le temps nécessaire pour effectuer l'enquête et l'analyse après une détection a une incidence directe sur la capacité de l'exploitant de l'installation à intervenir en temps voulu en cas d'acte malveillant.

4.47. Les activités suspectes ou non autorisées devraient être détectées et faire l'objet d'une enquête, car elles peuvent indiquer qu'un acte malveillant est en phase d'exploration ou de préparation. Par exemple, un initié peut tenter de contourner les procédures (p. ex. en introduisant des articles interdits dans une zone), tenter d'accéder à une zone pour laquelle il n'a pas de droit d'accès (p. ex. en entrant par une porte de secours), déclencher une alarme pour observer le déroulement temporel et la nature de l'intervention, ou tenter d'obtenir des

informations sensibles ou des informations réservées à ceux qui en ont besoin auxquelles il n'a pas le droit d'accéder.

4.48. Les mesures de protection visant à détecter les menaces internes doivent permettre de détecter, d'évaluer correctement et de signaler les actes suspects ou malveillants. Les mesures de détection mises en place contre les menaces internes dans une installation comprennent généralement des mesures relatives au contrôle des accès, au suivi du personnel, à la détection des articles interdits, à la surveillance, aux systèmes de comptabilité et de contrôle des matières nucléaires et à la sécurité informatique. Ces types de mesures sont l'objet des sections qui suivent.

Contrôle des accès

4.49. L'exploitant devrait établir et consigner des règles et des procédures de contrôle des accès strictes applicables aux matières nucléaires, au matériel utilisé pour transformer ou manipuler les matières nucléaires, et aux données relatives aux matières nucléaires ou aux systèmes intéressant la sûreté ou la sécurité. L'application rigoureuse de telles règles et procédures réduit au minimum l'accès des initiés aux matières, aux systèmes et au matériel. Les règles et les procédures de contrôle des accès peuvent aussi avoir un effet dissuasif, car elles peuvent rendre possible la détection ou l'identification lorsqu'un initié tente d'accéder à des matières, à du matériel ou à des données pour lesquels il n'a pas de droit d'accès.

4.50. Les règles et les procédures de contrôle des accès devraient s'appliquer dans diverses situations, notamment lors de l'autorisation d'accès à des zones contenant des matières nucléaires et lors du contrôle de matières nucléaires dans des conditions habituelles et inhabituelles, comme pendant une situation d'urgence réelle ou simulée. Par exemple, les règles de contrôle des accès pourraient s'appliquer au contrôle et à la divulgation des combinaisons de clés et de verrous des systèmes de contrôle des accès manuels ainsi qu'à l'impression des badges, à l'enregistrement des numéros d'identification personnels, à la collecte des données biométriques et au contrôle des verrous dans les systèmes électroniques.

4.51. L'exploitant de l'installation devrait protéger contre un accès non autorisé : a) le matériel servant à générer les badges, b) le matériel d'appui et les pièces de rechange associées, et c) les systèmes utilisés pour octroyer des autorisations d'accès. Il devrait contrôler rigoureusement l'accès au matériel de sécurité ou au matériel contribuant à la sécurité, à l'étalonnage et à la maintenance. Il devrait aussi établir des procédures destinées à assurer que ce matériel reste intact. Par exemple, afin de s'assurer qu'il n'a pas été manipulé frauduleusement, le matériel

devrait être testé par du personnel autorisé après la maintenance et avant sa remise en service.

4.52. Des règles de contrôle des accès devraient être définies pour les visiteurs et les accompagnateurs ainsi que pour les conditions inhabituelles, comme l'intervention en cas de situation d'urgence et d'arrêt du système.

4.53. Il conviendrait de vérifier des critères particuliers, comme l'habilitation et la détermination du besoin d'en connaître d'une personne, avant d'autoriser celle-ci à accéder à une zone dont l'accès est contrôlé. L'établissement des règles de contrôle des accès devrait se faire en coordination avec les organismes chargés de la comptabilité et du contrôle des matières nucléaires, des opérations, de la sûreté et de la protection physique.

4.54. Chaque accès ou tentative d'accès à des emplacements physiques et des systèmes informatiques sensibles devrait être consigné dans des registres de contrôle des accès. Les actes malveillants commis par des agresseurs internes peuvent être détectés lors du suivi et de l'inspection de ces registres. L'inspection des registres de contrôle des accès peut, par exemple, permettre de repérer des événements tels qu'un accès non programmé à une casemate d'entreposage, chaque tentative infructueuse d'entrée d'un numéro d'identification personnel, l'authentification biométrique infructueuse d'un badge autorisé ou d'autres indications de tentatives d'entrée par des personnes non autorisées. Une fois détectée, il est possible d'évaluer si l'irrégularité ou l'activité suspecte peut être un acte malveillant. Les mesures de détection et les procédures connexes appliquées pour surveiller et inspecter les registres de contrôle des accès devraient être considérées comme des mesures techniques et administratives de contrôle des accès lors de la conception et de la mise à niveau des systèmes.

4.55. Des registres de contrôle des accès devraient aussi être tenus pour toutes les personnes qui accèdent à des zones vitales ou qui ont accès à, ou ont en leur possession, des clés, des cartes d'accès et d'autres moyens permettant d'accéder à d'autres systèmes, notamment des systèmes informatiques contrôlant l'accès aux zones intérieures, aux zones vitales et à d'autres zones contenant des matières nucléaires [2].

4.56. S'ils sont tenus de manière appropriée, les registres de contrôle des accès peuvent être utilisés pour établir une liste d'éventuels suspects dans le cadre d'une enquête sur un acte malveillant. Les demandes d'accès autorisé à des zones de sécurité ou à des systèmes intéressant la sûreté ou la sécurité, qu'elles soient

approuvées ou rejetées, devraient aussi être examinées et inspectées en vue de repérer d'éventuelles activités malveillantes.

Suivi du personnel

4.57. Le suivi du déplacement et de la localisation du personnel dans une installation permet à l'exploitant de détecter une violation ou une tentative de violation des règles de contrôle des accès, comme la sortie de plusieurs personnes de l'installation à l'aide d'un seul badge de contrôle des accès. La technologie existante permet de suivre les personnes en temps réel ou après les faits en enregistrant les emplacements et les zones dans lesquels elles se rendent chaque jour, de même que l'heure et la durée de chaque visite.

4.58. Le fait de savoir qu'une installation possède un système de suivi peut dissuader les initiés de réaliser des activités non autorisées. En outre, les registres de suivi et les registres de contrôle des accès peuvent être utilisés pendant l'enquête menée sur un acte malveillant, à des fins d'évaluation, ou après un incident, pour établir une première liste de suspects.

Détection d'articles interdits

4.59. Ainsi qu'il est recommandé au paragraphe 4.43 de la référence [2] :

> « Les véhicules, les personnes et les colis devraient être soumis à une fouille lorsqu'ils pénètrent dans les *zones protégée* et *intérieure* aux fins de la *détection* et de la prévention d'un accès non autorisé et de l'introduction d'articles interdits. Les véhicules, les personnes et les colis qui sortent de la *zone intérieure* devraient être soumis à une fouille aux fins de la *détection* et de la prévention d'un *enlèvement non autorisé*. »

4.60. L'exploitant devrait recenser et consigner par écrit les articles interdits dans les zones à accès limité, les zones protégées, les zones intérieures et les zones vitales. Les articles interdits peuvent comprendre des outils et du matériel non autorisés, comme : les ordinateurs, les téléphones portables, les tablettes et autres dispositifs de technologies de l'information comportant une caméra ; le matériel de protection contre les rayonnements ; les armes et les explosifs. Ces articles pourraient servir à accéder ou à causer des dommages à des systèmes ou du matériel sensibles, ou à leurs composants, ou permettre l'enlèvement non autorisé ou le sabotage de matières nucléaires. D'autres articles interdits propres à une installation peuvent être identifiés pour préserver la protection physique, la

comptabilité et le contrôle des matières nucléaires, les systèmes de sûreté et les systèmes opérationnels ou protéger les informations contre des agresseurs internes.

4.61. L'exploitant devrait procéder immédiatement à une enquête après la détection de l'entrée d'articles interdits dans une zone, ou de leur sortie d'une zone, car il pourrait s'agir d'un acte malveillant commis par un initié. Lors de la préparation d'un acte malveillant, un agresseur interne peut tester le système de détection d'articles interdits pour vérifier la sensibilité des détecteurs ou l'efficacité des procédures d'évaluation. Les détections suspectes ou répétées d'articles interdits devraient être identifiées, évaluées et signalées, et donner lieu à une enquête.

4.62. Les mesures de détection d'articles interdits comprennent la fouille manuelle (tant périodique qu'aléatoire) 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 ou d'autres types de détecteurs de produits chimiques ou d'explosifs. Ces mesures devraient tenir compte des caractéristiques de l'installation et des menaces contre lesquelles une protection est nécessaire conformément à l'évaluation de la menace ou à la menace de référence, le cas échéant.

4.63. L'exploitant devrait élaborer et mettre en œuvre des politiques permettant d'identifier les articles interdits, et les procédures de fouille et de détection connexes. Le personnel effectuant les fouilles ou utilisant le matériel de détection des articles interdits devrait être formé à utiliser le matériel et à intervenir de manière appropriée après l'identification d'un article interdit. Les interventions peuvent comprendre la confirmation d'une exception autorisée, l'appréhension de l'agresseur interne potentiel ou l'enregistrement de l'événement aux fins de la détection des actes de malveillance potentiels à l'avenir.

4.64. La rigueur de la fouille et le lieu où elle sera effectuée devraient être déterminés compte tenu de la sensibilité de la zone où la fouille a été déclenchée et de la proximité entre cette zone et la cible. La fouille devrait être effectuée près de la zone où elle a été déclenchée. Les fouilles périodiques et aléatoires devraient servir à décourager encore l'enlèvement non autorisé ou le sabotage de matières nucléaires et radioactives. Les fouilles devraient également être effectuées lors des situations d'évacuation d'urgence, y compris lors des exercices.

4.65. Des procédures de surveillance devraient être appliquées lors de la fouille minutieuse d'un véhicule de transport avant le chargement et l'expédition pour s'assurer que les personnes procédant à la fouille ne peuvent pas introduire d'articles interdits qui faciliteraient un acte malveillant.

4.66. Des détecteurs de rayonnements fixes ou portatifs devraient être utilisés sur les personnes, dans les colis ou dans les véhicules entrant dans des zones protégées, intérieures ou vitales, ou en sortant, pour détecter l'enlèvement non autorisé de matières nucléaires. Des détecteurs de métaux devraient être installés en complément des détecteurs de rayonnements aux entrées et aux sorties des piétons pour renforcer l'efficacité de la détection des rayonnements, car un matériau de blindage peut être utilisé pour empêcher la détection des signatures radioactives si des matières nucléaires sont retirées de l'installation.

4.67. Des procédures particulières relatives à l'approbation d'exceptions à l'introduction d'articles interdits ou contrôlés (p. ex. sources d'étalonnage radioactives) dans l'installation devraient être établies [3].

Surveillance

4.68. Des mesures peuvent être appliquées pour surveiller de façon continue les activités des personnes à l'intérieur des zones désignées de l'installation où un acte malveillant pourrait être commis afin que les activités non autorisées soient identifiées, signalées et évaluées.

4.69. La surveillance comprend l'observation visuelle, la visualisation de vidéos en direct ou l'examen de séquences enregistrées par les systèmes de surveillance automatique. Elle peut être utile comme mesure de détection mais aussi pour dissuader un initié de commettre des actes malveillants, et aux fins de l'enquête relative à de tels actes.

4.70. Le personnel qui effectue les activités de surveillance devrait être capable de détecter les actes autorisés et non autorisés, et en mesure de signaler rapidement et de manière sûre toute activité non autorisée observée.

4.71. En cas de signalement d'une activité non autorisée, les enregistrements de vidéosurveillance peuvent servir à établir l'évaluation correcte d'un acte malveillant ou à identifier les éventuels suspects. Il peut être difficile d'évaluer en temps voulu les actes malveillants sans informations obtenues par la surveillance.

4.72. Ainsi qu'il est recommandé au paragraphe 4.48 de la référence [2], « lorsqu'une *zone intérieure* est occupée, la *détection* d'actions non autorisées devrait se faire par le biais d'une surveillance constante (*règle des deux personnes*, par exemple) ». Il conviendrait d'envisager d'appliquer les mesures de surveillance lors des opérations telles que la maintenance, et en particulier lors des opérations d'emballage, d'expédition et de transfert [14]. La surveillance peut être assurée

par des collègues, des responsables, les systèmes de surveillance automatique ou une combinaison de ces moyens.

4.73. L'exploitant devrait définir et effectuer des contrôles périodiques pour s'assurer que les mesures de contrôle des matières ou les autres mesures de protection sont mises en œuvre conformément aux procédures établies et que le matériel est utilisé correctement.

4.74. Lorsque la règle des deux personnes est la méthode de surveillance choisie dans une zone (p. ex. dans une zone contenant des matières de catégorie I), les deux personnes autorisées et bien informées devraient être physiquement placées de telle sorte qu'elles aient une vue dégagée l'une de l'autre et des matières nucléaires. En outre, chaque personne devrait être formée et techniquement qualifiée pour détecter les activités non autorisées ou les procédures irrégulières. Pour que la surveillance visuelle soit efficace, les personnes qui observent doivent être capables de reconnaître les activités non autorisées, d'évaluer correctement la situation et de signaler ces activités aux personnes appropriées chargées des interventions suffisamment vite pour qu'elles puissent empêcher l'enlèvement non autorisé. Si la règle des deux personnes est appliquée pour ce type de surveillance, chacune des deux personnes autorisées doit avoir suivi une formation appropriée, avoir une vue dégagée sur les matières et sur son collègue et être capable de détecter des activités non autorisées ou des procédures irrégulières [1].

4.75. En outre, cette règle n'est efficace que lorsque les deux personnes ne deviennent pas mutuellement complaisantes, par exemple du fait d'une amitié ou d'une collaboration de longue date. Chaque fois que cela est possible, les responsables devraient veiller à ce que les membres de chaque équipe de deux personnes alternent. Le fait d'appliquer la règle des deux personnes pour régir l'accès aux zones désignées peut décourager les agresseurs internes et contribuer à la détection rapide. En outre, la règle des deux personnes peut aider à empêcher que des agresseurs internes manipulent frauduleusement les systèmes de protection physique. Toute tentative de contrarier la règle des deux personnes devrait être signalée et donner lieu à une enquête.

Systèmes de comptabilité et de contrôle des matières nucléaires

4.76. La contribution des systèmes de comptabilité et de contrôle des matières nucléaires à la sécurité nucléaire est principalement due à la capacité de ceux-ci à maintenir une connaissance précise des types, des quantités et de l'emplacement des matières nucléaires dans l'installation, pour permettre d'effectuer des inventaires du stock physique de matières nucléaires et, dans certains cas, de

s'assurer que les activités effectuées en relation avec les matières nucléaires ont été dûment autorisées [9]. Il existe de nombreuses mesures grâce auxquelles un système de comptabilité et de contrôle des matières nucléaires peut aider à détecter des menaces internes. Ces mesures sont décrites plus en détails dans la référence [9].

4.77. La comptabilité et le contrôle des matières nucléaires ainsi que les autres mesures de détection devraient être appliqués rigoureusement pour empêcher l'enlèvement non autorisé de matières nucléaires supplémentaires d'une installation par un agresseur interne, ou avec l'aide d'un tel agresseur, lors d'une expédition non autorisée. Les autres mesures de détection peuvent inclure l'utilisation : a) de la règle des deux personnes lors de la préparation du mouvement, b) de mesures de matières, c) de dispositifs indicateurs de manipulation frauduleuse, d) de vérifications de documents, e) de détecteurs de rayonnements et f) de procédures opérationnelles standard.

Mesures de détection relatives aux systèmes informatisés

4.78. Des mesures techniques concernant le matériel informatique et les logiciels devraient être appliquées pour détecter des actes malveillants. Elles peuvent comprendre, par exemple, les activités suivantes :

a) l'établissement d'un état de référence pour le trafic réseau des actifs informatiques sensibles, la caractérisation de ce trafic, et l'inspection de l'état de référence ;
b) la mise en œuvre d'outils de détection d'intrusions logicielles pour détecter les schémas anormaux de comportements d'utilisateurs ;
c) la surveillance, l'inspection et l'évaluation des systèmes informatiques aux fins de la vérification du respect des politiques et des procédures par les initiés et de la détection des actes suspects. Par exemple, l'exploitant peut mettre en place de fausses cibles et les surveiller pour détecter les tentatives d'accès non autorisé à des informations sensibles, et mettre ainsi en lumière un agresseur interne potentiel tout en veillant à ce qu'aucune donnée sensible ne soit révélée ;
d) la restriction des voies qui pourraient servir à accéder à des données de sorte que seul le personnel autorisé ait la possibilité de les utiliser, et le contrôle et la surveillance des voies en vue de la protection contre une utilisation malveillante. Cette mesure pourrait comprendre la surveillance, le blocage physique, l'interdiction d'utilisation de supports amovibles et de dispositifs mobiles pour limiter l'accès d'un initié aux systèmes sensibles, ou le recours

à des zones de sécurité informatique pour isoler les systèmes de sécurité nucléaire et leurs réseaux des autres réseaux de l'installation [7].

Mesures de retardement

4.79. La mise en place de plusieurs niveaux de différentes mesures de protection physique et mesures procédurales, y compris la compartimentation et la séparation des tâches, peut compliquer la progression d'un agresseur interne en requérant divers outils et aptitudes, ce qui laisse ainsi plus de temps pour la détection et en accroît la probabilité. De telles mesures de retardement de l'acte malveillant pourraient permettre de détecter et de mettre en échec un agresseur interne. Elles peuvent aussi décourager les tentatives d'actes malveillants par des initiés.

4.80. Les mesures mises en œuvre près du matériel ou des matières nucléaires (p. ex. attaches, entraves, serrures) peuvent constituer des mesures de retardement efficaces contre les agresseurs internes lorsqu'une zone fait l'objet d'une surveillance continue ou lorsque d'autres mesures de détection appropriées sont en place. Ces mesures devraient être conçues de sorte qu'il soit difficile pour un agresseur interne de les utiliser pour retarder l'intervention face à un acte malveillant, en particulier un acte de sabotage.

4.81. Le fait de conserver les matières nucléaires dans un lieu sécurisé peut retarder encore la tentative d'acte malveillant par un agresseur interne. Lors d'une production ou d'une utilisation, la quantité minimale de matières nucléaires nécessaire devrait être retirée en une seule fois du lieu d'entreposage verrouillé, et des mesures devraient être prises pour contrôler les matières nucléaires entre les étapes du processus. Lorsque les matières ne peuvent pas être déplacées dans un lieu d'entreposage sécurisé en dehors des heures de travail, des mesures de protection physique et de surveillance supplémentaires devraient être mises en œuvre jusqu'à ce que les matières soient correctement restituées et entreposées dans un lieu sécurisé normal.

4.82. Certains types de mesures de retardement peuvent contraindre les agresseurs internes à utiliser des outils, des ressources, une logistique, une formation et des compétences plus sophistiquées pour les neutraliser. Il est possible que ces ressources sophistiquées ne soient pas disponibles dans l'installation et doivent y être introduites par l'agresseur interne ou être acquises ailleurs.

4.83. Les conceptions de sûreté d'un système qui assurent l'auto-protection de ce système (p. ex. matériel de remplacement, mise à l'arrêt automatique des équipements, fermeture automatique des vannes) peuvent contraindre l'agresseur

interne à neutraliser de multiples équipements et systèmes redondants et dispersés. Ces dispositifs peuvent retarder un acte malveillant et l'empêcher d'être mené à bien. Dans la mesure du possible, l'accès à l'information relative aux conceptions de sûreté d'un système devrait être limité selon le principe du « besoin de savoir » pour empêcher que cette information serve à commettre un acte malveillant.

Mesures de retardement des systèmes informatisés

4.84. Il est possible que les mesures de sécurité physique mises en œuvre pour retarder les agresseurs ne protègent pas efficacement les systèmes informatiques en raison de l'accès à distance à certains d'entre eux et de leur interconnectabilité. Par exemple, un initié bénéficiant d'un accès privilégié à des systèmes informatiques sensibles peut être en mesure de dégrader des biens physiquement séparés à distance et de façon simultanée. De plus, il se peut que les mesures de retardement ne soient pas efficaces contre un agresseur interne qui peut user de pouvoirs existants pour obtenir un accès privilégié. Par conséquent, les mesures concernant les systèmes informatisés devraient mettre l'accent sur la prévention et, dans une plus large mesure, la détection et l'intervention.

4.85. Par la conception et la mise en œuvre de zones et de niveaux de sécurité informatique dans une installation, il est possible de rendre plus compliquée la commission d'un acte malveillant à l'aide de systèmes informatiques et de prévoir des contrôles de sécurité qui peuvent également accroître la probabilité de détection [7].

Mesures d'intervention

4.86. Tant le personnel d'exploitation que le personnel de sécurité peuvent intervenir en cas d'irrégularité (p. ex. une différence d'inventaire, une porte ouverte qui devrait être fermée). Habituellement, le personnel d'exploitation intervient en cas d'irrégularité pour étudier la cause de celle-ci. Si l'on suspecte qu'une irrégularité est due à un acte malveillant, le personnel de sécurité devrait être informé et intervenir si nécessaire. À titre d'exemple :

a) L'intervention face à un agresseur interne passif devrait dépendre du moment où la détection a lieu (quand l'information est obtenue, quand elle est communiquée ou moment où l'enquête est achevée).
b) L'intervention face à un agresseur interne non-violent actif devrait être menée par le personnel d'exploitation ou le personnel de sécurité, suivant le moment où la détection a lieu, car un agresseur interne non-violent actif

interrompra un acte malveillant si on s'oppose à lui ou si on lui demande des explications.

c) L'intervention face à un agresseur interne violent actif devrait être la même que face à un agresseur externe.

4.87. Un agresseur interne est plus difficile à identifier qu'un agresseur externe et peut ne pas être facilement identifié comme une menace n'importe où dans l'installation. De plus, un acte malveillant commis par un agresseur interne peut consister en plusieurs actes distants dans le temps et dans l'espace. Par conséquent, s'il n'est pas identifié lors de la détection d'un acte suspect ou malveillant, il peut être difficile d'identifier un agresseur interne par la suite parmi les autres initiés.

4.88. Pour que l'intervention puisse être efficace, un vol sur la durée doit être détecté avant que l'agresseur interne n'accumule une quantité cible de matières sur le site ou hors du site. Les scénarios devraient tenir compte des systèmes et des mesures de sécurité en place dans le bâtiment et dans toute zone de bilan matières éventuelle, ainsi que des procédures de sécurité nucléaire particulières qui pourraient être appliquées pour détecter des activités non autorisées mettant en jeu des matières nucléaires suffisamment tôt pour permettre une intervention efficace. Pour les installations dans lesquelles un vol sur la durée peut être commis, l'analyse des scénarios devrait porter sur la probabilité de détection si des matières étaient : a) retirées du site chaque fois qu'une quantité de matières était volée ou b) accumulées dans l'installation ou dans une zone de processus pour être retirées du site en une seule fois lors d'un vol soudain.

4.89. Un agresseur interne peut commettre une série d'actes, devant aboutir en dernier lieu à un enlèvement non autorisé ou à un sabotage, dans un ordre inattendu ou avec des périodes d'inactivité entre chaque acte. Par exemple, un agresseur interne peut commettre un seul acte puis attendre de voir s'il est détecté. Cela peut compliquer l'intervention de sécurité nécessaire pour identifier et appréhender l'agresseur interne et requérir une enquête de plus grande ampleur. Il peut falloir que des spécialistes des opérations contribuent à l'enquête en analysant l'événement anormal ou irrégulier pour prédire les autres actes malveillants susceptibles d'être tentés.

4.90. Les initiés ayant accès à une installation devraient être formés à la détection des actes malveillants et à l'intervention afin qu'ils puissent se protéger et transmettre les alarmes conformément à une série de procédures établies. Ces procédures devraient être consignées et utilisées dans le cadre d'une formation de sensibilisation à la sécurité dispensée au personnel de l'installation par l'exploitant. Dans les procédures d'intervention, il conviendrait de tenir compte

de l'hypothèse selon laquelle une personne participant à l'intervention pourrait être un agresseur. Par exemple, un agresseur interne pourrait signaler une situation d'urgence fictive pour détourner l'attention des autres et les empêcher de détecter un acte malveillant, ou un agresseur interne faisant partie de l'équipe d'intervention pourrait utiliser un exercice d'intervention d'urgence ou créer une situation d'urgence pour dissimuler un acte malveillant.

Mesures d'intervention dans les systèmes informatisés

4.91. En ce qui concerne les incidents de sécurité informatique susceptibles de nuire aux systèmes contribuant à la sécurité nucléaire, les activités d'intervention devraient être coordonnées avec le personnel d'intervention en matière de sécurité nucléaire et consignées. Par exemple, la détection de changements non autorisés dans le contrôle des accès par un initié devrait donner lieu à une intervention coordonnée avec la participation du personnel de sécurité du site et du personnel de sécurité informatique, car de tels changements sont susceptibles de faciliter l'enlèvement non autorisé ou le sabotage. Dans le cas d'un tel incident de sécurité informatique, des mesures compensatoires concernant la sécurité du site et les autres organisations appropriées de l'installation devraient aussi être envisagées.

ÉLÉMENTS COMPLETS RENFORÇANT LES MESURES DE PRÉVENTION ET DE PROTECTION

Culture de sécurité nucléaire

4.92. La culture de sécurité nucléaire se fonde sur la reconnaissance de l'existence d'une menace crédible et de l'importance de la sécurité nucléaire [11].

4.93. La culture de sécurité nucléaire joue un rôle important en permettant de faire en sorte que les personnes, les organisations et les institutions restent vigilantes et que des mesures durables soient prises pour contrer les menaces internes. L'efficacité des mesures de prévention et de protection contre les menaces internes dépend des attitudes, des comportements et des actions des personnes [17].

4.94. La direction devrait promouvoir une culture de sécurité nucléaire solide pour contrer les menaces internes et externes. La culture de sécurité nucléaire crée les conditions générales permettant au personnel de mettre en œuvre les mesures de prévention et de protection. La culture de sécurité nucléaire d'une installation devrait améliorer la loyauté et le respect des politiques de sécurité. Par exemple, la direction devrait souligner la responsabilité qui incombe aux employés de signaler

des activités inhabituelles ou un comportement suspect, sans qu'ils craignent de subir des mesures disciplinaires [11].

Plans d'intervention spécialisés

4.95. Comme énoncé au paragraphe 3.58 de la référence [2] :

> « L'État devrait élaborer un *plan d'intervention spécialisé*. L'*autorité* nationale *compétente* devrait veiller à ce que l'*exploitant* établisse des *plans d'intervention spécialisés* pour faire efficacement échec à l'*évaluation de la menace* ou à la *menace de référence* en tenant compte de l'action des *forces d'intervention* ».

Au paragraphe 3.62 de la référence [2], il est énoncé que « [l]'*exploitant* devrait activer son *plan d'intervention spécialisé* après la *détection* et l'évaluation de tout *acte malveillant*. » Au paragraphe 5.44 de la référence [2], il est énoncé que « [l]e *plan d'intervention spécialisé* devrait comprendre des mesures visant à prévenir d'autres dommages, sécuriser l'*installation nucléaire* et protéger le matériel et le personnel d'intervention. »

4.96. Les plans d'intervention d'urgence élaborés par l'État et l'exploitant devraient comporter des mesures relatives aux menaces internes et externes. Les mesures de protection contre les menaces internes devraient être coordonnées avec les plans d'intervention d'urgence conformément aux procédures convenues. Le plan d'intervention d'urgence devrait requérir que le personnel évacuant un bâtiment au cours d'une situation d'urgence réelle ou simulée fasse l'objet d'un contrôle et d'un examen portant sur la contamination et les matières nucléaires aux fins de la protection contre les menaces internes.

4.97. Les mesures prises en réponse à des actes malveillants suspectés ou confirmés d'un agresseur interne peuvent être différentes de l'intervention face à un acte malveillant commis par un agresseur externe.

Programme de maintenance et de récupération des systèmes

4.98. Un programme de maintenance et de récupération de tous les systèmes de sécurité nucléaire d'une installation devant être protégés peut atténuer les conséquences d'un acte malveillant commis par un agresseur interne. Le programme de maintenance devrait comprendre des moyens de réparer rapidement les systèmes opérationnels et les autres systèmes essentiels, de remplacer rapidement les pièces ayant été endommagées et de mettre en œuvre

des mesures compensatoires selon les besoins. Une réparation et un remplacement rapides réduisent la durée de l'arrêt du système et le temps pendant lequel des actes malveillants peuvent être commis par suite de l'arrêt, et peuvent atténuer les conséquences de l'acte malveillant commis par l'agresseur interne.

4.99. Les exploitants devraient envisager de protéger les pièces de rechange (p. ex. en installant des barrières, en entreposant ces pièces à un endroit distant du système installé et en surveillant fréquemment le lieu d'entreposage) de sorte qu'il soit difficile pour un agresseur interne de détruire ou de dégrader à la fois les pièces installées et les pièces de rechange d'un équipement essentiel.

4.100. Les procédures d'exploitation d'une installation et les procédures de récupération des systèmes de sécurité et des systèmes opérationnels devraient être validées et appliquées dans le cadre d'exercices afin d'aider à assurer la récupération rapide de ces systèmes, et de protéger le matériel et le personnel d'intervention.

4.101. Les procédures mises en œuvre pour la protection du matériel répertorié devraient comprendre l'intervention appropriée en cas d'arrêts, comme la mise en œuvre de mesures compensatoires, la recherche de la cause de l'arrêt et la mise en œuvre d'un système de réparation rapide (remise en service), en vue de protéger contre la possibilité qu'un acte malveillant non évalué soit en cours.

4.102. Un système de secours sécurisé et des processus de récupération devraient être mis en œuvre pour les systèmes informatiques sensibles afin d'assurer l'exploitation ou les fonctions de sécurité. Les fichiers du système utilisés dans les processus de récupération devraient être entreposés dans une zone séparée avec contrôle des accès.

5. ÉVALUATION DES MESURES

OBJECTIFS ET APERÇU DU PROCESSUS D'ÉVALUATION

5.1. L'évaluation de l'efficacité des mesures de prévention et de protection contre les menaces internes est un élément clé de l'évaluation du risque destinée à identifier les systèmes vulnérables aux menaces internes. L'évaluation devrait se fonder sur des scénarios de menace crédibles basés sur l'évaluation de la menace ou la menace de référence.

5.2. Il conviendrait de comparer les résultats de l'évaluation aux critères établis au préalable concernant l'efficacité des mesures de prévention et de protection. Ces critères, généralement établis par l'autorité compétente, sont basés sur les conséquences potentielles d'un acte malveillant commis par un agresseur interne et la probabilité de succès de cet acte. Il conviendrait de consigner la façon dont l'exploitant satisfait à ces critères dans le plan de sécurité complet de l'exploitant, qui comprend les plans relatifs à la protection des systèmes de comptabilité et de contrôle des matières nucléaires et des systèmes de protection physique.

5.3. L'évaluation de l'efficacité des mesures de prévention et de protection devrait se fonder sur le plan de sécurité de l'exploitant. Si l'évaluation montre que les mesures de prévention et de protection définies dans le plan de sécurité ne satisfont pas aux critères, il conviendrait de procéder à des mises à niveau et d'effectuer à nouveau l'évaluation jusqu'à ce que les critères soient remplis.

5.4. Lors de l'évaluation, l'exploitant devrait prendre en considération la relative facilité avec laquelle un acte malveillant peut être commis et le niveau de risque associé à l'acte malveillant potentiel. Par exemple, un acte malveillant peut avoir des conséquences jugées acceptables mais être relativement facile à commettre (p. ex. modification non autorisée du niveau de détection d'un portique de détection des rayonnements) ; un tel acte peut par conséquent être jugé inacceptable et requérir une action corrective. De plus, le risque peut être acceptable mais proche du seuil à partir duquel il ne le serait plus. Par exemple, un agresseur interne pourrait enlever d'une zone de traitement de petites quantités de matières nucléaires de catégorie III, ce qui représente un risque faible ; mais si cet enlèvement non autorisé était répété, la quantité totale enlevée pourrait correspondre à une catégorie supérieure. Un tel cas ne devrait pas être négligé, et des pratiques de gestion prudentes conduiraient à l'établissement de mesures de protection supplémentaires.

5.5. L'efficacité des mesures de prévention et de protection devrait être réévaluée périodiquement, en particulier lorsque des changements surviennent dans l'évaluation de la menace, la menace de référence, les mesures de prévention et de protection ou les processus et les conditions d'exploitation.

5.6. Les critères et les prescriptions de performance pour un système de comptabilité et de contrôle des matières nucléaires sont établis dans le contexte général de la sécurité nucléaire et peuvent être utiles pour évaluer l'efficacité du système de sécurité nucléaire contre les menaces internes. Ils devraient tenir compte des différents types de matières nucléaires et porter sur les délais de détection de l'enlèvement non autorisé de ces matières.

5.7. Différentes méthodes peuvent être utilisées pour évaluer l'efficacité du système de sécurité nucléaire contre les menaces internes (p. ex. inspections et évaluations, test de performance, contrôle de la qualité des mesures, analyse des scénarios). L'analyse des scénarios est une méthode d'évaluation efficace contre les menaces internes. Les tests de performance appuient le processus d'analyse des scénarios en fournissant des informations concernant notamment la probabilité de détection et l'intervention qui y fait suite. Il conviendrait d'élaborer et de mettre en œuvre des plans de test de performance pour mettre à l'essai l'état de préparation des employés, de l'installation et des autorités compétentes à l'intervention face à un acte malveillant potentiel commis par un agresseur interne.

ÉVALUATION DES MESURES DE PRÉVENTION

5.8. Il conviendrait d'évaluer la mise en œuvre des mesures de prévention pour s'assurer qu'elles sont conformes à ce qui est prévu. Ces mesures, bien que difficiles à évaluer quantitativement, peuvent réduire efficacement l'éventualité de menaces internes. Les mesures de prévention devraient être évaluées au moyen de tests de performance des procédures pour déterminer si ces dernières sont adéquates pour répondre à la menace et si les employés les suivent.

5.9. L'occasion pour un agresseur interne de commettre un acte malveillant peut être réduite au minimum si l'on réduit la possibilité qu'un initié obtienne l'accès, l'autorité ou les connaissances nécessaires pour mener à bien un acte malveillant. Les scénarios d'évaluation crédibles tiendront compte de la mesure dans laquelle l'occasion est réduite au minimum et de la manière dont elle est ainsi réduite. Un examen visant à identifier les mesures de prévention en place et à déterminer si elles sont correctement appliquées devrait être effectué.

ÉVALUATION DES MESURES DE PROTECTION

5.10. L'efficacité des mesures mises en œuvre pour détecter et retarder les actes malveillants et intervenir face à de tels actes (mesures de protection) peut être analysée de manière quantitative ou qualitative. La probabilité de détection et le délai d'intervention sont souvent quantifiables et peuvent servir de base à l'évaluation de l'efficacité des mesures de protection.

5.11. Un moyen d'évaluer l'efficacité des mesures de protection contre les menaces internes consiste à élaborer des scénarios crédibles, notamment des scénarios de collusion avec d'autres agresseurs internes ou avec des agresseurs

externes, selon qu'il convient. On peut alors évaluer l'efficacité des mesures de protection pour contrer ces scénarios.

5.12. L'élaboration de scénarios suppose d'identifier la combinaison d'actions nécessaires pour qu'un agresseur interne mène à bien un acte malveillant. Les exploitants devraient envisager d'associer les cibles identifiées (voir la section 3) à un agresseur interne particulier (voir la section 2) lors de l'élaboration de scénarios. Il conviendrait de déterminer l'ensemble des actions qu'un agresseur interne devrait entreprendre pour atteindre son but, en tenant compte de l'évaluation de la menace ou de la menace de référence. Cet ensemble d'actions devraient comprendre les actions qui seraient effectuées ainsi que les lieux où elles seraient exécutées, et toutes les mesures de protection que les agresseurs internes pourraient rencontrer lorsqu'ils effectuent ces actions devraient être recensées. Étant donné que les agresseurs internes peuvent effectuer les actions requises pour commettre un acte malveillant sur une longue période, et que les actes peuvent ne pas être exécutés suivant une séquence prévisible, le concept de voie ou de chronologie peut ou non être pertinent pour l'analyse.

5.13. En ce qui concerne les scénarios de sabotage, il conviendrait de déterminer les actions devant être entreprises pour commencer une séquence d'événements qui entraîneraient des conséquences radiologiques inacceptables. Les scénarios de sabotage devraient inclure les attaques de cibles uniques et multiples.

5.14. En ce qui concerne les scénarios d'enlèvement non autorisé de matières nucléaires, il conviendrait de déterminer les actions devant être menées avec succès pour enlever des matières nucléaires de l'installation. Les scénarios d'enlèvement non autorisé de matières nucléaires devraient porter sur le vol sur la durée et le vol soudain, et inclure des situations dans lesquelles l'agresseur quitte l'installation directement avec les matières nucléaires ou cache les matières dans l'installation pour les retirer plus tard dans des circonstances plus favorables. Les scénarios devraient porter sur les attaques de systèmes informatiques ou la dégradation de tels systèmes, les combinaisons d'attaques physiques et de cyberattaques, et les attaques commises par des agresseurs internes violents et non violents.

5.15. Les stratégies susceptibles d'être adoptées par les agresseurs internes pour neutraliser les mesures de protection devraient aussi être prises en compte dans le cadre du processus d'élaboration de scénarios. L'exploitant peut élaborer de telles stratégies en examinant comment un accès, une autorité et des connaissances pourraient permettre à un agresseur interne de contrarier les mesures de détection et de retardement. Les efforts que les agresseurs internes sont susceptibles de déployer pour réduire l'efficacité de l'intervention devraient également être pris

en compte. Les conditions d'urgence qui entraînent l'évacuation d'une installation peuvent donner à un agresseur interne l'occasion de mener à bien un acte malveillant et devraient être prises en considération lors de l'élaboration des scénarios.

5.16. Une fois que des scénarios détaillés portant sur les menaces internes ont été élaborés, il est possible d'évaluer l'efficacité des mesures de protection en examinant l'effet cumulé de la détection et du retardement, ainsi que l'intervention face au scénario et l'atténuation de ses conséquences. Dans le cas d'un agresseur interne non violent actif, l'efficacité de l'intervention dépendra de la probabilité d'interruption ou de neutralisation[5] d'un acte malveillant.

5.17. Le processus d'évaluation devrait être répété pour les scénarios crédibles requérant une analyse plus poussée. Les conclusions relatives à l'efficacité des mesures de protection devraient être fondées sur les résultats de toutes les évaluations effectuées.

ÉVALUATION DES MESURES CONTRE LA COLLUSION ENTRE INITIÉS

5.18. Il est difficile d'élaborer suffisamment de scénarios portant sur la collusion entre deux agresseurs internes ou plus en raison des nombreuses combinaisons d'initiés ayant une autorité, des connaissances et un accès différents devant être prises en compte. L'évaluation de l'efficacité des mesures qui aident à empêcher la collusion (p. ex. compartimentation, surveillance, mesures de prévention) peut constituer une bonne approche.

ÉVALUATION DES MESURES CONTRE LE VOL SUR LA DURÉE

5.19. L'évaluation des mesures contre le vol sur la durée peut être abordée de la même manière que l'évaluation des mesures contre le vol soudain. Cependant, elle devrait tenir compte également des difficultés supplémentaires rencontrées par l'agresseur interne qui tente de procéder à l'enlèvement non autorisé de petites quantités de matières sur une longue période de temps. Ces difficultés

[5] « Interruption » signifie que l'intervention a lieu à temps pour empêcher que l'acte malveillant soit mené à bien. Dans le cas d'un agresseur interne violent actif, « neutralisation » signifie que la force d'intervention stoppe ou empêche l'attaque de façon permanente. Dans le cas d'un agresseur interne non violent actif, la neutralisation a lieu lorsque l'agresseur interne est identifié.

comprennent l'inventaire périodique, la détection possible de différences d'inventaire, le suivi des registres, la dissimulation des quantités de matières accumulées et la neutralisation des portiques de détection des rayonnements. La méthode d'évaluation devrait également tenir compte de la probabilité accrue de la détection lorsque la même action est répétée plusieurs fois.

ÉVALUATION DES MESURES CONTRE LE SABOTAGE

5.20. L'évaluation des mesures contre le sabotage par un agresseur interne peut se faire suivant le même processus que l'évaluation des mesures contre le vol soudain et le vol sur la durée, et peut faire référence à l'approche des modèles logiques (arbre de défaillances ou arbre d'événements) décrite dans la référence [16].

5.21. Les scénarios de sabotage à évaluer devraient inclure des scénarios concernant le sabotage direct de matières nucléaires et le sabotage indirect (c.-à-d. le sabotage de systèmes de l'installation), qui pourraient avoir des conséquences radiologiques inacceptables. Les scénarios de sabotage évalués devraient comprendre des scénarios faisant intervenir des individus qui ne bénéficient pas d'un accès direct aux matières ou au matériel.

5.22. Pour commettre un acte de sabotage, l'agresseur interne ne devrait pas nécessairement quitter l'installation pour mener à bien l'acte malveillant. Cependant, il y aurait également lieu de procéder à l'évaluation des mesures de prévention et de protection relatives à toute sortie d'un initié de l'installation.

ÉVALUATION DE LA PROTECTION D'UNE INSTALLATION CONTRE LES MENACES INTERNES

5.23. Le processus d'évaluation de la protection d'une installation contre les menaces internes commence par la caractérisation des initiés en fonction de leurs attributs, motivations et catégories pour identifier les menaces internes potentielles. L'étape suivante est l'identification de la cible, qui suppose l'évaluation des biens devant être protégés contre un enlèvement non autorisé ou un sabotage. Cette évaluation donne lieu à l'établissement d'une liste des cibles assortie de priorités.

5.24. Les mesures de prévention devraient être mises en œuvre suivant le concept de défense en profondeur et une approche graduée afin de réduire le plus possible la possibilité que les menaces identifiées se concrétisent et que les cibles identifiées fassent l'objet d'actes malveillants.

5.25. Les mesures de protection devraient être déterminées de manière à protéger les cibles dans les zones protégées, intérieures ou vitales en tenant compte de priorités. Les mesures visant à détecter et à retarder la menace interne et à y répondre devraient être renforcées en fonction des résultats de l'évaluation.

5.26. Les mesures de prévention et de protection contre le sabotage et l'enlèvement non autorisé de matières nucléaires devraient être évaluées au moyen d'une méthode telle que l'élaboration de scénarios crédibles. Les scénarios devraient être cohérents avec l'évaluation de la menace ou la menace de référence et peuvent comprendre des attaques physiques, des cyberattaques ou une combinaison des deux dans l'installation, sur les voies d'acheminement et sur les chaînes d'approvisionnement.

5.27. Il conviendrait de réévaluer le système périodiquement pour s'assurer que les mesures sont mises en place efficacement et maintenues. La réévaluation peut se faire de façon cyclique, ou lorsque se produisent des changements relatifs à la menace ou à l'installation et à son exploitation.

RÉFÉRENCES

[1] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Objectif et éléments essentiels du régime de sécurité nucléaire d'un État, nº 20 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2014).

[2] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Recommandations de sécurité nucléaire sur la protection physique des matières nucléaires et des installations nucléaires (INFCIRC/225/Révision 5), nº 13 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2011).

[3] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Recommandations de sécurité nucléaire relatives aux matières radioactives et aux installations associées, nº 14 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2011).

[4] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, INSTITUT INTERRÉGIONAL DE RECHERCHE DES NATIONS UNIES SUR LA CRIMINALITÉ ET LA JUSTICE, OFFICE DES NATIONS UNIES CONTRE LA DROGUE ET LE CRIME, OFFICE EUROPÉEN DE POLICE, ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE, ORGANISATION INTERNATIONALE DE POLICE CRIMINELLE-INTERPOL, ORGANISATION MONDIALE DES DOUANES, Recommandations de sécurité nucléaire sur les matières nucléaires et autres matières radioactives non soumises à un contrôle réglementaire, nº 15 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2011).

[5] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Sécurité des sources radioactives, nº 11 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2012).

[6] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Sécurité du transport des matières radioactives, nº 9 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2012).

[7] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, La sécurité informatique dans les installations nucléaires, nº 17 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2013).

[8] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Sécurité de l'information nucléaire, nº 23-G de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2017).

[9] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Utilisation de la comptabilité et du contrôle des matières nucléaires à des fins de sécurité nucléaire dans les installations, nº 25-G de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2018).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, IAEA Nuclear Security Series No. 4, IAEA, Vienna (2007).

[11] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Culture de sécurité nucléaire, nº 7 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2009).

[12] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Élaboration, utilisation et actualisation de la menace de référence, nº 10 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2012).
[13] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Sécurité des matières nucléaires en cours de transport, nº 26-G de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2019).
[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Establishing a System for Control of Nuclear Material for Nuclear Security Purposes at a Facility during Use, Storage and Movement, IAEA Nuclear Security Series No. 32-T, IAEA, Vienna (2019).
[15] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Protection physique des matières nucléaires et des installations nucléaires (Guide d'application de la publication INFCIRC/225/Révision 5), nº 27-G de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2019).
[16] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Identification des zones vitales des installations nucléaires, nº 16 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2015).
[17] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Autoévaluation de la culture de sécurité nucléaire dans les installations et activités, nº 28-T de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2019).

IAEA
Agence internationale de l'énergie atomique

Nº 26

OÙ COMMANDER ?

Vous pouvez vous procurer les publications de l'AIEA disponibles à la vente chez nos dépositaires ci-dessous ou dans les grandes librairies.

Les publications non destinées à la vente doivent être commandées directement à l'AIEA. Les coordonnées figurent à la fin de la liste ci-dessous.

AMÉRIQUE DU NORD

Bernan / Rowman & Littlefield
15250 NBN Way, Blue Ridge Summit, PA 17214 (États-Unis d'Amérique)
Téléphone : +1 800 462 6420 • Télécopie : +1 800 338 4550
Courriel : orders@rowman.com • Site web : www.rowman.com/bernan

Renouf Publishing Co. Ltd
22-1010 Polytek Street, Ottawa, ON K1J 9J1 (Canada)
Téléphone : +1 613 745 2665 • Télécopie : +1 613 745 7660
Courriel : order@renoufbooks.com • Site web : www.renoufbooks.com

RESTE DU MONDE

Veuillez-vous adresser à votre libraire préféré ou à notre principal distributeur :

Eurospan Group
Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
(Royaume-Uni)

Commandes commerciales et renseignements :
Téléphone : +44 (0) 176 760 4972 • Télécopie : +44 (0) 176 760 1640
Courriel : eurospan@turpin-distribution.com

Commandes individuelles :
www.eurospanbookstore.com/iaea

Pour plus d'informations :
Téléphone : +44 (0) 207 240 0856 • Télécopie : +44 (0) 207 379 0609
Courriel : info@eurospangroup.com • Site web : www.eurospangroup.com

Les commandes de publications destinées ou non à la vente peuvent 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 26007 22529
Courriel : sales.publications@iaea.org • Site web : https://www.iaea.org/fr/publications

La présente publication est une version mise à jour de la publication n° 8 de la collection Sécurité nucléaire de l'AIEA, publiée initialement en 2008. La révision a été entreprise afin de mieux aligner ce guide d'application sur les fondements de la sécurité nucléaire et les recommandations publiés après 2008, de faire référence aux autres guides d'application pertinents publiés depuis 2008, et d'ajouter des informations supplémentaires sur certains sujets sur la base de l'expérience d'utilisation de la publication no 8 de la collection Sécurité nucléaire de l'AIEA par cette dernière et par les États Membres. Cette publication donne des orientations à jour aux États et à leurs autorités compétentes, aux exploitants, aux expéditeurs et aux transporteurs concernant le choix, la mise en place et l'évaluation des mesures de réponse aux menaces internes. Elle concerne les installations nucléaires de tout type, notamment les centrales nucléaires, les réacteurs de recherche et les autres installations du cycle du combustible nucléaire (p. ex. usines d'enrichissement, usines de retraitement, usines de fabrication de combustible et installations d'entreposage), qu'elles soient à l'étape de conception, en construction, en service, en exploitation, à l'arrêt ou en cours de déclassement.

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE