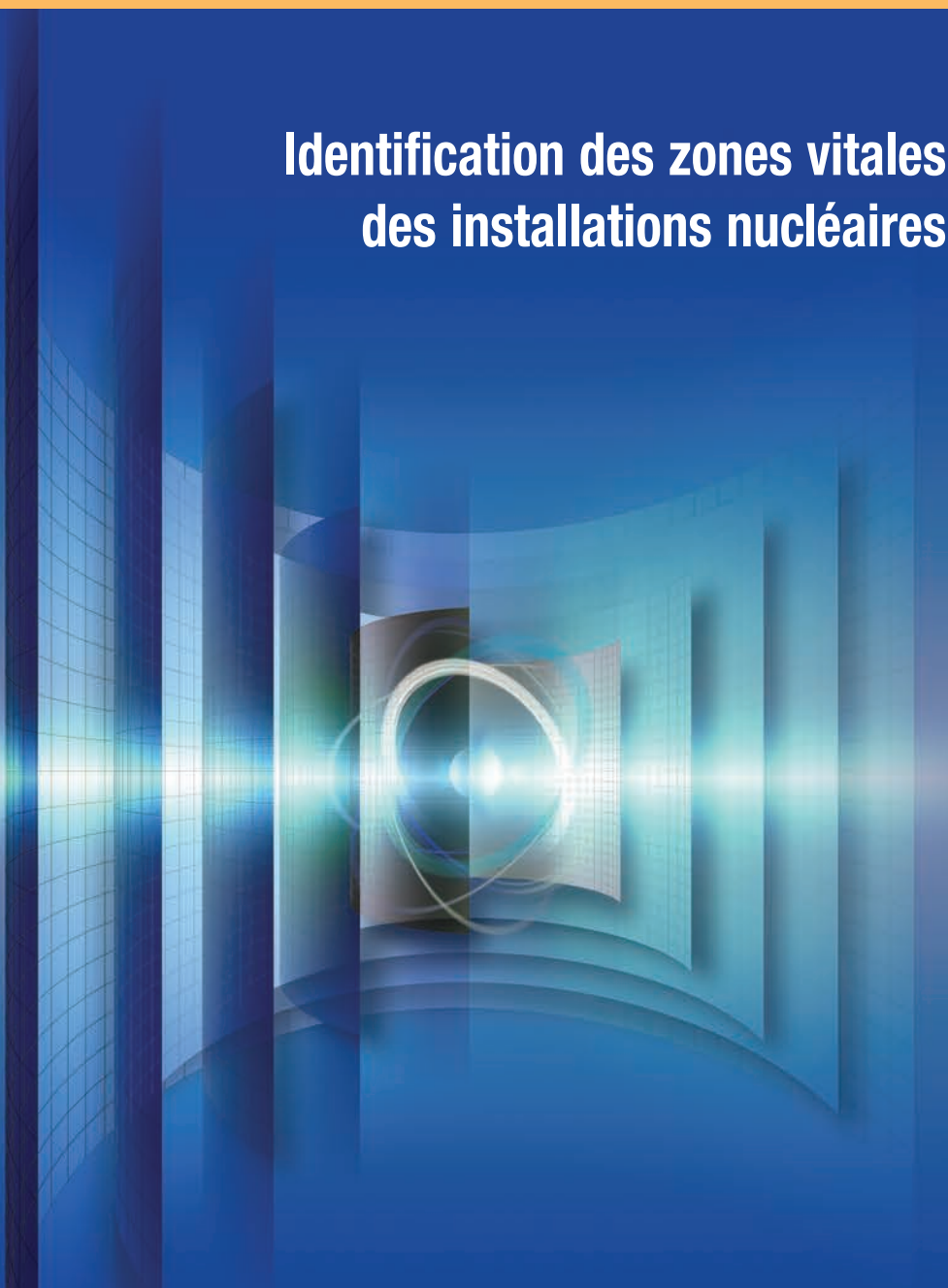
Collection Sécurité nucléaire de l'AIEA – N° 16

Orientations techniques
Manuel de référence

Identification des zones vitales des installations nucléaires



IAEA
Agence internationale de l'énergie atomique

LA COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA

Les publications de la **collection Sécurité nucléaire de l'AIEA** traitent des mesures à prendre en matière de prévention, de détection et d'intervention contre le vol, le sabotage et la cession illégale de matières nucléaires et de sources radioactives et des installations connexes, l'accès non autorisé à ces matières, sources et installations et les autres actes malveillants dont elles peuvent faire l'objet. Ces publications sont conformes aux instruments internationaux relatifs à la sécurité nucléaire, notamment à la Convention sur la protection physique des matières nucléaires telle qu'amendée, au Code de conduite sur la sûreté et la sécurité des sources radioactives, aux résolutions 1373 et 1540 du Conseil de sécurité des Nations Unies et à la Convention internationale pour la répression des actes de terrorisme nucléaire, et elles les complètent.

CATÉGORIES DANS LA COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA

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

- Les **Fondements de la sécurité nucléaire**, qui énoncent les objectifs, les concepts et les principes de la sécurité nucléaire et servent de base pour l'élaboration de recommandions en matière de sécurité.
- Les **Recommandations**, qui présentent les pratiques exemplaires que les États Membres devraient adopter pour la mise en œuvre des Fondements de la sécurité nucléaire.
- Les **Guides d'application**, qui complètent les Recommandations dans certains grands domaines et proposent des mesures pour en assurer la mise en œuvre.
- Les **Orientations techniques**, comprenant les **Manuels de référence**, qui présentent des mesures détaillées et/ou donnent des conseils pour la mise en œuvre des Guides d'application dans des domaines ou des activités spécifiques, les **Guides de formation**, qui présentent les programmes et/ou les manuels des cours de formation de l'AIEA dans le domaine de la sécurité nucléaire, et les **Guides des services**, qui donnent des indications concernant la conduite et la portée des missions consultatives de l'AIEA sur la sécurité nucléaire.

RÉDACTION ET EXAMEN

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

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

Le processus d'élaboration et d'examen des publications de la collection Sécurité nucléaire de l'AIEA tient compte des considérations de confidentialité et du fait que la sécurité nucléaire est indissociable des problèmes généraux et spécifiques concernant la sécurité nationale. La prise en compte, dans le contenu technique des publications, des normes de sûreté et des activités de garanties de l'AIEA se rapportant à la sécurité constitue une préoccupation sous-jacente.

IDENTIFICATION DES ZONES VITALES DES INSTALLATIONS NUCLÉAIRES

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

AFGHANISTAN
AFRIQUE DU SUD
ALBANIE
ALGÉRIE
ALLEMAGNE
ANGOLA
ANTIGUA-ET-BARBUDA
ARABIE SAOUDITE
ARGENTINE
ARMÉNIE
AUSTRALIE
AUTRICHE
AZERBAÏDJAN
BAHAMAS
BAHREÏN
BANGLADESH
BARBADE
BÉLARUS
BELGIQUE
BELIZE
BÉNIN
BOLIVIE, ÉTAT PLURINATIONAL DE
BOSNIE-HERZÉGOVINE
BOTSWANA
BRÉSIL
BRUNÉI DARUSSALAM
BULGARIE
BURKINA FASO
BURUNDI
CAMBODGE
CAMEROUN
CANADA
CHILI
CHINE
CHYPRE
COLOMBIE
CONGO
CORÉE, RÉPUBLIQUE DE
COSTA RICA
CÔTE D'IVOIRE
CROATIE
CUBA
DANEMARK
DJIBOUTI
DOMINIQUE
ÉGYPTE
EL SALVADOR
ÉMIRATS ARABES UNIS
ÉQUATEUR
ÉRYTHRÉE
ESPAGNE
ESTONIE
ÉTATS-UNIS D'AMÉRIQUE
ÉTHIOPIE
FÉDÉRATION DE RUSSIE
FIDJI
FINLANDE
FRANCE
GABON
GÉORGIE
GHANA
GRÈCE
GUATEMALA
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
L'EX-RÉPUBLIQUE YOUGOSLAVE DE MACÉDOINE
LIBAN
LIBÉRIA
LIBYE
LIECHTENSTEIN
LITUANIE
LUXEMBOURG
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
SAINT-MARIN
SAINT-SIÈGE
SÉNÉGAL
SERBIE
SEYCHELLES
SIERRA LEONE
SINGAPOUR
SLOVAQUIE
SLOVÉNIE
SOUDAN
SRI LANKA
SUÈDE
SUISSE
SWAZILAND
TADJIKISTAN
TCHAD
THAÏLANDE
TOGO
TRINITÉ-ET-TOBAGO
TUNISIE
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 16

IDENTIFICATION DES ZONES VITALES DES INSTALLATIONS NUCLÉAIRES

ORIENTATIONS TECHNIQUES

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE, 2015

DROITS D'AUTEUR

Toutes les publications scientifiques et techniques de l'AIEA sont protégées par les dispositions de la Convention universelle sur le droit d'auteur adoptée en 1952 (Berne) et révisée en 1972 (Paris). Depuis, le droit d'auteur a été élargi par l'Organisation mondiale de la propriété intellectuelle (Genève) à la propriété intellectuelle sous forme électronique. La reproduction totale ou partielle des textes contenus dans les publications de l'AIEA sous forme imprimée ou électronique est soumise à autorisation préalable et habituellement au versement de redevances. Les propositions de reproduction et de traduction à des fins non commerciales sont les bienvenues et examinées au cas par cas. Les demandes doivent être adressées à la Section d'édition de l'AIEA :

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

© AIEA, 2015

Imprimé par l'AIEA en Autriche
Décembre 2015
STI/PUB/1505

IDENTIFICATION DES ZONES
VITALES DES INSTALLATIONS
NUCLÉAIRES
AIEA, VIENNE, 2015
STI/PUB/1505
ISBN 978–92–0–210915–5
ISSN 1816–9317

AVANT-PROPOS

Dans la situation mondiale actuelle, on ne peut exclure que des matières nucléaires ou autres matières radioactives puissent être utilisées à des fins malveillantes. Les États ont réagi face à ce risque en s'engageant collectivement à renforcer la protection et le contrôle de ces matières et à intervenir efficacement en cas d'événement de sécurité nucléaire. Ils sont convenus de renforcer les instruments juridiques internationaux existants et en ont établi de nouveaux pour améliorer la sécurité nucléaire dans le monde. La sécurité nucléaire est absolument nécessaire pour la gestion des technologies nucléaires et pour les applications ou les matières nucléaires ou autres matières radioactives qui sont utilisées ou transportées.

Dans le cadre de son programme de sécurité nucléaire, l'AIEA aide les États à établir et à maintenir durablement un régime de sécurité nucléaire efficace. L'AIEA a adopté une approche globale de la sécurité nucléaire reconnaissant qu'un régime national de sécurité nucléaire efficace prend appui sur : l'application des instruments juridiques internationaux pertinents ; la protection de l'information ; la protection physique ; la comptabilité et le contrôle des matières ; la détection du trafic de ces matières et l'intervention en cas de trafic ; les plans nationaux d'intervention et les mesures d'urgence. Avec sa collection Sécurité nucléaire, l'AIEA s'emploie à aider les États à mettre en œuvre et à maintenir durablement un tel régime d'une manière cohérente et intégrée.

La collection Sécurité nucléaire de l'AIEA regroupe les publications suivantes : Fondements de la sécurité nucléaire, comprenant notamment les objectifs et les éléments essentiels du régime de sécurité nucléaire d'un État ; Recommandations ; Guides d'application et Orientations techniques.

Chaque État est pleinement responsable de la sécurité nucléaire et doit, en particulier, assurer la sécurité des matières nucléaires et autres matières radioactives, et des installations et des activités connexes, veiller à la sécurité de ces matières en cours d'utilisation, d'entreposage et de transport, et lutter contre le trafic illicite et les mouvements fortuits de ces matières. Il devrait aussi être prêt à intervenir en cas d'événement de sécurité nucléaire.

Les recommandations de l'AIEA pour la protection des installations nucléaires contre le sabotage sont contenues dans les Recommandations de sécurité nucléaire sur la protection physique des matières nucléaires et des installations nucléaires (INFCIRC/225/Rev.5), n° 13 de la collection Sécurité nucléaire de l'AIEA. Après les attentats du 11 septembre 2001, on a assisté à une nouvelle prise de conscience de la menace terroriste potentielle contre des installations nucléaires, et l'AIEA a entrepris d'élaborer une collection de publications d'orientations sur la sécurité des matières nucléaires et radioactives et des installations.

Cette publication présente une approche structurée visant à identifier les zones où se trouvent les équipements, systèmes et composants qui doivent être protégés contre le sabotage. Elle contient tout particulièrement des informations détaillées sur l'identification des zones vitales, c'est-à-dire les zones qui doivent être protégées dans les installations à haut risque. Cependant, le processus décrit est applicable à l'identification des zones qui devraient être protégées, quelle que soit l'installation nucléaire. La méthode s'appuie sur les analyses de la sûreté pour élaborer des modèles logiques de sabotage pour les scénarios de sabotage qui pourraient avoir des conséquences radiologiques inacceptables. Les actes de sabotage représentés dans les modèles logiques sont liés aux zones depuis lesquelles ils peuvent être commis. Ces modèles sont ensuite analysés afin de déterminer les zones qui devraient être protégées pour prévenir ces conséquences radiologiques inacceptables.

Les fonctionnaires de l'AIEA responsables de cette publication sont A. Stadalnikas et D. Ek du Bureau pour la sécurité nucléaire et A. Guerpinar et S.C. Kim de la Division de la sûreté des installations nucléaires.

NOTE DE L'ÉDITEUR

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

1.1. GÉNÉRALITÉS

L'AIEA prépare actuellement un ensemble de publications d'orientations qui paraîtra dans la collection Sécurité nucléaire de l'AIEA en vue d'assister les États Membres dans la conception, la mise en œuvre et l'évaluation de leurs systèmes de protection physique des matières nucléaires et des installations nucléaires. La présente publication décrit un processus systématique visant à identifier les *zones vitales* d'une installation nucléaire.

L'identification des zones vitales est une étape importante du processus de protection contre le sabotage. L'*identification des zones vitales* (IZV) est le processus d'identification des zones d'une installation nucléaire autour desquelles une protection sera assurée afin de prévenir un acte de sabotage ou d'en réduire la probabilité. Le document INFCIRC/225/Rev.5 (n° 13 de la collection Sécurité nucléaire de l'AIEA) [1] – ci-après désigné INFCIRC/225 – souligne que les matières nucléaires en quantité suffisante pour que leur dispersion risque d'entraîner des conséquences radiologiques graves (CRG), ainsi qu'un ensemble minimal d'équipements, systèmes ou dispositifs nécessaires pour éviter de telles conséquences, devraient se trouver dans une ou plusieurs zones vitales, elles-mêmes situées à l'intérieur d'une zone protégée[1]. Toutes les mesures qui ont été conçues dans l'installation à des fins de sûreté devraient être prises en considération lors de l'identification des zones vitales.

1.2. OBJECTIF

La présente publication a pour objectif de décrire un processus qui peut être utilisé pour : i) identifier tous les ensembles candidats de zones vitales au sein d'une installation nucléaire ; et ii) sélectionner un ensemble spécifique de zones

[1] On entend par « conséquences radiologiques graves », voir la réf. [1], des conséquences radiologiques relativement lourdes engendrées par des grandes installations nucléaires comme les centrales nucléaires. Le niveau de protection des zones vitales spécifiées à la réf. [1] est équivalent au niveau requis pour prévenir le vol de matières nucléaires de catégorie 1. Dans l'optique d'une approche graduée, les zones, où les stocks classés dans des catégories de conséquences moindres (supérieures aux conséquences radiologiques inacceptables mais inférieures aux conséquences radiologiques graves) doivent être protégés, peuvent être identifiées à l'aide du processus décrit dans la présente publication, bien que ces zones puissent nécessiter des niveaux de protection plus faibles que ceux qui sont exigés pour les zones vitales.

vitales qui seront protégées. Le processus de sélection d'un ensemble spécifique de zones vitales qui doivent être protégées se fonde sur l'examen des conséquences radiologiques potentielles d'un acte de sabotage et tient compte des caractéristiques d'exploitation, de sûreté et de protection physique d'une installation nucléaire.

1.3. PORTÉE

La présente publication s'intéresse uniquement au processus d'IZV des installations nucléaires. Ce processus peut être utilisé pour les installations existantes afin d'identifier les zones vitales et d'évaluer l'effet des modifications de conception sur la sélection des zones vitales. Il peut également être appliqué aux nouvelles installations au stade de la conception afin d'analyser comment optimiser les caractéristiques de conception et d'implantation pour la sélection des zones vitales. En outre, les concepts et principes (c'est-à-dire l'identification des équipements ou composants qui doivent être protégés dans une zone vitale sur la base des seuils de conséquences radiologiques inacceptables) énoncés dans la présente publication peuvent être appliqués à des installations autres que les installations nucléaires.

1.4. STRUCTURE

La section 1 présente le contexte, les objectifs et la portée de cette publication. La section 2 analyse le processus utilisé pour identifier les zones vitales et les résultats attendus de ce processus. Elle énonce en outre des considérations de politique générale dont les autorités compétentes (organisme de réglementation de l'État) devraient tenir compte et les mesures que doit prendre l'exploitant avant le début de l'IZV, et décrit le processus par étapes permettant de sélectionner un ensemble minimum de zones dans une installation nucléaire qui devraient être protégées en tant que zones vitales. La section 3 donne des orientations pour consigner par écrit les résultats des IZV et on trouvera dans l'annexe un exemple de la manière dont les modèles logiques peuvent être résolus pour identifier des ensembles candidats de zones vitales.

2. PROCESSUS D'IDENTIFICATION DES ZONES VITALES

La présente section décrit le processus utilisé pour identifier les zones vitales dans une installation nucléaire. Le concept de zone vitale sert à définir un périmètre autour des équipements, systèmes ou dispositifs vitaux ou des matières nucléaires qui peuvent être physiquement protégés. Le processus d'IZV a pour objectif d'identifier un ensemble de zones d'une installation où se trouvent les équipements, systèmes, structures, composants, dispositifs, ou les mesures prises par l'exploitant qui, avec une protection adéquate, éviteront des CRG.

Le processus d'IZV devrait être répété lorsqu'il est envisagé de modifier la conception, ou avant la modification, et lorsque la menace a changé. La phase de conception d'une installation est le meilleur moment pour appliquer ce processus car il est possible d'optimiser la protection physique et d'éviter ainsi une mise en conformité.

En règle générale, l'exploitant est responsable de l'identification des zones vitales et l'organisme de réglementation de l'État est responsable de la validation du processus d'IZV.

2.1. VUE D'ENSEMBLE DU PROCESSUS

Le processus d'IZV est décrit à la figure 1. Les étapes de ce processus sont les suivantes :

— Rassembler des informations pouvant contribuer au processus d'IZV.
  - Identifier l'équipe du processus d'IZV.
  - Considérations de politique générale. Identifier les considérations fondamentales qui sont essentielles pour le processus d'IZV.
  - Caractéristiques du site et de l'installation. Répertorier les stocks des matières nucléaires et autres matières radioactives. Évaluer les caractéristiques du site et de l'installation nécessaires pour déterminer si un sabotage pourrait avoir des CRG.
  - Analyse prudente de chaque stock de matières nucléaires et autres matières radioactives. Déterminer si le rejet total de l'un des stocks pourrait dépasser les critères de CRG. Inclure dans le modèle logique de sabotage la dispersion directe de l'un de ces stocks et poursuivre le processus décrit ci-dessous.

— Identifier tout événement initiateur [2] d'origine malveillante (EIOM) pouvant avoir indirectement des CRG.

— Identifier tout EIOM qui dépasse la capacité des systèmes d'atténuation. Inclure chacun des EIOM dans le modèle logique de sabotage comme un événement entraînant des CRG.

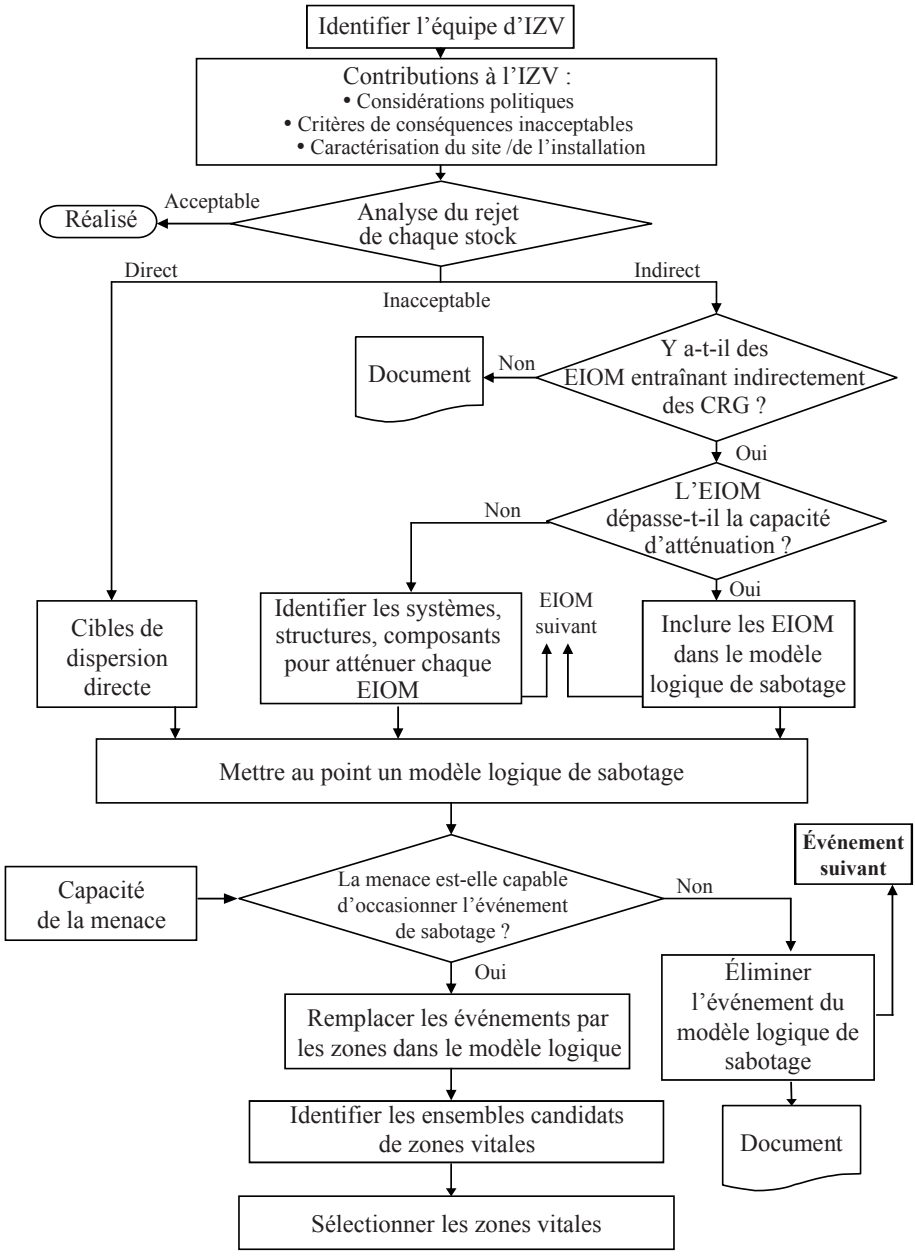


FIG. 1. Processus d'identification des zones vitales

— Identifier les systèmes, structures et composants permettant l'atténuation de chaque EIOM. Pour chaque EIOM qui ne dépasse pas la capacité des systèmes d'atténuation, identifier les fonctions de sûreté nécessaires à l'atténuation de l'EIOM, les systèmes, structures et composants qui assurent les fonctions de sûreté, et les critères de succès de ces systèmes.
— Mettre au point un modèle logique de sabotage qui identifie les combinaisons d'événements (dispersion directe, EIOM excédant la capacité des systèmes d'atténuation, EIOM dont les effets se conjuguent avec ceux d'une neutralisation des systèmes d'atténuation) qui entraîneraient des CRG.
— Éliminer du modèle logique de sabotage tout événement sur lequel la menace supposée ne pourrait pas déboucher.
— Identifier les lieux (zones) où il peut y avoir une dispersion directe, des EIOM ou tout autre événement dans le modèle logique de sabotage. Remplacer les événements dans le modèle de logique de sabotage par les lieux correspondants.
— Résoudre le modèle logique de zones de sabotage pour identifier les combinaisons d'emplacements qui devraient être protégés.
— Sélectionner l'ensemble de zones vitales qui seront protégées pour empêcher qu'un acte de sabotage n'entraîne des CRG.

Les analyses de sûreté de l'installation peuvent fournir des informations et des modèles utiles à l'appui de l'IZV. Si une étude déterministe de sûreté (EDS) ou une étude probabiliste de sûreté (EPS) a été réalisée pour l'installation, elle permettra d'analyser la réponse de l'installation face à différents événements initiateurs (EI) comme ceux qui sont provoqués par une défaillance fortuite, une erreur humaine, etc. Ces événements pourraient également résulter d'actes malveillants. Les EDS et EPS [3, 4] fournissent des informations détaillées sur la caractérisation du site et de l'installation qui seront utiles à l'équipe d'IZV. Chaque type d'analyse comportera des informations utilisables pour la mise au point des modèles logiques nécessaires à l'IZV [5–7].

2.2. CONTRIBUTIONS AU PROCESSUS D'IZV

2.2.1. Considérations de politique générale

Les considérations de politique générale dont il faut tenir compte avant d'entamer le processus d'IZV sont :

— la définition explicite des conséquences radiologiques inacceptables (CRI) qui nécessiteront une protection contre le sabotage ;

— la définition explicite des CRG qui nécessiteront la désignation et la protection des zones vitales ;
— les conditions de fonctionnement pour lesquelles les zones vitales devraient être identifiées et protégées ;
— l'état sûr auquel l'installation devrait être mise après un acte de sabotage, pour chaque condition de fonctionnement ;
— si des événements dus à la non-disponibilité des équipements autres que des actes d'origine malveillante visant à neutraliser l'installation devraient être considérés comme se produisant en même temps qu'un acte de sabotage ;
— si l'analyse peut prendre en considération les mesures de rétablissement et de gestion des accidents à la suite d'un acte de sabotage ;
— la menace contre laquelle l'installation devrait être protégée.

Ces questions seront examinées plus en détail dans les sections suivantes.

2.2.1.1. Conséquences radiologiques inacceptables

La première considération de politique générale importante est la décision explicite relative aux *conséquences radiologiques inacceptables* et aux conséquences radiologiques graves. En règle générale, ces niveaux de conséquences sont définis par rapport à un niveau inacceptable de dose, un niveau inacceptable de rejet de matières radioactives ou un état inacceptable de l'installation, par exemple l'endommagement du cœur d'une centrale nucléaire. Il convient de noter que si les CRG sont identiques à celles que l'État a définies pour la sûreté nucléaire, les analyses de la sûreté effectuées pour l'installation peuvent être utilisées pour l'IZV sans modification majeure. La question des conséquences radiologiques inacceptables est examinée plus à fond dans la réf. [8] qui contient en outre un exemple de tableau de catégorisation des conséquences d'un sabotage.

2.2.1.2. Détermination des états de fonctionnement devant être évalués

Certaines installations peuvent avoir plusieurs états de fonctionnement (exploitation normale, arrêt de la centrale, rechargement du combustible des réacteurs de puissance, etc.). Ces différents états de fonctionnement peuvent s'appuyer sur des équipements différents pour remplir les fonctions de sûreté nécessaires et peuvent nécessiter des mesures de protection physique différentes pour protéger les équipements et les matières. L'autorité compétente devrait identifier ou approuver les états de fonctionnement dont il faudra tenir compte dans le processus d'IZV. L'identification des zones vitales pour tous les états de fonctionnement peut se faire en analysant chaque état de fonctionnement

ou en identifiant un état de fonctionnement enveloppe qui garantira la protection pendant tous les états. Les états de fonctionnement qui doivent être évalués devraient être déterminés en tenant compte du fait qu'il peut y avoir des CRG pendant chaque état de fonctionnement.

2.2.1.3. État sûr de l'installation

Dans une installation, il y a un certain nombre d'états qui, après un accident ou un transitoire, peuvent être conçus pour maintenir l'installation dans un état sûr. En principe, toutes les installations nucléaires devraient maintenir les fonctions fondamentales de sûreté [9] suivantes :

— Contrôle de la réactivité ;
— Refroidissement des matières radioactives ;
— Confinement des matières radioactives ;

La fonction de sûreté pour le refroidissement des matières radioactives des réacteurs de puissance est souvent davantage détaillée (contrôle de la pression du fluide caloporteur du réacteur, contrôle de l'inventaire du fluide caloporteur du réacteur, évacuation de la puissance résiduelle).

Tous les états de l'installation acceptés à cette fin devraient permettre de remplir les fonctions de sûreté nécessaires pendant une durée raisonnable, soit grâce aux équipements de sûreté conçus pour remplir ces fonctions, soit par d'autres moyens, comme la gestion des accidents ou la préparation et la conduite des interventions sur le site en cas d'urgence[2]. L'(les) état(s) sûr(s) défini(s) pour l'installation peut (peuvent) varier lors de l'analyse des différents états de fonctionnement de l'installation. L'autorité compétente devrait identifier ou approuver l'état sûr de l'installation pour chaque état de fonctionnement de l'installation.

2.2.1.4. Indisponibilité du matériel

Bien que l'IZV soit axée sur les conséquences des actes malveillants, il n'est pas exclu que le matériel puisse être indisponible par hasard ou faute d'entretien, et être dû en même temps à un acte malveillant. Les résultats de l'IZV doivent être déterministes ; c'est-à-dire une zone est vitale ou non vitale. Par conséquent,

[2] Si on doit recourir à d'autres moyens comme la préparation et la conduite des interventions d'urgence, il faudra tenir compte du temps nécessaire et de la situation nécessitant de telles actions. Dans certains cas, en fonction du temps disponible, le déploiement et la disponibilité de ces mesures peuvent les rendre inapplicables pour empêcher des CRG.

les hypothèses sur lesquelles se fondent les règles applicables à l'IZV devraient spécifier si l'analyse doit aussi porter sur l'indisponibilité du matériel simultanée due à une défaillance aléatoire ou à une opération de maintenance[3].

2.2.1.5. Prise en considération des mesures de rétablissement

Les analyses de la sûreté ou autres analyses utilisées pour l'IZV contiennent souvent des hypothèses explicites ou implicites concernant les mesures que doit prendre le personnel. Il peut s'agir notamment des procédures d'urgence ou de routine appliquées par l'exploitant pour maintenir l'installation dans un état sûr. Il peut aussi s'agir d'hypothèses implicites dans la façon dont la réponse de l'installation aux événements est modélisée. L'équipe d'IZV devrait identifier avec soin toutes les hypothèses explicites et implicites concernant les mesures que doit prendre le personnel figurant dans les analyses de la sûreté ou autres utilisées pour l'IZV. Une fois ces mesures identifiées, l'équipe devrait déterminer si elles peuvent être prises en considération dans le cadre de la réponse de l'installation en cas de sabotage. Au cours de l'IZV, l'équipe peut également identifier les mesures de rétablissement qui permettraient de compenser la neutralisation des équipements. Dans ce cas aussi, l'équipe d'IZV devrait déterminer si ces mesures de rétablissement peuvent être prises en considération dans le cadre de la réponse de l'installation en cas de sabotage. Elle devrait justifier les raisons pour lesquelles il faut tenir compte des mesures prises par le personnel, y compris les mesures de rétablissement.

2.2.1.6. Caractéristiques de la menace

La protection physique des installations nucléaires devrait être basée sur l'évaluation actuelle par l'État de la menace [10]. L'autorité compétente devrait spécifier – dans un document sur les menaces de référence ou dans un autre énoncé de la menace – les caractéristiques de la menace face à laquelle l'exploitant devrait assurer une protection. Les caractéristiques de la menace sont utilisées lors du processus d'IZV pour déterminer les actes malveillants qui peuvent être dus à la menace. La réf. [11] donne des orientations pour l'élaboration, la mise en œuvre et le maintien d'une menace de référence.

[3] Pour s'assurer qu'une installation soit protégée de façon adéquate lors d'opérations de maintenance dans une zone vitale, l'autorité compétente peut exiger que l'exploitant désigne et protège des zones vitales temporaires ou prenne d'autres mesures compensatoires.

2.2.2. Caractéristiques du site et de l'installation

La première étape d'une IZV consiste à identifier les stocks de matières nucléaires ou radioactives présentes ainsi que les caractéristiques de l'installation et du site qu'il faudra connaître pour déterminer si un acte de sabotage peut entraîner des CRG. Pour cela, il faut avoir des informations sur :

— le site (zone où est située l'installation), notamment :
  - la densité de population aux environs de l'installation et d'autres caractéristiques du site afin de déterminer les conséquences d'un rejet radiologique potentiel lorsque les critères de CRG impliquent une exposition hors du site et non un substitut, par exemple un endommagement du cœur ou une défaillance de confinement.

— l'installation, notamment :
  - les emplacements, les fiches de stocks, les caractéristiques, et les quantités de matières nucléaires ou d'autres matières radioactives ;
  - Les fonctions critiques de sûreté de l'installation nucléaire (par exemple protection contre les rayonnements, prévention de la criticité, refroidissement, confinement, prévention des incendies, intégrité structurelle) ; les renseignements descriptifs détaillés sur le procédé et les systèmes de sûreté dont on a besoin pour déterminer quels équipements, systèmes, structures, composants, dispositifs et mesures prises par les exploitants devraient être protégés pour prévenir des CRG.

Il devrait être possible d'obtenir les informations nécessaires à la caractérisation du site et de l'installation en se référant à l'argumentaire de sûreté de l'installation ou à d'autres documents d'analyse de la sûreté.

2.2.3. Analyse des conséquences radiologiques

Une analyse prudente devrait être effectuée pour déterminer les conséquences radiologiques potentielles du rejet total de chaque stock de matières nucléaires ou d'autres matières radioactives se trouvant dans l'installation. Elle ne devrait pas tenir compte de la protection physique ni des mesures d'atténuation mises en place dans l'installation.

Si, dans le cadre de cette analyse prudente, les conséquences radiologiques potentielles pour un stock sont, selon les estimations, inférieures aux CRI,

un sabotage ne peut pas entraîner des CRI pour ce stock[4]. Par conséquent, il n'est pas nécessaire de désigner des zones qui doivent être protégées contre le sabotage pour ce stock. Pour ces stocks, l'exploitant devrait protéger les équipements et dispositifs de sûreté en contrôlant leur accès et en les sécurisant. Si les conséquences potentielles sont comprises entre les niveaux CRI et CRG fixés par l'État, l'exploitant devrait identifier les zones devant être protégées contre le sabotage et les protéger conformément à la réglementation de l'État. Si les conséquences potentielles sont supérieures au niveau CRG, l'exploitant devrait identifier les zones vitales de la manière décrite dans les sections suivantes et protéger ces zones conformément aux recommandations énoncées dans la réf. [1].

Si l'analyse prudente indique qu'il existe des CRI, il peut être judicieux d'effectuer une analyse plus sophistiquée et exigeant des ressources plus importantes pour pouvoir estimer de façon plus réaliste les conséquences potentielles résultant de la même quantité déterminée de matières radioactives. Le calcul des conséquences radiologiques devrait se fonder sur des données et hypothèses prudentes mais réalistes, en tenant compte de données comme les fractions de rejet ou le placage. Les paramètres de l'analyse devraient être définis ou approuvés par l'autorité compétente.

2.3. SABOTAGE DIRECT DE STOCKS DE MATIÈRES NUCLÉAIRES OU D'AUTRES MATIÈRES RADIOACTIVES

Les actes pouvant provoquer directement le rejet de matières radioactives sont ceux qui utilisent une énergie provenant d'une source externe (par exemple un dispositif explosif ou incendiaire) pour disperser les matières. Si les conséquences radiologiques potentielles du rejet de la totalité d'un stock sont égales ou supérieures au niveau CRG, il conviendrait d'inclure la dispersion directe du stock dans le modèle logique de sabotage comme acte malveillant potentiel entraînant directement des CRG, et les étapes restantes du processus d'identification des zones vitales devraient porter sur le stock. La possibilité que la menace cause une dispersion directe du stock est examinée au moment où les caractéristiques de la menace sont prises en considération à une étape ultérieure du processus.

[4] Dans certaines circonstances, un agresseur pourrait augmenter le stock de radionucléides grâce à la criticité. Par conséquent, un stock pour lequel les conséquences potentielles étaient initialement inférieures au niveau CRG pourrait, en cas d'acte malveillant, avoir des conséquences potentielles supérieures à ce niveau.

2.4. SABOTAGE INDIRECT DE STOCKS DE MATIÈRES NUCLÉAIRES OU D'AUTRES MATIÈRES RADIOACTIVES

Les actes malveillants pouvant provoquer indirectement le rejet de matières nucléaires ou d'autres matières radioactives sont les actes qui utilisent l'énergie potentielle (c'est-à-dire la chaleur ou la pression) contenue dans les matières nucléaires ou radioactives ou dans un procédé pour disperser les matières. Il n'est pas nécessaire qu'un agresseur ait accès à la zone où se trouvent les matières pour commettre un acte de sabotage indirect. Le sabotage vise en fait les équipements, les systèmes, les structures, les composants, les dispositifs ou les mesures prises par l'exploitant pour maintenir en règle générale l'installation à l'état sûr. Si les conséquences radiologiques potentielles du rejet de la totalité d'un stock sont égales ou supérieures à une limite CRG, il faut envisager la possibilité d'un sabotage qui pourrait indirectement provoquer des CRG. Afin de déterminer les zones devant être protégées pour empêcher des actes qui entraînent indirectement des CRG, il faudrait considérer deux types de sabotage, à savoir ceux qui :

— provoquent un EI [2] et une situation plus grave que celle à laquelle les systèmes d'atténuation de l'installation peuvent faire face (c'est-à-dire les événements hors dimensionnement) ;
— provoquent un EI et neutralisent les systèmes nécessaires à l'atténuation des effets de l'EI.

Un EI délibérément provoqué par un agresseur pour tenter de provoquer un rejet de matières d'une installation est appelé un EIOM.

2.4.1. Événements initiateurs d'origine malveillante

Cette étape du processus d'IZV a pour objectif principal d'établir une liste des actes malveillants que l'agresseur potentiel pourrait commettre pour déclencher une chaîne d'événements ayant des CRG. Nombre d'EI auront déjà été identifiés et analysés dans les documents relatifs à la sûreté de l'installation, par exemple dans les rapports EDS ou EPS [3, 4], et ces EI devraient être considérés comme des EIOM potentiels. Lors de l'identification des EIOM, l'équipe d'IZV devrait tenir compte de trois catégories d'événements susceptibles de ne pas figurer dans l'argumentaire de sûreté mais qui devraient faire partie du processus d'IZV :

1) La première catégorie d'EIOM ne figurant pas dans les évaluations de la sûreté concerne des situations dans lesquelles il n'y a pas de dispositif d'application

d'énergie ou d'autres sources d'énergie susceptibles de disperser des matières radioactives. Par exemple, les actes malveillants mettant en jeu des explosifs ou d'autres sources d'énergie en vue de créer une brèche ou de provoquer une dispersion pourraient entraîner une défaillance des barrières ou une dispersion des matières radioactives, chose impossible sans un acte malveillant. Étant donné que ces EI ne peuvent se produire en l'absence d'acte malveillant, ils ne sont généralement pas pris en considération dans l'analyse de la sûreté.

2) La deuxième catégorie d'EIOM qui va de pair avec la première et qui n'a peut-être pas été prise en considération dans l'analyse de la sûreté inclut les EI dont on ne tient pas compte vu leur faible probabilité de se produire de façon aléatoire. Par exemple, de nombreux EIOM indépendants, des brèches à grande échelle ou des défaillances de composants passifs, qui sont hautement improbables, peuvent être provoqués par un agresseur en possession d'explosifs ou d'autres ressources, y compris des ressources sur le site,

3) La troisième catégorie d'EIOM concerne des sources de rejet de matières radioactives qui pourraient ne pas avoir été prises en considération dans les documents relatifs à la sûreté. Les EPS de niveau 1 des réacteurs nucléaires de puissance ne s'intéressent qu'aux événements pouvant provoquer un endommagement du cœur et, partant, provoquer un rejet de matières radioactives à partir du cœur du réacteur. Il faut également tenir compte lors du processus d'IZV d'autres stocks de matières radioactives qui pourraient être à l'origine d'un rejet entraînant des CRG (par exemple du combustible irradié ou des déchets radioactifs).

Quatre approches peuvent être utilisées pour identifier les EIOM dont il faudra tenir compte lors du processus d'IZV. L'objectif étant d'établir une liste des EIOM la plus exhaustive possible, l'équipe d'IZV devrait envisager de les utiliser toutes les quatre :

1) *Examen des documents relatifs à la sûreté.* Cela devrait être le point de départ de cette partie du processus d'IZV. Il faudrait passer en revue les listes d'EI dans les EDS et EPS, dans les études incendie, les études sismiques et autres évaluations de sûreté de l'installation analysée et d'installations similaires. Puisque tout EI susceptible de se produire de façon aléatoire peut également être causé par des actes malveillants, cet ensemble d'EI devrait être inclus dans la liste des EIOM. Il est à noter que les hypothèses formulées dans les analyses de la sûreté en ce qui concerne la nature de ces EI et la manière dont l'installation y répond devraient être réexaminées dans le contexte d'actes malveillants et révisées si nécessaire.

2) *Référence à d'autres analyses de l'IZV.* Lorsque d'autres IZV ont été effectuées pour des installations similaires, les listes d'EIOM utilisées devraient être réexaminées. Il importe tout particulièrement d'identifier les EIOM qui ne correspondent pas à des EI dans les documents relatifs à la sûreté de l'installation.
3) *Évaluation de l'ingénierie.* Les systèmes de l'installation (exploitation et sûreté) et les composants majeurs devraient être systématiquement passés en revue afin d'identifier tout EIOM supplémentaire, par exemple lorsqu'une conséquence quelconque d'un acte malveillant, dont l'agresseur est jugé capable (par exemple neutralisation, fonctionnement simulé, effraction, brèche, effondrement, incendie), pourrait entraîner directement, ou en combinaison avec d'autres actes malveillants, des CRG. Des orientations relatives à ces analyses figurent dans la réf. [12].
4) *Analyse déductive.* Dans cette approche, les « conséquences radiologiques inacceptables » sont réparties systématiquement en fonction de tous les événements pouvant entraîner de telles conséquences. Le bon fonctionnement des systèmes et les autres mesures de prévention ne sont pas inclus. Les événements au niveau le plus fondamental sont ensuite susceptibles de figurer dans la liste des EIOM pour l'installation.

Chaque EIOM devrait être évalué afin de déterminer s'il existe des systèmes qui puissent l'atténuer. Les EIOM, seuls ou conjugués à la défaillance des systèmes d'atténuation, sont inclus dans le modèle logique de sabotage tel qu'indiqué ci-dessous.

2.4.2. EIOM dépassant la capacité des systèmes d'atténuation

Chaque EIOM qui dépasse la capacité des systèmes d'atténuation devrait être inclus dans le modèle logique de sabotage en tant qu'acte malveillant pouvant entraîner des CRG. La possibilité qu'une menace provoque un EIOM dépassant la capacité des systèmes d'atténuation est étudiée lorsque les caractéristiques de la menace sont examinées à une étape ultérieure du processus.

2.4.3. EIOM ne dépassant pas la capacité des systèmes d'atténuation

Afin de pouvoir examiner les EIOM qui ne dépassent pas la capacité des systèmes d'atténuation, il faudrait déterminer les EIOM qui, combinés à une neutralisation des systèmes d'atténuation, pourraient entraîner des CRG. Le système d'atténuation englobe les mesures prises par l'exploitant. Ces combinaisons d'événements qui peuvent avoir indirectement des CRG sont présentées en détail dans le modèle logique de sabotage. La possibilité

qu'une menace provoque un EIOM ou une neutralisation est examinée lorsque les caractéristiques de la menace sont examinées à une étape ultérieure du processus.

Les systèmes spécifiques utilisés pour atténuer les EI dépendent de l'installation et de la quantité ou de la nature des matières radioactives qui se trouvent dans l'installation ; ces systèmes peuvent être différents en fonction de l'état de fonctionnement de l'installation. Les systèmes qui sont utilisés pour atténuer les EI sont ceux qui remplissent des fonctions de sûreté comme le contrôle de la réactivité, l'évacuation de la chaleur résiduelle, l'intégrité du circuit de refroidissement et l'intégrité du confinement. Le concept des fonctions de sûreté est examiné dans les réf. [2, 4]. Les systèmes qui remplissent directement des fonctions critiques de sûreté sont définis comme étant des systèmes de première ligne, tandis que ceux qui sont nécessaires au bon fonctionnement des systèmes de première ligne sont définis comme étant des systèmes de soutien [4]. Le bon fonctionnement d'un système de première ligne peut dépendre de la disponibilité d'un ou de plusieurs systèmes de soutien ; il est primordial d'identifier ces interdépendances.

Si une EPS a été rédigée pour l'installation, les informations relatives aux systèmes de première ligne et de soutien devraient être aisément accessibles depuis les documents d'EPS ou les documents supports [7]. S'il existe uniquement une EDS, l'équipe d'IZV peut généralement déduire tout ou partie de ces informations des études d'accidents basées sur des appréciations techniques. Si l'EDS liste des groupes de sûreté, ces listes peuvent être utiles pour identifier les systèmes de première ligne et leurs dépendances. D'autres dépendances peuvent néanmoins exister en dehors de l'étude de sûreté et être liées à des scénarios spécifiques d'actes malveillants ou de sabotage. Par exemple, une brèche causée par l'explosion d'une conduite d'eau de refroidissement peut entraîner une inondation qui rend indisponible le matériel proche ou sous la brèche. Les interactions spatiales de ce type devraient être analysées lors du processus d'IZV (paragraphe 2.7.3).

Le fonctionnement efficace d'un système de première ligne (« critères d'efficacité ») correspond à la performance minimum nécessaire pour qu'un système remplisse sa fonction de sûreté dans le cadre des conditions spécifiques provoquées par un EIOM [8]. Les études de sûreté de l'installation contiennent les informations pertinentes pour l'établissement de critères d'efficacité des systèmes de première ligne et de soutien. Les critères d'efficacité des systèmes de première ligne sont particulièrement importants pour le processus d'IZV car ils définissent les points de départ des modélisations logiques ultérieures des scénarios de sabotage des systèmes. Les critères d'efficacité comprennent les mesures de performance (par ex., débit, temps d'intervention)

ainsi que les prescriptions en matériel comme le nombre de voies disponibles, de groupes électrogènes, etc.

La définition des critères d'efficacité des systèmes de soutien peut être plus compliquée. Dans la plupart des cas, les systèmes de soutien servent plus d'un système de première ligne. En conséquence, chaque état possible du système (par ex. trois groupes opérationnels, deux groupes opérationnels, un groupe opérationnel, aucun groupe opérationnel) a un effet différent sur chacun des systèmes de première ligne qui réalisent une certaine fonction de sûreté. Les critères d'efficacité d'un système de soutien varient ainsi en fonction des différentes fonctions de sûreté et des systèmes de première ligne associés.

Certaines installations peuvent être concernées par un grand nombre d'EIOM qui peuvent entraîner indirectement des CRG. Pour ces installations, il peut être préférable de regrouper les EIOM pour lesquels les prescriptions de performance des systèmes de mitigation sont les mêmes. Ce regroupement permettra de réduire la charge de travail à venir pour développer le modèle logique. Tous les EIOM d'un groupe nécessitent que les systèmes de première ligne et les systèmes de soutien répondent essentiellement aux mêmes critères d'efficacité afin de prévenir toute CRG. La même logique pourra ainsi modéliser des scénarios de sabotage qui commencent par l'un quelconque des EIOM d'un groupe. Il n'est pas forcément nécessaire de regrouper les EIOM d'une installation sujette à un faible nombre d'EIOM.

Si une EPS a été effectuée pour l'installation, les EI pris en considération dans l'EPS devraient être regroupés dans les documents de l'EPS ; les mêmes regroupements peuvent être employés pour les EIOM correspondants. Si aucune EPS n'a été effectuée, il peut être possible de commencer par regrouper les EI provenant d'autres documents de sûreté ou d'une autre source. Toutefois, les EIOM sont regroupés en fonction de la conception de l'installation ; il faudrait donc évaluer ces regroupements provenant d'autres sources avec soin afin d'être sûr qu'ils sont pertinents pour l'installation faisant l'objet d'une analyse.

Les étapes examinées à la section 2.6 permettent :

— d'élaborer une liste des EIOM qui dépassent les capacités d'atténuation des systèmes d'une installation ;
— d'élaborer une liste des EIOM qui peuvent être atténués et des systèmes de première ligne et de soutien nécessaires pour faire face à chaque EIOM ;
— d'établir des critères de succès des systèmes de première ligne et de soutien pour chaque EIOM susceptible d'être atténué ;
— de se référer aux documents présentés à l'appui ;
— de regrouper les EIOM (le cas échéant).

2.5. MODÈLE LOGIQUE DE SABOTAGE.

L'étape suivante de l'IZV consiste à construire un modèle logique de sabotage qui permet d'identifier les événements ou combinaisons d'événements pouvant avoir des CRG et nécessitant la protection des zones vitales, à savoir la dispersion directe de matières radioactives, les EIOM qui dépassent les capacités des systèmes d'atténuation, et la combinaison d'événements qui pourraient avoir des CRG si les EIOM ne dépassent pas les capacités des systèmes d'atténuation. Un modèle logique peut être un énoncé, une expression algébrique ou une représentation graphique, par exemple un arbre de défaillance ou un arbre d'événements. Le modèle logique de sabotage inclut tous les événements de dispersion directe et l'ensemble des EIOM et des défaillances associées du système d'atténuation qui entraîneraient des CRG.

La dispersion directe et les EIOM qui dépassent les capacités des systèmes d'atténuation sont inclus dans le modèle logique comme étant des événements uniques entraînant des CRG. On trouve dans la partie du modèle logique qui porte sur les EIOM ne dépassant pas les capacités des systèmes d'atténuation inclut chacun de ces EIOM associé à la neutralisation malveillante des systèmes conçus spécifiquement pour atténuer l'EIOM. Les modèles logiques de neutralisation des systèmes sont mis au point au niveau des composants en utilisant une approche de haut en bas. Leur mise au point devrait être suffisamment détaillée pour permettre de lier les événements de neutralisation et les emplacements (zones) de l'installation où une neutralisation est possible.

Les informations figurant dans les analyses de la sûreté de l'installation et d'autres documents de sûreté peuvent être utilisées pour mettre au point le modèle logique de sabotage pour les EIOM ne dépassant pas les capacités des systèmes d'atténuation. Cela se fait normalement en deux étapes. La première étape consiste à élaborer le modèle logique de sabotage de l'installation qui représente à la fois les EIOM et la neutralisation des systèmes de première ligne entraînant des CRG. Pour ce faire, il convient de se reporter aux informations figurant dans les sections 2.4.1., 2.4.2. et 2.4.3 et aux informations contenues dans l'analyse de la sûreté de l'installation. La deuxième étape consiste à mettre au point des modèles logiques de sabotage pour chaque système de première ligne et les systèmes de soutien dont ils dépendent. Pour se faire, il faut modifier les modèles logiques existants à partir de l'EPS de l'installation, si elle existe, ou mettre au point des modèles logiques en se servant des informations sur la configuration des systèmes de l'installation et des informations sur les interdépendances et les critères de succès. Ce processus produit la partie du modèle logique de sabotage de l'installation qui établit un lien entre chaque EIOM et la neutralisation des systèmes de première ligne et des systèmes

de soutien correspondants et les mesures prises par l'exploitant pour atténuer l'EIOM.

Les évènements de base du modèle logique de sabotage seront les événements de dispersion directe, les EIOM et les événements qui neutralisent les composants des systèmes d'atténuation. Un exemple simple de modèle logique de sabotage est fourni en annexe.

2.6. MENACE POUVANT DÉBOUCHER SUR DES ÉVÈNEMENTS DE SABOTAGE

Les événements de sabotage traités dans les sections précédentes ne tiennent pas compte du fait que la menace peut déboucher sur des actes malveillants. Qui plus est, tous les événements qui pourraient entraîner directement ou indirectement des CRG sont inclus pour faire en sorte qu'aucune zone vitale potentielle ne soit oubliée, que les menaces supposées puissent suffire ou non à provoquer un acte de sabotage. En cas de modification des caractéristiques de la menace supposée, les informations et les modèles mis au point au cours des étapes précédentes pourront être valablement utilisés pour identifier les zones vitales en tenant compte de la modification de la menace[5].

À cette étape du processus, tous les évènements qui ne sont pas crédibles au vu des conséquences que pourrait avoir la menace supposée ne devraient plus être pris en considération. Il conviendrait d'évaluer si la menace peut provoquer la dispersion directe de matières (Section 2.3), des EIOM (Section 2.4.1) et neutraliser les systèmes d'atténuation (Section 2.4.3). Les événements qui dépassent la capacité de menace peuvent être supprimés du modèle logique de sabotage.

En outre, tout événement qui dépasse la capacité de résistance du système de protection physique de l'installation devrait être identifié. Lors de l'analyse du modèle logique de sabotage, il sera supposé que de tels événements se produisent à chaque fois. De manière générale, tout événement pouvant être provoqué par la menace sans qu'il ne soit possible d'avoir accès au site devrait être considéré comme se produisant. Par exemple, il est pratiquement impossible que le système de protection physique de l'installation permette d'éviter une perte de réseau ; la menace peut entraîner une perte de réseau de plusieurs façons sans

[5] L'autorité compétente peut exiger que les étapes de l'IZV décrites aux sections 2.7 et 2.8 soient achevées avant d'évaluer si la menace pourrait déboucher sur les évènements inclus dans le modèle logique de sabotage. Une telle approche, bien qu'exigeant un travail d'analyse supplémentaire, permettra d'identifier tous les ensembles de zones vitales potentielles sans tenir compte des caractéristiques de la menace.

pour autant qu'il soit possible d'avoir accès à l'installation. Par conséquent, le processus d'IZV devrait partir du principe qu'il n'y a pas de réseau. Tout autre événement de ce type figurant dans le modèle logique de sabotage devrait être identifié et mis en évidence afin d'être traité de manière adéquate lors du processus d'identification des zones décrit à la section 2.7.

2.7. MODÈLE LOGIQUE DE ZONES DE SABOTAGE

L'étape suivante du processus d'IZV consiste à identifier et répertorier les zones depuis lesquelles un agresseur pourrait provoquer chaque évènement inclus dans le modèle logique de sabotage. Les informations relatives à ces zones sont recueillies dans le cadre d'un processus structuré puis elles sont vérifiées en effectuant une visite d'inspection visuelle de l'installation. Il faudrait tenir compte des interactions spatiales entres les zones contiguës ainsi qu'il est expliqué ci-dessous.

2.7.1. Collecte et saisie des données

Les données concernant les zones sont entrées dans le modèle logique de sabotage en remplaçant chaque évènement inclus dans le modèle (dispersion directe, EIOM et neutralisation des systèmes d'atténuation) par la ou les zones de l'installation nucléaire à partir de laquelle ou desquelles ledit événement peut être provoqué. Il en résulte un modèle logique de zones de sabotage. Le modèle logique de zones de sabotage peut être résolu ainsi qu'il est décrit à la section suivante afin de déterminer les combinaisons de zones depuis lesquelles des actes malveillants pourraient avoir des CRG et les combinaisons minimales de zones qui devraient être protégées pour éviter des CRG.

Les renseignements descriptifs de l'installation nucléaire fournissent les informations nécessaires à l'identification des zones où les événements de sabotage peuvent se produire. Les plans d'ensemble devraient fournir des informations sur les zones, salles, murs et portes et sur les voies d'accès. Les schémas de tuyauterie et d'instrumentation, les plans isométriques, les analyses d'une mise à l'arrêt sûre, les EPS en cas d'incendie, d'inondation et de séisme sont d'autres sources d'informations sur l'emplacement des équipements. Étant donné que toute zone figurant dans le modèle logique peut être sélectionnée comme zone vitale, il devrait être matériellement possible d'assurer un protection autour de chacune d'entre elles. Par conséquent, il devrait être possible d'utiliser les structures existantes ou des bâtiments nouveaux pour créer une barrière physique autour de chaque zone définie. Il faudrait également pouvoir contrôler l'accès à chaque zone afin de réduire au minimum le nombre d'entrées dans

la zone et de sorties de la zone et équiper tous les points d'accès de la zone de systèmes d'alarme et de dispositifs de sécurité appropriés.

Il faudrait mettre en évidence les zones en les indiquant sur les plans de l'installation ou dans d'autres documents relatifs à la conception et la configuration des lieux de l'installation pour pouvoir les délimiter clairement. Les informations relatives aux zones sont entrées dans le modèle logique de sabotage en remplaçant les évènements inclus dans le modèle par les zones où chaque événement peut se produire. En fonction de l'approche retenue, cela peut être fait automatiquement à l'aide d'une sorte de table de liaison (« plan de l'emplacement ») ou manuellement en modifiant directement le modèle logique de sabotage de sorte que tous les événements de base soient remplacés par les zones où ils peuvent se produire. Il en résulte un modèle logique de zones de sabotage.

2.7.2. Visite d'inspection visuelle

Il faudrait vérifier les informations relatives aux zones en faisant un tour d'inspection visuelle. Les membres de l'équipe devraient passer en revue les informations relatives à l'emplacement en prévision de la visite d'inspection visuelle pour l'IZV[6]. L'équipe d'inspection visuelle chargée de l'identification des zones vitales devrait être composée de représentants des organismes responsables de la sûreté, la sécurité, la conception et l'exploitation de l'installation.

L'inspection visuelle pour l'IZV a pour principaux objectifs de :

— vérifier les zones depuis lesquelles la menace pourrait provoquer une dispersion directe ;
— vérifier l'ensemble des zones à partir desquelles la menace pourrait provoquer chaque EIOM recensé à la section 2.4 ;
— vérifier l'ensemble des zones depuis lesquelles une personne constituant une menace pourrait commettre chacun des actes pouvant neutraliser le matériel, les systèmes, les structures, les composants, les dispositifs ou les mesures prises par l'opérateur qui sont identifiées dans le modèle logique de sabotage ;
— évaluer les possibilités d'interactions spatiales entre les zones contiguës.

---

[6] Pour les nouveaux modèles, une analyse des zones vitales devrait être effectuée avant la construction. Le tour d'inspection visuelle a lieu avant la remise de l'installation à l'exploitant afin de confirmer l'analyse. La question du tour d'inspection visuel est examinée dans la référence [12].

2.7.3. Interactions spatiales

Il est nécessaire d'examiner davantage les interactions spatiales entre les zones contiguës. Dans certains cas, un acte malveillant commis dans d'une zone peut neutraliser les équipements, les composants ou les dispositifs d'une ou de plusieurs zones contiguës. Les EPS portant sur des événements externes, comme les EPS en cas d'incendie, d'inondation ou de séisme, et la Réf. [12] donnent des informations utiles sur les interactions spatiales.

2.8. ENSEMBLES CANDIDATS DE ZONES VITALES

L'identification des ensembles candidats de zones vitales se fait en deux étapes :

1) *Identifier les ensembles cibles :* Le modèle logique de zones de sabotage est analysé afin de déterminer toutes les combinaisons de zones auxquelles un agresseur devrait avoir accès pour que des scénarios de sabotage qui pourraient avoir des CRG se produisent. Chacune de ces combinaisons de zones est un ensemble de coupures minimales du modèle logique de zones de sabotage et représente l'ensemble des zones cibles où un agresseur doit pénétrer pour qu'un scénario de sabotage se produise. Les combinaisons de zones depuis lesquelles des actes malveillants pourraient avoir des CRG peuvent servir à mettre au point et à évaluer le programme de protection physique de l'installation. Ces combinaisons de zones peuvent être passées en revue pour identifier les cibles d'agresseurs potentiels qui serviront de base à la mise au point de scénarios de sabotage en vue de concevoir et d'évaluer le système de protection physique.
2) *Identifier les ensembles de protection :* Le modèle logique de zones de sabotage est analysé pour déterminer les combinaisons minimales de zones qui devraient être protégées afin de garantir qu'aucun scénario de sabotage ne puisse se produire. Pour ce faire, il faut trouver des ensembles de prévention [13] pour le modèle logique de zones de sabotage. Chaque ensemble de prévention présente une formule possible pour déterminer ce qui pourrait être protégé pour prévenir tout scénario de sabotage. Un ensemble de prévention de niveau 1 contient au moins une zone de chaque ensemble de coupures minimales du modèle logique de zones de sabotage (et correspond à une des résolutions du complément booléen de ce modèle logique). S'il est impossible pour l'agresseur d'avoir accès à toutes les zones d'un ensemble de prévention, il ne pourra pas commettre les actes de sabotage représentés dans le modèle logique

de zones de sabotage, quels qu'ils soient. Chaque ensemble de prévention de niveau 1 contient un complément minimum d'équipements, de systèmes, de structures, de composants, de dispositifs et/ou de mesures que doit prendre l'exploitant qui, s'ils sont protégés contre le sabotage, empêchent tout acte de sabotage. Si chaque zone de l'un de ces ensembles est protégée, tous les scénarios de sabotage pouvant avoir indirectement des CRG seront rendus impossibles[7].

Le processus permettant de résoudre le modèle logique de zones de sabotage pour identifier les ensembles candidats de zones vitales est illustré par des exemples dans l'annexe.

2.9. SÉLECTION DES ENSEMBLES DE ZONES VITALES

Cette étape du processus d'IZV consiste à sélectionner un ensemble de zones vitales à partir des ensembles candidats de zones vitales recensés à la section 2.8. La présente publication fournit des recommandations concernant le processus de sélection mais ne prescrit pas l'emploi de méthodes spécifiques.

Chaque ensemble candidat de zones vitales se conforme à la recommandation formulée dans la section 7.1.5 de la réf.[1] pour un ensemble de zones vitales de l'installation. L'exploitant de l'installation peut choisir de protéger l'un ou l'autre de ces ensembles de zones vitales. Pour choisir un ensemble de zones à protéger, l'exploitant pourrait tenir compte de différents facteurs importants pour la sûreté et l'efficacité du fonctionnement de l'installation. Il pourrait par exemple sélectionner l'ensemble candidat de zones vitales qui combine au mieux les éléments suivants :

— un faible impact sur la sûreté, l'exploitation de l'installation et les mesures d'intervention d'urgence ;
— une moindre difficulté à assurer la protection ;
— des mesures de protection très efficaces ; et
— le faible coût de protection des zones vitales.

[7] Les ensembles de prévention de niveau 2 (qui contiennent au moins deux zones de chaque ensemble de coupures minimales) pourraient être utilisés pour identifier les ensembles candidats de zones vitales et s'assurer que la protection ou la défense en profondeur sont mieux assurées. Il n'y aura pas d'ensemble de prévention de niveau 2 ou supérieur dans les modèles logiques de zones de sabotage qui contiennent une seule zone à partir de laquelle un agresseur pourrait commettre des actes ayant des CRG.

Il est peu probable qu'un ensemble candidat de zones vitales obtienne la meilleure note pour chaque critère de sélection. Il faudra donc trouver des compromis entre les notes des différentes zones et sélectionner l'ensemble candidat de zones vitales qui globalement constitue le meilleur choix. Cela peut s'effectuer en appliquant des pratiques techniques reconnues ou en effectuant une analyse plus structurée (par exemple, le processus de hiérarchie analytique). Les références [14, 15] fournissent des exemples de méthodes d'analyse structurée des compromis.

Le processus de sélection des zones vitales permet d'établir :

1) un tableau qui évalue chaque ensemble candidat de zones vitales en fonction de chacun des attributs examinés lors de la sélection d'un ensemble de zones vitales et qui répertorie le score global ou le classement de chaque ensemble candidat de zones vitales, en y associant une explication logique.
2) un ensemble de zones vitales recommandé en se fondant sur le meilleur score global ou du meilleur classement.

L'ensemble de zones vitales qui devrait être protégé pour prévenir un acte de sabotage comprendra :

— toutes les zones depuis lesquelles la menace supposée peut provoquer une dispersion directe de matières radioactives supérieure aux critères CRG ;
— toutes les zones depuis lesquelles un agresseur peut provoquer des EI qui dépassent les capacités d'atténuation des systèmes de l'installation ; et
— toutes les zones où un agresseur peut déclencher des événements pouvant être atténués par les systèmes de sûreté, ou les zones dans lesquelles se trouvent des ensembles minimum d'équipements nécessaires pour atténuer les EI.

3. CONSIGNATION DES RÉSULTATS PAR ÉCRIT

3.1. OBJECTIFS DES DOCUMENTS ET PRINCIPES A SUIVRE

Les documents d'analyse ont pour objectif de démontrer que l'IZV est conforme aux prescriptions spécifiées par l'autorité compétente. Les documents devraient être bien structurés, concis et faciles à examiner et à mettre à jour. Des mises à jour peuvent être nécessaires pour tenir compte des changements

concernant les caractéristiques des agresseurs supposés ainsi que des modifications apportées au fonctionnement de l'installation, aux systèmes et mesures de sûreté et à l'emplacement des équipements, des systèmes, structures, composants, dispositifs et/ou aux mesures prises par l'exploitant. Les documents devraient présenter de manière explicite les hypothèses formulées dans les considérations de politique générale examinées dans la section 2.2.1 et se conformer aux prescriptions relatives à l'assurance qualité spécifiées par l'autorité compétente.

3.2. ORGANISATION DES DOCUMENTS

L'organisation des documents devrait être régie selon deux principes généraux :

1) *la traçabilité :* Pour examiner et mettre à jour l'analyse, il devrait être possible de conserver une trace de toute information avec un minimum d'efforts.
2) *l'ordre séquentiel :* L'analyse présentée dans le rapport devrait suivre l'ordre dans lequel l'analyse a été effectuée, comme suit :

— entrée :
  • hypothèses de base utilisées dans le processus ;
  • résultats des analyses prudentes.
— événements de dispersion directe potentielle ;
— identification des EIOM ;
— identification des systèmes de sûreté permettant d'atténuer les EIOM ;
— mise au point du modèle logique ;
— évaluation des menaces possibles ;
— identification des zones où peut avoir lieu un sabotage ;
— identification des ensembles candidats de zones vitales ;
— sélection d'un ensemble de zones vitales.

3.3. PROTECTION DES INFORMATIONS

Le processus d'IZV génère des informations sensibles qui devraient être protégées comme il convient, conformément aux prescriptions relatives à la sécurité de l'information établies par l'autorité compétente. Les prescriptions et procédures relatives à la sécurité de l'information varieront en fonction du système législatif de l'État où l'installation est située. Toute personne ayant

accès aux informations générées lors du processus d'IZV devrait comprendre et suivre les prescriptions relatives à la sécurité de l'information.

Annexe

EXEMPLE DE MODÈLE LOGIQUE DE SABOTAGE

La présente annexe propose une résolution étape par étape d'un modèle logique simple afin d'illustrer comment identifier des ensembles candidats de zones vitales. La résolution du modèle logique pris comme exemple démontre comment les concepts des ensembles de coupures minimales et d'ensembles de protection minimale sont appliqués dans le processus d'IZV.

Un modèle logique peut être un énoncé, une expression algébrique ou une représentation graphique, par exemple un arbre de défaillance ou un arbre d'événements. La résolution de différentes représentations du même problème logique aboutira aux mêmes résultats. Un modèle logique « se résout » en appliquant les règles d'algèbre booléenne au modèle. Le tableau 2 définit les symboles logiques et les règles d'algèbre booléenne classiques.

Examinons une installation fictive ayant les caractéristiques suivantes :

1) Deux événements initiateurs (EI) sont identifiés pour cette installation, EI1 et EI2 qui, s'ils ne sont pas atténués, produiront des rejets qui dépassent les limites des CRG établies par l'autorité compétente.
2) Le système de sûreté S1 est conçu pour atténuer EI1 et le système S2 est conçu pour atténuer EI2.
3) Le système S1 dispose de deux trains d'équipements, T1 et T2. Si l'un ou l'autre de ces trains fonctionne correctement, S1 peut atténuer efficacement EI1 (c'est-à-dire que les deux trains doivent être défaillants pour que S1soit défaillant).
4) Le système S2 a trois trains, T3, T4 et T5. T3 ou T4 et T5 doivent fonctionner pour que S2 puisse atténuer efficacement EI2 (c'est-à-dire que S2 ne pourra pas atténuer EI2 si T3 et T4 ou T3 et T5 sont défaillants).
5) Les trains des systèmes ont des composants (ci-après désignés par C) qui doivent fonctionner pour que les trains fonctionnent.
   — T1 est cesse de fonctionner si l'un ou l'autre composant (C1 ou C2) est défaillant.
   — T2 cesse de fonctionner si C3 ou C4 est défaillant.
   — T3 cesse de fonctionner si C5 ou C6 est défaillant.
   — T4 cesse de fonctionner si C7 ou C8 est défaillant.
   — T5 cesse de fonctionner si C9 ou C10 est défaillant.
6) Pour pouvoir provoquer des EI et neutraliser les différents composants, il faudrait qu'un saboteur ait accès à différents emplacements de la centrale, désignés ci-après par L.

Évènement	Emplacement
Neutralisation de C1	L1
Neutralisation de C2	L2
Neutralisation de C3	L2
Neutralisation de C4	L2
Neutralisation de C5	L3
Neutralisation de C6	L3
Neutralisation de C7	L5
Neutralisation de C8	L6
Neutralisation de C9	L6
Neutralisation de C10	L6
Origine de EI1	L8
Origine de EI2	L9

Les énoncés ci-dessus constituent une forme de modèle logique de sabotage de l'installation. En analysant soigneusement ces énoncés, il est possible de déterminer les combinaisons d'emplacements dans lesquels un saboteur devrait pénétrer pour provoquer tous les EI et toutes les défaillances des composants qui auraient des CRG. Par exemple, si un saboteur avait accès à L2 et L8, il pourrait provoquer EI1 et neutraliser S1, entraînant un rejet qui dépasse les limites des CRG. Le saboteur peut être à l'origine de EI1 s'il a accès à L8. Si le saboteur neutralise à la fois T1 et T2, S1 ne pourra pas atténuer EI1. La neutralisation de C2 peut neutraliser T1 et la neutralisation de C3 peut neutraliser T2. C2 et C3 peuvent tous deux être neutralisés à partir de L2. En ayant accès à la fois à L2 et à L8, le saboteur peut donc commettre un acte peut entraînant des CRG. En examinant en détail les énoncés et le tableau des emplacements, il pourrait être possible d'identifier toutes les combinaisons d'emplacements à partir desquels les EI peuvent être suffisant pour avoir des CRG.

Tant que l'installation est suffisamment simple, il est possible de déduire les combinaisons d'emplacements à partir desquels un acte de sabotage peut être

commis en effectuant une inspection comme dans le paragraphe précédent. Une approche plus utile consiste à représenter les liens entre les EI, les événements de neutralisation et les emplacements dans une équation logique. L'événement qui doit être représenté dans cette équation logique est un rejet dépassant les limites des CRG. À l'aide des définitions figurant dans le tableau 2, on pose les équations ci-après correspondant aux énoncés 1 à 5 ci-dessus :

$$CRG = EI1*S1 + EI2*S2 \quad (1)$$
$$S1 = T1*T2 \quad (2)$$
$$S2 = T3*T4 + T3*T5 \quad (3)$$
$$T1 = C1 + C2 \quad (4)$$
$$T2 = C3 + C4 \quad (5)$$
$$T3 = C5 + C6 \quad (6)$$
$$T4 = C7 + C8 \quad (7)$$
$$T5 = C9 + C10 \quad (8)$$

Dans ces équations, S1 signifie que le système de sûreté 1 est neutralisé, T1 signifie que le train 1 est neutralisé, C1 signifie que le composant 1 est neutralisé, etc. En remplaçant les événements dans ces équations par les emplacements où ils peuvent être provoqués et en les simplifiant à l'aide des règles d'algèbre booléenne, on obtient les résultats suivants :

$$T1 = L1 + L2 \quad (9)$$
$$T2 = L2 + L2 = L2 \quad (10)$$
$$T3 = L3 + L3 = L3 \quad (11)$$
$$T4 = L5 + L6 \quad (12)$$
$$T5 = L6 + L6 = L6 \quad (13)$$
$$S1 = (L1 + L2)*L2 = L2 \quad (14)$$
$$S2 = L3*(L5 + L6) + L3*L6 = L3*L5 + L3*L6 \quad (15)$$
$$CRG = L8*L2 + L9*(L3*L5 + L3*L6)$$
$$= (L8*L2) + (L9* L3*L5) + (L9*L3*L6) \quad (16)$$

Pour cet exemple simple, il existe trois combinaisons d'emplacements à partir desquels un acte commis par un saboteur peut avoir des CRG :

$$CRG = L8*L2 + L9* L3*L5 + L9*L3*L6 \quad (17)$$

Chaque combinaison d'emplacements à partir desquels un sabotage peut être provoqué est appelée ensemble de coupures de l'équation des emplacements où un sabotage peut avoir lieu. L'IZV a pour objectif de trouver un ensemble minimal de zones devant être protégées contre le sabotage pour

empêcher que tous les scénarios possibles entraînent des CRG. Cela signifie qu'il faut protéger au moins une des zones dans chaque combinaison de zones depuis lesquelles un acte de sabotage peut être commis. Chaque combinaison d'emplacements dont la protection empêchera tous les scénarios de sabotage est un ensemble de prévention du modèle logique et constitue un ensemble candidat de zones vitales. Pour les équations simples concernant les emplacements où un acte de sabotage peut être commis, il est possible de déterminer directement les combinaisons d'emplacements dont la protection empêchera le sabotage. L'équation 17 montre que si l'agresseur n'a pas accès aux combinaisons suivantes de zones, il ne peut pas y avoir de CRG.

$$\begin{aligned} \text{CRG empêchée} = {} & L8*L9 + \\ & \underline{L8}*L3 \pm \\ & \underline{L2}*L9 \pm \\ & \underline{L2}*L3 \pm \underline{L8}*L5*L6 \pm \\ & \underline{L2}*L5*L6 \end{aligned} \tag{18}$$

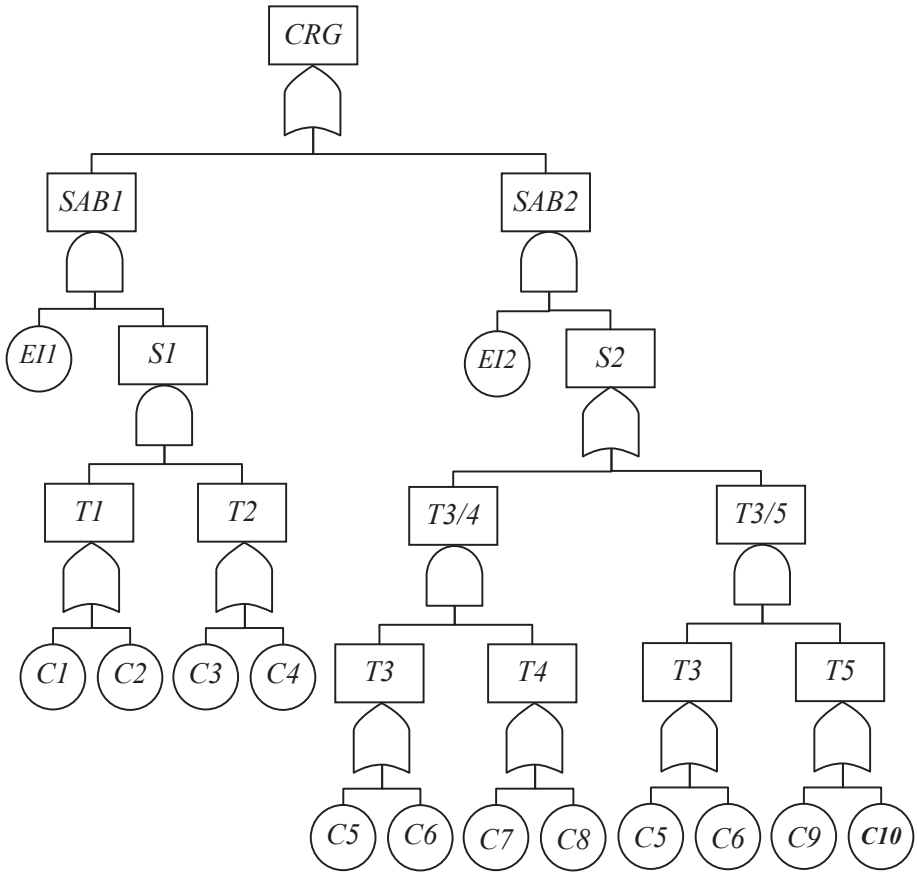
Le soulignement dans l'équation 18 indique que l'accès à l'emplacement n'est pas possible ; par exemple L8 signifie que l'accès à L8 est impossible. En termes d'algèbre booléenne, L8 est le complément (non-occurrence ou NON) de L8. Pour l'installation considérée dans l'exemple, il existe six ensembles candidats de zones vitales comme cela est décrit dans l'équation 18. Ce résultat peut être aussi déduit algébriquement en créant le complément de l'équation de l'emplacement où un acte de sabotage peut être commis et en le simplifiant à l'aide des règles de l'algèbre booléenne. La protection de l'un des ensembles candidats de zones vitales garantira qu'un acte commis par un saboteur ne peut avoir de CRG. Si, par exemple, on sélectionne l'ensemble L2 et L3 comme l'ensemble final de zones vitales, ce sont les deux seules zones de l'installation qui seraient protégées en tant que zones vitales. La protection de ces deux zones garantira qu'aucun des scénarios possibles de sabotage ne pourra se produire.

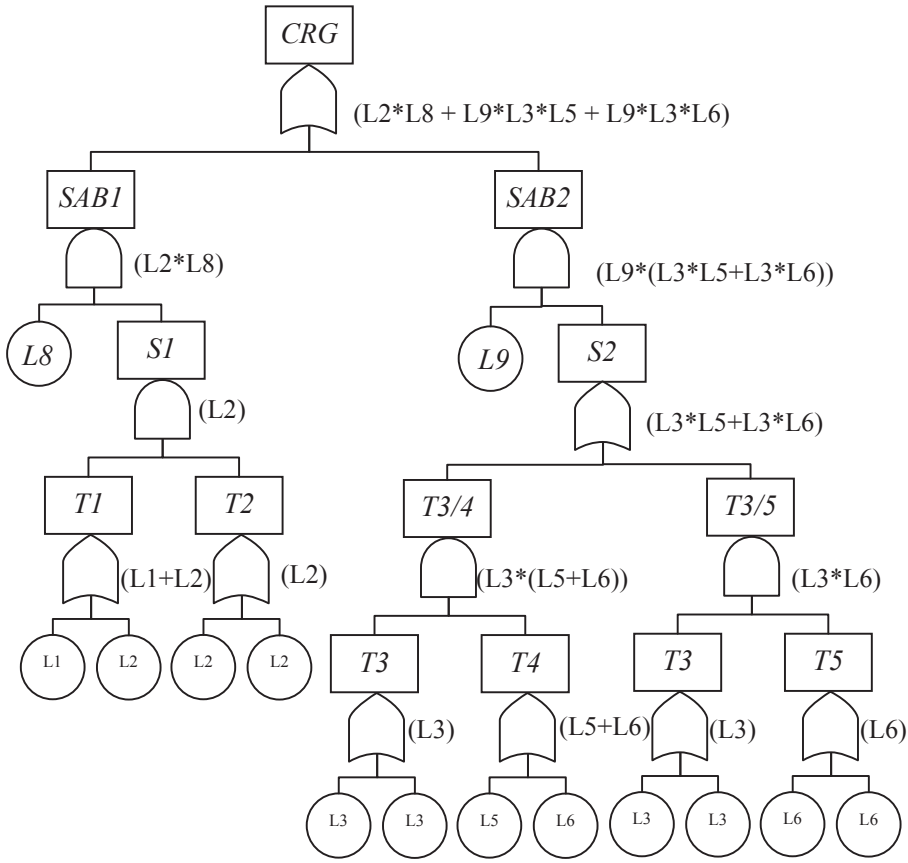
Les arbres de défaillance peuvent être utilisés pour représenter efficacement la logique de sabotage pour des installations plus compliquées. Pour l'installation considérée dans l'exemple, la figure 2 présente un arbre de défaillance dont la résolution mettra davantage en évidence le processus d'identification des ensembles candidats de zones vitales. Dans cet arbre, l'événement sommet est le rejet dépassant les limites des CRG (représenté par le symbole CRG). Les portes logiques montrent comment les événements de l'arbre se combinent pour provoquer l'événement sommet, et l'arbre est décomposé vers le bas jusqu'au niveau de défaillance des composants. La figure 3 montre l'arbre de défaillance où tous les événements de base sont remplacés par les emplacements à partir desquels les événements peuvent

être provoqués. Cet arbre de défaillance des emplacements où un sabotage peut se produire se résout en appliquant les concepts de l'algèbre booléenne appliqués dans les équations 1 à 17 pour obtenir les mêmes résultats. L'expression entre parenthèses à côté de chaque porte représente la solution pour la porte par rapport aux événements de base de l'arbre. Une façon de générer les ensembles de protection de niveau 1 d'un arbre de défaillance consiste à créer et à résoudre le double de l'arbre. On crée le double d'un arbre de défaillance en changeant chaque porte OU de l'arbre par une porte ET, chaque porte ET par une porte OU, et chaque événement par le complément (NON) de l'événement. Il existe divers logiciels pour résoudre les arbres de défaillance et générer les ensembles de prévention (ensembles candidats de zones vitales) nécessaires dans le processus d'IZV.

En résumé, le modèle logique de sabotage d'une installation peut être mis au point sous plusieurs formes équivalentes. La résolution du modèle logique produit des ensembles candidats de zones vitales qui peuvent être protégés pour empêcher un sabotage. Les ensembles candidats, quels qu'ils soient, contiendront un ensemble minimal d'équipements nécessaires pour garantir qu'aucun scénario de sabotage ne puisse produire.

Symboles logiques		
Symbole	Opération	Définition
+	OU	L'un ou l'autre des évènements se produit.
*	ET	Les deux évènements se produisent. A*B signifie que l'évènement A et l'évènement B se produisent.
Portes logiques		
Symbole	Nom de la porte	Définition
	Porte OU	La sortie correspond à l'une des entrées.
	Porte ET	La sortie correspond à toutes les entrées.
Règles d'algèbre booléenne		
A+A=A	A+A*B=A	$\overline{(A+B)} = \overline{A} * \overline{B}$
A*A=A	A*(B+C)=A*B+A*C	$\overline{(A*B)} = \overline{A} + \overline{B}$


CRG
SAB1
SAB2
EI1
S1
EI2
S2
T1
T2
T3/4
T3/5
C1
C2
C3
C4
T3
T4
T3
T5
C5
C6
C7
C8
C5
C6
C9
C10


CRG
(L2*L8 + L9*L3*L5 + L9*L3*L6)
SAB1
SAB2
(L2*L8)
(L9*(L3*L5+L3*L6))
L8
S1
L9
S2
(L2)
(L3*L5+L3*L6)
T1
T2
T3/4
T3/5
(L1+L2)
(L2)
(L3*(L5+L6))
(L3*L6)
L1
L2
L2
L2
T3
T4
T3
T5
(L3)
(L5+L6)
(L3)
(L6)
L3
L3
L5
L6
L3
L3
L6
L6

RÉFÉRENCES

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

[2] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Sûreté des centrales nucléaires : conception, collection Normes de sûreté, n° NS-R-1, AIEA, Vienne (2005).

[3] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Évaluation et vérification de la sûreté des centrales nucléaires, collection Normes de sûreté nº NSG1.2, AIEA, Vienne (2005).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-3, IAEA, Vienna (2010).

[5] SANDIA NATIONAL LABORATORIES, A Systematic Method for Identifying Vital Areas at Complex Nuclear Facilities, SAND2004-2866, SNL, Albuquerque, NM (2005).

[6] VARNADO, G.B., ORTIZ, N.R., Fault Tree Analysis for Vital Area Identification, NUREG/CR-0809, SAND79-0946, Albuquerque, NM, Nuclear Regulatory Commission, Washington, DC (1979)

[7] KOREA ATOMIC ENERGY RESEARCH INSTITUTE, The Application of PSA Techniques to the Vital Area Identification of Nuclear Power Plants, KAERI, Seoul (2004).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Facilities and Nuclear Material against Sabotage, IAEA, Vienna (in preparation)

[9] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Glossaire de sûreté de l'AIEA : Terminologie employée en sûreté nucléaire et en radioprotection - Édition 2007, AIEA, Vienne (2007).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Amendment to the Convention on the Physical Protection of Nuclear Material, IAEA International Law Series No. 2, IAEA, Vienna (2006).

[11] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Élaboration, utilisation et actualisation de la menace de référence, collection Sécurité nucléaire de l'AIEA n° 10, AIEA, Vienne (2012).

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

[13] WORRELL, R.B., BLANCHARD, D.P., "Top event prevention analysis : A deterministic use of PRA", Probabilistic Safety Assessment Methodology and Application (Proc. Int. Conf. Seoul, 1995).

[14] KEENY, R. L., RAIFFA, H., Decisions with Multiple Objectives : Preferences and Value Tradeoffs, Wiley, New York (1976).

[15] SAATY, T. L., Decision Making for Leaders : The Analytical Hierarchy Process for Decisions in a Complex World, Analytic Hierarchy Process Series, Vol. 2, RWS Publications, Pittsburgh (2002).

DÉFINITIONS ET ACRONYMES

Les définitions suivantes sont utilisées aux fins de la présente publication.

conséquences radiologiques inacceptables (CRI). Niveau de conséquences radiologiques, défini par l'État, au-dessus duquel la mise en œuvre des mesures de protection physique est une nécessité.

critères de succès. Performance minimale d'un système qui permettra à une fonction de sûreté d'un système de fonctionner dans la situation particulière créée par un événement initiateur.

dispersion ou rejet direct. Dispersion ou rejet de matières par application d'une énergie provenant d'une source externe (par exemple, un dispositif explosif ou incendiaire).

dispersion ou rejet indirect. Dispersion ou rejet de matières en utilisant l'énergie potentielle (c'est-à-dire, chaleur ou pression) contenue dans les matières radioactives ou nucléaires ou dans un système de processus en vue de disperser les matières.

ensemble candidat de zones vitales. Ensemble de prévention (en complément d'un ensemble de coupures ou d'un ensemble de chemins minimaux) pour un modèle logique de zones de sabotage qui identifie un ensemble de zones dont la protection empêchera que des actes malveillants entraînent des conséquences radiologiques inacceptables. Un acte de sabotage ne peut être commis que si le saboteur pénètre dans au moins une des zones de l'ensemble de prévention.

ensemble de coupures minimales. Un ensemble de coupures minimales est le plus petit ensemble d'événements qui suffit pour provoquer le résultat d'un modèle logique. Pour un arbre des défaillances, un ensemble de coupures minimales est le plus petit ensemble d'événements de base qui provoquera l'événement sommet.

ensemble de prévention. Un ensemble de prévention est le plus petit ensemble d'événements qui empêchera que le modèle logique n'aboutisse. Pour un arbre de défaillance, un ensemble de prévention est le plus petit ensemble d'événements de base qu'il faudrait empêcher afin d'empêcher l'événement sommet.

étude déterministe de sûreté (EDS). Analyse détaillée et structurée qui évalue la performance de l'installation par rapport à des conditions d'exploitation très diverses, des événements initiateurs postulés et d'autres circonstances en démontrant que l'exploitation normale ne présente pas de risque, de manière que les paramètres de l'installation ne dépassent pas les limites d'exploitation.

étude probabiliste de sûreté (EPS). Approche détaillée et structurée visant à identifier les scénarios de défaillance. Outil conceptuel et mathématique servant à calculer des estimations chiffrées du risque [9].

événement initiateur (EI). Événement identifié au stade de la conception comme pouvant déboucher sur des incidents de fonctionnement prévus ou des conditions accidentelles. Appelé dans la réf.[9] EI postulé.

événement initiateur d'origine malveillante (EIOM). EI ayant une origine malveillante. Acte malveillant qui perturbe l'exploitation au point que, si l'atténuation a échoué, les conséquences radiologiques en résultant seront inacceptables.

menace de référence. Moyens et caractéristiques d'un agresseur potentiel d'origine interne et/ou externe qui pourrait tenter d'effectuer un enlèvement non autorisé de matières nucléaires ou de commettre un sabotage en fonction desquels un système de protection physique est conçu et évalué.

menace. Personne ou groupe de personnes ayant la motivation, l'intention et la capacité de commettre un acte malveillant.

modèle logique de sabotage. Modèle logique qui consigne par écrit les événements malveillants ou combinaisons d'événements malveillants qui pourraient entraîner des conséquences radiologiques inacceptables. Un modèle logique de zones de sabotage identifie les zones physiques depuis lesquelles les événements malveillants peuvent se produire. Le modèle logique de zones de sabotage peut être analysé pour identifier les combinaisons de zones depuis lesquelles il est possible de commettre un sabotage qui entraînerait des conséquences radiologiques inacceptables et les zones qui doivent être protégées pour prévenir toute conséquence radiologique inacceptable.

modèle logique. Énoncé, expression algébrique ou représentation graphique qui capture les combinaisons de défaillances d'éléments entraînant un événement non souhaité ou un état non souhaité du système.

protection physique. Mesures (comprenant les mesures de protection structurelles, techniques et administratives) prises pour empêcher un agresseur de commettre un acte qui aurait une conséquence non souhaitable (par exemple un sabotage radiologique ou l'enlèvement non autorisé de matières radioactives ou nucléaires en cours d'utilisation, d'entreposage ou de transport) et pour en atténuer les conséquences ou les réduire au minimum si l'agresseur est à l'origine d'un tel acte malveillant.

sabotage. Tout acte délibéré dirigé contre une installation nucléaire ou des matières nucléaires et autres matières radioactives en cours d'utilisation, d'entreposage ou de transport, qui pourrait, directement ou indirectement, mettre en danger la santé et la sécurité du personnel, le public et l'environnement à la suite d'une exposition à des rayonnements ou du rejet de substances radioactives.

système de première ligne. Système qui remplit directement une fonction de sûreté de l'installation. Voir aussi la définition de système de soutien.

système de soutien. Système nécessaire au bon fonctionnement d'un ou plusieurs système(s) de première ligne.

zone protégée. Zone située à l'intérieur d'une zone d'accès limité et contenant des matières nucléaires de catégories I ou II et/ou des cibles de sabotage entourée d'une barrière physique et protégée par des mesures de protection physique supplémentaires.

zone vitale. Zone située à l'intérieur d'une zone protégée et contenant des équipements, des systèmes ou dispositifs, ou des matières nucléaires, dont le sabotage pourrait avoir, directement ou indirectement, des conséquences radiologiques importantes.

RÉUNIONS DE PRÉPARATION DE LA PRÉSENTE PUBLICATION

Réunions de consultants

Vienne (Autriche) 7–11 juin 2004 ;
Vienne (Autriche) 6–10 juin 2005 ;
Séoul (République de Corée) 6–10 décembre 2005

Réunion technique

Vienne (Autriche) 18–22 septembre 2006

IAEA
Agence internationale de l'énergie atomique

N° 24

OÙ COMMANDER ?

Dans les pays suivants, 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.

ALLEMAGNE

Goethe Buchhandlung Teubig GmbH
Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Düsseldorf, ALLEMAGNE
Téléphone : +49 (0) 211 49 874 015 • Fax : +49 (0) 211 49 874 28
Courriel : s.dehaan@schweitzer-online.de • Site web : http://www.goethebuch.de

BELGIQUE

Jean de Lannoy
Avenue du Roi 202, 1190 Bruxelles, BELGIQUE
Téléphone : +32 2 5384 308 • Fax : +32 2 5380 841
Courriel : jean.de.lannoy@euronet.be • Site web : http://www.jean-de-lannoy.be

CANADA

Renouf Publishing Co. Ltd.
22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA
Téléphone : +1 613 745 2665 • Fax : +1 643 745 7660
Courriel : order@renoufbooks.com • Site web : http://www.jean-de-lannoy.be

Bernan Associates
4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, ÉTATS-UNIS D'AMÉRIQUE
Téléphone : +1 800 865 3457 • Fax : +1 800 865 3450
Courriel : orders@bernan.com • Site web : http://www.bernan.com

ÉTATS-UNIS D'AMÉRIQUE

Bernan Associates
4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, ÉTATS-UNIS D'AMÉRIQUE
Téléphone : +1 800 865 3457 • Fax : +1 800 865 3450
Courriel : orders@bernan.com • Site web : http://www.bernan.com

Renouf Publishing Co. Ltd.
812 Proctor Avenue, Ogdensburg, NY 13669-2205, ÉTATS-UNIS D'AMÉRIQUE
Téléphone : +1 888 551 7470 • Fax : +1 888 551 7471
Courriel : orders@renoufbooks.com • Site web : http://www.renoufbooks.com

FÉDÉRATION DE RUSSIE

Scientific and Engineering Centre for Nuclear and Radiation Safety
107140, Moscou, Malaya Krasnoselskaya st. 2/8, bld. 5, FÉDÉRATION DE RUSSIE
Téléphone : +7 499 264 00 03 • Fax : +7 499 264 28 59
Courriel : secnrs@secnrs.ru • Site web : http://www.secnrs.ru

FRANCE

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

Lavoisier SAS
14 rue de Provigny, 94236 Cachan CEDEX, FRANCE
Téléphone : +33 1 47 40 67 00 • Fax : +33 1 47 40 67 02
Courriel : livres@lavoisier.fr • Site web : http://www.lavoisier.fr

L'Appel du livre
99 rue de Charonne, 75011 Paris, FRANCE
Téléphone : +33 1 43 07 43 43 • Fax : +33 1 43 07 50 80
Courriel : livres@appeldulivre.fr • Site web : http://www.appeldulivre.fr

HONGRIE

Librotrade Ltd., Book Import
Pesti ut 237. 1173 Budapest, HONGRIE
Téléphone : +36 1 254-0-269 • Fax : +36 1 254-0-274
Courriel : books@librotrade.hu • Site web : http://www.librotrade.hu

INDE

Allied Publishers
1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDE
Téléphone : +91 22 4212 6930/31/69 • Fax : +91 22 2261 7928
Courriel : alliedpl@vsnl.com • Site web : http://www.alliedpublishers.com

Bookwell
3/79 Nirankari, Delhi 110009, INDE
Téléphone : +91 11 2760 1283/4536
Courriel : bkwell@nde.vsnl.net.in • Site web : http://www.bookwellindia.com

ITALIE

Libreria Scientifica "AEIOU"
Via Vincenzo Maria Coronelli 6, 20146 Milan, ITALIE
Téléphone : +39 02 48 95 45 52 • Fax : +39 02 48 95 45 48
Courriel : info@libreriaaeiou.eu • Site web : http://www.libreriaaeiou.eu

JAPON

Maruzen Co., Ltd.
1-9-18 Kaigan, Minato-ku, Tokyo 105-0022, JAPON
Téléphone : +81 3 6367 6047 • Fax : +81 3 6367 6160
Courriel : journal@maruzen.co.jp • Site web : http://maruzen.co.jp

RÉPUBLIQUE TCHÈQUE

Suweco CZ, s.r.o.
SESTUPNÁ 153/11, 162 00 Prague 6, RÉPUBLIQUE TCHÈQUE
Téléphone : +420 242 459 205, • fax : +420 284 821 646
Courriel : nakup@suweco.cz • Site web : http://www.suweco.cz

ROYAUME-UNI

The Stationery Office Ltd. (TSO)
St. Crispins House, Duke Street, Norwich, NR3 1PD, ROYAUME-UNI
Téléphone : +44 (0) 333 202 5070
Courriel : customer.services@tso.co.uk • Site web : http://www.tso.co.uk

Les commandes de publications destinées ou non à la vente peuvent être adressées directement à :

Section d'édition de l'AIEA, 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 • Fax : +43 1 2600 29302
Courriel : sales.publications@iaea.org • Site web : http://www.iaea.org/books

La présente publication contient des orientations détaillées sur l'identification des zones vitales. Elle présente une approche structurée visant à identifier les zones où se trouvent les équipements, systèmes et composants qui doivent être protégés contre le sabotage. La méthode s'appuie sur des analyses de la sûreté pour mettre au point des modèles logiques de sabotage pour des scénarios de sabotage qui pourraient avoir des conséquences radiologiques inacceptables. Les actes de sabotage représentés dans les modèles logiques sont liés aux zones depuis lesquelles ils peuvent être commis. Les modèles logiques sont ensuite analysés afin de déterminer les zones qui devraient être protégées pour prévenir ces conséquences radiologiques inacceptables.

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE
ISBN 978–92–0–210915–5
ISSN 1816–9317