

La présente publication a été remplacée par la publication suivante : 17-T (Rev. 1).

Collection Sécurité nucléaire de l'AIEA – N° 17

Orientations techniques
Manuel de référence

La sécurité informatique dans les 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 (prévention, détection, intervention) contre le vol, le sabotage et la cession illégale de matières nucléaires et de sources radioactives et des installations connexes, l'accès non autorisé à ces matières, sources et installations et les autres actes malveillants dont elles peuvent faire l'objet. Ces publications sont conformes aux instruments internationaux relatifs à la sécurité nucléaire, notamment la Convention sur la protection physique des matières nucléaires telle qu'amendée, le Code de conduite sur la sûreté et la sécurité des sources radioactives, les résolutions 1373 et 1540 du Conseil de sécurité de l'ONU et la Convention internationale pour la répression des actes de terrorisme nucléaire, et elles les complètent.

CATÉGORIES DANS LA COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA

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

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

RÉDACTION ET EXAMEN

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

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

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

La présente publication a été remplacée par la publication suivante : 17-T (Rev. 1).

LA SÉCURITÉ INFORMATIQUE
DANS LES INSTALLATIONS
NUCLÉAIRES

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

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

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

COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA — N° 17

ORIENTATIONS TECHNIQUES

LA SÉCURITÉ INFORMATIQUE DANS LES INSTALLATIONS NUCLÉAIRES

MANUEL DE RÉFÉRENCE

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE, 2013

DROIT 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, 2013

Imprimé par l'AIEA en Autriche

Janvier 2013

**LA SÉCURITÉ INFORMATIQUE
DANS LES INSTALLATIONS NUCLÉAIRES**

AIEA, VIENNE, 2013

STI/PUB/1527

ISBN 978-92-0-237010-4

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 répondu à ce risque en prenant l'engagement collectif de renforcer la protection et le contrôle de ces matières et d'intervenir efficacement en cas d'événement de sécurité nucléaire. Ils sont convenus de renforcer les instruments existants et ont établi de nouveaux instruments juridiques internationaux pour améliorer la sécurité nucléaire à l'échelle mondiale. La sécurité nucléaire est capitale pour la gestion des technologies nucléaires et les applications mettant en jeu l'utilisation ou le transport de matières nucléaires ou autres matières radioactives.

Par le biais de son Programme sur la 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 exhaustive de la sécurité nucléaire tenant compte du fait que tout régime national de sécurité nucléaire efficace repose 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 et la répression du trafic de ces matières ; les plans nationaux d'intervention et les mesures d'urgence. Par sa collection Sécurité nucléaire, l'AIEA s'emploie à aider les États à mettre en œuvre et à soutenir un tel régime d'une manière cohérente et intégrée.

Cette collection regroupe les catégories 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.

La responsabilité de la sécurité nucléaire incombe entièrement à chaque État, qui doit, en particulier, garantir la sécurité des matières nucléaires et autres matières radioactives, ainsi que des installations et des activités connexes ; assurer la sécurité de ces matières en cours d'utilisation, d'entreposage et de transport ; lutter contre le trafic illicite et les mouvements fortuits de ces matières ; et être prêt à intervenir en cas d'événement de sécurité nucléaire.

La présente publication, qui fait partie de la catégorie Orientations techniques de la collection Sécurité nucléaire de l'AIEA, est consacrée à la sécurité informatique dans les installations nucléaires. Elle est basée sur l'expérience et les pratiques nationales, ainsi que sur des publications traitant de la sécurité informatique et de la sécurité nucléaire. Les orientations sont présentées pour examen par les États, les autorités compétentes et les exploitants.

L'élaboration de la présente publication de la collection Sécurité nucléaire de l'AIEA a été rendue possible par le concours d'un grand nombre d'experts d'États Membres. C'est le fruit d'un vaste processus de consultation de tous les

États Membres comprenant des réunions de consultants et des réunions techniques à participation non limitée. Le projet de document a ensuite été envoyé à tous les États Membres pour 120 jours afin de recueillir d'autres observations et suggestions. Les observations reçues des États Membres ont été examinées et prises en compte dans la version finale de la présente publication.

NOTE DE L'ÉDITEUR

Le présent rapport n'examine pas les questions de responsabilité, qu'elle soit juridique ou non, pour des actes ou des omissions imputables à une personne.

Bien qu'un soin particulier ait été pris pour assurer la précision des informations contenues dans la présente publication, l'AIEA, tout comme ses États Membres, déclinent toute responsabilité relativement aux conséquences pouvant dériver de son utilisation.

L'utilisation de désignations particulières de pays ou de territoires ne suppose aucun jugement de l'éditeur, l'AIEA, concernant le statut juridique de ces pays ou territoires, de leurs autorités et institutions ou de la délimitation de leurs frontières.

La mention de noms d'entreprises ou de produits spécifiques (qu'il soit ou non précisé qu'ils sont enregistrés) n'implique aucune intention de porter atteinte aux droits de propriété et ne doit pas non plus être interprétée comme un soutien ou une recommandation de la part de l'AIEA.

TABLE DES MATIÈRES

1.	INTRODUCTION	1
1.1.	Contexte	1
1.2.	Objectif	1
1.2.1.	Objectifs de la sécurité nucléaire et de la sécurité informatique	1
1.2.2.	Champ d'application	2
1.3.	Conditions propres aux installations nucléaires	3
1.4.	Structure	3
1.5.	Méthodologie	4
1.6.	Termes clés	5
	PARTIE I. GUIDE DE GESTION	7
2.	CONSIDÉRATIONS RELATIVES À LA RÉGLEMENTATION ET À LA GESTION	9
2.1.	Considérations juridiques	10
2.2.	Considérations relatives à la réglementation	11
2.3.	Cadre de sécurité du site	12
2.3.1.	Politique de sécurité informatique	13
2.3.2.	Systèmes informatiques des installations nucléaires ...	13
2.3.3.	Défense en profondeur	14
2.4.	Évaluation du contexte de la menace	14
3.	SYSTÈMES DE GESTION	15
4.	QUESTIONS D'ORDRE ORGANISATIONNEL	17
4.1.	Pouvoirs et responsabilités	17
4.1.1.	Direction	17
4.1.2.	Responsable de la sécurité informatique	17
4.1.3.	Équipe de sécurité informatique	19
4.1.4.	Autres responsabilités de la direction	19
4.1.5.	Responsabilités individuelles	19
4.2.	Culture de sécurité informatique	20
4.2.1.	Programme de formation en sécurité informatique	21

PARTIE II. GUIDE D'APPLICATION	23
5. GARANTIR LA SÉCURITÉ INFORMATIQUE	25
5.1. Plan et politique de sécurité informatique	25
5.1.1. Politique de sécurité informatique	25
5.1.2. Plan de sécurité informatique	25
5.1.3. Éléments du plan de sécurité informatique	26
5.2. Interaction avec d'autres domaines de la sécurité	27
5.2.1. Sécurité physique	27
5.2.2. Sécurité du personnel	28
5.3. Analyse et gestion des actifs	28
5.4. Classification des systèmes informatiques	29
5.4.1. Importance sur le plan de la sûreté	30
5.4.2. Systèmes de sécurité ou liés à la sécurité	32
5.5. Approche graduée de la sécurité informatique	32
5.5.1. Niveaux de sécurité	33
5.5.2. Zones	33
5.5.3. Exemple d'application d'un modèle des niveaux de sécurité	34
5.5.4. Zones de découplage	39
6. MENACES, VULNÉRABILITÉS ET GESTION DES RISQUES	39
6.1. Concepts de base et liens divers	40
6.2. Évaluation et gestion des risques	40
6.3. Recensement et détermination des menaces	42
6.3.1. Menace de référence	43
6.3.2. Profil des assaillants	43
6.3.3. Scénarios d'attaque	43
6.4. Résultats simplifiés d'une évaluation des risques	44
7. CONSIDÉRATIONS PARTICULIÈRES POUR LES INSTALLATIONS NUCLÉAIRES	49
7.1. Phases du cycle de vie et modes de fonctionnement d'une installation	50
7.2. Différences entre les systèmes de ti et les systèmes de contrôle industriel	50
7.3. Demande de connectivité supplémentaire et conséquences associées	52

7.4. Considérations concernant les mises à jour de logiciels	53
7.5. Conception sécurisée et spécifications relatives aux systèmes informatiques	53
7.6. Procédure de contrôle d'accès pour les tiers/fournisseurs	54
RÉFÉRENCES	55
BIBLIOGRAPHIE	57
ANNEXE I: SCÉNARIOS D'ATTAQUE CONTRE LES SYSTÈMES DES INSTALLATIONS NUCLÉAIRES	59
ANNEXE II: MÉTHODOLOGIE DE DÉTERMINATION DES EXIGENCES EN SÉCURITÉ INFORMATIQUE	64
ANNEXE III: RÔLE DE L'ERREUR HUMAINE EN SÉCURITÉ INFORMATIQUE	69
DÉFINITIONS	73

La présente publication a été remplacée par la publication suivante : 17-T (Rev. 1).

1. INTRODUCTION

1.1. CONTEXTE

Devant la preuve manifeste et récurrente de la vulnérabilité des systèmes informatiques, l'attention portée à la sécurité informatique s'est intensifiée ces dix dernières années. On a constaté que l'exploitation malveillante de ces vulnérabilités avait une fréquence et un impact de plus en plus grands. Dans un scénario de menace de plus en plus complexe, l'éventualité d'un cyber terrorisme comme moyen d'attaquer une infrastructure d'intérêt majeur dans un État a incité un certain nombre d'autorités nationales à préparer des moyens de défense et à publier une réglementation nouvelle. Cette réglementation prévoit des prescriptions en matière de sécurité informatique qui concernent les installations nucléaires à plusieurs niveaux et à différents stades d'exploitation. Parallèlement, la sécurité de l'information a très vite évolué, générant une gamme très riche de meilleures pratiques internationales et de documents normatifs, dont la norme ISO/CEI 27000 [1–5] qui a rapidement acquis un grand intérêt.

Tout en reconnaissant la validité intrinsèque de la série ISO 27000 et d'autres normes industrielles et commerciales, l'AIEA souhaite se concentrer sur les conditions spécifiques qui affectent la sécurité informatique dans les installations nucléaires. Elle a donc besoin d'une publication dans laquelle sont présentées les orientations pertinentes et les solutions adéquates. La présente publication se veut la somme des connaissances et de l'expérience de spécialistes qui ont appliqué, testé et passé en revue les orientations et les normes de sécurité informatique dans des installations nucléaires et autres infrastructures d'intérêt majeur. Elle réunit et présente les dispositions spéciales, les meilleures pratiques et les enseignements tirés qui s'appliquent dans le domaine nucléaire et elle les insère dans un programme de sécurité compatible avec les autres orientations de l'AIEA et les normes industrielles en vigueur.

1.2. OBJECTIF

1.2.1. Objectifs de la sécurité nucléaire et de la sécurité informatique

La sécurité nucléaire suppose la prévention, la détection et l'intervention en cas d'actes criminels ou d'actes non autorisés délibérés, mettant en jeu ou visant *des matières nucléaires, d'autres matières radioactives, des installations associées ou des activités associées*, qui pourraient avoir directement ou

indirectement des conséquences néfastes pour les personnes, les biens, la société ou l'environnement.

La sécurité informatique joue un rôle de plus en plus crucial dans la réalisation de ces objectifs. La présente publication porte donc sur la mise en place et l'amélioration des programmes visant à protéger les systèmes et les réseaux informatiques ou autres systèmes numériques qui sont déterminants pour exploiter l'installation de manière sûre et sécurisée et pour prévenir le vol, le sabotage ou d'autres actes malveillants.

Les dispositions de la présente publication s'étendront à tous les autres systèmes requis pour l'exploitation de l'installation, ou à tout système d'appui ou système interne dont la modification ou le remplacement non autorisé pourrait compromettre le degré de sécurité ou l'exploitabilité.

Dans ce contexte, les actes malveillants faisant intervenir des systèmes informatiques et concernant la sécurité nucléaire peuvent être regroupés comme suit :

- Attaques pour la collecte d'informations en vue de planifier et d'exécuter de nouveaux actes malveillants ;
- Attaques désactivant ou compromettant les attributs d'un ou de plusieurs ordinateurs cruciaux pour la sécurité ou la sûreté de l'installation ;
- Atteinte d'un ou de plusieurs ordinateurs simultanément à d'autres modes d'attaque, comme l'intrusion physique dans des emplacements ciblés.

Les objectifs en matière de sécurité informatique consistent en général à protéger la confidentialité, l'intégrité et la disponibilité d'attributs de données électroniques ou de systèmes et processus informatiques. Pour atteindre ces objectifs de sécurité, il convient de recenser et de protéger les attributs de données ou de systèmes susceptibles d'avoir un impact négatif sur les fonctions de sûreté dans les installations nucléaires.

1.2.2. Champ d'application

La présente publication vise essentiellement à faire prendre conscience de l'importance d'intégrer la sécurité informatique comme élément fondamental du plan de sécurité global des installations nucléaires.

Elle a en outre pour objectif de fournir des orientations propres aux installations nucléaires sur la mise en service d'un programme de sécurité informatique. Il convient à cette fin de proposer quelques approches, structures et procédures d'application qui sont conçues pour les installations nucléaires et qui sont toutes déterminantes pour l'obtention et le maintien du niveau de protection

défini dans la stratégie de sécurité du site et pour la conformité aux objectifs nationaux de sécurité nucléaire.

Le présent manuel de référence a aussi pour but de donner des conseils sur l'évaluation des programmes existants et des ressources numériques clés ainsi que sur la détermination des mesures appropriées pour la réduction des risques.

1.3. CONDITIONS PROPRES AUX INSTALLATIONS NUCLÉAIRES

Compte tenu des conditions spéciales qui caractérisent cette industrie, des orientations sur la sécurité informatique dans les installations nucléaires s'imposent. La liste ci-dessous donne un bref aperçu de ces conditions, qui seront traitées intégralement dans la présente publication :

- Les installations nucléaires doivent respecter les prescriptions établies par leur organisme de réglementation national, lequel peut réglementer directement ou indirectement les systèmes informatiques ou fixer des orientations.
- Les installations nucléaires peuvent avoir besoin de se protéger contre des menaces additionnelles qui ne sont pas habituellement prises en considération par d'autres industries. De telles menaces peuvent aussi résulter du caractère sensible de l'industrie nucléaire.
- Les prescriptions en matière de sécurité informatique s'adressant aux installations nucléaires peuvent différer des prescriptions s'adressant à d'autres industries. Les activités classiques d'une entreprise ne supposent qu'un nombre de prescriptions limité. Les installations nucléaires ont besoin de prendre en compte une base plus large ou une série complètement différente de considérations que, par exemple, le commerce électronique, les banques ou même les applications militaires. Ces différences sont indiquées et expliquées en détail dans la section 7.

1.4. STRUCTURE

Les orientations figurant dans la présente publication visent une large audience, notamment les décideurs, les responsables de la réglementation en matière de sécurité nucléaire, la direction dans les installations nucléaires, le personnel doté de responsabilités en matière de sécurité, le personnel technique, les vendeurs et les sous-traitants. Elles s'appliquent à tous les stades du cycle de vie des systèmes de l'installation, y compris la conception, l'élaboration, l'exploitation et la maintenance.

La présente publication comprend deux parties :

- La partie I (sections 2–4) a pour but d’aider les responsables à émettre des avis judicieux et à prendre des décisions éclairées en ce qui concerne la politique à appliquer, la conception et la gestion en matière de sécurité informatique dans les installations. Elle donne des orientations sur les dispositions en matière de réglementation et de gestion de la sécurité informatique.
- La partie II (sections 5–7) donne des orientations techniques et administratives pour la mise en œuvre d’un plan exhaustif de sécurité informatique.

1.5. MÉTHODOLOGIE

La méthode de base utilisée pour la sécurité informatique est similaire aux méthodes utilisées pour la sécurité et la sûreté nucléaires. D’où la nécessité et l’intérêt d’intégrer dès le début la sécurité informatique dans les plans généraux de sécurité de l’installation.

On peut parvenir à une protection efficace des systèmes informatiques en adaptant les méthodes et outils élaborés selon les meilleures pratiques dans le milieu de la sécurité informatique au sens large, tout en y intégrant les spécificités de l’industrie nucléaire.

La procédure logique suivante, présentée en détail dans la section 5, montre comment une installation nucléaire peut élaborer, appliquer, maintenir et améliorer la sécurité informatique :

- Suivre les prescriptions juridiques et réglementaires nationales ;
- Examiner les orientations pertinentes de l’AIEA et d’autres organismes internationaux ;
- S’assurer l’appui de la direction ainsi que des ressources suffisantes ;
- Définir un périmètre de sécurité informatique ;
- Recenser les interactions entre la sécurité informatique et l’exploitation de l’installation, la sûreté nucléaire et d’autres aspects liés à la sécurité du site ;
- Créer une politique de sécurité informatique ;
- Procéder à l’évaluation du risque ;
- Sélectionner, concevoir et appliquer des mesures protectrices de sécurité informatique ;
- Intégrer la sécurité informatique dans le système de gestion de l’installation ;

- Procéder à intervalles réguliers à la vérification, l'examen et l'amélioration du système.

La présente publication examinera plus en détail les étapes de la méthodologie où il existe des dispositions propres aux installations nucléaires. D'autres stades de méthodologie en matière de sécurité informatique peuvent être mis en œuvre en se référant directement aux normes nationales et internationales en vigueur (voir les références à la fin de la présente publication).

1.6. TERMES CLÉS

Du fait que les termes reflètent des sens différents suivant les différentes communautés de pratiques, la présente section clarifie le sens de certains termes importants employés tout au long de la publication.

Dans le contexte de la présente publication, on entend par **ordinateurs** et par **systèmes informatiques** des dispositifs de calcul, de communication, de contrôle et de commande constituant les éléments fonctionnels de l'installation nucléaire. Il s'agit non seulement des ordinateurs de bureau, des systèmes centraux, des serveurs et des dispositifs de réseaux, mais aussi des composants de niveau inférieur comme les systèmes intégrés et les PLC (automates programmables). La présente publication s'intéresse essentiellement à tous les composants susceptibles de subir une atteinte électronique.

Tout au long de la présente publication, l'expression **sécurité informatique** sera employée pour traiter de la sécurité de tous les ordinateurs tels qu'ils sont définis ci-dessus et de tous les systèmes et réseaux interconnectés qui sont constitués par la somme des éléments. Les expressions **sécurité TI** et **cyber sécurité** sont, aux fins de la présente publication, considérées comme des synonymes de sécurité informatique et ne seront pas employées ici.

La sécurité informatique telle qu'elle est définie ici est un sous-ensemble de la **sécurité de l'information** (comme définie par exemple dans ISO/IEC 27000 [1]) avec laquelle elle partage un grand nombre des objectifs, la méthodologie et la terminologie.

La définition d'autres termes employés dans la présente publication figure à la fin du document.

La présente publication a été remplacée par la publication suivante : 17-T (Rev. 1).

La présente publication a été remplacée par la publication suivante : 17-T (Rev. 1).

Partie I

GUIDE DE GESTION

La présente publication a été remplacée par la publication suivante : 17-T (Rev. 1).

2. CONSIDÉRATIONS RELATIVES À LA RÉGLEMENTATION ET À LA GESTION

La présente section fait ressortir les composantes essentielles du cadre de haut niveau pour la sécurité informatique des installations nucléaires. Elle traite en particulier des questions intéressant les organes législatifs et réglementaires ainsi que l'encadrement et la stratégie de sécurité des installations. La figure 1 présente un schéma simplifié de la hiérarchie des instruments normatifs importants pour l'établissement et l'application du programme de sécurité informatique d'une installation nucléaire.

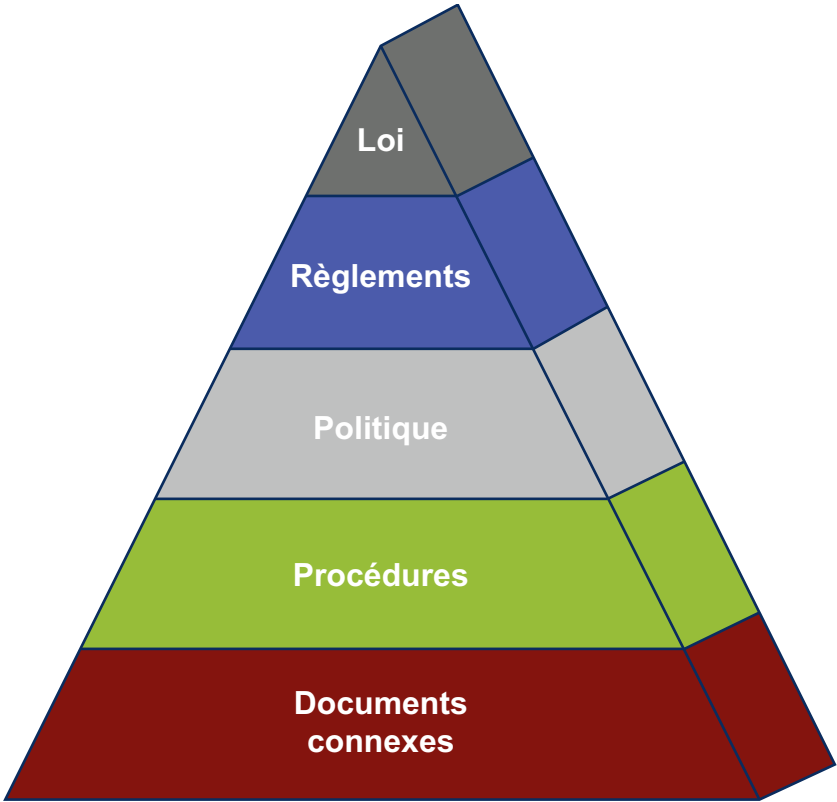


FIG. 1. Instruments normatifs pertinents.

2.1. CONSIDÉRATIONS JURIDIQUES

Un rôle clé de l'État est d'établir un cadre juridique pour la sécurité nucléaire et un cadre pour la sécurité informatique en général. Bien appliqués, ces cadres devraient avoir une incidence majeure sur la sûreté et la sécurité des installations nucléaires. Le système juridique de l'État devrait au moins prévoir un cadre législatif et réglementaire couvrant la protection des informations sensibles et visant toute activité susceptible de déboucher sur des atteintes à la sécurité nucléaire.

Compte tenu de la spécificité de ses éléments, la sécurité informatique peut nécessiter des dispositions législatives particulières afin de tenir compte des actes criminels et des modes opératoires typiquement associés aux systèmes informatiques. Les États devraient examiner attentivement leur législation en vigueur pour savoir si elle couvre, comme il convient, les actes malveillants pouvant être perpétrés à l'aide d'ordinateurs. Les lois importantes pouvant avoir une incidence sur la sécurité informatique et sa mise en œuvre sont notamment les suivantes :

- Les lois relatives aux délits informatiques ;
- Les lois relatives au terrorisme ;
- Les lois relatives à la protection des infrastructures essentielles nationales ;
- Les lois régissant la diffusion de l'information ;
- Les lois relatives au respect de la vie privée et au traitement des informations personnelles.

Il est important que la législation de l'État soit continuellement réexaminée et actualisée pour intégrer des dispositions visant les activités criminelles nouvelles et émergentes ainsi que toute autre menace potentielle à la sécurité informatique.

Compte tenu de la nature des réseaux informatiques, il est possible que des agresseurs se livrent à des actes malveillants à l'intérieur d'un État tout en étant hors de ses frontières physiques et soient ainsi hors d'atteinte du système judiciaire de l'État. À la date de rédaction de la présente publication, le seul instrument juridique international dans ce domaine, consacré à la réglementation de la coopération internationale sur la criminalité informatique, était la Convention sur la cybercriminalité du Conseil de l'Europe [6].

2.2. CONSIDÉRATIONS RELATIVES À LA RÉGLEMENTATION

L'organisme de réglementation devrait tenir compte de la législation applicable dans ses orientations et mettre à la disposition des exploitants les outils et les moyens d'interpréter correctement et d'observer les obligations juridiques. Les responsables de la réglementation pourraient aussi sélectionner ou indiquer des orientations de référence pertinentes comme les normes ISO ou les publications de l'AIEA.

Les activités des responsables de la réglementation concernant la sécurité informatique devraient reconnaître expressément l'objectif de protection contre le vol de matières nucléaires et le sabotage pouvant entraîner des rejets radioactifs. Par conséquent, les règlements relatifs à la sécurité et à la sûreté nucléaires devraient aussi être pris en considération lors de l'élaboration de règlements sur la sécurité informatique.

Il est souhaitable que les organismes de réglementation de l'État (lorsque plusieurs sont concernés) collaborent afin d'harmoniser les points de vue sur les prescriptions qui doivent être fixées.

Les organismes de réglementation de l'État pourraient au moins formuler à un haut niveau les prescriptions réglementaires en matière de sécurité informatique. Des prescriptions réglementaires plus détaillées pourraient en outre prévoir des dispositions dans les domaines suivants :

- Engagement de la direction en matière de sécurité informatique (section 4).
- Prise en charge du programme de sécurité informatique, définissant notamment les attributions du (des) responsable(s) et de l'équipe (ou des équipes) chargés de la sécurité informatique (section 4).
- Politique de sécurité informatique, plan d'application et plan d'exécution (section 5), comprenant les points suivants :
 - Détermination du périmètre de sécurité informatique ;
 - Recensement des risques ;
 - Stratégie de gestion des risques ;
 - Programme de formation et de sensibilisation à la sécurité informatique ;
 - Continuité du plan des opérations.
- Processus de vérification et d'examen, pouvant être conduit au niveau interne ou externe, ou par les responsables de la réglementation eux-mêmes.

Les prescriptions ne devraient pas recommander de solutions techniques détaillées, car l'évolution dans ce domaine peut rapidement rendre de tels détails obsolètes. Elles pourraient en revanche être axées sur les effets attendus car ceux-ci peuvent être formulés de manière à dépendre moins des technologies.

Des dispositifs peuvent être nécessaires pour démontrer la conformité aux prescriptions de sécurité nationales, dans le cadre d'un plan approuvé pour la sécurité générale du site ou de tout ensemble équivalent de documents. **Les organismes de réglementation de l'État devraient inclure des prescriptions pour la sécurité informatique dans celles du plan de sécurité du site.**

2.3. CADRE DE SÉCURITÉ DU SITE

La sécurité du site relève en premier lieu de la responsabilité de la direction, en particulier des hauts responsables, de veiller à ce que les prescriptions législatives et réglementaires soient pleinement respectées lors de la mise en œuvre du plan de sécurité du site.

Tous les domaines de la sécurité (y compris le personnel, la sécurité physique, la sécurité des informations et la sécurité informatique) s'influencent et se complètent mutuellement pour déterminer les caractéristiques de sécurité d'une installation, telle qu'elle peut être définie dans le plan de sécurité du site (voir la figure 2). Toute défaillance dans l'un de ces domaines peut avoir un impact sur les autres et imposer des exigences supplémentaires aux aspects de sécurité restants. La sécurité informatique est un domaine transversal qui a des interactions avec tous les autres domaines de la sécurité d'une installation nucléaire.

Toutes les dispositions figurant dans la présente publication devraient être appliquées en tenant constamment compte du cadre plus général du plan de

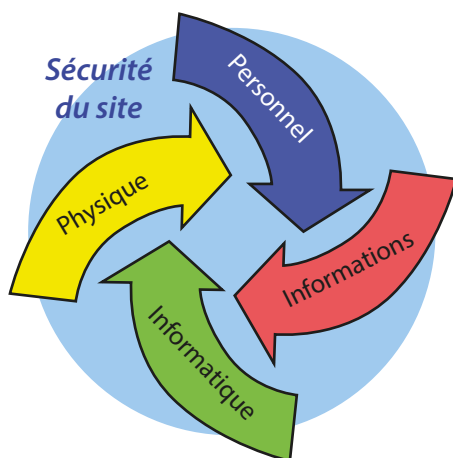


FIG. 2. Interactions entre les différents domaines de sécurité.

sécurité du site. De même, ce plan devrait être conçu en prenant en considération la sécurité informatique dès le départ.

La direction a en outre la responsabilité d'assurer une bonne coordination des différents domaines de la sécurité et l'intégration de la sécurité informatique au niveau approprié.

2.3.1. Politique de sécurité informatique

La direction devrait savoir que la technologie informatique est de plus en plus utilisée pour de nombreuses fonctions cruciales des installations nucléaires. Cette évolution a entraîné des avantages multiples pour la sûreté et l'efficacité des opérations. Néanmoins, pour assurer une bonne fonctionnalité du système informatique, il faut avoir en place des barrières de sécurité adéquates et équilibrées pour optimiser la protection contre les actes malveillants sans entraver inutilement les opérations du système.

Toutes les installations nucléaires devraient donc avoir une politique de sécurité informatique, approuvée et mise en application par le plus haut responsable du site. Cette politique précise l'ensemble des objectifs de sécurité informatique de l'installation.

La politique de sécurité informatique devrait faire partie intégrante de la politique de sécurité générale du site et être négociée et coordonnée en fonction des autres responsabilités en matière de sécurité. Lors de l'élaboration d'une politique de sécurité informatique, ses effets sur le plan juridique et des ressources humaines devraient en outre être pris en compte.

La politique de sécurité informatique et le plan connexe sont examinés plus en détail à la section 5.

2.3.2. Systèmes informatiques des installations nucléaires

Les systèmes et les réseaux informatiques appuyant les opérations des installations nucléaires comprennent de nombreux systèmes de technologie de l'information (TI) non courants en termes d'architecture, de configuration ou d'exigences de performance. Parmi eux peuvent figurer des systèmes de contrôle industriel spécialisés, des systèmes de contrôle d'accès, des systèmes d'alarme et de suivi, et des systèmes d'information relatifs à la sûreté et à la sécurité et aux interventions d'urgence. Bien que les systèmes de contrôle industriel spécialisés aient évolué, passant d'applications strictement exclusives à une architecture informatique plus courante, il subsiste des différences considérables entre eux et les systèmes de TI standard, qui doivent être prises en compte lors de l'élaboration du plan de sécurité du site. Un examen complet des particularités des systèmes informatiques des installations nucléaires est présenté à la section 7.

2.3.3. Défense en profondeur

Les prescriptions de protection devraient tenir compte du concept de niveaux et modalités de protection multiples (qu'ils soient structurels ou techniques, concernant le personnel ou organisationnels) que doit surmonter ou contourner un agresseur pour atteindre ses objectifs.

Le principal moyen de prévenir et d'atténuer les conséquences des atteintes à la sécurité est la « défense en profondeur ». Elle est essentiellement mise en œuvre à travers un ensemble de niveaux de protection consécutifs et indépendants qui doivent faillir ou être déjoués avant qu'un système informatique ne puisse être violé. En cas de défaillance d'un niveau ou d'une barrière de protection, le niveau ou la barrière suivant prend le relais. Bien appliquée, la défense en profondeur empêche une défaillance technique, humaine ou organisationnelle de permettre à elle seule la violation d'un système informatique, et réduit la probabilité des combinaisons de défaillances susceptibles d'entraîner un incident informatique à un très faible niveau. L'efficacité indépendante des différents niveaux de défense est un élément nécessaire de la défense en profondeur.

2.4. ÉVALUATION DU CONTEXTE DE LA MENACE

Le contexte de la menace à la sécurité informatique change et évolue rapidement. Même si un bon programme de sécurité informatique assure sa propre durabilité, les contrôles particuliers mis en place contre les menaces les plus courantes d'aujourd'hui ne garantissent pas une protection contre les menaces de demain.

L'autorité nationale responsable devrait publier périodiquement une évaluation de la menace, notamment des menaces à la sécurité des systèmes informatiques, et des informations relatives aux moyens d'attaque actuels utilisés contre la sécurité des systèmes informatiques des installations nucléaires. Un outil généralement utilisé pour déterminer les niveaux de menace et servant de base à la détermination des caractéristiques de sécurité est la menace de référence (voir la section 6.3.1).

Il est essentiel que les installations maintiennent une évaluation active et continue de la menace, communiquée régulièrement à la direction et au personnel des opérations.

La section 6 donne une description détaillée, mais non exhaustive, des sources d'attaque potentielles et de leurs mécanismes d'attaque contre des installations nucléaires, ainsi que des méthodologies utilisées pour évaluer et déterminer les menaces.

3. SYSTÈMES DE GESTION

Un système de gestion sert à établir les politiques et les objectifs et permet d'atteindre ces derniers de façon efficiente et efficace. Les systèmes de gestion sont des éléments d'appui essentiels à la culture de sécurité nucléaire. De nombreuses activités des installations nucléaires sont contrôlées par des systèmes de gestion. Ces derniers intègrent, dans l'idéal, des éléments relatifs à la sécurité, à la sûreté, à la santé, à l'environnement, à la qualité et à l'économie dans un outil de gestion unique ou dans un ensemble de systèmes intégrés qui se renforcent mutuellement [7, 8].

Les systèmes de gestion doivent être examinés pour garantir leur exhaustivité et leur conformité aux politiques de sécurité du site. Plus généralement, ils sont dynamiques par nature et doivent être adaptés aux conditions changeantes de l'installation et de l'environnement ; ils ne peuvent être mis en place comme mesure ponctuelle, mais doivent être continuellement évalués et améliorés. La figure 3 illustre le cycle de vie des processus de gestion.

La présente section vise à compléter les orientations relatives aux systèmes de gestion en donnant les détails nécessaires sur la gestion de la sécurité informatique. Les éléments clés à examiner ou à ajouter pour intégrer les dispositions de sécurité informatique nécessaires sont les suivants :

- Recensement et classification des ressources d'informations ;
- Analyse des risques formelle ;
- Conformité aux lois et aux réglementations ;
- Prescriptions opérationnelles ;
- Compétences requises pour les postes clés ;
- Continuité des opérations ;
- Gestion de l'accès logique ;
- Sécurité du cycle de vie des systèmes ;
- Gestion de la configuration ;
- Modification et approbation des mesures de sécurité informatique ;
- Application des mesures de sécurité informatique recensées ;
- Acceptation des mesures de sécurité informatique appliquées ;
- Conformité aux mesures de sécurité informatique approuvées ;
- Analyse immédiate des incidents de sécurité informatique et notification appropriée ;
- Établissement régulier de rapports sur la conformité ;
- Examens réguliers des mesures de sécurité appliquées (vérifications) par des parties internes et externes ;
- Formation à la sensibilisation ;

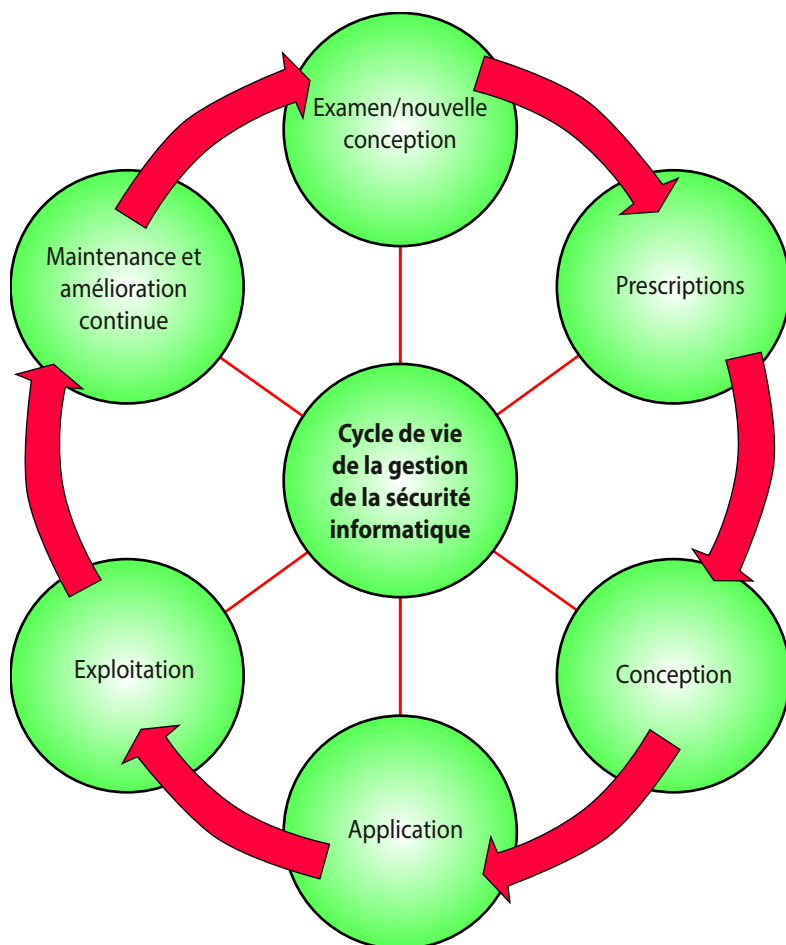


FIG. 3. Cycle de vie de la gestion de la sécurité.

- Nouveaux risques et évolution des risques recensés ;
- Modifications des prescriptions législatives et réglementaires ;
- Plans à moyen terme pour la sécurité de l'information.

Les processus décrits ci-dessus devraient être considérés comme des activités continues couvrant toutes les phases du cycle de vie des systèmes. Les détails de l'application devraient être précisés dans le plan de sécurité informatique examiné à la Section 5.

4. QUESTIONS D'ORDRE ORGANISATIONNEL

4.1. POUVOIRS ET RESPONSABILITÉS

Les sections suivantes précisent les prescriptions minimales concernant la direction et le personnel spécialisé nécessaire pour élaborer et maintenir un programme de sécurité informatique avec succès.

4.1.1. Direction

La direction d'une installation met en place la sécurité informatique en instaurant un processus adéquat et une organisation d'appui. Pour ce faire, elle devrait :

- Assumer la responsabilité générale de tous les aspects de la sécurité informatique ;
- Définir les objectifs de sécurité de l'installation ;
- S'assurer du respect des lois et des réglementations ;
- Fixer le degré d'acceptation du risque dans l'installation ;
- Attribuer des responsabilités organisationnelles en matière de sécurité informatique ;
- Assurer une communication adéquate en ce qui concerne les différents aspects de la sécurité ;
- Veiller à la mise en place d'une politique de sécurité informatique applicable ;
- Fournir des ressources adéquates pour la mise en œuvre d'un programme de sécurité informatique viable ;
- Veiller à ce que les politiques et procédures de sécurité informatique soient régulièrement vérifiées et mises à jour ;
- Appuyer les programmes de formation et de sensibilisation.

En règle générale, la mise en œuvre du processus de sécurité informatique permanent est déléguée à des spécialistes au sein de l'organisation.

4.1.2. Responsable de la sécurité informatique

La sécurité informatique concerne pratiquement toutes les activités de l'installation. Il importe donc de confier la surveillance générale de la sécurité informatique à un organe bien défini. On a utilisé le titre de « responsable de la sécurité informatique » dans la présente publication ; dans d'autres cas,

cette fonction peut être désignée par le titre de « responsable de la sécurité de la TI » ou de « responsable de la sécurité de l'information », ou peut être confiée à diverses personnes. Quelle que soit l'approche utilisée, cette fonction devrait être étroitement coordonnée dans l'ensemble de l'installation, rester indépendante des départements chargés de l'application et avoir des rapports hiérarchiques clairs et aisés avec la direction.

Le responsable de la sécurité informatique devrait avoir une connaissance approfondie de la sécurité informatique et une bonne connaissance des autres aspects de la sécurité dans les installations nucléaires. Il devrait aussi avoir une connaissance de la sûreté nucléaire et de la gestion de projets et être capable d'intégrer des personnes issues de disciplines différentes dans une équipe efficace.

Les responsabilités qui incombent généralement à un responsable de la sécurité informatique, ou son équivalent, sont les suivantes :

- Conseiller la direction de l'entreprise sur la sécurité informatique.
- Diriger l'équipe de sécurité informatique.
- Coordonner et contrôler l'élaboration d'activités relatives à la sécurité informatique (par exemple, l'application de politiques, de directives, de procédures, d'orientations et de mesures de sécurité).
- Coopérer avec le personnel chargé de la sécurité physique et d'autres aspects de la sécurité et de la sûreté pour prévoir les mesures de sécurité et intervenir en cas d'incident de sécurité.
- Recenser les systèmes essentiels à la sécurité informatique au sein de l'installation (par exemple, les normes de référence en matière de sécurité informatique). Les propriétaires d'actifs devraient être informés du rôle de leur matériel dans la sécurité informatique.
- Mener des évaluations périodiques des risques liés à la sécurité informatique.
- Conduire des inspections, des vérifications et des examens réguliers des normes de référence en matière de sécurité informatique et fournir des rapports d'étape à la direction.
- Élaborer et conduire une formation et une évaluation sur la sécurité informatique.
- Mettre au point et diriger des interventions pour les situations d'urgence pertinentes concernant la sécurité informatique, et notamment coopérer avec les organismes internes et externes concernés.
- Enquêter sur les incidents de sécurité informatique et mettre au point des procédures à appliquer à la suite d'incidents ainsi que des mesures préventives.
- Participer aux initiatives d'évaluation de la sécurité du site.

- Participer à l'analyse des besoins lors de l'acquisition/de l'élaboration de nouveaux systèmes.

4.1.3. Équipe de sécurité informatique

Il est essentiel que le responsable de la sécurité informatique ait accès à des compétences pluridisciplinaires appropriées dans les domaines de la sécurité informatique, de la sûreté des installations et de l'exploitation des centrales ainsi que de la sécurité physique et du personnel. Il peut s'agir d'une équipe de sécurité informatique dédiée ou d'un accès spécifique à des compétences particulières au sein de l'organisation. Cette équipe devra aider le/la responsable de la sécurité informatique à s'acquitter de ses responsabilités.

4.1.4. Autres responsabilités de la direction

Les responsables de l'organisation à divers niveaux doivent assurer un degré approprié de sécurité informatique dans leur domaine de responsabilité. Ils doivent généralement assumer les responsabilités suivantes :

- Agir conformément aux orientations données dans le plan de sécurité informatique du site ;
- Fournir des prescriptions opérationnelles et des informations en retour au responsable de la sécurité informatique et résoudre les éventuels conflits entre les prescriptions opérationnelles, de sécurité et de sûreté ;
- Signaler au responsable de la sécurité informatique toute circonstance susceptible de modifier les caractéristiques de sécurité informatique, comme les changements de personnel, de matériel ou de processus ;
- Veiller à ce que le personnel soit suffisamment formé et au fait des questions de sécurité informatique pertinentes dans le cadre de ses fonctions ;
- Veiller à ce que les sous-traitants et les vendeurs tiers travaillant pour l'entité contractante agissent dans le contexte du plan de sécurité du site ;
- Suivre, surveiller et signaler les événements pertinents sur le plan de la sécurité ;
- Appliquer les mesures de sécurité du personnel.

4.1.5. Responsabilités individuelles

Chaque membre de l'organisation est responsable de la mise en œuvre du plan de sécurité informatique. En particulier, chacun doit :

- Connaître les procédures de sécurité informatique de base ;
- Connaître les procédures de sécurité informatique propres à son poste ;
- Agir dans les limites des paramètres des politiques de sécurité informatique ;
- Signaler à la direction tout changement susceptible d'affaiblir les caractéristiques de la sécurité informatique ;
- Signaler à la direction tout incident ou tout incident possible pouvant compromettre la sécurité informatique ;
- Assister régulièrement à des formations initiales ou à des remises à niveau relatives à la sécurité.

4.2. CULTURE DE SÉCURITÉ INFORMATIQUE

Une solide culture de sécurité informatique est une composante essentielle de tout plan de sécurité efficace. Il est important que la direction veille à ce que la sensibilisation à la sécurité informatique fasse partie intégrante de la culture de sécurité générale du site. La culture de sécurité se caractérise par des croyances, des attitudes, des comportements et des systèmes de gestion qui, ensemble, accroissent l'efficacité du programme de sécurité nucléaire. Le fondement de la culture de sécurité nucléaire est la reconnaissance — par ceux qui interviennent dans la réglementation, la gestion ou l'exploitation d'installations ou d'activités nucléaires, ou même par ceux sur lesquels ces activités pourraient avoir des incidences — qu'une menace crédible existe et que la sécurité nucléaire est importante. (Pour de plus amples informations sur la culture de sécurité nucléaire, voir Réf. [9].) La culture de sécurité informatique est un sous-ensemble de la culture de sécurité générale et repose sur l'application des caractéristiques susmentionnées à la sensibilisation à la sécurité informatique.

L'expérience montre que la majorité des incidents de sécurité informatique sont d'origine humaine et que la sécurité de tout système informatique dépend largement du comportement de l'ensemble de ses utilisateurs. L'Annexe III donne des exemples d'erreurs humaines pouvant compromettre la sécurité. La culture de sécurité informatique est instaurée par le biais de nombreuses activités conçues pour informer le personnel et faire mieux connaître la sécurité informatique (par exemple des affiches, avis, exposés de la direction, formations, tests, etc.). Ses caractéristiques devraient être périodiquement évaluées et examinées, et continuellement améliorées. Les indicateurs suivants peuvent être utilisés pour évaluer la culture de sécurité informatique dans l'organisation :

- Les prescriptions en matière de sécurité informatique sont clairement consignées et bien comprises par le personnel.

- Des processus et des protocoles clairs et efficaces existent pour l'exploitation des systèmes informatiques, tant à l'intérieur qu'à l'extérieur de l'organisation.
- Le personnel comprend les contrôles effectués dans le cadre du programme de sécurité informatique et est conscient de l'importance de s'y conformer.
- Les systèmes informatiques font l'objet d'une maintenance afin d'être sécurisés et exploités conformément aux normes de référence et aux procédures de sécurité informatique.
- La direction s'engage pleinement en faveur des initiatives relatives à la sécurité et les appuie.

4.2.1. Programme de formation en sécurité informatique

Un solide programme de formation constitue l'une des pierres angulaires de la culture de sécurité informatique. Il est primordial de sensibiliser le personnel, les sous-traitants et les vendeurs tiers à l'importance d'observer les procédures de sécurité et de maintenir une culture de sécurité.

Le programme de sensibilisation devrait répondre notamment aux exigences suivantes :

- Suivre avec succès un programme de formation et/ou de sensibilisation à la sécurité informatique devrait être une condition préalable à l'accès aux systèmes informatiques. La formation devrait être proportionnée aux niveaux de sécurité des systèmes et aux rôles escomptés des utilisateurs.
- Il faudrait renforcer la formation / les qualifications des personnes ayant des responsabilités clés en matière de sécurité (par exemple le responsable de la sécurité informatique, l'équipe de sécurité informatique, les gestionnaires de projets et les administrateurs de TI).
- Il faudrait reprendre périodiquement la formation de l'ensemble du personnel pour tenir compte des procédures et des menaces nouvelles.
- Le personnel devrait être tenu de reconnaître qu'il comprend ses responsabilités en matière de sécurité.

Le programme de formation devrait inclure des paramètres destinés à évaluer la sensibilisation à la sécurité informatique, l'efficacité de la formation et les processus d'amélioration continue ou de remise à niveau.

La présente publication a été remplacée par la publication suivante : 17-T (Rev. 1).

Partie II

GUIDE D'APPLICATION

La présente publication a été remplacée par la publication suivante : 17-T (Rev. 1).

5. GARANTIR LA SÉCURITÉ INFORMATIQUE

La présente publication n'établit pas de normes minimales pour le risque acceptable ni d'ensemble particulier de mesures d'atténuation qui pourraient être utilisées. Un ensemble de normes déterminées serait rapidement dépassé, car les systèmes numériques évoluent, des menaces nouvelles apparaissent, de nouveaux outils d'atténuation deviennent disponibles et les prescriptions réglementaires changent. La partie II de la présente publication a pour objet d'établir un ensemble de recommandations méthodologiques et concrètes pour appuyer et guider l'application de mesures de sécurité informatique dans les installations nucléaires.

Ces recommandations ne sont ni prescriptives ni définitives et devraient servir d'orientations ; au besoin, d'autres mesures peuvent être adoptées pour atteindre le niveau de défense en profondeur souhaité ainsi que d'autres objectifs fondamentaux de sécurité nucléaire (voir [10] à [12]).

5.1. PLAN ET POLITIQUE DE SÉCURITÉ INFORMATIQUE

5.1.1. Politique de sécurité informatique

Comme il a été indiqué à la section 2.3.1, une politique de sécurité informatique fixe les grands objectifs d'une organisation dans ce domaine. Elle doit respecter les prescriptions réglementaires appropriées. Les prescriptions de la politique de sécurité informatique devraient être inscrites dans des documents de catégorie inférieure, qui serviront à appliquer et à contrôler cette politique. Par ailleurs, celle-ci doit être :

- Applicable ;
- Réalisable ;
- Vérifiable.

5.1.2. Plan de sécurité informatique

Le plan de sécurité informatique est l'outil d'application de cette politique et définit les rôles, les responsabilités et les procédures au sein de l'organisation. Il décrit précisément les moyens d'atteindre les objectifs de sécurité informatique dans l'installation et fait partie du plan général de sécurité du site (ou s'y rattache).

Ce plan devrait comprendre les principales dispositions à suivre pour ce qui est de la sensibilité aux vulnérabilités, des mesures de protection, de l'analyse des conséquences et des mesures d'atténuation visant à déterminer et à maintenir le risque informatique acceptable de l'installation nucléaire ainsi qu'à faciliter le retour à un état de fonctionnement sûr.

5.1.3. Éléments du plan de sécurité informatique

S'appuyant sur la politique de sécurité informatique établie, chaque élément du plan vise à atteindre ses propres buts et objectifs. Le plan de sécurité informatique pourrait au moins suivre la structure et comprendre les points ci-après :

- a) Organisation et responsabilités :
 - 1) Organigrammes ;
 - 2) Personnes responsables et responsabilités en matière de rapports ;
 - 3) Processus périodique d'examen et d'approbation.
- b) Gestion des avoirs :
 - 1) Liste de tous les systèmes informatiques ;
 - 2) Liste de toutes les applications des systèmes informatiques ;
 - 3) Schéma du réseau, incluant toutes les connexions à des systèmes informatiques externes.
- c) Évaluation des risques, de la vulnérabilité et de la conformité :
 - 1) Périodicité de l'examen et de la réévaluation du plan de sécurité ;
 - 2) Autoévaluation (y compris les procédures de tests d'intrusion) ;
 - 3) Procédures de vérification et détection et correction de défaillances ;
 - 4) Conformité aux règlements et aux lois.
- d) Conception de la sécurité des systèmes et gestion de la configuration :
 - 1) Architecture fondamentale et principes de conception ;
 - 2) Prescriptions relatives aux différents niveaux de sécurité ;
 - 3) Définition formelle des prescriptions de sécurité informatique pour les fournisseurs et les vendeurs ;
 - 4) Sécurité tout au long du cycle de vie.
- e) Procédures de sécurité opérationnelle :
 - 1) Contrôle de l'accès ;
 - 2) Sécurité des données ;
 - 3) Sécurité de la communication ;
 - 4) Sécurité de la plateforme et des applications (incluant le durcissement) ;
 - 5) Surveillance du système ;
 - 6) Maintien de la sécurité informatique ;
 - 7) Gestion des incidents ;

- 8) Continuité des opérations ;
- 9) Sauvegarde du système.
- f) Gestion du personnel :
 - 1) Enquête de sécurité ;
 - 2) Formation ;
 - 3) Qualification ;
 - 4) Cessation d'emploi/transfert.

Les éléments ci-dessus servent de cadre à l'élaboration d'un plan de sécurité informatique. De nombreuses références sont disponibles pour le compléter, les principales références internationales étant la norme ISO/CEI 27001 [2] pour les systèmes de gestion de la sécurité de l'information et la norme ISO/CEI 27002 [3] pour des recommandations de mise en œuvre.

Même si la majorité des éléments énumérés ci-dessus sont semblables dans les plans de sécurité informatique d'une entreprise ou d'une industrie, il existe toutefois des nuances pour ce qui est de leur mise en œuvre dans les installations nucléaires. Ces éléments du plan de sécurité informatique sont décrits plus en détail à la section 7. L'évaluation des risques, de la vulnérabilité et de la conformité est traitée à la section 6. L'analyse des actifs est décrite plus en détail à la section 5.3.

5.2. INTERACTION AVEC D'AUTRES DOMAINES DE LA SÉCURITÉ

Comme il est indiqué à la section 2.3, le plan de sécurité informatique devrait être exécuté et géré dans le cadre du plan général de protection de l'installation. Le plan de sécurité informatique propre à chaque installation devrait être élaboré en consultation étroite avec des spécialistes des domaines de la protection physique, de la sûreté, des opérations et de la TI. Il doit être régulièrement examiné et actualisé pour prendre en considération les événements de sécurité ainsi que l'expérience d'exploitation du système de sécurité du site.

5.2.1. Sécurité physique

Le plan de sécurité physique et le plan de sécurité informatique devraient se compléter. Les actifs informatisés font l'objet de prescriptions de contrôle d'accès physique, et inversement, une atteinte électronique peut entraîner la dégradation ou la perte de certaines fonctions de protection physique. Les scénarios d'attaque peuvent bien prévoir la coordination d'une attaque électronique et d'une attaque physique. Les équipes responsables du plan de sécurité physique et du plan de sécurité informatique devraient s'informer

mutuellement et coordonner leurs efforts pour assurer la cohérence entre les plans pendant le processus d'élaboration et d'examen.

5.2.2. Sécurité du personnel

Outre la sensibilisation et la formation, d'autres aspects de la sécurité — généralement traités dans le cadre de la sécurité du personnel — sont essentiels pour instaurer un cadre cohérent de sécurité informatique. Les dispositions nécessaires pour obtenir un niveau approprié d'enquête de sécurité, des engagements de confidentialité et des procédures de cessation d'emploi, ainsi que pour définir les compétences professionnelles requises, devraient être coordonnées entre l'administration chargée de la sécurité informatique et celle chargée de la sécurité du personnel. Un niveau d'enquête de sécurité plus élevé peut être requis en particulier pour le personnel ayant des responsabilités clés en matière de sécurité (administrateurs de systèmes, équipe de sécurité).

5.3. ANALYSE ET GESTION DES ACTIFS

L'interaction entre les systèmes informatiques des installations nucléaires peut avoir une incidence non manifeste sur la sécurité. Il est donc important que le plan de sécurité **recense tous les actifs** et comprenne **un inventaire plus exhaustif de ceux qui sont essentiels pour les fonctions de sécurité et de sûreté de l'installation**. Cet inventaire pourrait recouvrir les données, les systèmes informatiques, leurs interfaces et leurs propriétaires.

La méthodologie ci-après répond à ces besoins :

- a) Les informations pertinentes concernant les systèmes informatiques existants devraient être rassemblées afin de dresser une liste complète des actifs ;
- b) L'interconnexion entre les actifs recensés devrait être établie ;
- c) La pertinence pour les fonctions de sûreté et les systèmes de sûreté recensés, les systèmes liés à la sûreté et les systèmes de sécurité devrait être établie et évaluée.

La réalisation exhaustive de chaque étape est une condition essentielle pour passer aux suivantes.

Une analyse exhaustive des systèmes informatiques d'une installation nucléaire porte notamment sur les éléments suivants :

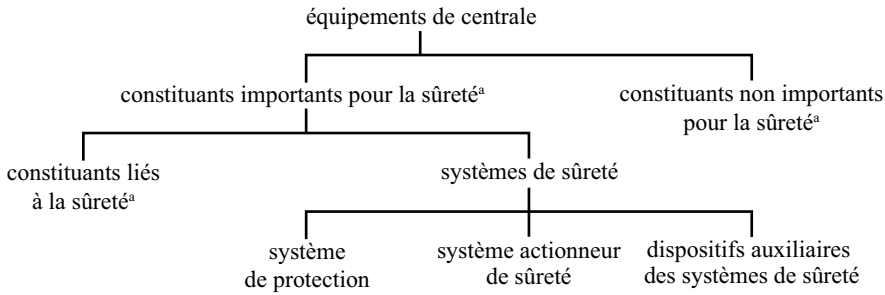
- Fonctions/tâches et modes de fonctionnement de tous les systèmes informatisés existants ;
- Recensement des interconnexions pertinentes, y compris des alimentations électriques ;
- Analyse du flux de données afin de déterminer quels éléments communiquent entre eux, comment et pourquoi ;
- Procédures d'établissement de la communication, fréquence des communications et protocoles ;
- Emplacement des systèmes informatiques et des équipements ;
- Analyse des groupes d'utilisateurs ;
- Propriété (des données et des systèmes informatisés) ;
- Niveau de sécurité correspondant (voir la section 5.5, approche graduée).

On suppose que la plupart des informations nécessaires à l'analyse sont déjà disponibles mais qu'elles devraient être regroupées et organisées. Les sources d'informations pertinentes comprennent les spécifications et les documents concernant les systèmes.

5.4. CLASSIFICATION DES SYSTÈMES INFORMATIQUES

Comme il est défini à la section 1.6, dans le contexte de la présente publication, on entend par ordinateurs et par systèmes informatiques des dispositifs de calcul, de communication, de contrôle et de détection constituant les éléments fonctionnels de l'installation nucléaire. Les fonctions informatiques au premier rang des préoccupations sont les processus relatifs au contrôle et aux données en rapport avec la sûreté et la sécurité. D'autres fonctions informatiques peuvent être un motif de préoccupation en ce qui concerne l'appui des fonctions susmentionnées, les atteintes possibles à la sécurité en raison d'effets secondaires ou indirects, ou la productivité générale de l'installation.

On trouvera ci-après une liste non exhaustive des systèmes informatiques que l'on peut rencontrer dans les installations nucléaires et qui sont importants pour les objectifs des présentes orientations. Ils sont classés séparément, selon leur importance sur les plans de la sûreté et de la sécurité. Ces deux types de classification devraient être pris en considération pour la définition du niveau de sécurité approprié à appliquer (section 5.5) et l'analyse de l'évaluation des risques (section 6.2). Il convient par ailleurs de noter que certaines fonctions sont clairement une source de préoccupation tant sur le plan de la sûreté que de la sécurité.



^a Dans le présent contexte, un « constituant » est une structure, un système ou un composant.

FIG. 4. Équipements de centrale classés selon leur fonction de sûreté.

5.4.1. Importance sur le plan de la sûreté

Les normes de sûreté de l'AIEA (voir par exemple les références [13] à [15]) classent les équipements des installations nucléaires selon leur fonction, comme le montre la figure 4.

Équipements de centrale

— Systèmes importants pour la sûreté

- Systèmes de sûreté

- Systèmes de protection : systèmes de contrôle-commande utilisés pour le déclenchement automatique d'actions protectrices du réacteur et de la centrale.
- Systèmes actionneurs de sûreté : systèmes de contrôle-commande accomplissant des actions de sûreté et déclenchés par les systèmes de protection et par des commandes manuelles.
- Dispositifs auxiliaires des systèmes de sûreté : contrôle-commande servant aux systèmes d'alimentation électrique de secours.

- Systèmes liés à la sûreté

- Systèmes de contrôle des processus : systèmes de contrôle-commande pour le contrôle de la centrale.

- Contrôle-commande de la salle de commande, incluant les systèmes d'alerte.
 - Systèmes informatiques de commande de processus recueillant et préparant les informations pour la salle de commande.
 - Systèmes de contrôle-commande pour la manutention et l'entreposage de combustible.
 - Systèmes de protection contre les incendies.
 - Systèmes de contrôle de l'accès.
 - Infrastructure de communication vocale et de communication de données.
- Systèmes non importants pour la sûreté
- Systèmes de contrôle des fonctions non importants pour la sûreté (comme la déminéralisation)

Il faudrait en outre prêter attention aux systèmes informatiques qui ne relèvent pas nécessairement des équipements de la centrale mais peuvent néanmoins avoir des incidences sur la sûreté.

Équipements non particuliers à une centrale

- Bureautique
- Systèmes d'autorisation et de commande de tâches : systèmes assurant la coordination des activités pour offrir un bon environnement de travail.
 - Systèmes d'ingénierie et de maintenance : systèmes s'occupant des détails de l'exploitation, de la maintenance et de l'appui technique de la centrale.
 - Systèmes de gestion de la configuration : systèmes destinés à suivre l'évolution de la configuration de la centrale, y compris les modèles, les versions et les parties mis en place dans l'installation nucléaire.
 - Systèmes de gestion des documents : systèmes utilisés pour conserver et extraire les informations relatives à la centrale, comme les plans ou les comptes rendus de réunions.
 - Intranet : système donnant accès à toute la documentation de la centrale — tant au niveau technique qu'administratif — sur la base du besoin d'en connaître. Il n'offre normalement qu'un accès en lecture seule.

— Connectivité externe

- Courriel : système utilisé pour transférer des informations à des parties externes.
- Site web public : système utilisé pour donner aux internautes des informations sur l'installation.
- Accès à distance/accès de tiers : systèmes d'accès sous contrôle strict à certaines fonctions d'un site depuis l'extérieur.

5.4.2. Systèmes de sécurité ou liés à la sécurité

Il n'y a pas encore de classification des systèmes de sécurité comme il en existe pour la sûreté. Pourtant, l'établissement d'une telle classification pour les systèmes de sécurité de l'installation constitue une partie importante de l'analyse des actifs. La liste ci-après peut appuyer cette classification :

- Systèmes de contrôle de l'accès physique : systèmes utilisés pour veiller à ce que seules les personnes autorisées accèdent aux zones d'un site qui correspondent à la fonction qu'elles exercent ;
- Infrastructure de communication vocale et de communication de données ;
- Base de données sur les habilitations de sécurité : elle est utilisée pour vérifier que les personnes détiennent l'habilitation de sécurité appropriée pour accéder à une partie du site ou à des informations détenues sur le site ;
- Systèmes de surveillance et de contrôle des alertes de sécurité : ils servent à surveiller toutes les alertes de sécurité sur le site et contribuent à les évaluer ;
- Éléments de sécurité informatique et de sécurité des réseaux ;
- Systèmes de comptabilité et de contrôle des matières nucléaires.

5.5. APPROCHE GRADUÉE DE LA SÉCURITÉ INFORMATIQUE

La sécurité des systèmes informatiques devrait être fondée sur une approche graduée, avec l'application de mesures de sécurité proportionnées aux conséquences éventuelles d'une attaque. Une façon pratique de mettre en œuvre cette approche est de classer les systèmes informatiques en *zones*, auxquelles sont appliqués des principes de protection gradués en fonction du *niveau* des exigences de sécurité attribué à chaque zone. L'affectation des systèmes informatiques à divers niveaux et à diverses zones devrait être basée sur l'importance de ces systèmes pour la sûreté et la sécurité (voir section 5.4).

Néanmoins, **le processus d'évaluation du risque devrait pouvoir enrichir et influencer l'approche graduée.**

5.5.1. Niveaux de sécurité

Les niveaux de sécurité sont une abstraction définissant les degrés de protection de la sécurité requis pour divers systèmes informatiques d'une installation. Dans une approche graduée, il faudra différentes séries de mesures de protection pour chaque niveau en vue de satisfaire aux exigences de sécurité de ce niveau. Certaines mesures de protection s'appliquent à tous les systèmes informatiques de tous les niveaux, alors que d'autres sont spécifiques à certains niveaux.

Le modèle des niveaux de sécurité permet d'affecter plus facilement des mesures de protection aux différents systèmes informatiques, sur la base de la catégorisation du système (son affectation à un niveau) et de la définition de la série de mesures de protection appropriées pour ce niveau.

Les niveaux et les mesures de protection connexes devraient faire l'objet d'une documentation appropriée dans le plan de sécurité informatique.

5.5.2. Zones

Les zones sont un concept logique et physique servant à regrouper les systèmes informatiques à des fins de gestion, de communication et d'application de mesures de protection. Le modèle des zones permet de regrouper les ordinateurs de même importance ou d'importance similaire pour la sûreté et la sécurité de l'exploitation de la centrale à des fins de gestion et d'application de mesures de protection.

Son utilisation devrait être régie par les principes directeurs suivants:

- Chaque zone comprend des systèmes de même importance ou d'importance comparable pour la sécurité et la sûreté de l'installation ;
- Les systèmes d'une zone ont des exigences similaires concernant les mesures de protection ;
- Les différents systèmes informatiques d'une zone constituent un espace fiable pour la communication interne dans cette zone ;
- Les frontières de zones requièrent des mécanismes de découplage des flux de données reposant sur les politiques spécifiques des zones ;
- On peut diviser les zones en sous-zones pour améliorer la configuration.

Étant donné que les zones sont constituées de systèmes de même importance ou d'importance comparable pour la sûreté et la sécurité de

l'installation, on peut attribuer à chacune d'entre elles un niveau qui indique les mesures de protection à appliquer pour tous les systèmes informatiques de cette zone. Cependant, il n'y a pas de correspondance directe entre les zones et les niveaux ; un même niveau de sécurité peut être affecté à plusieurs zones lorsqu'elles requièrent le même degré de protection. La zone est un regroupement logique et physique de systèmes informatiques, alors que le niveau représente le degré de protection requis.

Le modèle des zones devrait faire l'objet d'une documentation appropriée dans le plan de sécurité informatique, pour inclure un aperçu de l'ensemble des systèmes informatiques, toutes les lignes de communication pertinentes, tous les croisements de zones et toutes les connexions externes.

5.5.3. Exemple d'application d'un modèle des niveaux de sécurité

Un exemple de mesures de sécurité appliquées à différents niveaux est présenté ci-dessous. Il ne s'agit que d'une application possible de l'approche graduée ; le choix exact des niveaux et des mesures de sécurité correspondantes devrait dépendre de l'environnement considéré, des spécificités de l'installation et d'une analyse appropriée des risques pour la sécurité.

Dans l'application de ce modèle :

- Des mesures génériques de niveau de protection devraient s'appliquer à tous les systèmes informatiques.
- Les niveaux de sécurité vont de 5 (protection minimum nécessaire) à 1 (protection maximum nécessaire), comme le montre la figure 5.
- Les mesures correspondant à chaque niveau ne sont pas cumulatives (il peut donc y avoir des répétitions).

Mesures génériques

Pour les systèmes et les niveaux appropriés, il convient d'appliquer les mesures génériques suivantes :

- Des stratégies et des pratiques sont définies pour chaque niveau.
- Des procédures d'exploitation relatives à la sécurité sont rédigées pour tous les utilisateurs et ceux-ci les lisent.
- Le personnel autorisé à accéder au système doit être suffisamment qualifié et expérimenté et, si nécessaire, posséder une habilitation de sécurité.
- Les utilisateurs n'ont accès qu'aux fonctions des systèmes dont ils ont besoin dans le cadre de leur travail.

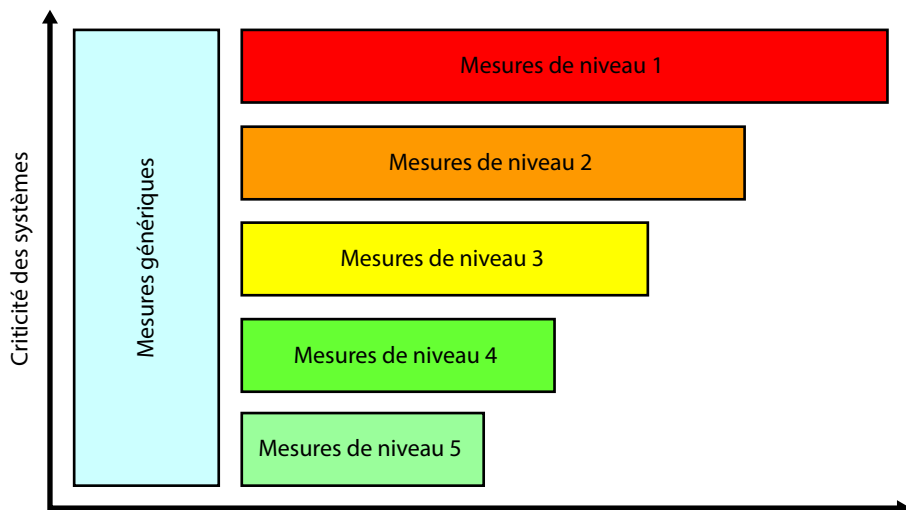


FIG. 5. Niveau de sécurité/intensité des mesures.

- Des systèmes appropriés de contrôle d'accès et d'authentification des utilisateurs sont en place.
- Des systèmes ou des procédures de détection des anomalies sont en place.
- La vulnérabilité des applications et des systèmes est surveillée, et des mesures appropriées sont prises.
- Des évaluations de la vulnérabilité des systèmes sont effectuées périodiquement.
- Les supports amovibles doivent être contrôlés conformément aux procédures d'exploitation relatives à la sécurité.
- Les éléments de sécurité informatique et de sécurité des réseaux devraient être rigoureusement entretenus.
- Les éléments de sécurité informatique et de sécurité des réseaux (par exemple les passerelles de sécurité, les systèmes de détection ou de prévention des intrusions et les serveurs de réseau privé virtuel (RPV)¹) sont scrupuleusement répertoriés et surveillés.
- Des procédures appropriées de sauvegarde et de récupération sont en place.
- L'accès physique aux éléments et aux systèmes est limité sur la base des fonctions.

¹ Un réseau privé virtuel (RPV) est un réseau constitué de nœuds connectés à l'aide de moyens de communication publics, doté de mécanismes de cryptage et d'autres mécanismes de sécurité qui limitent l'accès au réseau aux seuls utilisateurs autorisés et empêchent l'interception des données.

Niveau 1

Outre les mesures génériques, des mesures de protection de niveau 1 devraient être appliquées pour les systèmes (de protection, par exemple) essentiels pour l'installation et qui requièrent le niveau de sécurité le plus élevé. Les mesures suivantes sont notamment à envisager :

- Aucun flux de données en réseau de quelque sorte que ce soit (accusé de réception et signalisation, par exemple) provenant de systèmes de niveaux de sécurité plus faibles ne devrait pouvoir entrer dans les systèmes de niveau 1. Seules les communications vers l'extérieur devraient être possibles. Il convient de noter que ce type de communication rigoureusement unidirectionnelle ne garantit pas la fiabilité ni l'intégrité au niveau local (des corrections pour redondance/erreur peuvent être envisagées). Il convient également de noter que tout type de protocole d'établissement de liaison est exclu (y compris le protocole TCP/IP²), même avec des voies de raccordement contrôlées. Les exceptions sont fortement déconseillées et ne peuvent être envisagées strictement qu'au cas par cas, à condition d'être largement justifiées et étayées par une analyse des risques pour la sécurité³.
- Les mesures visant à garantir l'intégrité et la disponibilité des systèmes sont généralement expliquées dans les argumentaires de sûreté.
- Aucune télémaintenance n'est autorisée.
- L'accès physique aux systèmes est strictement contrôlé.
- Le nombre de membres du personnel ayant accès aux systèmes est limité au strict minimum.
- La « règle des deux personnes » est appliquée pour toute modification approuvée d'un système informatique.
- Toutes les activités devraient être répertoriées et surveillées.
- Toute entrée de données dans les systèmes est approuvée et vérifiée au cas par cas.
- Des procédures organisationnelles et administratives rigoureuses sont appliquées pour toutes les modifications, notamment la maintenance du matériel, les mises à jour et les modifications des logiciels.

² Protocole de contrôle de transmission/protocole Internet — protocoles de transmission des données.

³ Certains États Membres sont convaincus que les exceptions ne devraient en aucun cas être autorisées.

Niveau 2

Outre les mesures génériques, des mesures de protection de niveau 2 devraient être appliquées pour les systèmes (par exemple les systèmes de contrôle opérationnel) qui requièrent un niveau de sécurité élevé. Les mesures suivantes sont notamment à envisager :

- Seule une circulation vers l'extérieur, à sens unique, de données en réseau est autorisée des systèmes de niveau 2 à des systèmes de niveau 3. Seuls les messages d'accusé de réception ou les messages de signal contrôlé nécessaires peuvent être acceptés dans la direction opposée (vers l'intérieur) (pour TCP/IP par exemple).
- Une télémaintenance peut être autorisée au cas par cas et pour une durée de travail déterminée. Des mesures de protection rigoureuses sont alors nécessaires et les utilisateurs doivent respecter une politique de sécurité définie (par contrat).
- Le nombre de membres du personnel qui ont accès aux systèmes est maintenu au minimum et une distinction spécifique est établie entre les utilisateurs et le personnel administratif.
- Les connexions physiques aux systèmes devraient être strictement contrôlées.
- Toutes les mesures raisonnables ont été prises pour garantir l'intégrité et la disponibilité des systèmes.
- Une évaluation de la vulnérabilité impliquant une action sur les systèmes peut conduire à une instabilité de la centrale ou des processus, et ne devrait donc être envisagée qu'avec des bancs d'essai, des systèmes de rechange, pendant les essais d'acceptation en usine ou les longs arrêts programmés.

Niveau 3

Outre les mesures génériques, des mesures de protection de niveau 3 devraient être appliquées pour les systèmes de supervision en temps réel non requis pour les opérations, par exemple les systèmes de supervision en temps réel des processus installés dans une salle de commande, auxquels est attribué un degré de sévérité moyen pour diverses cybermenaces. Les mesures de protection suivantes sont notamment à envisager :

- L'accès à Internet depuis les systèmes de niveau 3 est interdit.
- L'enregistrement chronologique des données et les pistes de vérification concernant les ressources clés sont surveillés.

- Des passerelles de sécurité sont mises en place pour protéger ce niveau d'une circulation non contrôlée depuis les systèmes de niveau 4 et pour ne permettre qu'une activité spécifique et limitée.
- Les connexions physiques aux systèmes devraient être contrôlées.
- Une télémaintenance n'est autorisée qu'au cas par cas à condition d'être rigoureusement contrôlée ; les ordinateurs éloignés et leurs utilisateurs doivent respecter une politique de sécurité définie par contrat.
- Les fonctions des systèmes auxquelles les utilisateurs peuvent accéder sont soumises à des mécanismes de contrôle de l'accès et basées sur le principe du « besoin d'en connaître ». Toute exception à ce principe doit être soigneusement examinée et la protection devrait être assurée par d'autres moyens (accès physique, par exemple).

Niveau 4

Outre les mesures génériques, des mesures de protection de niveau 4 devraient être appliquées en ce qui concerne les systèmes de gestion des données techniques utilisés pour la maintenance ou la gestion des activités d'exploitation liées aux composants ou aux systèmes requis par les spécifications techniques pour l'exploitation (autorisation de tâches, commande de tâches, verrouillage et étiquetage, gestion de la documentation, par exemple), qui ont un degré de sévérité moyen pour diverses cybermenaces. Les mesures de niveau 4 comprennent les dispositions suivantes :

- Seuls les utilisateurs approuvés et qualifiés peuvent apporter des modifications aux systèmes.
- L'accès à Internet depuis les systèmes de niveau 4 peut être accordé aux utilisateurs sous réserve de l'application de mesures de protection appropriées.
- Des passerelles de sécurité sont mises en place pour protéger ce niveau d'une circulation non contrôlée depuis des réseaux d'entreprises ou de sites extérieurs et pour permettre des activités spécifiques contrôlées.
- Les connexions physiques aux systèmes devraient être contrôlées.
- La télémaintenance est autorisée et contrôlée ; les ordinateurs éloignés et leurs utilisateurs doivent respecter une politique de sécurité définie par contrat et contrôlée.
- Les fonctions des systèmes auxquelles les utilisateurs peuvent accéder sont soumises à des mécanismes de contrôle de l'accès. Toute exception à ce principe doit être soigneusement examinée et une protection devrait être assurée par d'autres moyens.

- L'accès à distance depuis l'extérieur est autorisé pour les utilisateurs approuvés, à condition que des mécanismes appropriés de contrôle d'accès soient en place.

Niveau 5

Des mesures de niveau 5 devraient être appliquées en ce qui concerne les systèmes qui ne sont pas directement importants pour le contrôle technique ou l'exploitation (systèmes de bureautique, par exemple), qui ont un degré de sévérité faible pour diverses cybermenaces. Les mesures de niveau 5 comportent notamment les dispositions suivantes :

- Seuls les utilisateurs approuvés et qualifiés peuvent apporter des modifications aux systèmes.
- L'accès à Internet depuis les systèmes de niveau 5 est autorisé sous réserve de l'application de mesures de protection appropriées.
- L'accès à distance depuis l'extérieur est accordé aux utilisateurs autorisés, à condition que des mécanismes appropriés de contrôle soient en place.

5.5.4. Zones de découplage

Des mécanismes de découplage des flux de données doivent être mis en place aux frontières de zones pour prévenir tout accès non autorisé et éviter que les erreurs ne se propagent d'une zone aux prescriptions de protection plus larges à une zone aux prescriptions plus strictes.

Les mesures techniques et administratives garantissant le découplage des zones doivent être adaptées aux diverses exigences des niveaux de protection. Aucune ligne de liaison directe entre plusieurs zones ne devrait être autorisée.

6. MENACES, VULNÉRABILITÉS ET GESTION DES RISQUES

La section ci-après présente les concepts fondamentaux utilisés dans le domaine de la gestion des risques pour les systèmes informatiques. La gestion des risques s'applique à tous les stades du cycle de vie des systèmes de l'installation, y compris la conception, l'élaboration, l'exploitation et la maintenance. La section 6.2 donne un aperçu des étapes qu'une méthodologie complète de la

gestion des risques doit comporter. Les sections 6.3 et 6.4 ont trait aux étapes où l'industrie nucléaire présente des caractéristiques particulières.

6.1. CONCEPTS DE BASE ET LIENS DIVERS

Dans le cadre de la sécurité informatique, le risque est la possibilité qu'une menace donnée exploite les vulnérabilités d'un actif ou d'un groupe d'actifs et cause ainsi un dommage à l'organisation. Il se mesure par une combinaison de la probabilité d'un événement et de la gravité de ses conséquences.

La figure 6 est un diagramme montrant les liens multiples qui existent entre les concepts de menace, de vulnérabilité et de risque [16].

6.2. ÉVALUATION ET GESTION DES RISQUES

L'évaluation des risques est un outil important pour déterminer l'endroit le plus approprié où investir des ressources et des efforts afin de remédier aux vulnérabilités et de faire face à la probabilité qu'elles soient exploitées.

C'est un processus par lequel on distingue et on répertorie des combinaisons particulières de la menace, de la vulnérabilité et de l'impact, et on conçoit des contrôles appropriés aux fins de la protection. L'évaluation des menaces et des vulnérabilités sert de base à l'élaboration des contre-mesures

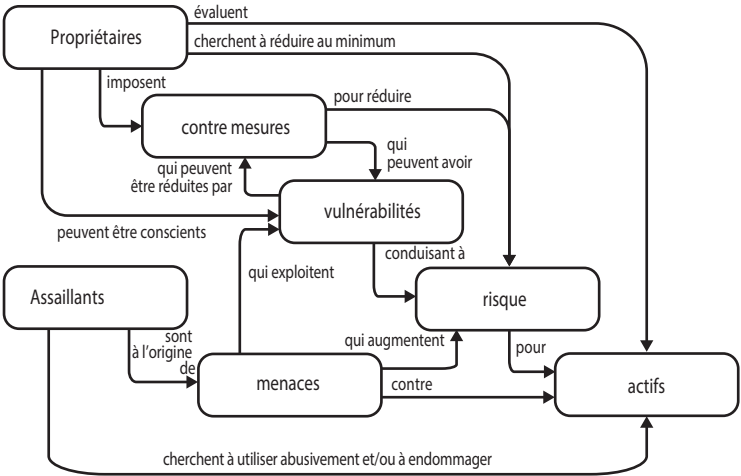


FIG. 6. Concepts de sécurité et liens divers (figure adaptée de la norme ISO 13335-1 2004 [16]).

nécessaires pour prévenir ou atténuer les conséquences des attaques contre les systèmes informatiques.

Les étapes fondamentales d'une méthodologie d'évaluation et de gestion des risques sont les suivantes :

- Définition du périmètre et du contexte ;
- Détermination et caractérisation des menaces ;
- Évaluation des vulnérabilités ;
- Élaboration de scénarios d'attaque ;
- Probabilité de succès de l'exploitation d'une vulnérabilité ;
- Évaluation du niveau de risque ;
- Définition de contre-mesures.

Pour conduire une analyse et une évaluation systématiques et cohérentes des risques, il faut utiliser un processus bien défini pouvant répondre aux normes existantes. Un grand nombre de méthodologies et d'outils d'évaluation ou de gestion des risques sont éprouvés et peuvent permettre de structurer efficacement un tel processus, ce qui leur vaut d'être largement acceptés. La plupart d'entre eux s'appuient sur des concepts communs et sur la logique. La norme internationale en vigueur à cet égard est la norme ISO/CEI 27005 — Gestion des risques en sécurité de l'information [4]. Un autre exemple précis de méthodologie est donné à l'annexe II. Les autorités nationales peuvent exiger l'utilisation d'une méthodologie ou d'une politique particulière d'évaluation des risques et les installations peuvent en outre avoir la leur.

Un panorama intéressant des méthodes et des outils d'évaluation des risques a été dressé par l'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information), qui a consacré une page web spéciale à cette étude [17].

La nécessité d'évaluer les systèmes, la précision de l'évaluation et la fréquence d'actualisation des analyses de risque dépendent de l'importance de la fonction de sûreté et de sécurité du système. Il convient d'envisager une nouvelle analyse ou au moins un examen lorsque le système est modifié, par exemple avec la mise en place d'équipements, de procédures ou de logiciels nouveaux, ou un changement majeur des compétences de l'exploitant. Le nombre de menaces ou de vulnérabilités potentielles augmente généralement avec le passage des systèmes autonomes aux systèmes interconnectés.

Lorsqu'on ne peut pas analyser les risques concernant des menaces précises, il est recommandé de suivre les pratiques optimales et les bons principes d'ingénierie.

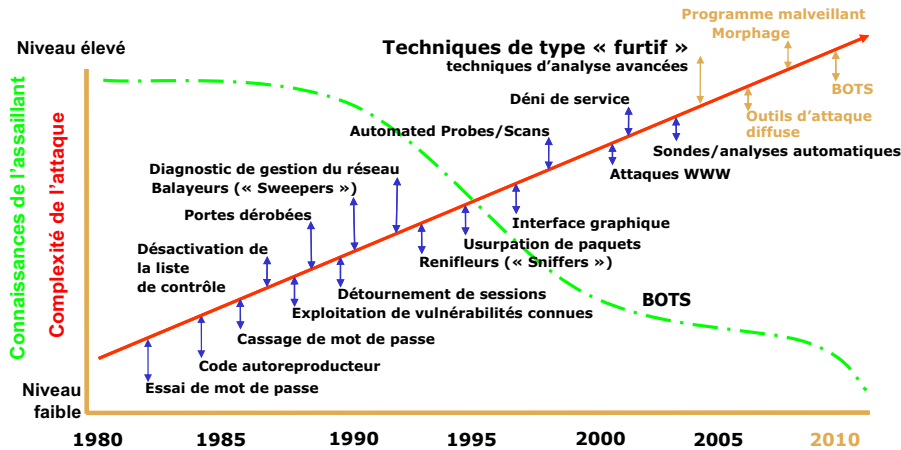


FIG. 7. Accroissement de la complexité des menaces avec l'augmentation du nombre d'assaillants.⁴

6.3. RECENSEMENT ET DÉTERMINATION DES MENACES

La figure 7 montre la tendance continue caractérisée par l'augmentation de la complexité des attaques et la diminution des connaissances requises pour les lancer. Les programmes de sécurité informatique devraient tendre à maintenir un niveau d'évaluation couvrant un très large éventail de scénarios d'attaque possibles.

Des publications sur la vulnérabilité des systèmes de contrôle industriel sont souvent disponibles lors de grandes manifestations sur le piratage. Cependant, elles donnent généralement une idée dépassée des compétences et des intérêts réels des pirates, un facteur à prendre en considération. En outre, les équipes nationales d'intervention en cas d'urgence informatique ont commencé récemment à publier les vulnérabilités des logiciels de systèmes de contrôle industriel spécialisés, ce qui permet à l'opinion publique et aux spécialistes de la sécurité informatique de mieux les connaître et attire l'attention sur les solutions à cet égard et les failles des produits.

Par conséquent, après la mise en place de l'appui et des ressources adéquates, les premières mesures dans le cadre de l'élaboration d'un programme de sécurité informatique devraient viser essentiellement à comprendre les

⁴ LIPSON, H.F., Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, Special Report CMS/SEI-2002-SR-009 (2000) 10.

menaces potentielles à partir de profils d'assaillants et de scénarios d'attaque crédibles. On pourrait dans un premier temps créer une matrice de profils d'assaillants répertoriant les assaillants crédibles, leurs motivations et leurs objectifs potentiels. Cette matrice pourrait ainsi servir à établir des scénarios d'attaque plausibles ; les parties suivantes décrivent plus en détail ce processus.

6.3.1. Menace de référence

Un outil important généralement utilisé pour déterminer les niveaux de menace et servant de base à la détermination des caractéristiques de sécurité est la menace de référence. Il s'agit d'une description des moyens et des caractéristiques d'agresseurs potentiels (internes et/ou externes). Une menace de référence est établie à partir d'informations crédibles émanant de services de renseignements, mais n'est pas censée être une déclaration concernant les menaces réelles les plus répandues. Compte tenu du contexte de menaces actuel, la menace de référence est la plus grande menace raisonnable contre laquelle une installation devrait prévoir des moyens de défense. Les États l'utilisent dans leur système réglementaire pour déterminer le niveau de ressources à allouer à la protection des matières et des installations nucléaires contre des actes hostiles. (Pour de plus amples informations sur la menace de référence, voir la Réf. [18]).

Il faudrait envisager d'intégrer dans ces scénarios les menaces d'attaque isolée utilisant/visant des systèmes informatiques ou les menaces d'attaque coordonnée pouvant utiliser ces systèmes.

6.3.2. Profil des assaillants

Les tableaux 1 et 2 présentent un ensemble possible de profils d'assaillants. Le tableau 1 porte sur les menaces interne/d'origine interne (voir aussi la Réf. [19] pour un examen de la menace interne) et le tableau 2 recense les menaces externes possibles. Ces tableaux décrivent les grands types d'assaillants et les ressources dont ils disposent, la durée des attaques, les outils qu'ils sont susceptibles d'utiliser, et leurs motivations. Les profils doivent être adaptés à chaque installation. Il faut donc un processus adéquat de collecte de renseignements pour que la matrice des profils d'assaillants de chaque installation soit complète et pertinente.

6.3.3. Scénarios d'attaque

Lors de l'établissement de scénarios d'attaque, on peut distinguer plusieurs possibilités. L'installation nucléaire peut être attaquée pour :

- Préparer une attaque coordonnée ultérieure destinée à saboter la centrale et/ou enlever des matières nucléaires ;
- Menacer la sûreté des personnes ou de l'environnement ;
- Lancer une attaque contre un autre site ;
- Semer la confusion et la peur ;
- Obtenir un gain monétaire au profit d'un groupe criminel ;
- Créer des instabilités majeures sur le marché et acquérir des gains au profit de certains acteurs du marché.

Selon les objectifs ou les buts de l'attaque, l'assaillant cherchera à exploiter différentes vulnérabilités du système. Ces attaques peuvent conduire à :

- L'accès non autorisé à des informations (perte de confidentialité) ;
- L'interception et l'altération d'informations, de logiciels, de matériel, etc. (perte d'intégrité) ;
- Blocage des voies de transmission de données et/ou arrêt des systèmes (perte de disponibilité) ;
- Intrusion non autorisée dans les systèmes de communication de données ou les ordinateurs (perte de fiabilité).

Tous ces aspects peuvent avoir des conséquences et des incidences majeures sur le fonctionnement des systèmes informatiques, ce qui peut compromettre directement ou indirectement la sûreté et la sécurité de l'installation. Lors de l'élaboration de scénarios d'attaque, les tendances technologiques et la facilité d'accès aux technologies d'attaque devraient être prises en considération. Des scénarios d'attaques fictives mais réalistes pouvant se produire dans une installation nucléaire sont présentés plus en détail à l'annexe I.

6.4. RÉSULTATS SIMPLIFIÉS D'UNE ÉVALUATION DES RISQUES

Le tableau 3 présente, à titre indicatif seulement, des systèmes que l'on peut rencontrer dans une installation nucléaire. Il détermine les impacts que pourraient avoir des attaques contre les systèmes considérés en cas de réussite, ainsi que les impacts correspondants sur l'installation, et donne des exemples génériques de contre-mesures appropriées.

La notion de probabilité, fondamentale dans l'évaluation des risques, n'est pas prise en compte dans ce tableau. La probabilité de réussite des attaques, et leurs conséquences potentielles, dépendent du contexte et de l'installation considérée. En outre, une évaluation plus approfondie des besoins en matière

TABLEAU 1. MENACES INTERNES

Assaillant	Ressources	Durée	Outils	Motivation
Agent infiltré	« Ingénierie sociale » facilitée. Accès au système à un certain niveau. Documentation et connaissances spécialisées à disposition concernant le système.	Variable, mais l'assaillant ne peut généralement pas y consacrer de longues heures.	Accès existant, connaissance de la programmation et de l'architecture du système : — Connaissance possible de mots de passe existants ; — Possibilité d'introduire des portes dérobées et/ou des chevaux de Troie spécialement mis au point ; — Appui spécialisé externe possible.	Vol d'informations internes, de secrets technologiques, d'informations personnelles. Profit économique (vente d'informations à la concurrence). Chantage.
Employé/ utilisateur mécontent	Ressources moyennes/importantes. Accès au système à un certain niveau. Documentation et connaissances spécialisées à disposition sur certains systèmes internes et opérationnels.	Variable, mais l'assaillant ne peut généralement pas y consacrer de longues heures.	Accès existant, connaissance de la programmation et de l'architecture du système. Connaissance possible de mots de passe existants. Aptitude à introduire des outils ou scripts « amateurs » (parfois plus élaborés s'il dispose de compétences informatiques particulières).	Vengeance, perturbation, chaos. Vol d'informations internes. Nuisance à l'employeur/à un autre employé. Dégradation de l'image publique ou de la confiance.

TABLE 2. MENACES EXTERNES

Assaillant	Ressources	Durée	Outils	Motivation
Pirate amateur	Compétences variables, mais généralement limitées. Peu de connaissances du système au-delà des informations publiques.	Très longue, l'assaillant n'est pas très patient.	Scripts et outils généralement disponibles. Mise au point d'outils possible.	Divertissement, statut. Cible fortuite. Exploitation des vulnérabilités « à portée de main ».
Militant opposé à l'électronucléaire	Ressources limitées, mais peut avoir l'appui financier de filières occultes. Accès aux outils de la communauté virtuelle. Peu de connaissances du système au-delà des informations publiques.	Les attaques peuvent être dirigées contre des manifestations connues à l'avance (par ex célébrations, élections). Très longue, l'assaillant est patient et motivé.	Compétences informatiques à disposition. Soutien possible de la communauté des pirates. « Ingénierie sociale ».	Conviction de sauver le monde. Influence sur l'opinion publique concernant certaines questions. Blocage d'opérations internes.
Ancient employé/ utilisateur mécontent	Ressources limitées s'il ne fait pas partie d'un groupe plus large. Peut-être encore en possession de documents relatifs au système. Peut utiliser un ancien accès non contrôlé. Liens possibles avec des membres du personnel de l'installation.	Variable et dépend du groupe auquel l'assaillant est associé.	Connaissance possible de mots de passe existants. L'assaillant peut utiliser un ancien accès non contrôlé. Il peut avoir créé des portes dérobées dans le système lorsqu'il était encore employé. « Ingénierie sociale ».	Vengeance, perturbation, chaos. Vol d'informations internes. Nuisance à l'employeur/à un autre employé. Dégradation de l'image publique ou de la confiance.

TABLE 2. MENACES EXTERNES (suite)

Assaillant	Ressources	Durée	Outils	Motivation
Crime organisé	Ressources importantes. Emploi de compétences informatiques spécialisées.	Variable, mais surtout de courte durée.	Scripts, outils « maison ». L'assaillant peut engager un pirate contre rémunération. Il peut engager un ancien employé/employé en fonctions. « Ingénierie sociale ».	Chantage. Vol de matières nucléaires. Extorsion (de fonds). Exploitation des craintes du secteur sur le plan financier et de l'image. Vente d'informations (techniques, internes ou personnelles).
État-nation	Ressources et compétences importantes. Activités de collecte de renseignements. Formation sur le système/expérience d'exploitation du système possibles	Variable.	Équipes d'experts informatiques formés. Outils complexes. L'assaillant peut engager un ancien employé/employé en fonctions. « Ingénierie sociale ».	Collecte de renseignements. Création de points d'accès pour des actions ultérieures. Vol de technologies.
Terroriste	Compétences variables. Formation sur le système/expérience d'exploitation du système possibles.	Très longue, l'assaillant est très patient.	Scripts, outils « maison ». L'assaillant peut engager un pirate contre rémunération. Il peut engager un ancien employé/employé en fonctions. « Ingénierie sociale ».	Collecte de renseignements. Création de points d'accès pour des actions ultérieures. Chaos. Vengeance. Impact sur l'opinion publique (peur).

TABLEAU 3. SYSTÈMES TYPES DES INSTALLATIONS NUCLÉAIRES

Système	Impact sur la sécurité informatique	Impact potentiel sur l'installation	Mesures de protection suggérées
Système de protection du réacteur	Perte d'intégrité des logiciels/données critiques pour la sûreté.	CRITIQUE	Mesures du niveau de sécurité 1
	Perte de disponibilité des fonctions.	Sûreté de la centrale compromise, rejets radioactifs.	
Système de contrôle des processus	Perte d'intégrité des logiciels/données de contrôle.	ÉLEVÉ	Mesures du niveau de sécurité 2
	Perte de disponibilité des fonctions.	Exploitation de la centrale compromise.	
Système d'autorisation et de commande de tâches	Perte d'intégrité des données et de disponibilité du système.	MOYEN	Mesures du niveau de sécurité 4
		Fausse manœuvres sur des éléments. Perturbation du fonctionnement normal et de la maintenance.	
Système de contrôle de l'accès physique	Perte de disponibilité et d'intégrité des systèmes d'accès au site.	ÉLEVÉ	Mesures du niveau de sécurité 2
	Perte de confidentialité des données d'accès au site.	Accès donné à des personnes non habilitées. Des personnes habilitées sont interdites d'accès à des zones auxquelles elles doivent accéder.	

TABLEAU 3. SYSTÈMES TYPES DES INSTALLATIONS NUCLÉAIRES (suite)

Système	Impact sur la sécurité informatique	Impact potentiel sur l'installation	Mesures de protection suggérées
Système de gestion des documents	Perte de confidentialité, de disponibilité et d'intégrité des données.	MOYEN Données utilisées pour la planifier des attaques plus graves.	Mesures du niveau de sécurité 4
Messagerie électronique	Perte de confidentialité, d'intégrité et de disponibilité.	FAIBLE Contraintes administratives. Activités quotidiennes rendues plus difficiles.	Mesures du niveau de sécurité 5

deconfidentialité, d'intégrité et de disponibilité devrait être conduite dans l'évaluation des risques pour chaque système considéré.

7. CONSIDÉRATIONS PARTICULIÈRES POUR LES INSTALLATIONS NUCLÉAIRES

Compte tenu du caractère unique de l'industrie nucléaire, la sécurité informatique des installations nucléaires doit répondre à des préoccupations supplémentaires par rapport à celles ayant trait à la sécurité informatique des réseaux de TI d'entreprises, voire de systèmes de contrôle des processus en dehors de l'industrie nucléaire. Les sections ci-après décrivent certaines de ces préoccupations liées à l'industrie nucléaire.

7.1. PHASES DU CYCLE DE VIE ET MODES DE FONCTIONNEMENT D'UNE INSTALLATION

Les modèles et les caractéristiques d'exploitation des installations nucléaires sont très variés. Elles ont plusieurs phases de cycle de vie et modes de fonctionnement, notamment :

- Conception, construction et mise en service.
- Exploitation :
 - Fonctionnement en régime de puissance ;
 - Démarrage de la centrale ;
 - Arrêt à chaud ;
 - Arrêt à froid ;
 - Rechargement en combustible et maintenance.
- Déclassement.

Ces multiples phases du cycle de vie et modes de fonctionnement peuvent exiger différents systèmes et différents environnements opérationnels. Par exemple, les périodes intenses de maintenance vont souvent de pair avec le remplacement, la modification et l'essai du matériel ou peuvent nécessiter le recrutement de personnel supplémentaire et l'accès de tiers/sous-traitants. Cet aspect devrait être pris en compte dans le plan de sécurité informatique. Différentes phases du cycle de vie pourraient en particulier impliquer des révisions importantes de ce plan.

7.2. DIFFÉRENCES ENTRE LES SYSTÈMES DE TI ET LES SYSTÈMES DE CONTRÔLE INDUSTRIEL

Les systèmes informatiques et les architectures de réseau appuyant les opérations des centrales nucléaires ne sont pas des systèmes courants en termes d'exigences d'architecture, de configuration ou de performance. Ils peuvent être classés en tant que systèmes de contrôle industriel spécialisés. Bien que les systèmes de contrôle industriel aient évolué, passant d'applications strictement propriétaires à une architecture informatique plus courante, il subsiste entre ces systèmes et les systèmes de TI standard des différences considérables qui doivent être prises en compte dans tout plan de sécurité informatique.

Le tableau 4 ci-dessous, établi sur la base d'un document du NIST [20], présente les principales différences entre les systèmes de contrôle industriel et les systèmes de TI classiques.

TABLEAU 4. DIFFÉRENCES ENTRE LES SYSTÈMES DE TI ET LES SYSTÈMES DE CONTRÔLE INDUSTRIEL [20]

Catégorie	Système de technologie de l'information	Système de contrôle industriel
Exigences de performance	Temps différé La réaction doit être cohérente Le haut débit est exigé Un retard et un sautellement importants peuvent être acceptables	Temps réel La réaction doit être rapide Un débit limité est acceptable Un retard ou un sautellement important est un problème grave
Exigences de disponibilité	Des mesures telles que la réinitialisation sont acceptables Une disponibilité insuffisante peut être souvent tolérée, en fonction des besoins opérationnels du système	Des mesures telles que la réinitialisation peuvent ne pas être acceptables du fait des exigences de disponibilité des processus Les arrêts doivent être planifiés et programmés plusieurs jours/semaines à l'avance Une disponibilité élevée exige des essais complets préalables au déploiement
Exigences de gestion des risques	Temps différé La réaction doit être cohérente Le haut débit est exigé Un retard et un sautellement importants peuvent être acceptables	Temps réel La réaction doit être rapide Un débit limité est acceptable Un retard ou un sautellement important est un problème grave
Priorité de la sécurité de l'architecture	Des mesures telles que la réinitialisation sont acceptables Une disponibilité insuffisante peut être souvent tolérée, en fonction des besoins opérationnels du système	Des mesures telles que la réinitialisation peuvent ne pas être acceptables du fait des exigences de disponibilité des processus Les arrêts doivent être planifiés et programmés plusieurs jours/semaines à l'avance Une disponibilité élevée exige des essais complets préalables au déploiement
Conséquences imprévues	Temps différé La réaction doit être cohérente Le haut débit est exigé Un retard et un sautellement importants peuvent être acceptables	Temps réel La réaction doit être rapide Un débit limité est acceptable Un retard ou un sautellement important est un problème grave
Rapidité de l'interaction	Des mesures telles que la réinitialisation sont acceptables Une disponibilité insuffisante peut être souvent tolérée, en fonction des besoins opérationnels du système	Des mesures telles que la réinitialisation peuvent ne pas être acceptables du fait des exigences de disponibilité des processus Les arrêts doivent être planifiés et programmés plusieurs jours/semaines à l'avance Une disponibilité élevée exige des essais complets préalables au déploiement
Fonctionnement du système	Temps différé La réaction doit être cohérente Le haut débit est exigé Un retard et un sautellement importants peuvent être acceptables	Temps réel La réaction doit être rapide Un débit limité est acceptable Un retard ou un sautellement important est un problème grave
Contraintes de ressources	Des mesures telles que la réinitialisation sont acceptables Une disponibilité insuffisante peut être souvent tolérée, en fonction des besoins opérationnels du système	Des mesures telles que la réinitialisation peuvent ne pas être acceptables du fait des exigences de disponibilité des processus Les arrêts doivent être planifiés et programmés plusieurs jours/semaines à l'avance Une disponibilité élevée exige des essais complets préalables au déploiement
Communications	Temps différé La réaction doit être cohérente Le haut débit est exigé Un retard et un sautellement importants peuvent être acceptables	Temps réel La réaction doit être rapide Un débit limité est acceptable Un retard ou un sautellement important est un problème grave

TABLEAU 4. DIFFÉRENCES ENTRE LES SYSTÈMES DE TI ET LES SYSTÈMES DE CONTRÔLE INDUSTRIEL [20] (suite)

Catégorie	Système de technologie de l'information	Système de contrôle industriel
Gestion du changement	Des mesures telles que la réinitialisation sont acceptables Une disponibilité insuffisante peut être souvent tolérée, en fonction des besoins opérationnels du système	Des mesures telles que la réinitialisation peuvent ne pas être acceptables du fait des exigences de disponibilité des processus Les arrêts doivent être planifiés et programmés plusieurs jours/semaines à l'avance Une disponibilité élevée exige des essais complets préalables au déploiement
Appui encadré	Temps différé La réaction doit être cohérente Le haut débit est exigé Un retard et un sautellement importants peuvent être acceptables	Temps réel La réaction doit être rapide Un débit limité est acceptable Un retard ou un sautellement important est un problème grave
Durée de vie des éléments	Des mesures telles que la réinitialisation sont acceptables Une disponibilité insuffisante peut être souvent tolérée, en fonction des besoins opérationnels du système	Des mesures telles que la réinitialisation peuvent ne pas être acceptables du fait des exigences de disponibilité des processus Les arrêts doivent être planifiés et programmés plusieurs jours/semaines à l'avance Une disponibilité élevée exige des essais complets préalables au déploiement
Accès aux éléments	Temps différé La réaction doit être cohérente Le haut débit est exigé Un retard et un sautellement importants peuvent être acceptables	Temps réel La réaction doit être rapide Un débit limité est acceptable Un retard ou un sautellement important est un problème grave

7.3. DEMANDE DE CONNECTIVITÉ SUPPLÉMENTAIRE ET CONSÉQUENCES ASSOCIÉES

Une question de plus en plus préoccupante concernant les systèmes de contrôle industriel spécialisés est le souhait croissant d’interconnectivité entre les systèmes internes et d’ingénierie et les systèmes opérationnels. Compte tenu du souci des sièges d’entreprise, des planificateurs et des ingénieurs d’accéder en temps réel aux données d’une centrale, des passerelles sont établies entre les réseaux de contrôle très limités faisant fonctionner la centrale et les réseaux de données illimités utilisés pour l’accès interne. Ces passerelles peuvent être des moyens d’intrusion dans les réseaux.

Une autre caractéristique architecturale spécifique est l’existence de centres d’exploitation à distance en cas d’urgence. Ces centres permettent la surveillance et les opérations d’urgence de la centrale à distance au cas où un incident rendrait inutilisable l’installation principale. Les exigences de surveillance/maintien de certains aspects du contrôle de la centrale obligent à assurer la circulation des données à travers des supports de communication. Ceux-ci peuvent être utilisés pour porter atteinte au système principal ou pour y pénétrer. De plus, la nécessité de dupliquer les fonctions oblige à maintenir des exigences de sécurité

homogènes dans deux systèmes. Si un système n'est pas maintenu, cela pourrait ouvrir la voie à des intrusions et à l'exploitation des injections.

La nécessité d'analyse, de maintenance et de mises à jour à distance peut également induire des vulnérabilités semblables. Avant d'approuver ce type de connectivité supplémentaire, il faut procéder à une analyse approfondie des risques.

7.4. CONSIDÉRATIONS CONCERNANT LES MISES À JOUR DE LOGICIELS

Un grand nombre de règlements en vigueur sur la validation ou la certification d'équipements de centrales nucléaires ont été élaborés compte tenu des équipements analogiques. Ceux-ci ne sont pas rapidement dépassés. En revanche, les plans de sécurité et les pratiques optimales de TI nécessitent des mises à jour régulières et des correctifs pour les logiciels et les composants numériques, car ces derniers deviennent plus vite obsolètes.

Il est donc important de tenir compte du problème des correctifs et des mises à jour de logiciels dans les systèmes numériques de contrôle ou de surveillance nucléaire. Dans l'hypothèse la plus pessimiste, chaque modification ou révision de logiciel peut être considérée comme un changement au système et donner lieu à une validation spécifique du système, voire au renouvellement de la certification pour certains systèmes essentiels. Il s'agit d'un processus compliqué qui peut retarder l'application des correctifs ou conduire à une décision délibérée de repousser la mise à jour de logiciels. Pour limiter ces effets, il faudrait établir une distinction entre les activités de maintenance courante, qui ne nécessitent pas ces procédures, et les modifications de systèmes, qui obligent à tester ou à certifier de nouveau les systèmes essentiels. Dans tous les cas, toute modification apportée aux systèmes de sûreté, ou aux systèmes liés à la sûreté, et aux systèmes de sécurité doit suivre les procédures approuvées.

7.5. CONCEPTION SÉCURISÉE ET SPÉCIFICATIONS RELATIVES AUX SYSTÈMES INFORMATIQUES

Au moment de la conception initiale et de l'élaboration de nombreux systèmes et instruments de contrôle de processus et de contrôle industriel existants, la sécurité informatique ne constituait pas une préoccupation majeure. La tendance récente à la connectivité des systèmes et des processus, l'intégration de systèmes informatiques commerciaux et l'expansion des activités

informatiques malveillantes (comme le piratage) obligent à considérer la sécurité informatique comme une exigence clé dans l'achat de nouveaux équipements.

Par conséquent, les exigences de sécurité devraient être établies formellement lors de la négociation de contrats avec des fournisseurs. Le document ISO sur les critères communs (ISO 15408) [21] peut servir d'outil à cet égard. Un autre exemple est l'effort de définition d'un langage relatif aux achats pour les systèmes de contrôle [22] accompli par le Département de la sécurité intérieure des États-Unis, qui a publié des orientations et des recommandations sur la définition d'exigences en matière de cybersécurité et l'élaboration d'un langage propre aux achats pour l'acquisition de systèmes de contrôle.

7.6. PROCÉDURE DE CONTRÔLE D'ACCÈS POUR LES TIERS/FOURNISSEURS

Il est essentiel de tenir compte du niveau de sécurité de toutes les personnes tierces/tous les fournisseurs. Le département chargé de la sécurité devra nécessairement travailler en étroite collaboration avec le département chargé des contrats pour veiller à ce que les dispositions de sécurité figurent dans chaque contrat.

Les contrats sont souvent octroyés à des entités externes par des organismes de l'industrie nucléaire ; certains de ces contrats amèneront les sous-traitants à détenir sur leurs propres sites des informations ou des actifs protégés. À moins que l'octroi d'un tel contrat et la gestion ultérieure ne respectent des règles strictes, les informations et les actifs protégés risquent d'être mis en péril ou d'être divulgués sans autorisation.

Compte tenu des facteurs susmentionnés, il est important que la direction responsable de chaque site/organisme de l'industrie nucléaire entretienne une relation de travail étroite avec les sous-traitants afin que les aspects de sécurité essentiels soient pris en compte tout au long de l'élaboration et de l'exécution du contrat, ainsi que lors du transfert final.

Si cela est jugé nécessaire, des vérifications et des contrôles devraient être effectués pour s'assurer que le système de gestion du sous-traitant tient compte adéquatement de questions de sécurité et que les pratiques et mesures de celui-ci sont conformes à son système.

RÉFÉRENCES

- [1] COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE, Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire, ISO/CEI 27000:2009, ISO, Genève (2009).
- [2] COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE, Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences, ISO/CEI 27001:2005, ISO, Genève (2005).
- [3] COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE, Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information, ISO/CEI 27002:2005, ISO, Genève (2005).
- [4] COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE, Technologies de l'information — Techniques de sécurité — Gestion des risques en sécurité de l'information, ISO/CEI 27005:2008, ISO, Genève (2008).
- [5] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Requirements for Bodies Providing Audit and Certification of Information Security Management Systems, ISO/IEC 27006:2007, ISO, Geneva (2007).
- [6] CONSEIL DE L'EUROPE, Convention sur la cybercriminalité, STE n° 185, Conseil de l'Europe, Strasbourg (2001).
- [7] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Système de gestion des installations et des activités, collection Normes de sûreté n° GS-R-3, AIEA, Vienne (2011).
- [8] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-G-3.1, IAEA, Vienna (2006).
- [9] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Culture de sécurité nucléaire, collection Sécurité nucléaire de l'AIEA n° 7, AIEA, Vienne (2009).
- [10] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Objectifs et principes fondamentaux de la protection physique, résolution GOV/2001/41, AIEA, Vienne (2001).
- [11] La protection physique des matières et installations nucléaires, INFCIRC/225/Rev.4 (Corrigé), AIEA, Vienne (2000).
- [12] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Orientations et considérations concernant l'application du document INFCIRC/225/Rev.4, La protection physique des matières et installations nucléaires, IAEA-TECDOC-967 (Rev.1)/F, AIEA, Vienne (2002).
- [13] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté des centrales nucléaires, collection Normes de sûreté n° NS-G-1.3, AIEA, Vienne (2005).
- [14] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Logiciels destinés aux systèmes programmés importants pour la sûreté des centrales nucléaires, collection Normes de sûreté n° NS-G-1.1, AIEA, Vienne (2004).

- [15] 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).
- [16] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Management of Information and Communications Technology Security — Part 1: Concepts and Models for Information and Communications Technology Security Management, ISO/IEC 13335-1:2004, ISO, Geneva (2004).
- [17] EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, Inventory of Risk Management/Risk Assessment Methods and Tools, <http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/rm-ra-tools>.
- [18] 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).
- [19] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures Against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).
- [20] STOUFFER, K.A., FALCO, J.A., SCARFONE, K., Guide to Industrial Control Systems (ICS) Security — Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC), Rep. NIST SP-800-82, National Institute of Standards and Technology, Chicago (2011).
- [21] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Evaluation Criteria for IT Security, ISO/IEC 15408:2008, ISO, Geneva (2008).
- [22] UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Cyber Security Procurement Language for Control Systems, September (2009), http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_100809.pdf
- [23] COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE, Management du risque — Vocabulaire, ISO Guide 73:2009, ISO/CEI, Genève (2009).

BIBLIOGRAPHIE

AMERICAN NATIONAL STANDARDS INSTITUTE, INTERNATIONAL SOCIETY FOR AUTOMATION, Security Technologies for Industrial Automation and Control System, ANSI/ISA-TR99.00.01-2007, ANSI, Washington DC, (2007).

FEDERAL MINISTRY OF THE INTERIOR, National Plan for Information Infrastructure Protection, BMI, Berlin (2005).

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Objectifs et principes fondamentaux de la protection physique, résolution GOV/2001/41, AIEA, Vienne (2001).

INTERNATIONAL SOCIETY FOR AUTOMATION, Integrating Electronic Security into the Manufacturing and Control Systems Environment, Instrumentation, Systems and Automation Society, ISA-TR99.00.02-2004, ISA, Research Triangle Park, NC (2004).

KOREA INSTITUTE OF NUCLEAR SAFETY, Cyber Security of Digital Instrumentation and Control Systems in Nuclear Facilities, KINS/GT-N09-DR, KINS, Seoul (2007).

NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE, Good Practice Guide: Process Control and SCADA Security, Version 2.0, NISCC, November (2006).

NUCLEAR ENERGY INSTITUTE, Cyber Security Plan for Nuclear Power Reactors, NEI 0809 (Rev. 5), NEI, Washington DC (2010).

NUCLEAR REGULATORY COMMISSION, Cyber Security Programs for Nuclear Facilities, Regulatory Guide 5.71, NRC, Rockville, MD (2010).

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité, OCDE, Paris (2002).

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, Plan d'application des lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité, DSTI/ICCP/REG(2003)5/REV1, OCDE, Paris (2003).

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries, DSTI/ICCP/REG (2005) 1/FINAL, OECD, Paris (2005).

La présente publication a été remplacée par la publication suivante : 17-T (Rev. 1).

Annexe I

SCÉNARIOS D'ATTAQUE CONTRE LES SYSTÈMES DES INSTALLATIONS NUCLÉAIRES

Comme indiqué à la section 6.3, les attaques informatiques, qui doivent être toutes prévenues, peuvent être de nature et de forme très variées. Malgré ces différences, elles ont des conséquences à un haut niveau, notamment :

- L'accès non autorisé à des informations ou l'interception d'informations (perte de confidentialité) ;
- L'altération non autorisée d'informations, de logiciels, de matériel, etc. (perte d'intégrité) ;
- Le blocage des voies de transmission de données et/ou l'arrêt des systèmes (perte de disponibilité).

Lorsque l'on élabore des mesures de prévention contre des attaques informatiques, il est extrêmement important de connaître la nature des attaques et les voies qui pourraient servir à une attaque ou à des assaillants pour obtenir les informations pertinentes et accéder aux systèmes informatiques cibles. **Les scénarios ci-après ne sont que des exemples destinés à encourager les lecteurs — lorsqu'ils ont une meilleure connaissance des menaces — à réfléchir sur leur propre organisme/système et, si besoin, à corriger les caractéristiques de sécurité en conséquence.** Bien que les attaques présentées soient fictives, elles se rapportent à des scénarios plausibles, qui s'inspirent d'attaques semblables observées dans d'autres secteurs. Réfléchir sur ces scénarios est un bon moyen de s'assurer que le plan de sécurité tient compte de l'évolution du contexte de menaces.

Une attaque informatique bien organisée comprend plusieurs phases, à savoir notamment :

- Identification de la cible ;
- Reconnaissance ;
- Accès/atteinte au système ;
- Exécution de l'attaque ;
- Camouflage des traces pour pouvoir réfuter l'attaque.

Les parties ci-après dressent une liste de trois scénarios fictifs d'attaques informatiques. Le premier, dont l'un des objectifs est la collecte d'informations, pourrait servir de prélude aux deux scénarios suivants.

Scénario I — Collecte d'informations en vue d'un acte malveillant

Objectif de l'attaque — obtenir un accès physique à des zones contrôlées (à accès limité) de l'installation pour appuyer une attaque ultérieure.

La cible visée est la personne qui gère les cartes d'accès et attribue les droits d'accès. Pour obtenir un accès physique à des zones restreintes, il faudra porter atteinte à la fois à l'ordinateur de la personne chargée des cartes et au système des codes d'accès. L'assaillant choisit de se faire passer pour un sous-traitant livrant des pièces de matériel.

La collecte d'informations précédant une attaque peut notamment viser les éléments suivants :

- Informations relatives au personnel pouvant être utilisées à des fins d'extorsion ou d' « ingénierie sociale » ;
- Documents de conception du système de contrôle de l'accès ;
- Plans stratégiques et techniques des systèmes de sécurité et d'autres zones pertinentes de la centrale ;
- Calendrier d'opérations — calendrier de la centrale, activités quotidiennes, personnes en service, périodes de travail, personnes en vacances, périodes d'introduction de certains changements ;
- Liste des fournisseurs et leurs périodes de travail sur les équipements ;
- Équipements et stock de pièces ;
- Mots de passe et mesures de contrôle de l'accès ;
- Mesures administratives et techniques de contrôle de l'accès ;
- Informations sur les concepteurs de logiciels et les projets en cours ;
- Architecture du réseau ;
- Architecture des télécommunications.

Les méthodes possibles de collecte de ces informations sont notamment les suivantes :

- « Ingénierie sociale » ;
- Recherches d'informations publiques sur le web ;
- Fouille de poubelles ;
- Exploration de points d'accès (« war dialling »), traque des réseaux sans fil (« war driving ») ;

- Attaques par courriers électroniques — « hameçonnage »¹ pour avoir un accès au réseau, enregistreurs de frappe ;
- Installation de logiciels ou d'appareils sur des machines hôtes — au moyen d'un disque, d'une clé USB ou d'un CD ;
- Interception (manuelle, par un système audio ou par surveillance vidéo) du mot de passe ou du code d'accès.

L'attaque peut comprendre les activités suivantes :

- Obtention d'une carte d'accès (carte magnétique) et un code ;
- Vol/reproduction d'une carte d'accès existante ;
- Accès à l'appareil produisant les cartes pour en créer une nouvelle ;
- Enregistrement d'un nouvel employé ;
- Usurpation de l'identité d'un employé ayant cessé de travailler récemment ;
- Autorisation d'accès au niveau souhaité.

Une fois qu'il a obtenu la carte et les codes, l'assaillant utilise les informations qu'il a acquises sur l'activité de l'organisme pour entrer dans l'installation sans éveiller l'attention, en se faisant passer pour un livreur de matériel.

Scénario II — Attaque désactivant ou perturbant un ou plusieurs systèmes informatiques

Objectif de l'attaque — saboter une centrale nucléaire et empêcher son redémarrage immédiat.

Dans cet exemple, lors d'une période de mise à l'arrêt, un sous-traitant effectue des essais sur le système de commande de l'eau d'alimentation. Le prestataire installe un point d'accès à distance pour surveiller et tester le système depuis son bureau. Après la fin des travaux, le point d'accès reste en place par mégarde.

L'assaillant a recueilli sur la centrale des informations présentant le sous-traitant comme un ancien employé et une cible de choix pour obtenir des informations sur la centrale. Il lance une attaque par courrier électronique (« hameçonnage ») contre le bureau du sous-traitant et installe dans le système un programme malveillant furtif qui lui donne des droits d'administrateur. Il a dès lors accès au réseau informatique du prestataire et découvre les plans d'essais

¹ L'« hameçonnage » est une tentative d'acquisition frauduleuse d'informations sensibles comme les noms d'utilisateurs, les mots de passe et les détails de carte de crédit, en se faisant passer pour une entité fiable dans une communication électronique.

prévus dans la centrale ainsi que le point d'accès à distance qui n'a pas été désactivé par la centrale.

À l'aide de ces informations, il est en mesure de lancer une attaque par déni de service² sur le système de commande de l'eau d'alimentation en inondant le réseau de trafic pour provoquer la défaillance du système. Celui-ci avait été conçu pour ne traiter qu'un trafic minimum.

Une fois que l'assaillant a obtenu un accès, cartographié le réseau et découvert le protocole de communication, il lance l'attaque. Celle-ci empêche le système de commande de l'eau d'alimentation de répondre, ce qui oblige à arrêter d'urgence la centrale manuellement. La raison du dysfonctionnement ne peut être déterminée immédiatement et la centrale reste à l'arrêt pour permettre une enquête.

Scénario III — Atteinte à des systèmes informatiques pour une attaque coordonnée

Objectif de l'attaque — voler des matières nucléaires en transit entre des installations d'entreposage. Il s'agit de lancer une attaque informatique pour modifier le stock et le système de suivi afin de dissimuler la perte des matières volées.

Des activités de reconnaissance et de collecte de renseignements permettent de découvrir le processus de marquage et de traçage des expéditions de matières radioactives entre des installations d'entreposage. Ce processus comprend un étiquetage RFID³ de chaque élément décrivant le composant et son contenu.

Le plan de l'attaque suppose une aide interne pour enlever les matières transportées. Les phases de l'attaque sont notamment les suivantes :

- Interception du transport ;
- Retrait d'une petite quantité des matières radioactives expédiées ;
- Reprogrammation de la puce RFID pour qu'elle donne la quantité réelle restante ;
- Modification du système de suivi des stocks pour indiquer que la nouvelle quantité est en cours d'expédition et que la quantité volée est encore dans les stocks de l'installation d'origine.

² Le déni de service bloque l'autorisation d'accès aux ressources d'un système ou retarde les opérations et le fonctionnement du système.

³ Identification par radiofréquence : technologie d'identification et de suivi à l'aide des ondes radioélectriques.

L'attaque informatique vise à obtenir, via le réseau, un accès à la base de données relative au stock et à modifier les entrées de l'inventaire et du transport.

Annexe II

MÉTHODOLOGIE DE DÉTERMINATION DES EXIGENCES EN SÉCURITÉ INFORMATIQUE

Le processus de définition, de contrôle, d'élimination ou de limitation des menaces pouvant nuire à la sécurité informatique d'une installation nucléaire devrait être appliqué de manière systématique et cohérente, conformément aux normes existantes. La présente annexe étudie plus en détail une méthodologie particulière. Le choix de cette méthodologie parmi de nombreuses autres disponibles ne signifie pas que l'AIEA l'approuve ; elle devrait être considérée simplement comme un exemple détaillé. Une introduction générale à l'évaluation des risques est présentée à la section 6.1.

De manière générale, pour comprendre les menaces et les vulnérabilités en ce qui concerne un système informatisé particulier, il faut d'abord analyser ce système, sur les plans fonctionnel et technique, ensuite définir les facteurs de sûreté de fonctionnement pertinents qui doivent être maintenus, et enfin déterminer et analyser les risques associés à ces facteurs.

Les paragraphes ci-après donnent un aperçu de la méthode EBIOS. Cet acronyme français signifie « Expression des besoins et identification des objectifs de sécurité ». Cette méthode a été mise au point en France par la Direction centrale de la sécurité des systèmes d'information (DCSSI)¹.

Établie de manière formelle, elle permet d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information et comprend des outils destinés à la maîtrise d'ouvrage, à la rédaction de documents et à la sensibilisation.

On ne trouvera ici que les principes de base de la méthode, lesquels sont adaptés des documents disponibles sur le site web de la DCSSI.

Principes de la méthode EBIOS

Étude du contexte et définition du périmètre



La première étape consiste à définir le contexte technique, opérationnel et réglementaire de l'étude. Un système d'information repose en particulier sur des

¹ EBIOS 2010 – Expression des Besoins et Identification des Objectifs de Sécurité : <http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.html>

éléments essentiels, fonctions et informations, qui constituent la valeur ajoutée du système d'information pour l'organisme.

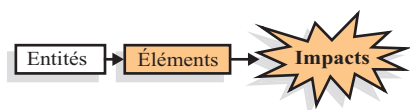
Par exemple, le système de surveillance du circuit de refroidissement d'une centrale s'appuie sur diverses informations comme des mesures, des paramètres et des résultats de calculs, et sur diverses fonctions permettant de réaliser ces calculs.

Les éléments essentiels sont liés à un ensemble d'**entités** de différents types : matériels, logiciels, réseaux, organisations, ressources humaines et sites.

Prenons l'exemple d'un paramètre utilisé pour le déclenchement de l'activation d'une pompe du circuit de refroidissement. Il est lié aux ordinateurs de contrôle, aux logiciels de traitement, aux opérateurs, à l'état des sources froides, à l'état de la centrale, aux règlements applicables, etc.

Résultat : Cible de l'étude (contexte + éléments + entités)

Expression des sensibilités



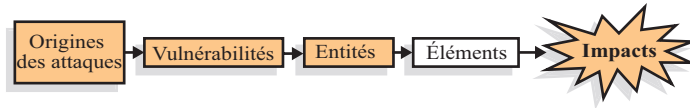
Pour garantir le fonctionnement correct des opérations, la **sensibilité** de chaque élément essentiel doit être exprimée.

Cette expression s'appuie sur différents **critères de sécurité** tels que la disponibilité, l'intégrité et la confidentialité. Si cette sensibilité n'est pas étudiée, cela aura sur l'organisme un **impact** qui peut prendre différentes formes, comme une atteinte à la sécurité nucléaire, à la sûreté, ou au bon déroulement des activités, la perte de confiance du client ou des pertes financières.

Reprenons l'exemple du paramètre de déclenchement de l'activation de la pompe du circuit de refroidissement d'une centrale. Les exigences de disponibilité et d'intégrité pour ce paramètre devraient être élevées pour éviter tout impact préjudiciable sur le matériel, l'environnement ou le personnel, mais aussi pour garantir la disponibilité de la centrale.

Résultat : sensibilités.

Étude des menaces



Chaque organisme est exposé à divers éléments menaçants, de par son environnement naturel, sa culture, son image, son domaine d'activité, etc. Un élément menaçant peut être caractérisé selon son type (naturel, humain ou environnemental) et selon sa cause (accidentelle ou délibérée).

L'élément menaçant peut employer diverses **méthodes d'attaque**, qu'il convient donc d'identifier. Une méthode d'attaque se caractérise par les critères de sécurité qu'elle peut affecter (disponibilité, intégrité, confidentialité) et par les éléments menaçants susceptibles de l'utiliser.

Poursuivons avec notre exemple. Une centrale nucléaire doit prendre en compte un grand nombre d'éléments menaçants, comme il est précisé à la section 6.3 :

- Espion/voleur de technologie ;
- Employé/utilisateur (interne ou externe) mécontent ;
- Pirate amateur ;
- Cyberactiviste ;
- Crime organisé ;
- État-nation ;
- Terroriste.

Elle doit également prendre en compte les méthodes d'attaque :

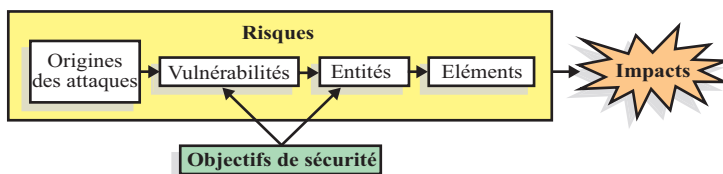
- Écoute ;
- Inondation de réseau/déni de service ;
- Installation d'un piège/d'une porte dérobée dans le logiciel ;
- Attaques contre l'identifiant/le mot de passe (attaque en force, attaque par dictionnaire, etc.).

Chaque entité possède des **vulnérabilités** qui pourront être exploitées par les éléments menaçants selon chaque méthode d'attaque. On pourra mettre en évidence plusieurs vulnérabilités liées au circuit de refroidissement de la centrale nucléaire :

- Possibilité d'existence de fonctions cachées introduites en phase de conception ou de développement (logiciels) ;
- Utilisation d'équipements non évalués (matériel informatique) ;
- Possibilité de créer ou de modifier des commandes de systèmes en ligne (réseaux) ;
- Utilisation du réseau pour agir sur des logiciels de ressources du système (réseaux) ;
- Facilité de pénétrer sur le site par des accès indirects (locaux) ;
- Non-respect des consignes de la part des opérateurs (personnel) ;
- Absence de mesures de sécurité dans les phases de conception, d'installation et d'exploitation (organisation).

Résultat : Établissement formel des menaces (y compris des scénarios).

Expression des objectifs de sécurité



Il faut maintenant déterminer comment les éléments essentiels peuvent être affectés par les éléments menaçants et par leurs méthodes d'attaque : il s'agit du **risque**.

Le risque représente un sinistre possible. C'est le fait qu'un élément menaçant puisse affecter des éléments essentiels en exploitant les vulnérabilités des entités sur lesquelles ils reposent avec une méthode d'attaque particulière.

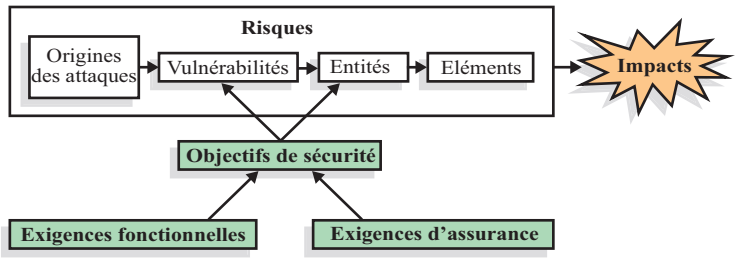
Dans notre exemple, il existe un risque d'atteinte à des informations sensibles par piégeage de logiciel, car il est possible de créer ou de modifier des commandes de systèmes liées au réseau, ce qui pourrait avoir un impact sur le matériel, l'environnement, la sûreté du personnel, la disponibilité de la centrale et la confiance du public.

Les **objectifs de sécurité** consistent principalement à couvrir les vulnérabilités des entités qui composent l'ensemble des risques retenus. Il est bien entendu inutile de protéger ce qui n'est pas exposé. Toutefois, plus le potentiel de risque est important, plus le niveau des objectifs de sécurité sera élevé. Ces objectifs constituent ainsi un cahier des charges parfaitement adapté.

L'un des objectifs de sécurité de la centrale nucléaire de l'exemple est de protéger la création et la modification des commandes de systèmes liés au réseau du circuit de refroidissement.

Résultat : objectifs de sécurité.

Détermination des exigences de sécurité



L'équipe en charge de la mise en œuvre de la méthode doit ensuite préciser exactement les fonctionnalités attendues en matière de sécurité. Elle doit alors démontrer la parfaite couverture des objectifs de sécurité par ces **exigences fonctionnelles**.

Dans notre exemple, les exigences fonctionnelles visant à protéger la création et la modification des commandes de systèmes liés au réseau pourraient être les suivantes :

- Série d'auto-vérifications conduites à intervalles réguliers par le système pendant les opérations courantes pour s'assurer qu'il fonctionne correctement ;
- Contrôle de l'accès physique et logique.

Enfin, l'équipe en charge doit spécifier les **exigences d'assurance** qui permettent d'obtenir le niveau de confiance requis, pour ensuite le démontrer.

L'une des exigences d'assurance pourrait être que : le concepteur doit effectuer une analyse de la résistance des fonctions de sécurité du système selon le niveau de résistance requis.

Résultat : exigences fonctionnelles et exigences d'assurance.

Annexe III

RÔLE DE L'ERREUR HUMAINE EN SÉCURITÉ INFORMATIQUE

La présente annexe examine les questions de performance humaine liées à la sécurité informatique, et en particulier la manière dont cette performance peut influencer la capacité de l'organisation de résister à une attaque, de la reconnaître, de récupérer des données/services essentiels et de s'adapter aux menaces émergentes. La recherche continue d'encourager la mise au point de solutions techniques comme des logiciels de surveillance de sécurité, des programmes de détection/prévention des intrusions, des systèmes d'authentification plus robustes et des méthodes de cryptage plus solides, mais bien souvent, l'élément humain n'est pas considéré comme pouvant causer ou prévenir une attaque en sécurité informatique.

De nombreux rapports ont montré que l'erreur humaine était la principale cause d'atteintes à la sécurité informatique. Des estimations récentes indiquent que 60 à 80 % des atteintes étaient liées à une erreur humaine. La plupart de ces erreurs auraient pu être prévenues grâce à des investissements accrus dans la sensibilisation et une plus grande diligence dans les opérations et le contrôle.

La capacité de survie du système / des opérations est l'un des objectifs d'un programme de sécurité informatique. Les éléments de la capacité de survie d'un système sont les suivants :

- Résistance du système à une attaque ;
- Reconnaissance d'une attaque et évaluation des dommages ;
- Service essentiel et récupération totale du service ;
- Adaptation et évolution du système comme moyen de défense contre de futures attaques.

Le tableau III-1 illustre ces principaux domaines en classant les types courants d'erreurs humaines dans les processus et les applications. Ces erreurs sont répertoriées tant pour les administrateurs que pour les utilisateurs des systèmes. Cette liste ne se veut pas exhaustive mais est conçue pour illustrer le niveau d'interaction humaine associé à l'utilisation de ces systèmes et processus.

Bien que ce tableau soit axé sur les aspects négatifs de la performance humaine, il convient aussi de noter que celle-ci a aussi un impact positif. Même s'il est parfois le maillon faible de la chaîne, l'opérateur humain ou l'employé peut être aussi un rempart contre la défaillance ou la perturbation du système. La technologie ne sera jamais une solution complète. Les employés sont l'un des niveaux d'une stratégie de défense en profondeur visant à assurer la sécurité / la capacité de survie du système. Les enquêtes montrent régulièrement

TABLE III–1. ERREURS HUMAINES COMMUNES

Processus/application	Erreurs humaines communes
Résistance à une attaque	
Restriction de l'accès (Administration du système)	— Permissions de fichier inadéquates. — Services inutilement laissés en marche. — Ports vulnérables laissés ouverts. — Accès physique autorisé. — Non utilisation d'économiseurs d'écran avec mot de passe. — Correctifs de système non installés. — Méconnaissance des incidences de l'installation d'un correctif. — Téléchargement/installation d'un logiciel malveillant/corrompu.
Génération/utilisation de mot de passe	— Mots de passe notés sur papier. — Mots de passe vulnérables. — Utilisation de mots de passe par défaut. — Divulgation du mot de passe. — Non utilisation d'un mot de passe. — Utilisation du même mot de passe dans les systèmes sécurisés et non sécurisés.
Reconnaissance d'une attaque et des dommages	
Systèmes de détection d'intrusion	— Configuration inadaptée (ensemble de règles). — Pas de mise à jour des systèmes. — Manque de vigilance dans l'examen du registre d'activités.
Vérification des registres d'activités	— Pas d'examen appliqué des registres d'activités. — Pas de reconnaissance des tendances sur plusieurs périodes couvertes par les registres d'activités.
Récupération de système	
Sauvegarde et restauration	— Absence de procédure de sauvegarde. — Absence de procédure de sauvegarde en temps opportun. — Configuration inappropriée. — Endommagement physique des supports de sauvegarde. — Suppression accidentelle de données. — Dispositifs de sauvegarde conservés dans un emplacement non sécurisé/non protégé. — Utilisation de supports défectueux. — Erreur de marquage de supports. — Destruction physique de supports.

TABLE III–1. ERREURS HUMAINES COMMUNES (suite)

Processus/application	Erreurs humaines communes
Sauvegarde et restauration	— Pas d’essai des procédures de restauration. — Pas de copies multiples des informations cruciales relatives au système. — Supports de sauvegarde non conservés dans un emplacement hors site.
Adaptation aux menaces nouvelles	
Procédures internes	— Méconnaissance de la politique interne. — Violation de la politique interne. — Absence de politique interne pour la récupération. — Utilisation d’une politique dépassée. — Non vérification de la politique / de la procédure à suivre. — Non-exécution de la politique.

que le principal problème de sécurité est l’inadéquation de la sensibilisation et de la formation à la sécurité informatique.

Pour que les employés soient pleinement utilisés comme atout pour la sécurité informatique et la capacité de survie des systèmes, ils doivent :

- bien comprendre l’importance de leur rôle dans l’ensemble du plan de sécurité informatique ;
- avoir les connaissances et les compétences requises en matière de sécurité informatique pour pouvoir s’acquitter de leurs responsabilités ;
- comprendre qu’une culture de sécurité efficace commence avec eux.

La présente publication a été remplacée par la publication suivante : 17-T (Rev. 1).

DÉFINITIONS

On trouvera ci-après le sens donné aux termes ci-dessous dans le contexte de la présente publication. Ces définitions peuvent être différentes dans d'autres disciplines. Lorsqu'elles existent, les définitions sont extraites d'autres publications existantes de l'AIEA, même si quelques termes sont utilisés ici dans le contexte particulier de la sécurité informatique. D'autres définitions proviennent des normes internationales (par exemple les références [1, 15, 23] de la présente publication).

attaque. Tentative de détruire, de rendre public, de modifier, d'invalider, de voler ou d'obtenir un accès non autorisé ou d'utiliser sans autorisation un actif (ISO).

authentification. Moyen pour une entité d'assurer la légitimité d'une caractéristique revendiquée (ISO).

besoin de savoir. Principe en vertu duquel les utilisateurs, les processus et les systèmes ne peuvent avoir accès qu'aux informations, possibilités et ressources nécessaires à l'exécution de leurs fonctions autorisées.

confidentialité. Propriété selon laquelle l'information n'est pas rendue disponible ou divulguée à des personnes, des entités ou des processus non autorisés (ISO).

contremesure. Mesure prise pour contrer une menace, ou pour éliminer ou réduire des vulnérabilités.

contrôle de l'accès. Moyens mis en œuvre pour assurer que l'accès aux actifs est autorisé et limité selon les exigences propres à la sécurité et à l'activité métier (ISO).

défense en profondeur. Combinaison de niveaux successifs de systèmes et de mesures visant à protéger des objectifs contre des menaces à la sécurité nucléaire.

disponibilité. Propriété d'être accessible et utilisable à la demande par une entité autorisée (ISO).

évaluation du risque. Processus général de détermination, d'estimation, d'analyse et d'évaluation systématiques du risque.

incident de sécurité informatique. Événement qui nuit effectivement ou peut nuire à la confidentialité, à l'intégrité, ou à la disponibilité d'un système informatique, de réseau ou d'information numérique ou aux informations traitées, conservées ou transmises par le système, ou qui constitue une violation ou présente un risque imminent de violation des politiques de sécurité, des procédures de sécurité ou des politiques d'utilisation acceptables.

ingénierie sociale. Forme non technique de collecte d'informations ou d'attaque utilisant les relations humaines pour manipuler les gens et les amener à violer involontairement les procédures de sécurité, par exemple en divulguant des informations ou en posant d'autres actes ayant un impact du point de vue de la sécurité.

installation nucléaire. Installation (y compris les bâtiments et équipements associés) dans laquelle des matières nucléaires sont produites, traitées, utilisées, manipulées, entreposées ou stockées définitivement et pour laquelle une autorisation ou une licence est exigée.

intégrité. Propriété de protection de l'exactitude et de la complétude des actifs (ISO).

menace. Cause potentielle d'un incident indésirable, qui peut nuire à un système ou une organisation (ISO).

Note : dans d'autres publications de la collection Sécurité nucléaire, la « menace » est normalement définie comme une « personne ou [un] groupe de personnes ayant la motivation, l'intention et les moyens de commettre un acte malveillant ». Toutefois, ce terme est utilisé dans la présente publication dans le contexte de la sécurité informatique, où la menace n'est pas nécessairement une personne ou un groupe de personnes.

périmètre de sécurité informatique. Frontière logique autour d'un réseau à laquelle des actifs critiques sont connectés et dont l'accès est contrôlé.

politique de sécurité informatique. Ensemble de directives, réglementations, règles et pratiques régissant la manière dont une organisation gère et protège ses ordinateurs et ses systèmes informatiques.

risque. Possibilité qu'une menace donnée exploite les vulnérabilités d'un actif ou d'un groupe d'actifs et cause ainsi un dommage à l'organisation. Elle se mesure par une combinaison de la probabilité d'un événement et de la gravité de ses conséquences.

sécurité de l'information. Protection de la confidentialité, de l'intégrité et de la disponibilité de l'information.

Note : En outre, d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité, peuvent également être concernées (ISO).

sécurité informatique. Aspect particulier de la sécurité de l'information touchant les systèmes informatiques, les réseaux et les systèmes numériques.

vulnérabilité. Faille dans un actif ou dans une mesure de sécurité qui peut être exploitée par une menace (ISO).

La présente publication a été remplacée par la publication suivante : 17-T (Rev. 1).



IAEA

Agence internationale de l'énergie atomique

N° 22

Lieux de vente des publications de l'AIEA

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

ALLEMAGNE

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

AUSTRALIE

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

BELGIQUE

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

CANADA

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

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

CHINE

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

CORÉE, RÉPUBLIQUE DE

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

ESPAGNE

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

ÉTATS-UNIS D'AMÉRIQUE

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

Renouf Publishing Company Ltd., 812 Proctor Ave., Ogdensburg, NY, 13669
Téléphone : +888 551 7470 (n° vert) • Télécopie : +888 568 8546 (n° vert)
Courriel : order.dept@renoufbooks.com • Site web : <http://www.renoufbooks.com>

FINLANDE

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

FRANCE

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

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

HONGRIE

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

INDE

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

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

ITALIE

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

JAPON

Maruzen Company Ltd, 1-9-18, Kaigan, Minato-ku, Tokyo, 105-0022
Téléphone : +81 3 6367 6079 • Télécopie : +81 3 6367 6207
Courriel : journal@maruzen.co.jp • Site web : <http://www.maruzen.co.jp>

NOUVELLE-ZÉLANDE

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

ORGANISATION DES NATIONS UNIES

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

PAYS-BAS

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

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

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

RÉPUBLIQUE TCHÈQUE

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

ROYAUME-UNI

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

Commandes en ligne

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

Ouvrages sur l'environnement

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

SLOVÉNIE

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

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

Unité de la promotion et de la vente, Agence internationale de l'énergie atomique

Centre international de Vienne, B.P. 100, 1400 Vienne (Autriche)
Téléphone : +43 1 2600 22529 (ou 22530) • Télécopie : +43 1 2600 29302
Courriel : sales.publications@iaea.org • Site web : <http://www.iaea.org/books>

La présente publication vise à sensibiliser à la nécessité de tenir compte de la sécurité informatique en tant qu'élément fondamental de la sécurité générale des installations nucléaires. Elle a en outre pour objectif de fournir des orientations aux installations nucléaires sur la mise en œuvre d'un programme de sécurité informatique, de donner des conseils sur l'évaluation des programmes existants, d'évaluer les biens numériques essentiels et de déterminer les mesures appropriées de réduction des risques.

**AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE**

ISBN 978-92-0-237010-4

ISSN 1816-9317