Collection Sécurité nucléaire de l'AIEA nº 17-T (Rev. 1)

Orientations techniques

Techniques de sécurité informatique pour les installations nucléaires

IAEA
Agence internationale de l'énergie atomique

COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA

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

CATÉGORIES DANS LA COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA

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

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

RÉDACTION ET EXAMEN

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

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

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

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

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

TECHNIQUES DE SÉCURITÉ INFORMATIQUE POUR LES INSTALLATIONS NUCLÉAIRES

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

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

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

COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA –
Nº 17-T (Rev. 1)

TECHNIQUES DE SÉCURITÉ INFORMATIQUE POUR LES INSTALLATIONS NUCLÉAIRES

ORIENTATIONS TECHNIQUES

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE, 2024

DROIT D'AUTEUR

Unité de la promotion et de la vente
Section d'édition
Agence internationale de l'énergie atomique
Centre international de Vienne
B.P. 100
1400 Vienne (Autriche)
Télécopie : +43 1 26007 22529
Téléphone : +43 1 2600 22417
Courriel : sales.publications@iaea.org
https://www.iaea.org/fr/publications

Imprimé par l'AIEA en Autriche
Avril 2024
STI/PUB/1921

TECHNIQUES DE SÉCURITÉ INFORMATIQUE POUR LES INSTALLATIONS NUCLÉAIRES
AIEA, VIENNE, 2024
STI/PUB/1921
ISBN 978-92-0-210023-7 (imprimé) | ISBN 978-92-0-209523-6 (pdf) | ISBN 978-92-0-209623-3 (ePub)
ISSN 2520-6931

AVANT-PROPOS

de Rafael Mariano Grossi
Directeur général

La collection Sécurité nucléaire de l'AIEA fournit des orientations faisant l'objet d'un consensus international sur tous les aspects de la sécurité nucléaire afin d'aider les États à honorer leurs responsabilités en la matière. L'AIEA établit et tient à jour ces orientations dans le cadre de sa mission centrale d'assistance et de coordination internationales concernant la sécurité nucléaire.

Lancée en 2006, la collection Sécurité nucléaire est actualisée en permanence par l'AIEA, en coopération avec des experts des États Membres. En tant que Directeur général, je m'engage à veiller à ce que l'AIEA entretienne et améliore cet ensemble intégré, complet et cohérent de publications de qualité adaptées à l'utilisateur, aux réalités de l'époque et aux besoins en matière de sécurité. L'utilisation adéquate de ces orientations dans le cadre des applications de la science et de la technologie nucléaires devrait permettre d'atteindre un niveau élevé de sécurité nucléaire et établir la confiance nécessaire à l'utilisation continue de la technologie nucléaire pour le bien de tous.

C'est aux pays qu'il appartient de garantir la sécurité nucléaire. Les publications de la collection Sécurité nucléaire de l'AIEA complètent les instruments juridiques internationaux en la matière et servent de référence mondiale pour aider les parties à honorer leurs obligations. Bien qu'elles ne soient pas juridiquement contraignantes pour les États Membres, les orientations sur la sécurité sont largement appliquées. Elles sont devenues une référence indispensable et un dénominateur commun pour la grande majorité des États Membres qui les appliquent dans leur réglementation nationale pour améliorer la sécurité nucléaire des centrales nucléaires, des réacteurs de recherche et des installations du cycle du combustible ainsi que des applications nucléaires en médecine, dans l'industrie, dans l'agriculture et dans la recherche.

Les orientations de la collection Sécurité nucléaire de l'AIEA se basent sur l'expérience pratique des États Membres et font l'objet d'un consensus international. La participation des membres du Comité des orientations sur la sécurité nucléaire et d'autres personnes est particulièrement importante, et je suis reconnaissant à tous ceux qui, par leurs connaissances et leurs compétences, contribuent à l'élaboration de ces orientations.

L'AIEA utilise également les orientations de la collection Sécurité nucléaire lorsqu'elle apporte une assistance aux États Membres dans le cadre de missions d'examen et de services consultatifs, aidant ainsi ces États Membres à appliquer lesdites orientations et facilitant l'échange de données d'expérience et d'idées

utiles. Les informations en retour sur ces missions et services, de même que les enseignements tirés des événements et l'expérience relative à l'utilisation et à l'application des orientations sur la sécurité, sont pris en compte lors de la révision périodique de ces dernières.

Je suis convaincu que les orientations de la collection Sécurité nucléaire de l'AIEA et leur application contribuent de manière inestimable à assurer un niveau élevé de sécurité nucléaire dans le cadre de l'utilisation de la technologie nucléaire. J'encourage tous les États Membres à les promouvoir et à les appliquer et à collaborer avec l'AIEA pour en maintenir la qualité, aujourd'hui comme demain.

NOTE DE L'ÉDITEUR

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

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

Les termes relatifs à la sécurité ont le sens donné dans la publication où ils figurent, ou dans les orientations que la publication soutient. Les autres termes sont utilisés dans leur sens courant.

Lorsqu'une norme comporte un appendice, celui-ci est réputé faire partie intégrante de la norme. Les informations figurant dans un appendice ont le même statut que le corps du texte. Les annexes ont pour objet de donner des exemples concrets ou des précisions ou explications. Elles ne sont pas considérées comme faisant partie intégrante du texte principal.

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

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

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

TABLE DES MATIÈRES

1. INTRODUCTION

CONTEXTE

1.1. La sécurité nucléaire est destinée à prévenir et à détecter les actes criminels et les actes non autorisés délibérés mettant en jeu ou visant des matières nucléaires, d'autres matières radioactives, des installations associées ou des activités associées, et à intervenir si de tels actes sont commis. La sécurité nucléaire des matières et installations nucléaires englobe la protection physique, les aspects de la sécurité qui concernent le personnel (habilitation et mesures de protection contre les menaces internes, par exemple) et la sécurité de l'information.

1.2. Les groupes ou les individus qui préparent ou commettent un acte malveillant mettant en jeu des matières nucléaires ou une installation nucléaire peuvent tirer parti d'informations sensibles et de ressources d'informations sensibles qui concernent les matières, l'installation ou les mesures de sécurité en vigueur.

1.3. Les Fondements de la sécurité nucléaire [1] et les trois Recommandations de sécurité nucléaire [2–4] soulignent qu'il importe de protéger les informations sensibles. La publication n° 23-G de la collection Sécurité nucléaire de l'AIEA, intitulée « Sécurité de l'information nucléaire » [5], donne des orientations sur les mesures qui permettent de recenser, de classer et de protéger les informations sensibles afin d'atteindre une sécurité de l'information efficace dans le cadre d'un régime de sécurité nucléaire national.

1.4. Une cyberattaque contre une installation nucléaire peut contribuer à causer des dommages matériels à l'installation ou à désactiver ses systèmes de sûreté ou de sécurité (c'est-à-dire à les saboter), ou faciliter l'accès à des informations nucléaires sensibles ou permettre un enlèvement non autorisé de matières nucléaires. Dans une installation nucléaire, la sécurité informatique est donc indispensable pour préserver la sécurité et la sûreté nucléaires.

1.5. La protection des ressources numériques sensibles[1] (RNS) est recommandée au paragraphe 4.10 de la référence [2], selon lequel

> « [l]es systèmes informatisés utilisés pour la protection physique, la sûreté nucléaire et la comptabilité et le contrôle des matières nucléaires devraient

[1] Les ressources numériques sensibles sont des ressources d'informations sensibles qui sont des systèmes informatiques (ou en font partie).

être protégés contre la compromission (cyberattaque, manipulation ou falsification, par exemple) conformément à l'*évaluation de la menace* ou à la *menace de référence*. »

Le besoin particulier de protection des systèmes informatiques contre les menaces internes est confirmé dans la référence [6].

1.6. Des orientations générales sur la sécurité informatique pour la sécurité nucléaire figurent dans la publication n° 42-G de la collection Sécurité nucléaire de l'AIEA, intitulée « Sécurité informatique pour la sécurité nucléaire » [7], et des orientations plus précises sur la sécurité informatique des systèmes de contrôle-commande figurent dans la publication n° 33-T de la collection Sécurité nucléaire de l'AIEA, intitulée « Sécurité informatique des systèmes de contrôle-commande dans les installations nucléaires » [8]. La présente publication vise à compléter ces orientations en donnant des informations détaillées sur les techniques de sécurité informatique pour d'autres systèmes utilisés dans les installations nucléaires.

OBJET

1.7. La présente publication a pour objet d'aider les États Membres à mettre en œuvre la sécurité informatique dans les installations nucléaires afin d'empêcher l'enlèvement non autorisé de matières nucléaires, le sabotage d'installations nucléaires et l'accès non autorisé à des informations nucléaires sensibles, et d'assurer une protection contre de tels actes. Elle traite la question de la sécurité informatique pour les activités de soutien et les organismes qui apportent un appui, comme les vendeurs, les sous-traitants et les fournisseurs. La présente publication est principalement consacrée à la sécurité des installations nucléaires, mais l'application de ces orientations peut également avoir un effet positif sur la sûreté des installations et la performance d'exploitation.

1.8. La présente publication porte aussi sur l'utilisation d'approches fondées sur les risques pour mettre en place et améliorer les politiques, les programmes et les mesures de sécurité informatique qui visent à protéger les RNS et les autres ressources numériques. Une installation nucléaire est tributaire de RNS et d'autres ressources numériques pour sa sûreté et sa sécurité. La présente publication décrit l'intégration de la sécurité informatique dans le système de gestion d'une installation ou d'une organisation, et contient des orientations sur la définition des règles et des exigences et sur les activités menées pour élaborer, appliquer, pérenniser, maintenir, évaluer et améliorer continuellement les mesures de sécurité

informatique qui protègent l'installation contre les cyberattaques conformément à l'évaluation de la menace ou à la menace de référence [9].

1.9. La présente publication donne également des orientations techniques pour protéger d'autres ressources numériques présentes dans une installation nucléaire.

1.10. La présente publication est destinée aux organismes de réglementation et aux autres autorités compétentes, ainsi qu'aux exploitants d'installations nucléaires et à leurs vendeurs, à leurs sous-traitants et à leurs fournisseurs.

CHAMP D'APPLICATION

1.11. Les orientations qui figurent dans la présente publication concernent la mise en œuvre et la gestion de la sécurité informatique pour la sécurité nucléaire dans les installations nucléaires. Elles s'appliquent à toutes les étapes de la vie d'une installation nucléaire [10].

1.12. Dans une installation nucléaire, la sécurité informatique vise à protéger différents systèmes qui contribuent à assurer différents aspects de la sécurité nucléaire, comme le système de protection physique ou le système de comptabilité et de contrôle des matières nucléaires. La question de la conception ou du fonctionnement de ces systèmes n'est pas abordée dans la présente publication, sauf dans la mesure où elle a un rapport avec la protection des systèmes par des mesures de sécurité informatique.

1.13. La présente publication prend en compte toutes les ressources numériques associées à une installation nucléaire, y compris les systèmes de contrôle-commande de l'installation. Des orientations supplémentaires sur les questions particulières de sécurité informatique pour les systèmes de contrôle-commande d'une installation qui exécutent des fonctions de sûreté ou de sécurité, ou des fonctions auxiliaires, figurent dans la référence [8].

STRUCTURE

1.14. Après la présente introduction, la section 2 définit les termes essentiels et les notions de base, et décrit les relations qui existent entre ces notions. La section 3 expose des considérations générales sur la sécurité informatique dans les installations nucléaires. Les sections 4 et 5 donnent des orientations sur la gestion des risques liés à la sécurité informatique (GRSI), respectivement au niveau d'une

installation et d'un système. La section 6 contient des orientations sur la GRSI pour une installation ou un système qui concernent les différentes étapes de la vie de l'installation concernée. La section 7 donne une vue d'ensemble du programme de sécurité informatique (PSI). La section 8 présente un exemple d'utilisation d'une architecture de sécurité informatique défensive (ASID) et de mise en œuvre des mesures de sécurité informatique correspondantes.

1.15. L'appendice contient des orientations portant spécifiquement sur certains éléments du PSI. L'annexe I donne des exemples de scénarios d'attaque qui peuvent servir à évaluer la sécurité dans une installation nucléaire. L'annexe II présente un exemple d'affectation des niveaux de sécurité informatique dans une centrale nucléaire. L'annexe III donne un exemple d'application du principe des niveaux et des zones de sécurité informatique.

2. NOTIONS DE BASE ET RELATIONS QUI EXISTENT ENTRE ELLES

2.1. La présente section clarifie le sens de termes importants qui sont employés dans toute la publication.

SÉCURITÉ NUCLÉAIRE ET SÉCURITÉ INFORMATIQUE

2.2. Selon les Fondements de la sécurité nucléaire [1], les cibles sont les suivantes dans le domaine de la sécurité nucléaire :

> « *Matières nucléaires*, *autres matières radioactives*, *installations associées*, *activités associées* ou autres emplacements ou objets pouvant être exploités par une *menace contre la sécurité nucléaire*, y compris les *grandes manifestations publiques*, les *emplacements stratégiques*, les *informations sensibles* et les *ressources d'informations sensibles*. »

Les informations sensibles comprennent les informations stockées dans les RNS, mais aussi les logiciels installés sur ces ressources, notamment les logiciels exécutés, les micrologiciels embarqués, les outils de développement, les outils de tests, les logiciels de maintenance et les systèmes d'exploitation.

2.3. Selon la référence [1],un système de sécurité nucléaire est un « [e]nsemble intégré de *mesures de sécurité nucléaire* ». Les mesures de sécurité nucléaire sont définies comme suit :

> « Mesures visant soit à prévenir une *menace contre la sécurité nucléaire* découlant de l'accomplissement d'actes criminels ou d'actes non autorisés délibérés mettant en jeu ou visant des *matières nucléaires*, d'*autres matières radioactives*, ou des *installations* ou *activités associées*, soit à détecter des *événements de sécurité nucléaire* ou à intervenir en cas de tels événements. » [1]

2.4. Selon les orientations générales sur la sécurité informatique [7] : « Dans le cadre de son régime de sécurité nucléaire, l'État devrait élaborer et pérenniser une stratégie nationale de sécurité informatique. » Comme les installations nucléaires relèvent du régime de sécurité nucléaire, les mesures de sécurité informatique applicables dans ces installations doivent être intégrées dans la stratégie nationale. Les fonctions d'une installation qui contribuent à la sûreté et à la sécurité doivent être protégées contre les adversaires. Lorsque ces fonctions reposent sur des techniques numériques ou en dépendent ou en bénéficient, des mesures de sécurité informatique doivent être adoptées pour les protéger.

2.5. La sécurité informatique concerne les systèmes informatiques, surtout ceux qui exécutent ou appuient des fonctions d'une installation importantes pour la sécurité et la sûreté nucléaires (c'est-à-dire les ressources numériques) ou ayant un rapport avec ces domaines. Elle se compose de techniques et d'outils qui permettent de se protéger contre les cyberattaques et contre les actes ou les omissions qui pourraient compromettre la sécurité.

Fonctions d'une installation, niveaux de sécurité informatique et zones de sécurité informatique

2.6. Pour protéger méthodiquement des systèmes selon une approche graduée, l'une des techniques classiques consiste à recourir aux notions de niveau de sécurité informatique et de zone de sécurité informatique. Le niveau de sécurité informatique qui est attribué à une zone de sécurité informatique est déterminé par la plus forte protection de la sécurité qui est nécessaire pour chaque fonction de l'installation qui est exécutée par un système présent dans cette zone. Le même niveau de sécurité informatique est attribué à tous les systèmes d'une zone. Lorsque ce modèle est appliqué, une installation nucléaire se compose généralement de nombreuses zones différentes, et plusieurs zones peuvent avoir le même niveau de sécurité informatique.

2.7. Une fonction d'une installation est un ensemble coordonné d'actions et de processus qui doivent être exécutés dans une installation nucléaire. Les fonctions d'une installation comprennent les fonctions qui sont importantes pour la sécurité nucléaire ou qui intéressent la sécurité nucléaire, et les fonctions qui sont importantes pour la sûreté nucléaire ou qui intéressent la sûreté nucléaire (c'est-à-dire les fonctions de sûreté)[2]. Les fonctions d'une installation sont confiées à des systèmes[3], et chacun d'entre eux exécute une ou plusieurs de ces fonctions.

2.8. Le niveau de sécurité informatique est un chiffre qui indique le degré de protection de la sécurité qui est nécessaire pour une fonction d'une installation, et donc pour le système qui exécute la fonction en question. Chaque niveau de sécurité informatique s'accompagne d'une série d'exigences imposées par l'exploitant pour que les ressources numériques auxquelles a été attribué le niveau concerné bénéficient d'une protection appropriée selon une approche graduée. Chacun d'entre eux requiert différentes séries de mesures de sécurité informatique pour répondre aux exigences de sécurité informatique du niveau en question.

2.9. Une zone de sécurité informatique est un regroupement logique ou physique de ressources numériques auxquelles est attribué le même niveau de sécurité informatique et qui sont soumises aux mêmes exigences de sécurité informatique en raison des caractéristiques des systèmes ou de leurs connexions avec d'autres systèmes (des critères supplémentaires sont utilisés au besoin). Le recours aux zones de sécurité informatique vise à simplifier la gestion, la communication et l'application des mesures de sécurité informatique[4].

2.10. Les critères supplémentaires qui sont appliqués pour la définition des zones de sécurité informatique peuvent notamment être les suivants :

a) les responsabilités au sein de l'organisation, par exemple des zones de sécurité informatique différentes pour des systèmes qui relèvent de départements différents ;
b) la nécessité de maintenir une séparation, par exemple des zones de sécurité informatique différentes pour des systèmes redondants qui ont le même niveau de sécurité informatique et exécutent la même fonction d'une installation ;

---

[2] Les fonctions d'une installation comprennent également les fonctions opérationnelles et administratives (ou organisationnelles).

[3] Un système peut se trouver sur le site ou hors du site, ou être un système en nuage.

[4] La notion de zone de sécurité informatique peut être appliquée aux installations existantes ou anciennes et aux nouveaux bâtiments.

c) les zones déjà définies à d'autres fins ; par souci de simplicité, une zone de sécurité informatique est par exemple définie de la même manière qu'une zone déjà créée pour des besoins administratifs ou à des fins de communication.

2.11. Les relations théoriques entre les notions de fonction d'une installation, de niveau de sécurité informatique, de système et de zone de sécurité informatique sont représentées sur la figure 1.

2.12. Sur la figure 1, chacune des relations théoriques est associée à une lettre, et on trouvera ci-après la description correspondante :

a) Chaque fonction d'une installation se voit attribuer un seul niveau de sécurité informatique.
b) Chaque niveau de sécurité informatique peut être attribué à une ou plusieurs fonctions d'une installation.

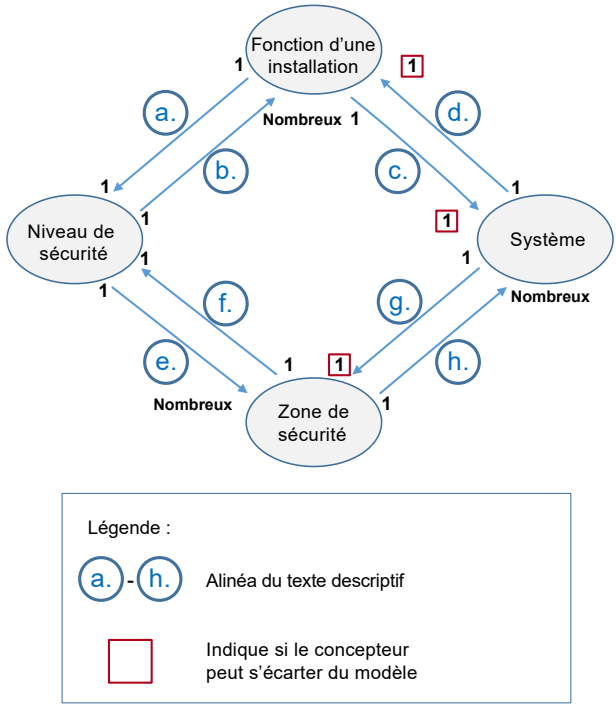

FIG. 1. Relations théoriques entre une fonction d'une installation, un niveau de sécurité informatique, un système et une zone de sécurité informatique.

c) Chaque fonction d'une installation est idéalement affectée à un seul système, dans la mesure du possible[5].
d) Chaque système exécute idéalement une seule fonction d'une installation, dans la mesure du possible[6].
e) Chaque niveau de sécurité informatique peut être attribué à une ou plusieurs zones de sécurité.
f) Chaque zone de sécurité informatique se voit attribuer un seul niveau de sécurité informatique.
g) Chaque système est installé dans une seule zone de sécurité informatique, dans la mesure du possible[7].
h) Chaque zone de sécurité informatique peut contenir un ou plusieurs systèmes.

Gestion des risques liés à la sécurité informatique

2.13. La GRSI pour une installation (voir la section 4) concerne les fonctions de l'installation et permet d'attribuer un niveau de sécurité informatique à ces fonctions et de les confier à un ou plusieurs systèmes. Les systèmes se voient attribuer le niveau de sécurité informatique des fonctions qui leur sont confiées.

2.14. La GRSI pour un système (voir la section 5) fait partie de la GRSI pour une installation, est consacrée à un système particulier et permet de déterminer a) les limites des zones de sécurité informatique à partir des fonctions de l'installation exécutées et des connexions des systèmes, et b) les mesures de sécurité informatique à appliquer pour répondre aux exigences du niveau de sécurité informatique de la zone.

---

[5] Une fonction peut par exemple être affectée à deux systèmes d'arrêt indépendants et différents.

[6] Une interface homme-machine, par exemple. Du point de vue de la sécurité, l'idéal est qu'un système exécute une seule fonction d'une installation, mais les concepteurs peuvent au besoin affecter plusieurs fonctions à un système au bénéfice des performances humaines, de la performance d'exploitation ou de la performance en matière de sûreté.

[7] Du point de vue de la sécurité, l'idéal est que chaque fonction d'une installation soit exécutée par un seul système, qui se trouve dans une seule zone de sécurité informatique et qui s'est donc vu attribuer un seul niveau de sécurité, mais les concepteurs peuvent s'écarter de ce modèle pour certaines raisons, par exemple dans le cas du système de protection contre l'incendie et du système de protection physique, qui s'étendent sur toute l'installation (ou sur une part importante de celle-ci) et peuvent donc traverser des parties où se trouvent des zones auxquelles ont été attribués des niveaux de sécurité différents.

2.15. Pour obtenir des résultats en gestion des risques, il faut le plus souvent élaborer et analyser des scénarios, et parfois les simuler pour renforcer la confiance dans les évaluations qualitatives. Il existe deux catégories de scénarios : les scénarios fonctionnels et les scénarios techniques. Les scénarios fonctionnels sont généralement utilisés dans le cadre de la GRSI pour une installation, et les scénarios techniques dans le cadre de la GRSI pour un système.

Concilier simplicité, efficacité et sécurité informatique

2.16. Il faut pouvoir concilier simplicité, efficacité et sécurité informatique pour les actions suivantes :

a) recenser les fonctions d'une installation ;
b) confier ces fonctions à des systèmes ;
c) mettre au point les systèmes ;
d) définir les exigences de sécurité informatique pour les différents niveaux de sécurité informatique selon une approche graduée ;
e) fixer des limites logiques ou physiques pour les zones de sécurité informatique.

2.17. La simplicité peut conduire à confier une fonction à un seul système. L'ASID permettra alors probablement d'élaborer des mesures de sécurité informatique adaptées à chaque zone pour chaque fonction d'une installation (en supposant que la relation entre les systèmes et les fonctions est bijective). Les systèmes ont cependant besoin d'interconnexions pour pouvoir intégrer des fonctions distantes d'une installation. L'ensemble des niveaux et des zones de sécurité informatique peut donc devenir plus complexe en raison du grand nombre de zones de sécurité informatique et des interconnexions qui existent entre ces zones.

2.18. Une exécution efficace des fonctions de l'installation par les systèmes peut toutefois conduire à confier plusieurs fonctions à un seul système intégré. Ce choix peut entraîner une baisse du nombre de zones de sécurité informatique, mais le système peut devenir plus complexe, de sorte qu'il sera difficile d'appliquer des mesures de sécurité informatique efficaces dans toutes les zones. En outre, attribuer à une zone de sécurité informatique un niveau de sécurité informatique adapté à la fonction la plus importante du système peut réduire l'efficacité, car une protection plus forte qu'il n'est nécessaire pourrait être mise en place pour des fonctions moins importantes qui ont été intégrées dans le système.

2.19. Pour trouver un équilibre entre efficacité et simplicité, il faut parfois aussi parvenir à un équilibre entre la performance des fonctions de l'installation

exécutées par les systèmes, et le classement des systèmes dans des zones de sécurité informatique et l'attribution d'un niveau de sécurité informatique aux systèmes. La GRSI donne donc généralement lieu à plusieurs définitions successives des zones de sécurité informatique et des mesures de sécurité informatique correspondantes afin de trouver le meilleur équilibre entre simplicité et efficacité. Dans le cadre des définitions successives, il faudra établir que les modifications des zones de sécurité informatique proposées ne provoqueront pas une compromission des fonctions de l'installation qui aurait des conséquences plus néfastes.

Modèle conceptuel des zones d'une installation nucléaire

2.20. On trouvera sur la figure 2 un exemple de modèle conceptuel des zones d'une installation nucléaire. Ce modèle présente les caractéristiques suivantes :

a) Pour l'installation modélisée, un enlèvement non autorisé de matières ou un acte de sabotage aurait de graves conséquences.
b) Le nombre de niveaux de sécurité informatique est limité à cinq, les impératifs de protection étant les plus stricts pour le niveau 1 et les moins stricts pour le niveau 5.
c) Chaque système se trouve dans une zone de sécurité informatique.
d) Un niveau de sécurité informatique est attribué à chaque zone (y compris les systèmes qui s'y trouvent).
e) Le même niveau de sécurité informatique peut être attribué à plusieurs zones.

2.21. La figure 2 représente un modèle conceptuel de systèmes, de niveaux de sécurité informatique et de zones de sécurité informatique. Le niveau de sécurité informatique attribué a les conséquences suivantes pour les exigences applicables aux fonctions de l'installation, aux systèmes et aux zones de sécurité informatique :

a) Les niveaux de sécurité informatique les plus contraignants sont généralement imposés à un nombre de fonctions plus faible (et concernent donc moins de systèmes) que les niveaux de sécurité les moins contraignants. Sur la figure 2, le niveau de sécurité 1 concerne un tout petit nombre de fonctions critiques, qui sont dans l'idéal confiées à un seul système, tandis que, pour le niveau de sécurité 5, de nombreuses fonctions peuvent être confiées à un seul système.
b) Les niveaux de sécurité informatique les plus contraignants sont généralement plus simples que les niveaux les moins contraignants. Sur la figure 2, la zone Z_{1A} contient un seul système déterministe, dont les relations logiques et physiques avec d'autres zones (et d'autres systèmes) sont réduites au

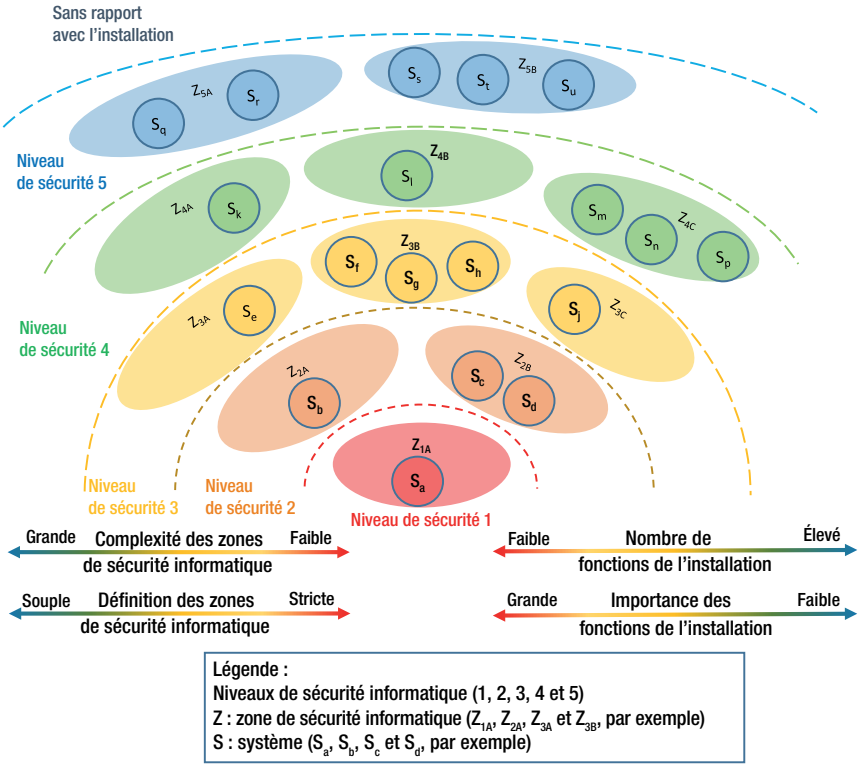

FIG. 2. Modèle conceptuel de niveaux et de zones de sécurité informatique.

minimum autant que possible, tandis qu'il y a très peu de restrictions aux relations avec les autres zones (et les autres systèmes) pour la zone Z_{5B}.

c) La complexité des zones est souvent étroitement liée à leur taille physique et logique. Dans la zone Z_{1A} par exemple, les RNS seront probablement physiquement regroupées dans une zone vitale, tandis que dans la zone Z_{3C}, les ressources numériques peuvent se trouver à n'importe quel endroit de la zone protégée. L'augmentation de l'espace physique entre la zone vitale (Z_{1A}) et la zone protégée (Z_{3C}) peut conduire à une hausse du nombre de points d'accès et du nombre de personnes habilitées qui ont besoin d'accéder à une zone et qui pourraient donc être en contact avec les ressources numériques.

d) La taille logique d'une zone est égale au nombre de ressources numériques connectables et installées dans un système. Ainsi, la zone Z_{3A} pourrait être dimensionnée de telle sorte qu'elle accepte un petit nombre d'adresses attribuables pour un petit nombre de ressources numériques, tandis que la zone Z_{5A} pourrait avoir des limites plus larges et disposer d'un plus grand

nombre d'adresses logiques pour les ressources numériques actuelles et futures.

e) Dans ces exemples, le nombre de ressources numériques connectables augmente de la même manière que la taille de la zone physique au par. 2.21 c). Néanmoins, l'installation de ressources numériques supplémentaires a une incidence notable sur la taille logique d'une zone, mais pas sur sa taille physique[8]. Le nombre de relations logiques possibles augmente donc seulement lorsque de nouvelles ressources numériques sont installées dans une zone et que par conséquent le nombre et la complexité de ces relations augmente dans la zone et à ses limites.

2.22. La rigueur avec laquelle les zones de sécurité informatique sont définies peut dépendre des niveaux de sécurité qui sont attribués à ces zones. Pour la zone Z_{1A}, les limites physique et logique sont ainsi strictement définies, tandis que, pour la zone Z_{5A}, il ne sera peut-être nécessaire de définir précisément que la limite logique, tandis que la limite physique pourra être fixée de manière plus approximative (pour un centre de données, un système en nuage ou des bureaux, par exemple).

2.23. Les limites (logiques et physiques) d'un système peuvent être utiles pour définir les limites d'une zone de sécurité informatique. En pratique, une zone peut contenir un ou plusieurs systèmes, et chaque système peut comprendre une ou plusieurs ressources numériques ou se servir de telles ressources pour exécuter la fonction de l'installation qui lui a été confiée ou contribuer à son exécution[9].

2.24. Les limites des zones de sécurité informatique sont généralement protégées par des dispositifs de contrôle des accès physiques (meuble verrouillé, barrières, bloqueurs de ports, par exemple) et par des mécanismes de découplage (filtrage de paquets, pare-feu ou *data diodes*, par exemple) pour empêcher les cyberattaques et les autres formes d'accès non autorisé, et pour empêcher les erreurs de se propager d'une zone à une autre (surtout d'une zone où les exigences en matière de protection sont peu contraignantes vers une zone où les exigences sont plus strictes).

---

[8] La taille physique d'une zone vitale est généralement plusieurs dizaines de fois supérieure à celle des ressources numériques qui se trouvent dans la zone, et ne limite donc pas le nombre de ressources numériques qui pourraient y être installées.

[9] Il peut être nécessaire d'attribuer un niveau de sécurité informatique à certains systèmes analogiques qui exécutent des fonctions d'une installation (voir par. 3.2) et de les placer dans une zone de sécurité informatique. On suppose que les systèmes analogiques utilisent des ressources numériques, par exemple un outil numérique permettant d'étalonner un système analogique.

2.25. Le recours aux zones permet d'appliquer une approche graduée et le principe de la défense en profondeur. Un adversaire qui lancerait une cyberattaque de l'extérieur de l'installation devrait neutraliser ou contourner plusieurs couches de mesures de sécurité informatique avant de pouvoir porter atteinte à un système de niveau de sécurité informatique 1, 2 ou 3. Les mesures en vigueur pour les niveaux de sécurité informatique 4 et 5 peuvent également contribuer à protéger les niveaux les plus critiques[10]. Mettre en place des moyens de détection précoce dans les zones ayant un niveau de sécurité 4 ou 5 permettrait par exemple de contenir une cyberattaque et d'en atténuer les conséquences avant que les RNS des niveaux 1, 2 et 3 ne soient touchées.

MESURES DE SÉCURITÉ INFORMATIQUE

2.26. Dans le cadre d'une approche graduée, l'importance des mesures de sécurité informatique qui sont mises en place pour protéger une fonction d'une installation est directement proportionnée aux conséquences les plus défavorables d'une éventuelle compromission de la fonction concernée.

2.27. Les mesures de sécurité informatique servent à :

a) prévenir, détecter et retarder les actes criminels et les autres actes non autorisés délibérés, et à intervenir si de tels actes sont commis ;
b) atténuer les conséquences de tels actes ;
c) effacer les conséquences de tels actes.

2.28. Les mesures de sécurité informatique peuvent également servir à :

a) diminuer le risque que les ressources numériques subissent un acte malveillant ;
b) empêcher que des actes non malveillants ne dégradent la sécurité nucléaire.

2.29. Les mesures de sécurité informatique qui peuvent être appliquées appartiennent à l'une des trois catégories suivantes : mesures de contrôle technique, mesures de contrôle physique et mesures de contrôle administratif (voir réf. [7]).

---

[10] Certaines zones représentées sur la figure 2 pourraient être isolées et dépourvues d'une connexion réseau permanente. Néanmoins, les zones de ce type qui contiennent des ressources numériques devront recevoir des informations de l'extérieur par intermittence – des mises à jour par un CD-ROM ou une connexion USB peuvent par exemple être nécessaires –, ce dont peut profiter l'adversaire.

2.30. Les mesures de sécurité informatique peuvent également contribuer à la mise en œuvre d'autres mesures appliquées à des fins de protection physique, de sécurité qui concerne le personnel ou de sécurité de l'information, ou bénéficier de telles mesures. La section 8 donne un exemple d'application de mesures de sécurité informatique dans le cadre d'une ASID à cinq niveaux.

SYSTÈMES INFORMATIQUES ET RESSOURCES NUMÉRIQUES (Y COMPRIS LES RESSOURCES NUMÉRIQUES SENSIBLEs)

2.31. Les systèmes informatiques reposent sur des techniques numériques, en dépendent ou en bénéficient. Ces systèmes jouent un rôle sans cesse croissant pour l'exécution de fonctions importantes dans les installations nucléaires, et des opérations connexes. Ils sont aussi de plus en plus souvent pris en compte dès la conception et peuvent être mis en place dans des installations existantes à l'occasion d'une modernisation ou pour accroître la productivité ou la fiabilité.

2.32. Les systèmes informatiques sont des dispositifs techniques qui produisent, calculent, communiquent ou stockent des données numériques, y donnent accès ou assurent, fournissent ou contrôlent des services qui utilisent de telles données. Ces systèmes peuvent être physiques ou virtuels. Ils comprennent des ordinateurs de bureau, des ordinateurs portables, des tablettes et d'autres ordinateurs personnels, des smartphones, des ordinateurs centraux, des serveurs, des logiciels, des bases de données, des supports amovibles, des appareils de contrôle-commande numérique, des automates programmables, des imprimantes, des dispositifs réseau et des composants et des dispositifs embarqués. Certains systèmes informatiques sont programmables, ce qui permet de modifier des étapes de traitement sans changer le matériel. Les systèmes informatiques sont exposés aux cyberattaques.

2.33. Dans la présente publication, l'expression « ressource numérique » désigne un système informatique qui est associé à une installation nucléaire. Toute ressource numérique qui joue un rôle important dans la sûreté ou la sécurité d'une installation nucléaire sera considérée comme une RNS[11].

[11] Certains États Membres emploient des appellations qui ressemblent à RNS, telles que « ressources numériques cruciales » ou « cyber-ressources essentielles ». Ces expressions n'ont pas forcément tout à fait le même sens que RNS.

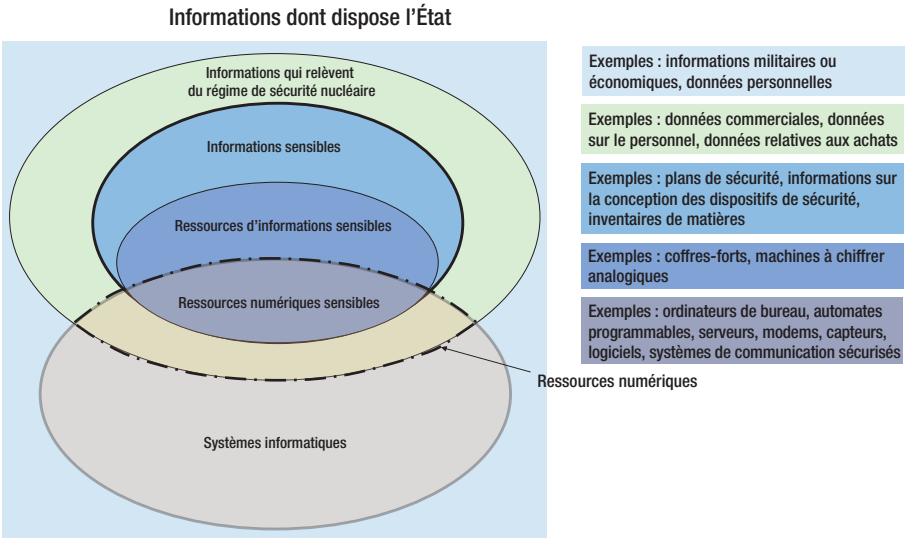

FIG. 3. Informations et systèmes informatiques dans l'État et le régime de sécurité nucléaire.

2.34. La sécurité informatique consiste à protéger les systèmes informatiques contre toute compromission[12]. La sécurité informatique est un sous-ensemble de la sécurité de l'information (telle qu'elle est définie par exemple dans la norme ISO/IEC 27000 [11]). Une grande partie des objectifs, des méthodes et de la terminologie est identique dans les deux cas.

2.35. Les relations qui existent entre la sécurité de l'information, les informations sensibles, les ressources d'informations sensibles, les ressources numériques et les RNS sont représentées sur la figure 3.

CYBERATTAQUE

2.36. Une cyberattaque est un acte malveillant qui vise à empêcher d'avoir accès à une cible particulière ou de la voler, la modifier ou la détruire par accès non autorisé à un système sensible (ou par des actions dans un tel système) [8]. Elle peut être menée par des personnes ou par des organisations, et peut prendre

[12] Des expressions comme « sécurité des systèmes d'information » ou « cybersécurité » sont considérées comme des synonymes de « sécurité informatique » et ne sont pas employées dans la présente publication.

pour cibles des informations sensibles ou des ressources d'informations sensibles. Les cyberattaques présentent les caractéristiques particulières suivantes :

a) Elles peuvent être dissimulées.
b) Leur exécution peut être différée, conditionnelle ou lancée à distance.
c) Des membres du personnel (techniciens, gardiens, personnes chargées de l'exploitation et de la maintenance ou sous-traitants, par exemple) peuvent être amenés par tromperie à soutenir involontairement l'attaque.

2.37. La compromission de ressources numériques peut ouvrir la voie à des cyberattaques prenant pour cible des RNS, les faciliter ou les favoriser, ce qui a des conséquences néfastes pour la sécurité et la sûreté nucléaires. Il faut donc prévoir une protection appropriée – selon une approche graduée et le principe de la défense en profondeur – pour toutes les ressources numériques associées à l'installation afin d'empêcher qu'elles ne soient utilisées pour porter atteinte à des RNS. La compromission d'une RNS dégrade la sécurité nucléaire et peut déclencher un événement de sécurité nucléaire[13] dont les conséquences possibles sont les suivantes (des moins graves aux plus graves) :

a) aucune conséquence ;
b) conséquences négligeables ;
c) conséquences limitées (y compris des conséquences pour la sûreté, comme un incident de fonctionnement prévu, ou des effets sur l'exploitation, par exemple sur le fonctionnement d'une centrale) ;
d) conséquences modérées (diminution des capacités à prévenir et détecter les événements de sécurité nucléaire, ainsi qu'à intervenir en pareil cas, par exemple) ;
e) conséquences importantes (divulgation non autorisée ou perte d'informations sensibles, par exemple) ;
f) graves conséquences (comme des conséquences radiologiques inacceptables dues à un sabotage ou à un enlèvement non autorisé de matières nucléaires ou d'autres matières radioactives).

2.38. Les compétences des adversaires potentiels peuvent comprendre le lancement efficace de cyberattaques. Les RNS sont donc des cibles à la fois pour leur effet sur les fonctions de l'installation et comme moyen pour les adversaires de se rapprocher de leurs objectifs et de les atteindre, et peuvent être spécifiquement prises pour cible.

---

[13] Un événement de sécurité nucléaire peut avoir des conséquences pour la sécurité nucléaire, la sûreté nucléaire ou les deux.

INTERFACE AVEC LA SÛRETÉ

2.39. Une fonction de sûreté est un « [b]ut particulier à atteindre aux fins de la *sûreté* » [12]. Les fonctions de sûreté sont nécessaires pour « une *installation* ou [...] une *activité*, pour prévenir ou atténuer les conséquences radiologiques associées au *fonctionnement normal*, à des *incidents de fonctionnement prévus* et à des *conditions accidentelles* » [12].

2.40. Ainsi, les fonctions de sûreté principales qui sont prescrites pour tous les états d'une centrale {prescription 4 de la publication n° SSR-2/1 (Rev. 1) de la collection Normes de sûreté de l'AIEA, intitulée « Sûreté des centrales nucléaires : conception » [13]} sont les suivantes :

a) maîtrise de la réactivité *;*
b) évacuation de la chaleur provenant du réacteur et de l'installation d'entreposage de combustible ;
c) confinement des matières radioactives, blindage contre les rayonnements et maîtrise des rejets radioactifs programmés, ainsi que limitation des rejets radioactifs accidentels.

2.41. Selon le paragraphe 3.46 de la référence [2], les fonctions de la protection physique sont la détection, le retardement et l'intervention. Ces fonctions reposent sur la défense en profondeur et suivent une approche graduée de sorte à fournir une protection efficace appropriée.

2.42. Les fonctions de la protection physique et les fonctions de sûreté n'étant pas intrinsèquement liées, il est difficile de les traiter de manière cohérente dans le cadre des évaluations du risque. Décrire et désigner les fonctions d'une installation qui sont importantes pour la sécurité et qui ont un rapport avec la sécurité de manière semblable aux fonctions d'une installation qui sont importantes pour la sûreté (c'est-à-dire les fonctions de sûreté) permet donc de déterminer plus facilement l'importance des fonctions d'une installation et de traiter de la même manière les fonctions de sûreté et les fonctions de sécurité qui ont la même importance. Exemples de fonctions d'une installation qui sont importantes pour la sécurité :

a) détection des intrusions (y compris évaluation) aux points de détection critiques ;
b) contrôle de l'accès des personnes et du matériel aux matières de catégorie I ou aux zones vitales ;
c) communications destinées à coordonner les forces d'intervention pendant un événement de sécurité nucléaire.

3. CONSIDÉRATIONS GÉNÉRALES SUR LA SÉCURITÉ INFORMATIQUE

RECENSEMENT DES FONCTIONS D'UNE INSTALLATION

3.1. Selon la référence [7] :

> « La première étape d'une procédure systématique [relative à l'application de mesures de sécurité informatique pour la sécurité nucléaire] devrait consister à recenser les fonctions qui prennent directement en compte un ou plusieurs aspects de la sécurité nucléaire (comme la protection physique, la comptabilité et le contrôle des matières nucléaires ou la gestion des informations sensibles) et de la sûreté nucléaire. Il faudrait ensuite recenser les systèmes informatiques et leurs ressources numériques qui contribuent à l'exécution de ces fonctions. »

Dans le cas d'une installation nucléaire, ces ressources numériques sont les systèmes informatiques qui doivent être protégés contre la compromission, selon la recommandation du paragraphe 4.10 de la référence [2], et les RNS traitées dans la présente publication.

3.2. L'exploitant devrait recenser la totalité des fonctions de l'installation de manière cohérente afin que ces fonctions puissent être évaluées de manière globale. L'exploitant devrait communiquer la liste des fonctions de l'installation à l'autorité compétente[14], conformément à la réglementation nationale. Les exigences de sécurité informatique[15] applicables à ces fonctions devraient être prises en compte, quels que soient les moyens permettant d'exécuter les fonctions (par exemple la technique précise qui a été employée, qu'elle soit analogique ou numérique).

---

[14] Dans la présente publication, l'expression « autorité compétente » désigne l'autorité à laquelle l'État a confié la responsabilité de la sécurité informatique dans le cadre de la sécurité nucléaire. Il peut s'agir de l'autorité compétente pour la sécurité nucléaire ou de l'autorité compétente pour la sécurité informatique.

[15] Dans la présente publication, les exigences de sécurité informatique comprennent les exigences écrites particulières qui sont imposées par l'autorité compétente concernée ou par l'exploitant pour respecter les exigences de sécurité informatique définies par l'autorité compétente ou les prescriptions réglementaires.

3.3. Pour pouvoir être exécutées, les fonctions d'une installation utilisent des informations sensibles, des ressources d'informations sensibles et d'autres ressources numériques, ou en bénéficient.

PROTECTION DES INFORMATIONS SENSIBLES ET DES RESSOURCES NUMÉRIQUES

3.4. L'exploitant devrait appliquer des mesures de sécurité informatique afin de protéger (et de tracer) adéquatement les informations sensibles, les ressources d'informations sensibles et les RNS. La sécurité informatique est assurée par des mesures qui visent à garantir la confidentialité, l'intégrité et la disponibilité, et à satisfaire aux autres exigences établies par l'autorité compétente.

3.5. L'exploitant devrait déterminer quelles sont les informations sensibles, en tenant compte des conséquences de leur compromission et des prescriptions édictées par l'État concernant leur sécurité. La référence [5] donne des orientations détaillées sur la manière dont l'État peut établir des prescriptions pour ce type d'informations.

3.6. Il est possible de déterminer directement quelles sont les informations sensibles par une analyse des conséquences possibles de leur divulgation non autorisée (comme l'explique la référence [5]), par exemple pour les informations relatives aux dispositifs de sécurité, qu'un adversaire pourrait exploiter pour préparer un acte malveillant. Pour ce type d'informations, la confidentialité est généralement l'aspect qui doit être le mieux protégé. Il est également possible de déterminer quelles sont les informations sensibles de manière plus indirecte par une analyse de leur importance fonctionnelle (c'est-à-dire de leur importance pour la mise en place et l'exécution d'une fonction d'une installation), comme les données exactes et actualisées sur la pression de la chaudière nucléaire, qu'un adversaire pourrait récupérer pour les modifier ou les détruire. Pour ce type d'informations, l'intégrité et la disponibilité sont au moins aussi importantes que la confidentialité.

3.7. Les informations contenues dans le plan de sécurité du site peuvent être considérées comme sensibles et des mesures peuvent être mises en œuvre pour préserver leur confidentialité sur une longue durée, puisqu'elles resteront sensibles pendant toute la durée de validité de ce plan.

3.8. S'agissant d'un système de contrôle-commande et de ses données de processus, un exploitant pourrait donner la priorité aux mesures qui garantissent la disponibilité et l'intégrité du système et mettre celles qui garantissent la confidentialité au

second plan. Dans ce cas, les données de processus sont importantes pour la bonne exécution et la disponibilité de la fonction ; et ne sont sensibles que pendant des durées très courtes où le système exécute une action de contrôle qui s'appuie sur ces données. Cependant, une fois que ces données ne jouent plus aucun rôle pour l'exécution et la disponibilité de la fonction (c'est-à-dire qu'elles ne peuvent plus servir pour une action de contrôle), c'est uniquement leur sensibilité qui détermine leur importance. Il faut donc comparer les avantages d'une meilleure garantie de confidentialité (pour la protection des informations sensibles) et ceux d'un maintien de l'intégrité et de la disponibilité sur le plan de la sécurité.

3.9. Préserver la confidentialité des données de processus de ces systèmes ne devrait pas exiger de mesures rigoureuses, alors que la perte de la confidentialité d'autres données relatives aux systèmes, tels que les mots de passe administrateur, le code source et d'autres éléments essentiels, donnerait un avantage notable à l'adversaire pour la préparation et la conduite de cyberattaques contre le système, et pourrait imposer de prendre des mesures plus sévères. En outre, une classification des données de processus antérieures (journaux d'exploitation, par exemple) pour limiter leur diffusion (application d'une mesure de contrôle administratif, par exemple) pourrait être nécessaire pour maîtriser le risque de divulgation non autorisée.

APPROCHE FONDÉE SUR LES RISQUES

3.10. La sécurité informatique devrait être mise en œuvre selon une approche fondée sur les risques. La figure 4 de la référence [7] présente schématiquement une approche fondée sur les risques pour les mesures de sécurité informatique.

3.11. En sécurité informatique, le risque est le risque lié à un adversaire qui exploite les vulnérabilités d'une ressource numérique ou d'un groupe de ressources numériques pour commettre un acte malveillant ou faciliter la commission d'un tel acte. Il correspond à la combinaison de la probabilité qu'une attaque réussisse et de la gravité de ses conséquences éventuelles.

ÉVALUATION ET GESTION DU RISQUE

3.12. L'exploitant devrait définir et appliquer un processus de GRSI (sauf si le processus de gestion est mis en œuvre par l'autorité compétente). L'autorité compétente peut imposer des exigences à respecter et une méthode d'évaluation du risque particulière. Elle peut aussi autoriser un exploitant à utiliser sa propre méthode [7]. Pour une installation, on peut suivre l'exemple de l'évaluation

des risques liés à la sécurité informatique au niveau d'une organisation qui est présentée aux paragraphes 7.10 à 7.16 de la référence [7].

3.13. La GRSI devrait comprendre un processus cyclique d'amélioration continue[16] pour la gestion des risques liés aux cyberattaques contre l'installation.

3.14. En gestion du risque, les évaluations périodiques et itératives servent à faciliter la prise de décisions. Une évaluation des risques liés à la sécurité informatique est le plus souvent qualitative, et se traduit alors par des indicateurs relatifs (risque élevé, moyen ou faible, par exemple), mais peut être quantitative si l'on dispose de données suffisamment fiables[17]. Les résultats de ce type d'évaluation permettent de déterminer plus facilement les exigences de sécurité informatique à respecter.

3.15. L'exploitant devrait effectuer une GRSI pour l'installation afin de respecter les prescriptions réglementaires. La référence [7] montre que cette GRSI peut comprendre deux évaluations complémentaires, l'une menée à l'échelle de l'organisation et l'autre à l'échelle du système. Il conviendrait d'effectuer ces évaluations pour les installations complexes et à haut risque (installations nucléaires, par exemple). Dans les orientations qui figurent dans la présente publication, on considère donc que la GRSI pour une installation nucléaire comprend une phase d'évaluation et de gestion du risque au niveau du système (GRSI pour un système) (voir fig. 4). Deux étapes sont alors nécessaires :

a) Évaluer et gérer globalement les risques liés à la sécurité informatique pour l'ensemble des fonctions de l'installation. L'exploitant évaluera ainsi complètement l'installation et permettra à l'autorité compétente d'évaluer l'efficacité générale de la GRSI dans l'installation**.** La section 4 donne des orientations sur la mise en œuvre d'une GRSI pour une installation.
b) Évaluer et gérer les risques liés à chaque système qui exécute ou appuie les fonctions de l'installation. L'exploitant évaluera ainsi en détail chaque système qui exécute ou appuie une fonction. L'autorité compétente peut imposer une évaluation détaillée pour contrôler l'efficacité de certaines applications de la GRSI dans l'installation. La section 5 donne des orientations sur la mise en œuvre d'une GRSI pour un système.

---

[16] Comme le cycle PDCA (planifier, faire, vérifier, agir), par exemple.

[17] Au moment où le présent ouvrage a été publié, il n'existait aucune méthode internationalement reconnue pour laquelle des valeurs quantitatives étaient calculées dans le cadre des évaluations des risques liés à la sécurité.

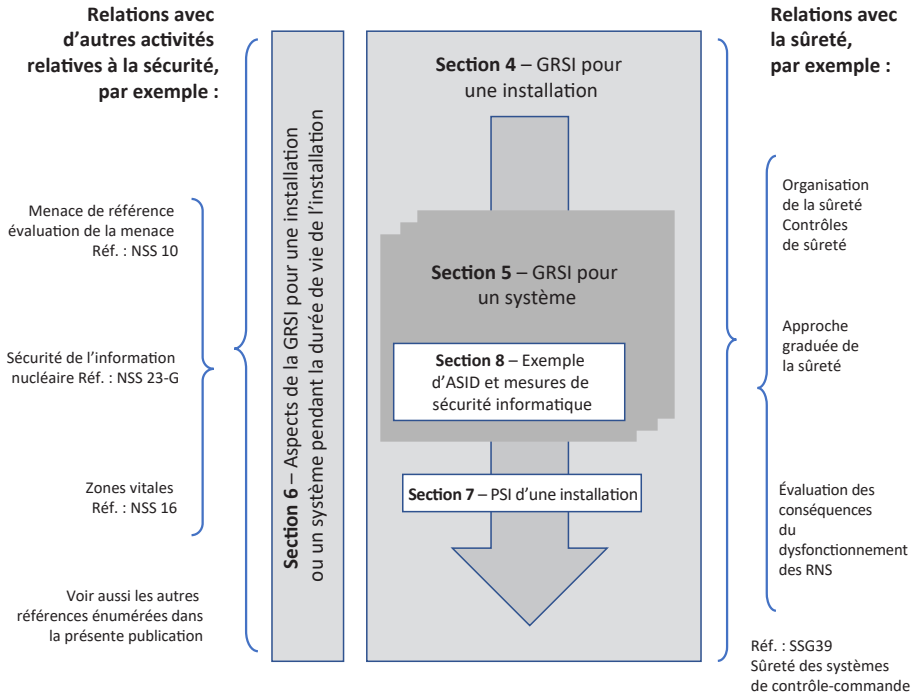

FIG. 4. Structure générale des orientations sur la gestion des risques liés à la sécurité informatique (GRSI) dans la présente publication. PSI : programme de sécurité informatique ; ASID : architecture de sécurité informatique défensive ; NSS : collection Sécurité nucléaire ; RNS : ressources numériques sensibles ; SSG : guide de sûreté particulier.

3.16. L'exploitant devrait faire en sorte que les équipes qui mettent en œuvre toute la GRSI afin de fixer des exigences de sécurité informatique pour l'installation, celles qui s'occupent de la mise en œuvre de ces exigences et celles qui sont chargées de veiller au respect de leur application soient indépendantes.

3.17. La gestion du risque est importante à toutes les étapes de la vie d'une installation et de ses systèmes et contribue à l'élaboration, à l'application et au maintien des mesures de sécurité informatique. Les activités de gestion du risque pendant toute la durée de vie d'une installation sont répertoriées dans la section 6.

3.18. L'évaluation du risque devrait être examinée, et au besoin mise à jour, dans les cas suivants :

a) De nouvelles informations ou des données importantes pourraient invalider certaines hypothèses qui figurent dans la politique de sécurité informatique, le PSI, l'évaluation de la menace propre au site et l'ASID qui ont été adoptés.
b) On découvre une vulnérabilité qui rend inactives des mesures de sécurité informatique ou qui invalide des hypothèses formulées dans une évaluation du risque pour un système.
c) Un incident de sécurité informatique se produit dans l'installation.
d) La menace de référence ou l'énoncé de la menace nationaux sont modifiés (et ces modifications concernent les adversaires qui lancent des cyberattaques ou des attaques combinées), par exemple pour prendre en compte de nouvelles menaces ou un renforcement des capacités ou des moyens de l'adversaire qui pourrait accroître les chances de succès d'une cyberattaque.
e) Une modification est apportée à une fonction de l'installation, à un système, à une RNS ou à une mesure de sécurité informatique. Les modifications concernées devraient notamment être la mise en service d'un nouvel appareil ou d'un nouveau logiciel, l'adoption d'une nouvelle procédure ou une évolution importante des compétences du personnel d'exploitation. Le niveau de protection qui est attribué à la RNS (niveau de sécurité informatique, par exemple) permet de déterminer l'ampleur du travail à accomplir pour mettre à jour l'évaluation du risque.
f) Les prescriptions réglementaires sont modifiées.
g) Dans le cadre de la démarche d'amélioration continue, un réexamen périodique doit être effectué pour que l'évaluation reste valide.

3.19. Les activités réglementaires qui portent sur la sécurité d'une installation, comme la délivrance de licences, les inspections ou la coercition, devraient comprendre un examen pertinent des questions de sécurité informatique. Les dossiers de gestion du risque et les décisions et actions qui résultent de cette dernière devraient être mis à la disposition de l'autorité compétente à sa demande pour lui permettre de déterminer si les prescriptions réglementaires sont respectées.

3.20. Pour la gestion du risque, la structure et la conception d'ensemble devraient comprendre les éléments suivants :

a) GRSI pour une installation :
    i) définition du périmètre de la GRSI ;
    ii) caractérisation de l'installation ;
    iii) caractérisation des menaces ;

iv) définition des exigences ;
v) vérification et validation ;
vi) accord de l'autorité compétente.

b) GRSI pour un système :
i) définition des limites du système ;
ii) recensement des ressources numériques (notamment des RNS) ;
iii) exigences de sécurité informatique applicables au système ;
iv) vérification.

3.21. Il existe de nombreuses méthodes d'évaluation du risque (voir la norme ISO/IEC 27005 [14], par exemple). L'organisme concerné doit choisir une méthode et l'adapter à sa situation et à ses objectifs particuliers, tout en séparant la gestion du risque au niveau de l'installation et la gestion du risque au niveau des systèmes.

NIVEAUX DE SÉCURITÉ INFORMATIQUE DANS LE CADRE D'UNE APPROCHE GRADUÉE

3.22. Les exigences de sécurité informatique et la conception et la mise en œuvre de mesures qui permettent de respecter ces exigences devraient reposer sur une approche graduée, pour laquelle les mesures de sécurité informatique sont directement proportionnées aux conséquences possibles de la compromission de la fonction concernée. Comme l'explique la section 2, un des moyens concrets de mise en œuvre d'une approche graduée consiste à attribuer aux fonctions de l'installation un niveau de sécurité informatique. Chaque niveau est lui-même caractérisé par des exigences de sécurité informatique graduées et l'on peut choisir des mesures de sécurité préventives et protectrices pour satisfaire aux exigences du niveau correspondant. La figure 5 illustre l'approche graduée par la notion de niveau de sécurité informatique.

3.23. Les exigences (restrictions claires appliquées aux communications entre des RNS auxquelles des niveaux différents ont été attribués, par exemple) sont déterminées par le niveau de sécurité informatique, alors que les mesures de sécurité (comme le type de pare-feu employé pour limiter ces communications) qui visent à protéger des ressources numériques (notamment des RNS) peuvent être choisies en fonction de l'architecture mise en place pour le niveau de sécurité informatique et des techniques utilisées par les ressources numériques concernées (notamment des RNS).

3.24. Lorsque des niveaux de sécurité informatique sont attribués, il convient de définir les exigences de sécurité informatique pour chaque niveau, les éléments suivants étant pris en compte :

a) Les exigences générales devraient s'appliquer à toute l'installation et à l'organisme exploitant, et peuvent s'appliquer à toutes les ressources numériques. Elles permettent d'améliorer la culture de sécurité nucléaire grâce à une meilleure sensibilisation à la sécurité informatique. Elles renforcent également la sécurité informatique et permettent dans certains cas d'ajouter un niveau de défense en profondeur. Les exigences générales ne présentent pas d'intérêt notable pour un niveau de sécurité informatique ou un système particuliers, car les mesures générales s'appliquent habituellement à un large éventail de ressources numériques et l'on ne peut compter sur leur mise en œuvre systématique et efficace.

b) Des niveaux de sécurité sont attribués et vont de 5 (protection minimum nécessaire) à 1 (protection maximum nécessaire) (voir fig. 5). Dans ce cas, le niveau de sécurité informatique est compris entre 1 et 3 pour les systèmes qui contiennent des RNS, et est égal à 4 ou 5 pour ceux qui contiennent d'autres ressources numériques.

c) Les exigences de sécurité informatiques sont définies et appliquées en fonction du niveau de sécurité informatique qui est attribué, conformément à une approche graduée. Elles devraient reposer sur le principe de la défense en profondeur, selon lequel les ressources numériques auxquelles est attribué un niveau de sécurité qui offre une protection plus forte ne s'appuient pas seulement sur les ressources numériques ou sur les mesures de sécurité informatique dont le niveau assure une protection moins forte, ou exercent un contrôle à cet égard.

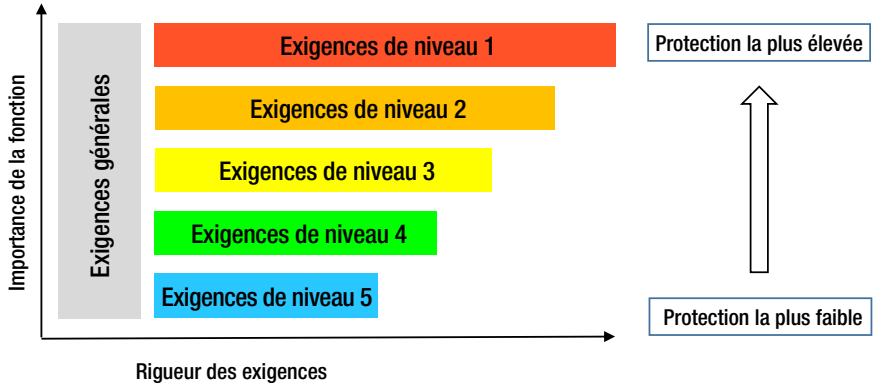

FIG. 5. L'approche graduée, illustrée par la notion de niveau de sécurité informatique.

d) Les mesures de sécurité informatique qui sont mises en œuvre pour répondre aux exigences de chaque niveau de sécurité informatique devraient tenir compte de l'indépendance et de la diversité des mesures visant à réduire les vulnérabilités communes qui permettent de contourner ou de neutraliser plusieurs couches de défense en profondeur. Il peut cependant être nécessaire de mettre en place pour d'autres niveaux certaines mesures qui s'appliquent à un niveau de sécurité informatique particulier.

e) Lorsqu'une approche multidimensionnelle et le principe de la défense en profondeur sont adoptés, les mesures de sécurité informatique des niveaux les moins contraignants peuvent protéger les niveaux plus critiques, surtout en ce qui concerne la détection précoce des cyberattaques.

f) Aucun niveau n'est attribué aux systèmes informatiques qui ne relèvent pas du PSI, et toutes les autres ressources numériques devraient exercer un contrôle sur les données qu'ils transmettent.

3.25. La section 8 donne des orientations sur les exigences de sécurité informatique à définir dans le cadre d'une approche graduée et prend l'exemple de cinq niveaux de sécurité informatique, auxquels s'ajoutent des exigences de sécurité informatique générales.

4. GESTION DES RISQUES LIÉS À LA SÉCURITÉ INFORMATIQUE POUR UNE INSTALLATION

4.1. La GRSI pour une installation est une tâche complexe, qui devrait être exécutée par une équipe pluridisciplinaire dont les membres ont des compétences dans le domaine de la sécurité nucléaire, de la sûreté nucléaire, de l'exploitation, de la maintenance, de la sécurité informatique et de l'ingénierie[18]. La composition de cette équipe peut être semblable à celle qui est proposée pour les évaluations de la protection physique (voir réf. [15]).

4.2. La GRSI pour une installation est un processus itératif qui se déroule en plusieurs phases. Il peut être nécessaire de réexaminer et de modifier les hypothèses, les décisions ou les résultats qui découlent d'une phase précédente à

[18] Certains États Membres emploient des expressions comme « équipe de cybersécurité » pour désigner les membres du personnel qui sont nécessaires pour assurer la sécurité informatique.

la lecture des résultats d'une phase ultérieure. Des activités de vérification doivent être menées entre les différentes phases.

OBJECTIF DE LA GESTION DES RISQUES LIÉS À LA SÉCURITÉ INFORMATIQUE POUR UNE INSTALLATION

4.3. L'objectif de la GRSI pour une installation est d'évaluer et de gérer les risques liés aux cyberattaques qui peuvent dégrader la sécurité ou la sûreté nucléaires de l'installation.

4.4. Dans le cadre de la GRSI pour une installation, il faudrait s'assurer que les prescriptions réglementaires relatives à la sécurité informatique sont respectées.

4.5. Il faudrait également prendre en compte l'évaluation des adversaires connus qui pourraient attaquer l'installation et une étude de leurs objectifs (sabotage, enlèvement non autorisé de matières nucléaires ou radioactives ou accès non autorisé à des informations sensibles, par exemple), y compris l'évaluation de l'attractivité des cibles[19] présentes dans l'installation pour ces adversaires. L'État peut évaluer les menaces en établissant un énoncé national de la menace ou une menace de référence[20].

4.6. Dans le cadre de la GRSI pour une installation, il faudrait déterminer l'importance de chaque fonction au regard des objectifs de l'exploitant. Il est alors possible d'établir une liste hiérarchisée[21] des événements de sécurité nucléaire (qui va des événements ayant les plus graves conséquences à ceux qui n'ont aucune conséquence) que peut provoquer la compromission d'une fonction[22]. La figure 7 de la référence [7] peut être utilisée à cette fin.

---

[19] La question de l'attractivité des cibles peut être traitée dans l'évaluation de la menace ou dans la menace de référence, et l'État peut communiquer des informations complémentaires par l'intermédiaire des autorités compétentes.

[20] Une menace de référence découle de l'évaluation actuelle de la menace par l'État et sert de point de départ à l'élaboration des mesures de sécurité nucléaire. La responsabilité de mettre en place des mesures de sécurité nucléaire adaptées aux moyens de la menace qui sont décrits dans la menace de référence incombe en premier lieu à l'exploitant. Certains États Membres établissent un autre énoncé national de la menace, et non une menace de référence.

[21] Liste ordonnée où sont regroupées les fonctions de l'installation qui ont à peu près les mêmes conséquences.

[22] L'exploitant peut également tenir compte des fonctions qui ont une importance pour l'installation, mais ne concernent ni la sûreté ni la sécurité.

4.7. Dans le cadre de la GRSI pour une installation, il faudrait tenir compte des fonctions, mais pas de leur mise en œuvre concrète dans les systèmes et les ressources numériques, qui est examinée dans le cadre de la GRSI pour le système concerné (voir section 5).

4.8. Le fait de mener la GRSI pour une installation de manière uniforme dans toutes les installations d'un État peut aider les autorités compétentes à exercer un contrôle efficace sur la mise en œuvre de la sécurité informatique dans les installations nucléaires.

VUE D'ENSEMBLE DE LA GESTION DES RISQUES LIÉS À LA SÉCURITÉ INFORMATIQUE POUR UNE INSTALLATION

Éléments d'entrée de la gestion des risques liés à la sécurité informatique pour une installation

4.9. Dans le cadre de la GRSI pour une installation, l'exploitant devrait se servir des éléments d'entrée suivants :

a) Menace de référence ou énoncé de la menace nationaux, et analyse correspondante si elle existe.
b) Prescriptions réglementaires applicables et autres documents. Ces prescriptions peuvent comprendre celles qui sont édictées par l'État en matière de classification des informations.
c) Analyse de la sûreté qui a été menée sur les systèmes informatiques de l'installation. Cette analyse peut être utilisée pour définir les exigences de sécurité informatique, mais elle n'est pas suffisante pour y parvenir, car elle ne prend pas en compte tous les dysfonctionnements, surtout ceux qui sont provoqués par un acte malveillant.
d) Plan de sécurité du site [15]. Il peut servir à déterminer quelles fonctions de l'installation sont importantes pour la sécurité ou ont un rapport avec celle-ci, et leur importance au regard des objectifs de l'exploitant. Le PSI ou certains de ses aspects peuvent figurer dans ce plan.
e) Politique de sécurité informatique applicable à l'installation.
f) Documents actuels et antérieurs concernant le PSI de l'installation, notamment la liste des fonctions qui sont confiées aux différents systèmes et l'évaluation de la menace propre à l'installation.

Phases de la gestion des risques liés à la sécurité informatique pour une installation

4.10. Les phases de la gestion des risques liés à la sécurité informatique pour une installation sont les suivantes :

a) Définition du cadre de l'évaluation : Définir le cadre de l'évaluation du risque, compte tenu des objectifs de l'exploitant pour l'installation (sûreté, sécurité, exploitation et préparation des interventions d'urgence, par exemple), des limites physique et logique et du stade où se trouve l'installation. Il faudrait dresser la liste des conditions nécessaires pour mener l'évaluation et des éléments d'entrée correspondants pendant cette phase.

b) Caractérisation de l'installation : Déterminer quelles sont les fonctions de l'installation, leurs relations et leurs liens d'interdépendance, déterminer quelles informations sensibles pourraient être utiles pour préparer une attaque contre l'installation et établir une liste des cibles à partir des fonctions de l'installation et des informations sensibles qui ont été répertoriées.

c) Caractérisation de la menace : Analyser la menace de référence ou l'énoncé de la menace nationaux et toute autre information pertinente ou analyse des menaces afin de déterminer quelles tactiques, techniques, procédures et compétences un adversaire pourrait utiliser dans le cadre de cyberattaques (y compris d'attaques combinées) contre des cibles dans l'installation nucléaire. La caractérisation de la menace est un modèle qui est établi par analyse des aspects pertinents des informations concernant la menace. On peut ainsi obtenir une représentation des adversaires qui font courir le plus grand risque. La phase de caractérisation permet de délimiter les scénarios d'attaque plausibles.

d) Définition des exigences de sécurité informatique : Fixer des exigences de sécurité informatique pour l'installation. Cette phase consiste à :
   i) élaborer et consigner un PSI ;
   ii) formuler des recommandations concernant les modifications à apporter à la politique de sécurité informatique ;
   iii) attribuer des niveaux de sécurité informatique aux fonctions de l'installation ;
   iv) fixer ou modifier les exigences applicables à l'ASID.

   Pendant cette phase, des techniques d'analyse (évaluation de la vulnérabilité ou de la menace, par exemple) et des méthodes d'évaluation (voir par. 4.98) peuvent être appliquées pour définir des exigences à partir de la caractérisation de l'installation et de la menace, ainsi que des prescriptions réglementaires.

e) GRSI pour un système : Le PSI et l'ASID sont mis en œuvre pour chaque système. La GRSI pour un système est décrite plus en détail dans la section 5. Il peut être nécessaire d'apporter des changements au PSI et à l'ASID à la lumière de l'expérience acquise lors de leur mise en œuvre pour chaque système.

f) Assemblage et intégration des systèmes dans l'installation : Cette phase n'est pas abordée dans la présente publication. Il peut être nécessaire d'apporter des changements au PSI et à l'ASID à la lumière de l'expérience pratique acquise lors de l'assemblage et de l'intégration des systèmes.

g) Activités d'assurance : Il ne s'agit pas d'une phase de la GRSI pour une installation à proprement parler, mais plutôt d'une série d'activités continues qui sont également menées dans le cadre de la GRSI pour chaque système. Ces activités sont de trois types différents :
   i) évaluation du respect des exigences de sécurité informatique ;
   ii) vérification de chaque phase de la GRSI ;
   iii) contrôle de la sécurité informatique dans l'installation.

   Les scénarios constituent une part essentielle des activités d'évaluation, de vérification et de contrôle.

h) Documents issus de la GRSI : Ils comprennent le PSI (révisé), l'ASID, l'évaluation de la menace propre au site et le rapport de conformité de la GRSI pour l'installation. Tout ou partie de ces documents est soumis à l'approbation de l'autorité compétente. Ces documents peuvent servir de base à une évolution des prescriptions réglementaires qui sont édictées par l'État.

4.11. Les différentes phases de la GRSI sont représentées sur la figure 6, qui donne une vue d'ensemble du processus. Elles sont décrites plus en détail dans la suite de la présente section.

4.12. La GRSI pour une installation (processus unique) comprend une GRSI distincte pour chaque système. Pour un site qui compte plusieurs installations ou pour une organisation qui exploite plusieurs installations, il peut y avoir un seul processus pour l'ensemble du site ou pour toute l'organisation, de sorte que la GRSI pour l'installation aboutit à une ou plusieurs séries de documents. En pareil cas, l'exploitant peut décider combien de séries de documents seront établies, mais devrait veiller à ce que le processus soit mis en œuvre intégralement pour chaque installation.

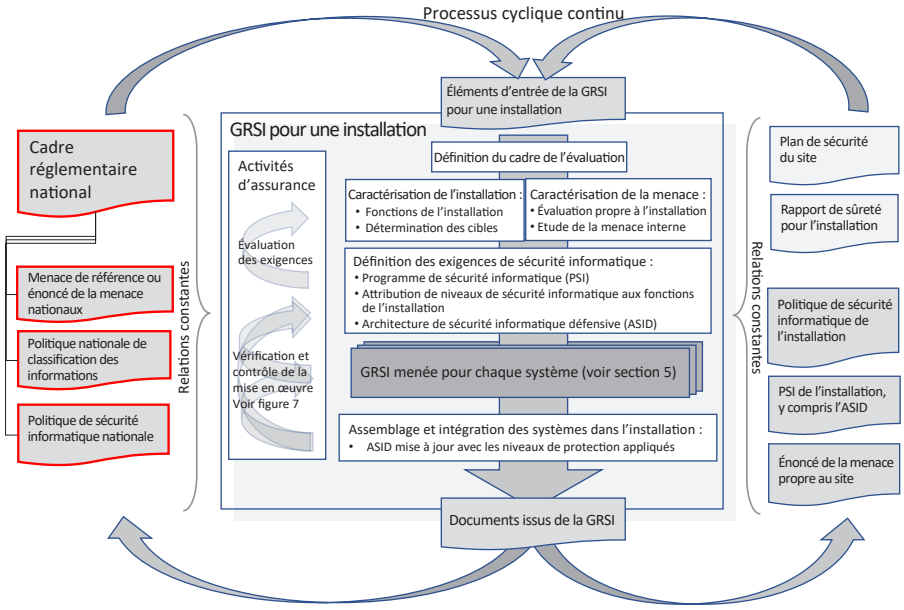

FIG. 6. Vue d'ensemble de la gestion des risques liés à la sécurité informatique (GRSI) pour une installation.

DÉFINITION DU CADRE DE L'ÉVALUATION

4.13. L'exploitant devrait définir le cadre de la GRSI pour l'installation, qui correspond aux limites physiques ou logiques des fonctions de l'installation et des systèmes correspondants qui intéressent la sécurité nucléaire. Les points à prendre en considération pour la définition de ce cadre peuvent notamment être les suivants : périmètre physique de l'installation ; lieu où se trouvent les vendeurs, les sous-traitants et les fournisseurs ; bureaux de l'organisme exploitant ; centres de données fonctionnant en dehors du site ; autres emplacements stratégiques. Le cadre de l'évaluation peut également dépendre du stade où se trouve l'installation ou des moyens et du degré de maturité de l'organisme exploitant (voir par. 5.26 à 5.29 de la référence [7]).

CARACTÉRISATION DE L'INSTALLATION

Recensement des fonctions de l'installation

4.14. L'exploitant devrait recenser toutes les fonctions de l'installation sans tenir compte de la manière dont ces fonctions sont exécutées. Si des ressources numériques existent et sont utilisées dans toute l'installation et pendant toute sa durée de vie, il est probable que de telles ressources serviront à accomplir la majorité des tâches et des activités relatives à ces fonctions ou contribueront à leur bon déroulement.

4.15. Le stade où se trouve l'installation [10] devrait être pris en compte pour la caractérisation de l'installation et le recensement de ses fonctions. Les différentes fonctions ne jouent pas un rôle au même stade de la vie de l'installation, et leur importance relative peut changer.

4.16. Les fonctions de l'installation sont caractérisées par les éléments suivants :

a) Importance intrinsèque : Importance de la fonction pour la sécurité et la sûreté nucléaires, et conséquences possibles pour l'installation si la fonction ne s'exécute pas correctement[23]. Il s'agit de la caractéristique principale.
b) Effets possibles d'une compromission : Formes sous lesquelles la fonction de l'installation pourrait ne pas s'exécuter correctement.
c) Interdépendance de fonctions : L'importance d'une fonction peut résulter d'autres fonctions qui en dépendent.
d) Délai d'exécution et exactitude nécessaires pour l'exécution de la fonction.

Importance intrinsèque des fonctions de l'installation

4.17. Il faudrait comparer l'importance de toutes les fonctions de l'installation afin de regrouper celles qui ont une importance similaire, si possible à l'aide de critères communs qui tiennent compte des questions de sécurité et de sûreté.

---

[23] Il y a souvent un lien entre l'importance de la fonction pour la sécurité nucléaire et les conséquences d'une mauvaise exécution de la fonction. Pour les installations nucléaires, les conséquences jugées les plus importantes sont l'enlèvement non autorisé de matières nucléaires et le sabotage qui ont des conséquences radiologiques inacceptables. D'autres conséquences, comme la divulgation non autorisée d'informations sensibles, peuvent être prises en compte. D'autres conséquences possibles peuvent avoir un lien avec d'autres objectifs de l'organisation, comme le maintien de la réputation ou le respect d'autres règlements relatifs à l'environnement. La norme ISO 27005:2018 [14] contient une liste des conséquences possibles.

4.18. S'agissant des fonctions qui sont importantes pour la sécurité nucléaire ou qui ont un rapport avec ce domaine, il faudrait employer une classification en fonction des conséquences pour la sécurité nucléaire, comme celle qui est représentée sur la figure 7 de la référence [7], afin de déterminer leur importance.

4.19. S'agissant des fonctions qui sont importantes pour la sûreté nucléaire ou qui ont un rapport avec ce domaine, une classification de sûreté reconnue peut être utilisée pour déterminer leur importance. Pour des questions de sécurité, il peut cependant être nécessaire d'accorder à une fonction une importance plus grande que celle qui figure dans la classification de sûreté.

4.20. Lorsque l'on détermine l'importance des fonctions de l'installation, il faudrait tenir compte du fait que l'exécution de fonctions de sûreté (par les systèmes) peut contribuer à la sécurité et que l'exécution de fonctions de sécurité peut contribuer à la sûreté. Par conséquent, l'importance accordée à une fonction de sûreté sur le plan de la sécurité informatique peut ne pas correspondre à la classe de sûreté de la fonction.

4.21. Par exemple, un système qui exécute une fonction consistant à détecter les rayonnements pour protéger le personnel (un des objectifs de la sûreté) peut aussi détecter les enlèvements non autorisés de matières nucléaires (un des objectifs de la sécurité nucléaire). Si la défaillance de la fonction de radioprotection du point de vue de la sûreté peut avoir des conséquences limitées, les conséquences d'une défaillance pour la sécurité nucléaire peuvent être plus graves. Dans cet exemple, l'importance accordée aux fonctions de l'installation qui sont exécutées par le système dépendra de leur importance au regard des objectifs de la sécurité nucléaire. (Sinon, l'exploitant peut décider de mettre en service des systèmes indépendants pour séparer les fonctions qui contribuent à la sûreté nucléaire et celles qui contribuent à la sécurité nucléaire ; dans cet exemple, une importance moindre pourrait être accordée aux fonctions qui contribuent à la sûreté nucléaire.)

Effets possibles de la compromission d'un système sur une fonction de l'installation

4.22. Après avoir déterminé l'importance intrinsèque de la fonction de l'installation, l'exploitant devrait prendre en considération les effets d'une

compromission du système destiné à exécuter la fonction sur celle-ci. Ces effets sont les suivants (des plus graves aux moins graves) :

a) La fonction s'exécute de manière indéterminée, c'est-à-dire qu'elle est peut-être altérée d'une quelconque manière sans que la compromission ne soit détectée.
b) L'exécution de la fonction change de manière inattendue (et d'autres actions peuvent être exécutées), mais les anomalies peuvent être vues par l'exploitant.
c) La fonction ne s'exécute pas.
d) La fonction s'exécute comme prévu, car la compromission n'a pas eu de conséquences néfastes pour la fonction (le système est donc tolérant aux pannes).

4.23. Un système destiné à exécuter une fonction de l'installation peut être défaillant de différentes manières lorsqu'il est compromis, et les effets de la défaillance dépendent des circonstances et de la situation au moment de la compromission, de la nature de la cyberattaque qui a provoqué la compromission et de l'importance de la fonction. Un système qui exécute une fonction d'importance moindre peut par exemple être utilisé pour attaquer un système qui exécute une fonction plus importante par exploitation des interdépendances et des relations entre les fonctions.

4.24. Pour chaque système compromis et chacun des effets de la compromission (c'est-à-dire des dysfonctionnements), les conséquences pour l'installation seront différentes. Il faudrait évaluer ces conséquences, et l'importance accordée aux fonctions de l'installation devrait dépendre de ces conséquences. Lors de cette évaluation, la perte de confidentialité, l'intégrité ou la disponibilité des informations sensibles, ainsi que les conséquences qui résultent d'un enlèvement non autorisé de matières ou d'un sabotage, devraient être prises en compte.

4.25. L'importance accordée à une fonction de l'installation devrait dépendre du fait de savoir s'il existe une définition de la fonction qui s'applique à n'importe quel cas de figure ou mode dont la fonction dépend. S'il n'est pas possible de définir la fonction de cette manière, la liste des conséquences sera parfois incomplète et il peut être nécessaire de procéder à une analyse complémentaire ou d'accorder une importance plus grande à la fonction (par prudence).

Interdépendance des fonctions de l'installation

4.26. Pour l'attribution d'un degré d'importance à une fonction, il faudrait tenir compte des conséquences possibles d'une compromission (ou de dysfonctionnements) sur les autres fonctions qui en dépendent. Exemples de dépendances entre fonctions :

a) Dépendance en matière d'informations : Une fonction transmet des informations à une autre fonction. Exemples de dysfonctionnements :
   i) interruption des instructions de contrôle automatisé pour un processus mis en œuvre dans l'installation ;
   ii) compromission des messages d'alerte qui sont envoyés aux agents de sécurité ;
   iii) affichage d'informations erronées qui concernent la surveillance de la centrale et sont destinées au personnel d'exploitation ;
   iv) impossibilité de fournir des informations aux membres des équipes d'intervention ou aux responsables de la sécurité nucléaire ;
   v) perte ou altération de procédures ou d'instructions, ou des dossiers qui contiennent les résultats de ces procédures.
b) Dépendance en matière d'ingénierie ou de ressources physiques : Une fonction apporte une ressource physique à une autre fonction. Les ressources concernées comprennent les ressources directement nécessaires pour que l'autre fonction puisse s'exécuter et les ressources nécessaires au maintien des ressources en question. Exemples de dysfonctionnements :
   i) interruption de l'approvisionnement en eau ou en électricité ;
   ii) conditions ambiantes imprévues ;
   iii) impossibilité de planifier des tâches de maintenance préventive ;
   iv) défaillance des systèmes de protection physique (contrôles des accès, détection d'intrusions).
c) Dépendance en matière de règles ou de procédures : Un changement opéré sur une fonction nécessite une modification d'une autre fonction. Si une règle exige par exemple que les fonctions source froide primaire et secondaire soient exécutées lorsqu'un réacteur est en état critique, l'indisponibilité de l'une de ces sources impose de placer le réacteur en état sous-critique.
d) Effets à faible distance : Pour une fonction, effets des dysfonctionnements ou des défaillances physiques d'autres systèmes qui se trouvent à proximité de ceux qui exécutent la fonction concernée.

4.27. Dans certains cas, une analyse des relations et des interdépendances montre qu'une fonction importante n'a pas été prise en compte lors de l'évaluation. Les dépendances ne se limitent pas toujours à l'installation (approvisionnement en eau

ou électricité, par exemple). Pour l'analyse des dépendances, il est donc parfois nécessaire d'examiner certaines fonctions qui sont assurées par des organismes externes. En pareil cas, il peut être nécessaire d'élargir le cadre de l'évaluation pour prendre en compte ces dépendances ou de faire des modifications dans l'installation pour les éliminer.

4.28. Séparer les systèmes qui exécutent les fonctions pour limiter leurs relations et leurs interdépendances permet parfois de simplifier la définition des niveaux et des exigences de sécurité informatique et d'améliorer l'efficacité et l'efficience des mesures de sécurité informatique.

Délai d'exécution et exactitude nécessaires pour l'interdépendance des fonctions

4.29. Pour l'attribution d'un degré d'importance aux fonctions de l'installation, il faut parfois aussi tenir compte du délai et de l'exactitude nécessaires lorsqu'une fonction doit répondre à une autre fonction. Le délai d'exécution peut être examiné au regard des exigences à respecter pour la disponibilité des informations sensibles, et l'exactitude au regard des exigences à respecter pour l'intégrité de ces informations :

a) Les informations sont par exemple disponibles lorsque les messages d'alerte qui sont envoyés par une fonction sont rapidement émis pour que d'autres fonctions comme l'évaluation de ces messages ou les interventions en cas d'alerte soient exécutées.
b) Les informations sont par exemple intègres lorsqu'une fonction envoie des données exactes qui concernent l'environnement (température, pression, fréquence ou niveau, par exemple) et dont d'autres fonctions dépendent.

Détermination des cibles

4.30. Dans la référence [1], une cible est définie comme suit :

> *« Matières nucléaires, autres matières radioactives, installations associées, activités associées* ou autres emplacements ou objets pouvant être exploités par une *menace contre la sécurité nucléaire*, y compris les *grandes manifestations publiques*, les *emplacements stratégiques,* les *informations sensibles et* les *ressources d'informations sensibles. »*

4.31. Certains systèmes qui exécutent des fonctions sont des cibles et il faudrait se servir de la liste des fonctions qui a été établie lorsque la GRSI pour l'installation

a été menée pour les répertorier, à l'aide des définitions de la zone vitale [16] et des informations sensible [5]. Le fait qu'un système de ce type soit qualifié de cible n'a pas d'incidence sur l'importance d'une fonction, mais est pris en compte lorsque les exigences de sécurité informatique sont définies.

4.32. Les cibles qui sont associées à des fonctions de sûreté et de sécurité importantes devraient être considérées comme des RNS à l'issue de la procédure qui est décrite aux paragraphes 3.6 à 3.9. Il faudrait aussi analyser ces RNS pour déterminer l'intérêt éventuel des informations sensibles correspondantes. Les RNS et ces informations seront ainsi prises en compte dans le programme de sécurité de l'information et le PSI de l'installation, et seront convenablement protégées.

Documentation relative aux fonctions de l'installation

4.33. L'exploitant devrait consigner des informations sur toutes les fonctions qui ont été recensées et évaluées lorsque la GRSI pour l'installation a été menée.

4.34. Pour recenser toutes les fonctions qui se trouvent à l'intérieur de l'installation, il faut disposer de dossiers complets et précis, où figurent les relations entre les fonctions et les interdépendances. Ces dossiers permettront d'évaluer les fonctions qui peuvent avoir des effets négatifs sur d'autres fonctions si elles ne s'exécutent pas correctement.

4.35. Les relations et les interdépendances peuvent être internes ou externes, durables ou temporaires. Pendant la phase de mise au point des systèmes, il peut par exemple être nécessaire d'établir des relations entre l'environnement où les systèmes sont mis au point et l'environnement opérationnel par un transport physique de logiciels, de données ou d'appareils nouveaux, mais il est possible d'y mettre fin dès que les systèmes sont opérationnels.

4.36. Lorsque l'exploitant analyse les conséquences d'une attaque lancée contre une fonction, il devrait envisager qu'elle entre dans le cadre d'une attaque qui touche plusieurs fonctions ou d'une attaque combinée (type d'attaque qui associe une cyberattaque et une attaque physique).

4.37. Dans le cadre de l'analyse, il peut être nécessaire de procéder à une évaluation itérative de chaque fonction : dans ce cas, on effectue une première évaluation pour déterminer l'importance intrinsèque de la fonction, et une seconde pour déterminer l'importance de la fonction compte tenu des relations avec d'autres fonctions et des interdépendances des fonctions. Il faudrait retenir le degré d'importance le plus élevé des deux résultats obtenus grâce à ces évaluations.

4.38. Il faudrait attribuer le degré d'importance le plus élevé aux fonctions pour lesquelles il existe un lien direct entre une mauvaise exécution de la fonction concernée et les conséquences les plus graves (par exemple aux fonctions qui ont un rapport étroit avec les trois fonctions de sûreté principales, à savoir la maîtrise de la criticité, l'évacuation de la chaleur et le confinement des matières [12])[24]**.** En pareil cas, il ne faudrait pas tenir compte d'autres paramètres ou d'autres facteurs pour l'attribution d'un degré d'importance.

CARACTÉRISATION DE LA MENACE

4.39. La caractérisation de la menace dépend de deux opérations continues et distinctes, qui sont interdépendantes :

a) l'évaluation par l'État des menaces et l'élaboration et la mise à jour de la menace de référence ou de l'énoncé de la menace nationaux grâce aux éléments obtenus par les services de renseignement ;
b) l'évaluation de la menace propre à l'installation, qui prend en compte l'analyse d'informations qui concernent uniquement l'installation et d'informations sur des adversaires particuliers.

Sources d'information sur la menace

4.40. Selon le paragraphe 3.34 de la référence [2] :

> « Les autorités nationales compétentes devraient définir, à partir de diverses sources d'information crédibles, la *menace* et les moyens associés sous forme d'une *évaluation de la menace* et, s'il y a lieu, d'une *menace de référence*. Une *menace de référence* est définie à partir de l'évaluation par l'État de la menace d'*enlèvement non autorisé* et de *sabotage*. »

On trouvera de plus amples informations sur la menace de référence dans la référence [9].

[24] S'agissant des relations qui existent entre les catégories de sûreté et les fonctions examinées dans le cadre de l'analyse des événements initiateurs postulés, voir également le tableau 1 de la référence [17].

4.41. L'exploitant devrait mettre en place des mesures pour recenser, conserver et gérer les informations[25] qui concernent les cyberattaques et les adversaires éventuels (courriels d'hameçonnage ou logiciels malveillants détectés, par exemple), afin de pouvoir effectuer une analyse ultérieure qui facilitera la caractérisation de la menace. Il devrait veiller à ce que ces mesures soient mises en œuvre sans porter atteinte à la sécurité nucléaire ou à la sûreté nucléaire.

4.42. La caractérisation de la menace qui est effectuée par l'exploitant comprend parfois des éléments d'évaluations de la menace qui ont été menées par d'autres organismes (évaluations menées par l'exploitant lui-même ou rapports contenant des informations provenant de sources librement accessibles, par exemple).

4.43. L'autorité compétente concernée est encouragée à analyser rapidement et dans un esprit de coopération les informations obtenues par l'exploitant, et à faciliter les échanges sur cette analyse et d'autres informations importantes, conformément aux prescriptions édictées par l'État en matière d'informations sensibles [5]. Il peut être utile que l'exploitant signale périodiquement les incidents détectés à l'autorité compétente concernée au titre de l'analyse de la menace. D'autre part, la caractérisation est une activité continue qui exige une actualisation des informations.

4.44. Lors de l'élaboration de la menace de référence ou de l'énoncé de la menace nationaux, l'autorité compétente et les autres autorités nationales concernées devraient avoir des compétences et des connaissances dans le domaine des incidents de sécurité informatique (cyberattaques, par exemple) qui peuvent se produire dans une installation nucléaire, ou avoir accès à ce type de compétences et de connaissances.

4.45. La référence [7] donne des orientations sur l'évaluation des cybermenaces qui pèsent sur un régime de sécurité nucléaire, et décrit en détail l'origine possible des attaques et les mécanismes d'attaque correspondants qui concernent les installations nucléaires, ainsi que les méthodes utilisées pour évaluer et recenser les menaces.

[25] Ces informations peuvent être communiquées par l'exploitant, une autorité compétente ou un autre organisme national. Elles peuvent être classées et doivent donc être traitées conformément aux exigences de l'État en matière de recensement et de gestion des informations sensibles.

Caractérisation de la menace propre à l'installation

4.46. L'exploitant devrait élaborer et tenir à jour une caractérisation de la menace propre à l'installation, afin de faciliter l'évaluation des risques liés à la sécurité informatique pour l'installation. Cette caractérisation devrait comprendre une analyse de la menace de référence ou de l'énoncé de la menace nationaux afin de caractériser les menaces qui pèsent sur la sécurité nucléaire de l'installation et qui créent un risque lié à la sécurité informatique. Cette analyse devrait présenter les objectifs, les capacités, les tactiques et les techniques possibles des menaces concernées, et servir de point de départ pour élaborer la politique de sécurité informatique et le PSI de l'installation, et pour en confirmer l'efficacité.

4.47. L'exploitant devrait caractériser la menace dans les cas suivants :

a) Il évalue les risques liés à la sécurité informatique pour l'installation. Parfois, cette analyse est moins approfondie et a pour objet de vérifier les analyses et les hypothèses précédentes.
b) L'autorité compétente diffuse une nouvelle menace de référence ou un nouvel énoncé national de la menace.
c) L'exploitant reçoit des informations qui peuvent invalider des hypothèses sur lesquelles se fonde l'analyse actuelle.

4.48. La caractérisation de la menace faite par l'exploitant devrait présenter les connaissances, les moyens et le financement dont disposent les adversaires recensés, mais aussi les campagnes, les cibles, les tactiques, les techniques et les modes opératoires possibles, ainsi que tous les autres attributs qui revêtent une importance particulière. Le paragraphe 5.19 de la référence [9] contient une liste d'autres attributs qui peuvent être utilisés pour caractériser la menace.

4.49. La caractérisation de la menace faite par l'exploitant devrait permettre de déterminer les combinaisons de tactiques et de techniques qui peuvent être employées pour une attaque, par exemple des actions coordonnées à distance et sur place, le recours à des initiés et à des adversaires externes ou encore des attaques combinées, qui associent des cyberattaques et des attaques physiques. Dans le cadre de la caractérisation de la menace, il faudrait prévoir la possibilité de cyberattaques parallèles ou successives aux effets cumulatifs, lancées par un ou plusieurs adversaires, ainsi que les cas où il n'y a aucun signe de collusion entre les différents adversaires (attaques indépendantes).

4.50. La caractérisation de la menace faite par l'exploitant devrait permettre de dresser la liste des types d'attaque crédibles et de les évaluer. Cette liste servira de référence pour les exigences de sécurité informatique et la définition de l'ASID.

4.51. La caractérisation de la menace devrait permettre de déterminer si l'adversaire a les moyens de mener un type d'attaque particulier et s'il peut compromettre un système qui exécute une fonction de telle manière que son comportement soit indéterminé (c'est-à-dire qu'il n'est pas prévu par la base de conception).

Considérations supplémentaires pour les menaces internes

4.52. Dans le cadre de la caractérisation de la menace, il faudrait examiner les menaces internes. On trouvera des orientations sur cette question dans la référence [6]. S'agissant de la sécurité informatique, on peut classer les menaces internes comme suit :

a) Initié passif : Initié qui est suffisamment motivé pour faciliter la commission d'actes malveillants, mais pas pour en prendre l'initiative. Les mesures de sécurité informatique qui sont mises en œuvre pour neutraliser un initié passif peuvent reposer sur des mesures préventives, notamment sur le fait d'avoir instauré une solide culture de sécurité. L'initié passif ne se laisse généralement pas décourager par les mesures de détection, parce qu'il peut légitimement accéder aux informations et aux systèmes, mais il cherche à éviter que l'on ne découvre qu'il agit avec malveillance.
b) Initié actif : Initié qui est suffisamment motivé pour entreprendre des actes malveillants. Les initiés actifs sont probablement moins nombreux que les initiés passifs. Les contrôles de sécurité informatique qui sont appliqués pour neutraliser un initié actif doivent être plus exhaustifs que ceux qui visent à contrer un initié passif, et devraient comprendre des mesures de protection, par exemple une séparation des tâches et un cloisonnement des informations, des accès physiques ou des privilèges qui sont associés aux différents systèmes.
c) Initié involontaire : Initié qui ne souhaite pas commettre un acte malveillant et qui n'a pas conscience d'être exploité par un adversaire. Dans le cas d'une cyberattaque par exemple, un initié involontaire peut ne pas savoir que certaines actions (par exemple un clic sur un lien malveillant dans un courriel qui semble provenir d'une source fiable) peuvent donner des informations ou un accès authentifié à un adversaire.

4.53. En cas de menace interne, les chemins exploités par l'adversaire et la chronologie correspondante ne sont pas les mêmes que pour les autres menaces, car les initiés

bénéficient d'un accès autorisé. Cet accès leur permet par exemple d'exécuter une série d'actions discontinue sur une longue période. Ainsi, la collecte d'informations sur les comptes administrateur (par ingénierie sociale ou par la compromission de systèmes) pour neutraliser des mesures comme le contrôle des accès ou la séparation des tâches peut se dérouler sur plusieurs semaines, plusieurs mois ou plusieurs années.

DÉFINITION DES EXIGENCES DE SÉCURITÉ INFORMATIQUE

Politique et programme de sécurité informatique

4.54. La politique de sécurité informatique de l'exploitant[26] précise les objectifs et les exigences globales pour la sécurité informatique de l'installation, selon une approche graduée et le principe de la défense en profondeur. Ces exigences sont définies par l'exploitant, conformément aux prescriptions réglementaires en vigueur, et s'appliquent sans exception. La politique de sécurité informatique est examinée dans le cadre de la GRSI pour l'installation, et peut être complétée et précisée dans ce cadre.

4.55. L'exploitant devrait concevoir et rédiger son PSI[27] lorsqu'il effectue la GRSI pour l'installation. Le PSI offre un cadre pour la mise en œuvre de la politique de sécurité informatique de l'installation, et sera utilisé pendant toute la durée de vie de l'installation. Le contenu d'un PSI type figure dans la section 7. Le PSI comprend les exigences de sécurité informatique propres à l'installation, en plus des exigences formulées grâce à une approche fondée sur les risques.

4.56. L'exploitant devrait définir les exigences de sécurité informatique dans le PSI pour les éléments suivants, qui sont décrits en détail dans la section 7 :

a) rôles et responsabilités au sein de l'organisation ;
b) évaluation des risques, des vulnérabilités et du respect des règles ;
c) procédures de sécurité au sein de l'organisation ;
d) conception et gestion de la sécurité des systèmes ;
e) gestion des ressources et de la configuration ;
f) gestion du personnel.

---

[26] Dans certaines organisations, la politique de sécurité informatique est appelée « stratégie de sécurité informatique ».

[27] Dans certaines organisations, le PSI est appelé « plan de sécurité informatique ».

4.57. Dans le PSI, l'exploitant devrait dresser la liste des mesures de sécurité informatique qui sont obligatoires pour chaque niveau de sécurité informatique. Ces mesures prennent généralement la forme d'exigences fixées pour des règles et des processus de l'organisation concernée, et donneront lieu à des procédures.

4.58. Pour chaque niveau de sécurité informatique, il faudrait définir l'intensité des mesures de sécurité informatique conformément aux prescriptions réglementaires (le cas échéant). Il est fortement déconseillé de déroger à l'application d'une mesure particulière prévue pour un certain niveau de sécurité informatique, et les exceptions de ce type devraient être justifiées et consignées dans le cadre de la GRSI pour l'installation.

4.59. Les principaux produits de la phase de définition de la GRSI pour l'installation sont les documents qui établissent le PSI (ou le PSI révisé) et un rapport de conformité adressé à l'autorité compétente, qui montre comment la mise en œuvre du PSI garantit le respect des prescriptions réglementaires. Le PSI peut être constitué d'un ou plusieurs documents, mais ceux-ci devraient comprendre :

a) Un énoncé contenant le degré de protection à prévoir pour chaque niveau de sécurité informatique. Cet énoncé peut être de nature qualitative ou quantitative, mais devrait être vérifiable.
b) L'obligation de procéder régulièrement à un examen de la sécurité informatique et à une évaluation du risque et d'en consigner les résultats à chaque étape de la durée de vie de l'installation.
c) Une définition des rôles et des responsabilités qui sont nécessaires pour la sécurité informatique.
d) Une description de l'ASID, où figurent d'une part les exigences de sécurité informatique découlant de l'approche fondée sur les risques qui est appliquée par l'exploitant, et d'autre part les prescriptions qui s'imposent à l'installation de par la législation ou la réglementation nationales. Cette description devrait comprendre :
    i) les exigences relatives à l'application d'une approche graduée (nombre de niveaux de sécurité informatique, par exemple) ;
    ii) les exigences relatives à la défense en profondeur ;
    iii) d'autres exigences (concernant l'authenticité, la non-répudiation ou la traçabilité, par exemple) qui sont nécessaires pour que la protection prévue pour chaque niveau de sécurité informatique soit suffisante ;
    iv) les exigences qui permettront constamment à l'exploitant de prévenir, de détecter et de retarder les cyberattaques, d'en atténuer les effets et d'en effacer les conséquences ;

v) les exigences particulières à appliquer dans le cadre des mesures de sécurité informatique pour chaque niveau attribué à une zone de sécurité informatique.

e) Les scénarios fonctionnels ou une description des autres méthodes d'évaluation qui sont utilisées dans le cadre de l'analyse pour définir les exigences. Il importe que d'autres scénarios soient élaborés séparément afin de renforcer la confiance. L'utilisation de scénarios pour renforcer la confiance dans les documents issus de la phase de définition est présentée plus en détail aux paragraphes 4.116 à 4.122.

4.60. L'exploitant devrait communiquer le PSI et le rapport de conformité à l'autorité compétente pour examen.

Attribution d'un niveau de sécurité informatique aux systèmes qui exécutent des fonctions de l'installation

4.61. Dans le cadre de la GRSI pour l'installation, il faudrait dresser ou utiliser une liste hiérarchisée des fonctions de l'installation, établie selon le degré d'importance de la fonction concernée, afin d'appliquer une approche graduée et de garantir la plus grande protection aux fonctions qui sont les plus susceptibles d'avoir les plus graves conséquences en cas de défaillance.

4.62. L'attribution de niveaux de sécurité informatique vise à simplifier l'application d'une approche graduée. Le niveau de sécurité informatique permet de déterminer quelles exigences de sécurité informatiques sont mises en œuvre pour que le système qui exécute une fonction soit convenablement protégé.

4.63. L'exploitant devrait définir le nombre de niveaux de sécurité informatique à utiliser, en tenant compte des prescriptions réglementaires applicables. Un exploitant peut par exemple choisir d'attribuer un niveau de sécurité différent à chaque fonction. Cette solution est cependant d'autant plus complexe à appliquer que le nombre de niveaux de sécurité est élevé. La limitation du nombre de niveaux de sécurité permet d'appliquer les mêmes approches et les mêmes méthodes à différents systèmes. Il peut donc être décidé d'utiliser un plus petit nombre de niveaux dans l'installation. Il faudrait mettre en balance d'une part la simplicité induite par la réduction du nombre de niveaux et, d'autre part, le coût des ressources et la perte d'efficacité qui résultent de l'application de mesures plus strictes qu'il n'est absolument nécessaire dans tous les cas pour les fonctions.

4.64. L'exploitant devrait veiller à ce que chaque fonction d'une installation se voie attribuer un seul niveau de sécurité informatique.

4.65. Dans certains cas, les fonctions qui sont importantes pour la sécurité ou ont un rapport avec celle-ci ne sont pas définies avec une précision suffisante pour bien les distinguer des autres fonctions. L'incapacité à distinguer une fonction d'une autre rend plus complexe l'attribution d'une importance à une fonction. Dans la mesure du possible, les fonctions de l'installation devraient donc être distinctes et indépendantes les unes des autres. L'exploitant peut envisager de modifier une fonction pour simplifier la mise en œuvre de l'approche graduée, qui peut elle-même également être utile pour l'application du principe de la défense en profondeur.

4.66. L'exploitant devrait faire figurer les éléments suivants dans le PSI :

a) nombre de niveaux de sécurité informatique et exigences applicables aux mesures de sécurité correspondantes ;
b) liste ordonnée des fonctions, où il est expliqué comment les niveaux de sécurité informatique ont été attribués aux fonctions.

Élaboration de l'architecture de sécurité informatique défensive

4.67. L'exploitant devrait concevoir et mettre en œuvre une ASID pour laquelle tous les systèmes qui exécutent des fonctions se voient attribuer un niveau de sécurité informatique et sont protégés conformément aux exigences de sécurité informatique qui ont été définies pour le niveau en question.

4.68. Dans ce cadre, l'exploitant devrait dresser la liste des mesures de sécurité informatique qui sont obligatoires pour chaque niveau de sécurité informatique. Ces mesures peuvent être des mesures de contrôle technique, de contrôle administratif ou de contrôle physique.

4.69. L'ASID devrait être conçue pour barrer ou restreindre les chemins (énumérés dans la caractérisation de la menace) qui pourraient être exploités par un adversaire pour commettre une cyberattaque et compromettre des systèmes qui exécutent des fonctions. Des méthodes analogues qui permettent de restreindre les itinéraires physiques qui s'offrent à l'adversaire sont présentées en détail dans la référence [16].

4.70. Il faudrait mettre en place des limites de sécurité informatique[28] entre les systèmes qui exécutent des fonctions auxquelles des niveaux de sécurité informatique différents ont été attribués.

Exigences qui doivent figurer dans le document décrivant l'ASID pour mettre en œuvre une approche graduée

4.71. Dans le document qui décrit l'ASID, il faudrait définir les exigences générales (notamment le nombre de niveaux de sécurité informatique), l'intensité des mesures à mettre en œuvre pour chaque niveau de sécurité et des mesures qui s'appliquent entre ces différents niveaux, et les règles de communication à respecter entre les zones qui ne sont pas soumises au même niveau de sécurité.

4.72. Dans le même document, il faudrait que les fonctions les plus importantes se voient attribuer le niveau de sécurité informatique le plus strict. Il faudrait définir des exigences pour la communication entre les systèmes qui exécutent des fonctions différentes. Il faudrait contrôler les flux de données qui circulent entre les fonctions auxquelles des niveaux de sécurité informatique différents ont été attribués, conformément à une approche fondée sur les risques.

4.73. L'ASID devrait être élaborée de telle manière que la conception des systèmes soit peu complexe, dans la mesure du possible, afin de simplifier la mise en œuvre des mesures de sécurité informatique. En réduisant la complexité de ces mesures, on peut améliorer l'efficacité et la fiabilité.

Exigences qui doivent figurer dans le document décrivant l'ASID pour pouvoir appliquer le principe de la défense en profondeur

4.74. Dans le document décrivant l'ASID, il faudrait exiger l'application du principe de la défense en profondeur au moyen de couches successives[29] de mesures de sécurité informatique, qui doivent être neutralisées ou contournées par un adversaire pour que les systèmes qui exécutent des fonctions soient compromis.

---

[28] Dans la présente publication, les « limites de sécurité informatique » désignent les limites logiques et physiques d'un système ou d'un ensemble de systèmes qui ont le même niveau de sécurité et qui peuvent donc être protégées par les mêmes mesures de sécurité (zones de sécurité informatique, par exemple).

[29] Dans la présente publication, le terme « couches » désigne les couches de défense en profondeur. Dans le domaine de la sécurité informatique, cette défense est généralement assurée grâce à l'aménagement de zones de sécurité informatique (y compris la mise en place des mesures correspondantes), qui sont établies en conformité avec les exigences associées aux niveaux de sécurité informatique et avec l'ASID.

4.75. L'ASID devrait prévoir une combinaison de mesures de contrôle technique, de contrôle physique et de contrôle administratif pour assurer la défense en profondeur.

4.76. Le même document devrait imposer une conception garantissant qu'une compromission ou la défaillance d'une seule mesure de sécurité informatique n'aura pas de conséquences inacceptables.

4.77. Dans le document décrivant l'ASID, il faudrait exiger l'adoption de mesures indépendantes et diversifiées, afin qu'une vulnérabilité commune ne permette pas à un adversaire de compromettre ou de contourner plusieurs couches de défense en profondeur en employant une seule tactique.

4.78. Dans ce même document, il faudrait exiger l'application du principe de la défense en profondeur entre les couches et à l'intérieur de chaque couche. Pour ces couches, une combinaison de mesures applicables à différents niveaux de sécurité informatique peut être utilisée et appliquée aux différentes zones de sécurité informatique. S'agissant des conséquences les plus graves (c'est-à-dire les graves conséquences radiologiques dues à un sabotage ou à un enlèvement non autorisé de matières nucléaires de catégorie I), des mesures de sécurité informatique devraient être mises en œuvre dans plusieurs couches indépendantes afin que les systèmes aient un comportement déterministe et un fonctionnement à sécurité intégrée[30] en cas de cyberattaque.

4.79. Le document décrivant l'ASID devrait s'appuyer sur un rapport d'analyse qui recense les mesures de sécurité informatique à sécurité intégrée et déterministes pour l'application du principe de la défense en profondeur. L'autorité compétente peut demander que ce rapport soit soumis à un examen.

Défense en profondeur entre les couches

4.80. Dans le document décrivant l'ASID, il faudrait exiger que chaque couche de défense en profondeur soit protégée contre les cyberattaques qui frappent des couches adjacentes. Les couches et les mesures de sécurité informatique correspondantes devraient empêcher ou retarder la progression des attaques.

4.81. Dans le document mentionné au paragraphe précédent, il faudrait exiger que les mesures de sécurité informatique qui sont appliquées à une couche donnée

[30] Le terme « sécurité intégrée » signifie que la défaillance d'une mesure censée protéger une fonction conduit à une situation dans laquelle la sécurité de cette fonction est préservée.

soient sélectionnées et mises en œuvre de manière diversifiée et indépendante par rapport aux mesures de sécurité informatique qui sont employées pour une couche adjacente, afin de limiter les défaillances de cause commune des mécanismes de protection qui sont utilisés pour isoler les couches les unes des autres. Conformément à une approche graduée, les exigences devraient être plus strictes pour les couches qui nécessitent la protection la plus rigoureuse (c'est-à-dire les niveaux de sécurité informatique 1 et 2).

Défense en profondeur dans une couche

4.82. Dans le document décrivant l'ASID, il faudrait exiger qu'une combinaison de mesures de sécurité informatique soit appliquée à chaque couche, afin de réduire au minimum le risque qu'une seule compromission permette de neutraliser ou de contourner plusieurs mesures. Conformément à une approche graduée, les exigences devraient être les plus fortes pour les couches qui nécessitent la protection la plus rigoureuse (c'est-à-dire les niveaux de sécurité informatique 1 et 2, le niveau 1 étant le niveau de protection le plus élevé).

Modèle de confiance

4.83. La mise en œuvre d'une approche graduée et du principe de la défense en profondeur devrait être compatible avec un modèle de confiance applicable. Les modèles de confiance qui peuvent être appliqués sont notamment les suivants :

a) habilitation du personnel (c'est-à-dire la protection contre les menaces internes) [6] ;
b) protection des informations sensibles (c'est-à-dire classées) (modèle Bell-LaPadula[31], par exemple) ;
c) protection de l'intégrité (modèle Biba ou Clark-Wilson[32], par exemple).

[31] Le modèle Bell-LaPadula assure le respect de la confidentialité : pour accéder à des informations, une personne ou un dispositif devrait avoir un réel besoin d'en connaître ; cette personne ou ce dispositif devrait alors au moins pouvoir connaître le degré de classification des informations sensibles.

[32] Les modèles Biba et Clark-Wilson protègent l'intégrité de l'information : Le modèle Biba empêche la modification des données par des personnes non autorisées, mais n'empêche pas la modification non autorisée par des personnes autorisées (c'est-à-dire des initiés), alors que le modèle Clark-Wilson empêche les deux types de modifications.

RAPPORT AVEC LA GESTION DES RISQUES LIÉS À LA SÉCURITÉ INFORMATIQUE POUR LES SYSTÈMES (MENÉE POUR CHAQUE SYSTÈME)

4.84. Une fois définies, les exigences de sécurité informatique sont mises en œuvre selon le processus qui est représenté sur la figure 6 (voir également la figure 7). Pour pouvoir mettre en œuvre les exigences, il faut comprendre comment les fonctions de l'installation sont exécutées par les ressources numériques.

4.85. Il y a une réelle interdépendance entre la GRSI pour l'installation et la GRSI pour ses systèmes (voir fig. 6 et 7). La GRSI pour l'installation comprend l'attribution d'une ou plusieurs fonctions à un système particulier, et définit donc le cadre de la GRSI pour chaque système, mais les résultats de la GRSI pour un système peuvent aussi avoir une incidence sur la GRSI pour l'installation, car cette dernière est itérative. Plusieurs fonctions peuvent par exemple être attribuées à un seul système de protection physique, car il n'existe pas de système de ce type qui puisse exécuter des fonctions séparées. De ce fait, il n'est guère possible de séparer un tel système en zones distinctes, de sorte que les zones ne peuvent être définies que par une limite physique ou par une limite logique.

4.86. Dans des installations ou des systèmes anciens, certaines structures, certains systèmes ou certains composants peuvent ne pas être modifiables ou transformables. Lorsque l'on effectue la GRSI pour un système, il n'est donc pas toujours possible de respecter toutes les exigences qui ont été définies dans le cadre de la GRSI pour l'installation, et l'exploitant peut être amené à revoir cette dernière pour élaborer un PSI et une ASID qui soient appropriés et conformes aux exigences de sécurité.

4.87. Il faudrait examiner la GRSI pour l'installation et la GRSI pour un de ses systèmes, et il pourrait être nécessaire de les réviser dans les cas suivants :

a) La GRSI pour l'installation ou l'analyse de la sûreté de l'installation a été revue.
b) Le système ne peut respecter complètement les exigences qui figurent dans les documents issus de la GRSI.
c) Des modifications qui peuvent avoir une incidence sur la GRSI pour l'installation sont apportées à un système.
d) Des événements ou des incidents de sécurité à prendre en considération ont eu lieu.
e) Des menaces ou vulnérabilités nouvelles ou ayant évolué ont été détectées.

4.88. Dans le cadre de la gestion du changement pour une installation, il faut prévoir des révisions de la GRSI pour l'installation concernée et de la GRSI pour ses systèmes afin qu'elles soient harmonisées et actualisées. Ces analyses facilitent également la définition des exigences (définition des niveaux de sécurité informatique, par exemple) pour des modalités d'utilisation ou des systèmes nouveaux.

4.89. Il faudrait régulièrement évaluer les tendances qui se dégagent des itérations appliquées successivement à la GRSI pour l'installation ou pour un de ses systèmes afin de détecter les évolutions préoccupantes suivantes :

a) Un risque qui augmente de telle manière qu'il va manifestement atteindre ou dépasser le seuil de risque inacceptable. En pareil cas, il conviendrait d'examiner les moyens propres à empêcher le dépassement du seuil de risque.
b) Un risque qui atteint ou dépasse le seuil. En pareil cas, les décisions appropriées devront être prises (signalement à l'autorité compétente ou mise en œuvre de mesures compensatoires qui soient adaptées à la gravité évaluée grâce aux données sur l'évolution du risque, par exemple).

4.90. Il faudrait analyser les évolutions qui concernent un système particulier, afin de s'assurer que les documents issus de la GRSI pour l'installation restent pertinents. Des évaluations portant sur la surveillance d'un système peuvent par exemple être menées continuellement, et des rapports consacrés au contrôle du fonctionnement du système concerné peuvent alors être régulièrement approuvés. Dans le cadre de la GRSI pour l'installation, il faudrait revoir les documents issus de la GRSI pour les systèmes correspondants afin de s'assurer que le risque global pour l'installation n'a pas changé.

ACTIVITÉS D'ASSURANCE

4.91. Il existe trois types d'activités d'assurance :

a) L'évaluation, qui permet de confirmer les résultats obtenus à l'issue d'une phase lorsqu'aucune vérification n'est possible (par exemple pour les phases de caractérisation de la menace et de définition des exigences de sécurité informatique). Compte tenu de la nature des informations qui sont utilisées pour établir les exigences de sécurité informatique (appréciation de la menace et hypothèses concernant les modes de défaillance des fonctions de l'installation qui sont provoqués par la compromission de systèmes, par

exemple), l'exploitant ne peut être certain que les exigences sont pertinentes. Il faut donc procéder à une évaluation pour que l'exploitant ait confiance dans les documents issus de la phase de définition des exigences de sécurité informatique, c'est-à-dire le PSI et l'ASID.

b) La vérification, qui permet de confirmer que les résultats d'une phase satisfont aux objectifs et aux exigences qui ont été définis pour la phase en question. Dans la mesure du possible, les activités de vérification sont menées entre les phases successives de la GRSI pour l'installation et pour ses systèmes. Dans ce cadre, plusieurs méthodes ou analyses relatives au fonctionnement peuvent être mises en œuvre pour vérifier les résultats de chaque phase avant qu'ils ne soient utilisés comme élément d'entrée pour une phase ultérieure.

c) La validation, qui permet de déterminer si les mesures de sécurité informatique prévues pour l'installation offrent une protection suffisante contre la menace (telle qu'elle est définie dans la caractérisation de la menace) et sont conformes aux prescriptions réglementaires.

Évaluation

4.92. L'exploitant devrait évaluer le PSI et l'ASID pour vérifier que, s'ils sont mis en œuvre, ils permettront de limiter les failles qui pourraient être exploitées par les adversaires pour compromettre des systèmes qui exécutent des fonctions de l'installation. Pour ce faire, il devrait notamment accomplir les tâches suivantes :

a) recensement des fonctions et attribution d'un niveau de sécurité informatique aux fonctions ;
b) association entre les mesures de sécurité informatique et ces niveaux ;
c) définition des mesures de sécurité informatique.

4.93. L'évaluation du PSI et de l'ASID devrait comprendre des essais de fonctionnement et des tests de performance conformément aux prescriptions réglementaires. Dans ce cadre, il faudrait prendre en considération la GRSI pour l'installation et pour ses systèmes, ainsi que toute la durée de vie de l'installation.

4.94. L'exploitant devrait envisager de faire appel à des experts indépendants afin d'examiner le PSI et l'ASID.

4.95. L'exploitant devrait justifier toutes les hypothèses qui concernent la probabilité d'attaque ou de réussite d'une attaque (vulnérabilité, exposition ou circonstances favorables, par exemple) et sur lesquelles repose l'évaluation. Il faudrait supposer que ces probabilités sont égales à 1 pour les scénarios envisagés

qui peuvent avoir des conséquences radiologiques inacceptables[33] ou donner lieu à un enlèvement non autorisé de matières nucléaires (c'est-à-dire à une compromission de RNS).

4.96. La menace de référence ou l'énoncé de la menace nationaux, ainsi que l'évaluation de la menace propre à l'installation servent de référence permettant à l'exploitant d'effectuer une analyse pour confirmer les hypothèses qui ont été formulées lorsqu'un niveau de sécurité informatique a été attribué aux fonctions de l'installation. L'utilisation de scénarios fonctionnels crédibles [par. 4.120 a)] peut contribuer à donner une plus grande assurance dans la qualité de l'évaluation (on trouvera des exemples de scénarios dans l'annexe I).

4.97. Les mesures de sécurité informatique qui découlent du PSI et de l'ASID permettent d'assurer des fonctions de détection, de retardement et d'intervention par l'intermédiaire de mesures de contrôle physique (relatives à la structure, par exemple), technique (pare-feu, par exemple), et administratif (qui concernent le personnel ou les procédures, par exemple). En raison des relations qui existent entre ces mesures de sécurité informatique, les fonctions de l'installation qui sont importantes pour la sûreté et la sécurité, et les systèmes qui exécutent ces fonctions, il est difficile d'évaluer l'efficacité du PSI.

4.98. Quelques méthodes d'évaluation possibles :

a) Analyse de l'arbre d'attaque (également appelée « analyse des vecteurs d'attaque »). Méthode consistant à envisager plusieurs chemins qui pourraient être exploités par l'adversaire afin de déterminer s'il est fort probable que toutes les attaques échoueront (c'est-à-dire qu'il est possible d'empêcher l'adversaire d'exploiter ces chemins), ou seront détectées et feront l'objet d'une intervention avant que l'adversaire n'atteigne son objectif. Associée à la caractérisation de la menace, cette méthode peut être appliquée pour déterminer si les mesures qui découlent du PSI et de l'ASID permettent réellement d'éliminer ou de réduire au minimum le risque qu'un adversaire mène les attaques envisagées avec succès.
b) Simulation. Cette méthode consiste à effectuer des simulations informatiques d'éléments du PSI (y compris de l'ASID) et des exercices sur table qui permettent d'examiner le plan de sécurité, le plan d'urgence et les décisions prises par l'adversaire et par les personnes qui interviennent en cas d'incident de sécurité informatique. Ces moyens sont employés pour

[33] Une définition des conséquences radiologiques inacceptables est proposée dans la référence [16].

estimer la performance globale du PSI, compte tenu de toutes les mesures qui ont été mises en place. Les exercices sur table peuvent par exemple contribuer à déterminer quelles failles un adversaire pourrait exploiter compte tenu de ses capacités et de ses caractéristiques (fait de savoir s'il est composé d'initiés, par exemple), ou à connaître les vulnérabilités de la fonction concernée.

c) Exercices. Les exercices peuvent comprendre des tests de performance de l'installation et de ses systèmes (tests de pénétration, par exemple) et des exercices d'attaque simulée (pour les attaques combinées, par exemple) en conditions réelles ou en conditions d'essai. Ils peuvent porter sur la capacité du PSI à protéger toute l'installation, certaines de ses parties, certains de ses systèmes ou certaines mesures contre une attaque simulée. Dans le cadre de cette activité, les données qui concernent la performance des mesures de sécurité informatique sont recueillies et utilisées pour évaluer l'efficacité globale du PSI.

4.99. La simulation et les exercices sont généralement effectués dans le cadre d'une analyse de scénarios, pour laquelle des attaques envisagées (des scénarios) sont décrites en détail et sont simulées ou servent de point de départ pour les exercices. Dans le cas de l'analyse de scénarios, on utilise habituellement l'analyse de l'arbre d'attaque et on examine les tactiques et les techniques qui sont employées par l'adversaire pour neutraliser les mesures de sécurité informatique.

4.100. L'efficacité du PSI, de l'ASID ou de chaque mesure de sécurité informatique peut être évaluée de manière quantitative ou qualitative, ou des deux manières. L'autorité compétente peut imposer des méthodes d'évaluation déterministes qui doivent être utilisées pour différents types de cibles, de menaces et de scénarios. Il est recommandé de définir l'efficacité globale du PSI et de l'ASID comme l'efficacité la plus faible qui est conforme aux objectifs réglementaires, lorsque toutes les tactiques et toutes les techniques de l'adversaire, ainsi que les scénarios crédibles ont été pris en compte.

Vérification

4.101. Dans ce contexte, l'objectif de la vérification est d'évaluer la qualité des résultats d'une phase au regard des documents descriptifs avant qu'ils ne soient utilisés dans une phase ultérieure.

4.102. Dans la mesure du possible, la vérification devrait être menée entre les phases successives de la GRSI pour l'installation et pour ses systèmes.

4.103. Les résultats de la vérification peuvent amener l'exploitant à engager les actions suivantes :

a) corriger les défauts qui concernent la conception ou la mise en œuvre des mesures de sécurité informatique afin de respecter les exigences ;
b) recenser, analyser et appliquer les mises à niveau qui peuvent être nécessaires pour corriger les défauts qui ont été relevés et pour améliorer la performance.

4.104. Dans le cadre de ces activités de vérification, on peut utiliser des méthodes d'évaluation, notamment des exercices, des tests de performance, une simulation ou une analyse (évaluation de la vulnérabilité, par exemple) (voir par. 4.98).

4.105. Ainsi, l'évaluation des documents à l'aide de l'analyse de l'arbre d'attaque comprend l'examen des informations qui sont échangées entre les systèmes, les appareils, les réseaux et les emplacements. L'échange d'informations entre systèmes peut permettre à des adversaires d'exploiter les chemins concernés, ce qui peut aboutir à la compromission de systèmes et donc de fonctions de l'installation. À ce stade, pour l'analyse de l'arbre d'attaque, on examine les chemins généraux afin de réduire ou d'éliminer le risque qu'un adversaire ait accès à ces chemins.

4.106. L'exploitant devrait adopter une approche graduée lorsqu'il évalue l'ampleur des activités de vérification et de validation. Il faudrait consacrer le plus d'efforts aux fonctions ou aux systèmes auxquels les niveaux de sécurité informatique les plus contraignants ont été attribués (c'est-à-dire à ceux qui exigent la protection la plus forte).

4.107. Il faudrait effectuer une vérification régulièrement (chaque année, par exemple) ou au besoin pour prendre en compte les modifications des cibles ou des exigences du programme de sécurité nucléaire.

Validation

4.108. L'exploitant devrait s'assurer que les systèmes, une fois intégrés, sont suffisamment protégés pour satisfaire aux exigences de sécurité informatique qui figurent dans le PSI et dans l'ASID. Les activités de vérification et de validation qui sont menées dans le cadre de la GRSI, du PSI et de l'ASID sont présentées schématiquement sur la figure 7.

4.109. L'exploitant devrait s'assurer que les systèmes, tels qu'ils sont mis en place dans l'installation, sont suffisamment protégés sur le plan de la sécurité

informatique pour pouvoir exécuter les fonctions prévues conformément aux exigences de sécurité qui sont applicables à l'installation.

4.110. L'exploitant devrait s'assurer que la protection est suffisante sur le plan de la sécurité informatique pour que l'installation soit exploitée conformément aux prescriptions réglementaires ou aux exigences de sécurité qu'il a définies pour l'installation.

4.111. Lorsque la validation montre que la protection n'est pas suffisante, l'exploitant devrait réviser le PSI et l'ASID pour améliorer la protection. Il ne peut affaiblir la protection sans l'accord de l'autorité compétente.

4.112. L'exploitant devrait valider les résultats de la GRSI pour l'installation et pour ses systèmes. Il faudrait s'assurer que les résultats de la GRSI pour l'installation tiennent dûment compte des exigences définies par l'exploitant

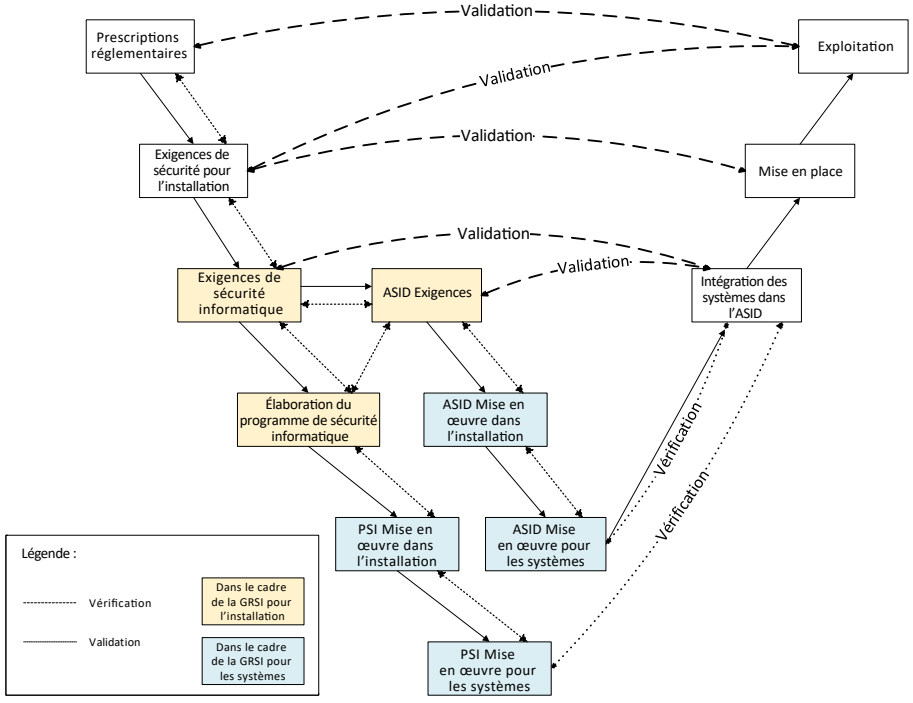

FIG. 7. Présentation schématique des activités de vérification et de validation qui sont menées dans le cadre de la gestion des risques liés à la sécurité informatique (GRSI). PSI : programme de sécurité informatique ; ASID : architecture de sécurité informatique défensive.

et des prescriptions réglementaires. Les résultats de la GRSI pour un système devraient être conformes aux exigences du PSI et de l'ASID.

4.113. L'exploitant devrait regrouper les niveaux de risque pour l'installation, en se référant notamment aux prescriptions réglementaires et aux exigences de conception applicables. Ces niveaux devraient comprendre les niveaux de risque pour chaque système qui contient une RNS.

4.114. L'exploitant devrait s'assurer que l'évaluation du risque pour l'installation et ses systèmes tient dûment compte de la menace de référence ou de l'énoncé de la menace nationaux, à l'aide de scénarios dans lesquels les attaques concernent plusieurs systèmes et l'architecture globale. Ces scénarios diffèrent de ceux qui sont utilisés dans le cadre de la GRSI pour un système [par. 5.5 j)] et de ceux qui sont décrits dans la menace de référence ou dans l'énoncé de la menace nationaux. Dans ces scénarios, des attaques combinées qui compromettent plusieurs systèmes peuvent être lancées afin de détecter les vulnérabilités dans l'installation.

4.115. Pour vérifier complètement les résultats de la GRSI pour l'installation et pour ses systèmes, il faudrait prendre en considération les scénarios techniques et les scénarios fonctionnels, qui sont décrits ci-après.

Définition et élaboration des scénarios

4.116. L'exploitant devrait définir et élaborer des scénarios qui s'appuient sur l'évaluation nationale des menaces contenue dans la menace de référence ou l'énoncé de la menace nationaux et, le cas échéant, dans l'évaluation de la menace propre à l'installation. Pour l'élaboration de ces scénarios, les exploitants sont vivement encouragés à faire appel à des spécialistes des cyberattaques et des moyens dont dispose la menace dans ce domaine. Les autorités compétentes, les services de renseignement et les forces de l'ordre disposent des compétences correspondantes. L'exploitant peut être tenu de soumettre ces scénarios détaillés à l'examen et à l'approbation de l'autorité compétente.

4.117. L'analyse de ces scénarios peut donner des informations sur les points qui sont les plus vulnérables dans l'installation, les processus, l'architecture des systèmes et les procédures. Une analyse plus approfondie peut être nécessaire pour recenser les mesures de sécurité informatique qui sont en vigueur ou celles qui doivent être prises pour remédier aux vulnérabilités qui ont été détectées.

4.118. Les scénarios devraient servir à vérifier les résultats de l'évaluation des risques liés à la sécurité informatique pour l'installation, y compris l'analyse des

tactiques que pourrait employer un adversaire, de la probabilité d'une attaque et de ses conséquences éventuelles.

4.119. Il faudrait régulièrement réévaluer les scénarios pour qu'ils restent adaptés aux objectifs de sécurité**,** compte tenu de l'évolution des menaces.

4.120. Il existe deux catégories de scénarios :

a) Les scénarios fonctionnels, qui s'appuient sur l'évaluation de la menace et qui mettent en évidence les effets que la compromission de systèmes exécutant des fonctions de l'installation peut avoir sur ces fonctions. Ils comprennent les scénarios dans lesquels un sabotage qui a des conséquences radiologiques inacceptables et donne lieu à un enlèvement non autorisé de matières nucléaires est commis. Il est également possible de se servir de scénarios fonctionnels pour détecter les dépendances critiques qui existent entre fonctions ou entre systèmes.
b) Les scénarios techniques, qui s'appuient sur la mise en œuvre technique de mesures de sécurité informatique et dans lesquels figurent des informations détaillées sur l'exploitation effective ou possible des ressources numériques. On peut évaluer ces scénarios par des exercices relatifs au fonctionnement ou par des exercices sur table, généralement dans le cadre de la vérification et de la validation des résultats de la GRSI pour l'installation et pour ses systèmes.

4.121. Les scénarios sont élaborés et analysés entre la GRSI pour l'installation et les GRSI pour ses systèmes, et dans le cadre d'une partie de la GRSI pour l'installation si cela est nécessaire pour l'analyse. Ils sont nécessaires pour accroître la confiance dans les résultats de la phase de définition des exigences, mais peuvent aussi être utilisés pour définir ces exigences. La série de scénarios qui sert dans le cadre de l'analyse pour définir les exigences ne peut être identique à celle qui est utilisée pour les activités d'assurance.

4.122. Pour les scénarios envisagés, il faudrait prendre en compte des attaques lancées par plusieurs chemins simultanément (via différents réseaux et systèmes locaux, par exemple), des attaques auxquelles participent des initiés et des attaques combinées. Il faudrait également prendre en compte le risque de cyberattaques successives, qui décuplent les conséquences, mais ne montrent aucun signe de collusion entre les différents adversaires (attaques indépendantes).

4.123. Les scénarios peuvent par exemple prendre en compte les éléments suivants :

a) attaques isolées menées par un seul adversaire ;
b) attaques coordonnées menées par un groupe d'adversaires qui agissent ensemble ;
c) attaques opportunistes, dans lesquelles des adversaires indépendants réussissent à lancer une attaque combinée. Une vulnérabilité est par exemple dévoilée publiquement par un adversaire, ce qui permet à d'autres adversaires de prendre pour cible les systèmes et le matériel de l'installation ;
d) moyens particuliers de la menace [9] ;
e) attaques combinées, pour lesquelles des aspects informatiques et physiques sont utilisés de manière coordonnée.

L'analyse de l'arbre d'attaque peut permettre de définir des scénarios de menace et des stratégies de protection.

4.124. Il faudrait réexaminer et actualiser régulièrement les scénarios lorsque :

a) la menace de référence ou l'énoncé de la menace nationaux ont été mis à jour ;
b) une modification importante est apportée à l'installation ;
c) des modifications sont apportées aux processus de sécurité, aux contre-mesures critiques et aux architectures ;
d) de nouveaux chemins qui pourraient être utilisés pour une attaque sont découverts ;
e) de nouvelles prescriptions réglementaires ont été adoptées ;
f) de nouvelles vulnérabilités critiques[34] sont découvertes, en particulier lorsqu'elles concernent des mesures de sécurité informatique importantes ;
g) la caractérisation de la menace a évolué.

4.125. Pour les scénarios les plus représentatifs, il faudrait recenser des caractéristiques et des vecteurs d'attaque précis, et rassembler des informations sur les risques correspondants.

[34] Sont par exemple considérées comme « critiques » (note de 9.0 à 10) par le Système de notation des vulnérabilités communes (version 3.0) les vulnérabilités qui peuvent être exploitées dans le cadre du réseau, qui ouvrent la voie à des attaques faciles et qui peuvent entraîner une compromission totale de la confidentialité, de l'intégrité et de l'accessibilité.

RÉSULTATS DE LA GESTION DES RISQUES LIÉS À LA SÉCURITÉ INFORMATIQUE POUR L'INSTALLATION

4.126. Le PSI de l'installation devrait décrire les mesures de sécurité informatique qui sont nécessaires pour se protéger contre les adversaires qui ont fait l'objet d'une analyse durant l'évaluation.

4.127. Les résultats de la GRSI pour l'installation devraient comprendre le PSI et l'ensemble des risques pour l'installation, définis à l'aide d'une évaluation de l'efficacité des mesures mentionnées dans le PSI et assurant une protection contre les adversaires qui ont été décrits dans la menace de référence ou dans l'énoncé de la menace nationaux**.**

4.128. Le rapport de la GRSI pour l'installation devrait contenir un examen et une analyse de haut niveau concernant la conception du système de sécurité et la gestion de la configuration, tels qu'ils figurent dans le PSI. Il faudrait procéder à une analyse plus approfondie dans le cadre de la GRSI pour les systèmes.

4.129. Les fonctions de l'installation et les systèmes correspondants qui figurent dans les documents issus de la GRSI pour l'installation devraient être examinés dans le cadre d'une évaluation complète du risque au niveau des systèmes, telle qu'elle est présentée dans la section 5**.**

4.130. L'exploitant devrait communiquer à l'autorité compétente l'évaluation des risques associés aux différentes fonctions et l'évaluation de l'ensemble des risques qui pèsent sur l'installation .

5. GESTION DES RISQUES LIÉS À LA SÉCURITÉ INFORMATIQUE POUR UN SYSTÈME

CONSIDÉRATIONS GÉNÉRALES

5.1. L'exploitant devrait prévoir un examen périodique et systématique afin de gérer les risques liés à la sécurité informatique pour les ressources numériques (notamment les RNS) des systèmes qui exécutent les fonctions recensées dans

le cadre de la GRSI pour l'installation[35]. La compromission de RNS peut généralement avoir des conséquences de gravités diverses (qui sont décrites dans la référence [7]). Dans le cadre de la GRSI pour l'installation, il faudrait prévoir une GRSI pour chaque système, selon les modalités décrites dans la présente section. Au titre de la GRSI pour un système, il faudrait examiner toutes les ressources numériques du système concerné, notamment les RNS.

5.2. La GRSI pour un système devrait être assurée par une équipe pluridisciplinaire, semblable à celle qui a effectué la GRSI pour l'installation. La composition de l'équipe qui assure la GRSI pour un système peut cependant être adaptée afin de pouvoir aborder des questions propres au système concerné.

5.3. L'exploitant devrait adopter une approche graduée lorsqu'il évalue l'ampleur des activités de gestion du risque pour chaque système. Il faudrait consacrer le plus d'efforts aux systèmes qui exécutent ou appuient les fonctions d'une installation auxquels les niveaux de sécurité informatique les plus contraignants ont été attribués (c'est-à-dire à ceux qui exigent la protection la plus forte), tels qu'ils ont été définis dans le cadre de la GRSI pour l'installation.

VUE D'ENSEMBLE

5.4. L'objectif principal de la GRSI pour un système est d'évaluer et de gérer les mesures de sécurité informatique afin qu'elles protègent convenablement le système concerné (c'est-à-dire selon son niveau de sécurité informatique), conformément aux exigences qui sont définies dans les documents issus de la GRSI pour l'installation.

5.5. Pour atteindre cet objectif, la GRSI pour un système comprend les étapes suivantes :

a) Évaluation de chaque fonction de l'installation, des systèmes qui exécutent la fonction concernée et du niveau de sécurité informatique qui est appliqué à ces systèmes – compte tenu des autres fonctions ayant des relations et des interdépendances qui ont été recensées lorsque l'installation a été caractérisée dans le cadre de la GRSI pour l'installation – afin de déterminer les limites fonctionnelles des systèmes.

---

[35] Il peut être nécessaire d'élargir cette analyse pour prendre en compte d'autres systèmes qui ont été exclus du cadre de l'évaluation des risques liés à la sécurité informatique pour l'installation et qui n'ont pas de lien direct avec les objectifs de la sécurité nucléaire.

b) Définition du rôle de chaque système, notamment pour les systèmes appuyant d'autres fonctions de l'installation qui sont en relation avec la fonction exécutée par le système ou qui en dépendent. Dans ce cadre, il peut être nécessaire d'analyser l'architecture globale des systèmes pour déterminer l'emplacement, les limites, les interfaces et les voies de transmission des systèmes qui contiennent des ressources numériques, notamment des RNS.
c) Recensement (et création d'un inventaire) des ressources numériques de ces systèmes.
d) Définition et création de zones de sécurité informatique en fonction des exigences qui figurent dans le PSI de l'installation et dans l'ASID.
e) Recensement des RNS et des autres ressources numériques qui se trouvent dans chaque zone grâce à une analyse des ressources, qui consiste à examiner les ressources numériques pour déterminer si elles sont indispensables pour exécuter une fonction.
f) Attribution aux ressources numériques, notamment aux RNS, du niveau de sécurité informatique qui a été attribué à leur fonction de sécurité ou de sûreté dans le cadre de la GRSI pour l'installation.
g) Application à toute une zone du niveau de sécurité informatique le plus strict qui a été attribué aux fonctions exécutées par des ressources numériques dans la zone concernée, et attribution de ce niveau à toutes les ressources numériques de la zone.
h) Application aux RNS et aux autres ressources numériques (y compris aux limites de zone) de mesures de sécurité informatique minimales (voir par. 4.58 et 4.68) et de mesures de sécurité informatique supplémentaires, les spécificités de chaque système recensé étant prises en compte afin de satisfaire aux exigences fixées pour les niveaux de sécurité informatique qui ont été attribués.
i) Mise en place d'une procédure pour déterminer quelles mesures de contrôle technique, de contrôle administratif ou de contrôle physique peuvent être appliquées pour respecter les mesures de sécurité informatique minimales.
j) Analyse de modes d'attaque, de vulnérabilités et de scénarios particuliers, afin de contrôler l'efficacité des mesures de sécurité informatique qui ont été mises en place.
k) Application de mesures supplémentaires ou compensatoires pour ramener le risque à un niveau satisfaisant si l'analyse révèle que le système n'est pas suffisamment protégé par les mesures de sécurité informatique prévues.
l) Élaboration d'un rapport concernant la GRSI pour le système concerné.

5.6. Ces étapes peuvent permettre de recenser d'autres ressources numériques qui ne faisaient pas partie des systèmes qui ont été associés aux fonctions dans le cadre de la GRSI pour l'installation, ou qui ont été considérées comme hors limite

d'un système ou d'une zone lorsque la GRSI pour un système a été effectuée. En pareil cas, une nouvelle analyse devrait être menée pour s'assurer que toutes ces ressources numériques figurent dans l'évaluation et dans le PSI.

5.7. Les résultats de la GRSI pour un système devraient comprendre une hiérarchisation des risques associés au système, afin de déterminer comment mettre en œuvre adéquatement les mesures de sécurité informatique. Dans ce cadre, il faudrait prendre en compte l'emplacement des composants du système, les vulnérabilités et les zones et niveaux de sécurité informatique s'ils sont définis, ainsi que l'importance des RNS et des autres ressources numériques du système qui est évalué.

PROCESSUS DE GESTION DES RISQUES LIÉS À LA SÉCURITÉ INFORMATIQUE POUR UN SYSTÈME

5.8. L'exploitant devrait effectuer une GRSI pour un système lorsque :

a) l'installation est construite (GRSI pour tous les systèmes) ;
b) l'installation a subi des modifications (GRSI pour tous les systèmes) ;
c) une ressource numérique ou un système nouveaux sont mis en place (GRSI pour tous les systèmes pour lesquels cette mise en place a une incidence) ;
d) un système ou une ressource numérique ont été modifiés (GRSI pour tous les systèmes pour lesquels cette modification a une incidence) ;
e) la GRSI pour l'installation a été révisée (GRSI pour tous les systèmes).

5.9. Il faudrait rassembler et mettre à disposition les éléments d'entrée suivants afin de pouvoir mener la GRSI pour un système :

a) résultats de la GRSI pour l'installation (PSI et ASID, par exemple) ;
b) rapport de sûreté ;
c) plan de sécurité du site ;
d) politique de sécurité informatique.

Exigences générales applicables à l'architecture de sécurité informatique défensive pour la sécurité informatique

5.10. S'agissant de l'ASID, l'exploitant devrait se servir des exigences fixées dans le cadre de la GRSI pour l'installation afin de concevoir, de mettre en place et de maintenir des mesures de sécurité informatique pour les systèmes et les ressources

numériques en vue de prévenir, de détecter et de retarder les cyberattaques, d'en atténuer les effets et d'en effacer les conséquences.

5.11. Les mesures de sécurité informatique devraient être en vigueur pendant toute la durée de vie de l'installation, y compris pendant les périodes de maintenance et le déclassement par exemple, lorsque d'importantes modifications peuvent être apportées à la configuration. Les activités de surveillance, de maintenance ou de remise en état ne devraient pas permettre à un adversaire de contourner des mesures de sécurité informatique, par exemple en contournant la protection des voies de communication qui sont établies entre des fonctions qui ont des niveaux de sécurité informatique différents.

5.12. Il faudrait mettre en place des limites de sécurité informatique[36] entre les zones de sécurité informatique et il faudrait les protéger à l'aide de mesures de sécurité informatique différentes.

5.13. Il faudrait contrôler les flux de données entre les zones dont les niveaux de sécurité informatique sont différents et entre celles qui ont le même niveau de sécurité à l'aide d'une approche fondée sur les risques, afin que l'ASID reste pertinente.

Définition des limites d'un système

5.14. Les limites d'un système permettent de définir le cadre de la GRSI pour le système en question et concernent les systèmes qui, d'après la caractérisation de l'installation, exécutent une fonction particulière. À cette fin, il faudrait examiner les interdépendances qui existent entre les fonctions de l'installation et les systèmes qui les exécutent.

5.15. Dans le cadre de la GRSI pour un système, il faudrait déterminer et décrire les limites du système concerné. Celles-ci englobent l'ensemble des composants, des sous-composants, des interfaces et des environnements du système en question qui existent au cours de la vie de l'installation, ainsi que les autres systèmes qui apportent un appui ou exécutent des fonctions auxiliaires.

[36] Dans la présente publication, les « limites de sécurité informatique » désignent les limites logiques et physiques d'un système ou d'un ensemble de systèmes qui ont le même niveau de sécurité et qui peuvent donc être protégés par les mêmes mesures de sécurité (c'est-à-dire une zone de sécurité informatique).

5.16. Les étapes suivantes peuvent servir à définir les limites du système qui fait l'objet d'une évaluation :

a) Recenser toutes les interfaces du système.
b) Répertorier tous les endroits où les données entrent et sortent du système (endroits où un adversaire pourrait essayer d'introduire un programme malveillant). Dans le cadre de l'évaluation des risques liés à la sécurité du système, il faudrait examiner tous les moyens qui permettent d'introduire un programme malveillant dans le système. Un tel programme peut par exemple être introduit via des liens de communication, par des produits ou des services fournis, ou via des appareils portables qui sont temporairement connectés au matériel cible.
c) Répertorier les procédures pour lesquelles il existe des relations avec le système, que ce soit en fonctionnement normal ou dans des circonstances particulières (application de correctifs, par exemple).
d) Recenser les voies de transmission de données (s'il en existe) qui ne sont utilisées dans le cadre d'aucune procédure durant l'exploitation et la maintenance du système. Les voies de transmission de donnée qui ne sont pas utilisées constituent une vulnérabilité importante.
e) Déterminer quel niveau de sécurité informatique a été attribué au système (à partir des résultats de la GRSI pour l'installation).
f) Recenser les mesures de sécurité informatique qui sont appliquées au système ou à son environnement.

Définition et contenu des zones de sécurité informatique

5.17. Le PSI et l'ASID qui ont été élaborés lorsque la GRSI pour l'installation a été effectuée imposent des exigences de sécurité informatique pour l'application du modèle de zone. Le PSI comprend aussi une liste des fonctions de l'installation et des systèmes qui les exécuteront.

5.18. L'exploitant devrait mettre en œuvre des mesures de sécurité informatique pour que les exigences qui ont été fixées dans le cadre de la définition de l'ASID soient respectées. Ce faisant, il faudrait également envisager d'atteindre les objectifs suivants [8] :

a) Les systèmes situés dans la même zone forment un ensemble fiable pour la communication interne entre systèmes, et le niveau de sécurité informatique qui est appliqué dans une zone où se trouve un tel ensemble est le niveau le plus strict de tous ceux qui ont été attribués aux systèmes.

b) Les exigences de sûreté applicables à l'architecture (redondance, diversité, séparation physique et électrique, et critère de défaillance unique, par exemple) restent en vigueur.

c) Le principe de la défense en profondeur est mis en œuvre dans chaque zone de sécurité informatique (à l'aide de mesures de contrôle administratif, de contrôle physique et de contrôle technique qui sont variées et indépendantes, et qui se chevauchent) et entre ces différentes zones.

d) Les mesures de contrôle technique qui visent à exécuter des actions préventives ou protectrices continues ou automatiques (c'est-à-dire des actions qui ne nécessitent pas d'intervention humaine) complètent les mesures de contrôle physique ou administratif (qui requièrent une intervention humaine), le cas échéant.

e) Toutes les connexions entre les zones sont dotées de mécanismes de découplage qui sont soumis à des règles propres aux zones concernées, afin de prévenir les accès non autorisés et les échanges inopportuns entre les zones. Ces connexions comprennent les connexions au réseau en continu et les connexions intermittentes, au moyen de supports amovibles, par exemple.

f) L'importance du découplage entre zones dépend du niveau de sécurité informatique des deux zones concernées. Les mesures de découplage comprennent des mesures de contrôle technique (filtrage de paquets, pare-feu ou *data diodes*, par exemple) aux limites des zones afin de restreindre le flux de données et les communications entre les différentes zones.

g) Les communications autorisées entre des zones ayant des niveaux de sécurité différents s'effectuent conformément aux exigences qui figurent dans le PSI pour les niveaux concernés. Pour l'élaboration d'exigences relatives aux communications autorisées, des modèles de confiance peuvent être pris en compte (voir par. 4.83).

h) Si les exigences qui figurent dans le PSI permettent à des RNS situées dans des zones qui ont des niveaux de sécurité différents de communiquer, seule la RNS à laquelle a été attribué le niveau de sécurité informatique le plus élevé (le plus strict) peut établir une connexion de ce type. Les RNS qui exécutent des fonctions relatives à la gestion d'informations sensibles n'autorisent généralement pas les communications des niveaux les plus stricts vers les niveaux les moins contraignants (c'est-à-dire les flux d'informations en sens inverse), conformément au modèle de confiance Bell-LaPadula (voir par. 4.83).

i) Si des communications établies par la RNS à laquelle le niveau de sécurité informatique le moins contraignant est appliqué[37] ne peuvent être évitées et ne sont pas conformes au modèle de confiance retenu, des mécanismes de découplage particulièrement stricts sont utilisés.

j) L'accès logique ou physique d'appareils mobiles autorisés ou d'autres types de matériel temporaire à des ressources numériques d'une zone est considéré comme une forme de connexion temporaire à cette zone. Il est soumis à des mesures de sécurité informatique pour la zone concernée et pour les appareils temporairement connectés. Ces appareils sont soumis à des mesures de sécurité informatique supplémentaires s'ils se connectent à plusieurs zones.

k) Les zones peuvent être divisées en sous-zones pour améliorer la configuration et prévenir les échanges inopportuns avec d'autres systèmes.

5.19. Il faudrait envisager de répartir les ressources numériques dans des zones distinctes lorsque l'une des conditions suivantes est remplie :

a) Les ressources numériques font partie de systèmes qui exécutent des fonctions différentes.

b) Les systèmes qui contribuent à l'exécution de la même fonction se voient attribuer des niveaux de sécurité informatique différents.

c) Les systèmes qui contribuent à l'exécution de la même fonction et auxquels a été attribué le même niveau de sécurité informatique sont gérés par des unités différentes au sein de l'organisation.

d) Les serveurs communiquent avec plusieurs clients (ils communiquent avec des systèmes numériques de contrôle-commande ou avec des automates programmables, par exemple). La zone pour laquelle la protection doit être la plus stricte devrait contenir le moins de ressources distinctes possible.

e) Les systèmes doivent communiquer avec des composants d'infrastructure qui sont utilisés par plusieurs systèmes (services d'annuaire, serveurs de temps ou dispositifs où sont enregistrés les journaux de sécurité, par exemple), mais ne communiquent pas entre eux. Les communications entre les zones qui contiennent de tels systèmes et celles qui contiennent ces composants d'infrastructure doivent être surveillées et contrôlées.

[37] Pour les installations à haut risque ou à très haut risque, certains États Membres n'autorisent pas que des communications soient établies des niveaux les moins contraignants vers les niveaux les plus stricts. Pour d'autres types d'installations (installations du cycle du combustible nucléaire ou petits réacteurs modulaires, par exemple), l'autorité compétente peut laisser la question de l'utilisation de chemins bidirectionnels à la discrétion de l'exploitant.

f) Les systèmes sont des systèmes d'administration (surtout lorsque les mêmes systèmes sont utilisés pour gérer plusieurs systèmes fonctionnels).
g) La réglementation exige une séparation des zones.

5.20. Même si leur niveau de sécurité informatique est identique, on peut envisager de placer les ressources numériques dans des zones différentes dans les cas suivants :

a) Les ressources numériques font partie de systèmes qui exécutent des fonctions différentes. En pareil cas, le fait de placer les ressources numériques dans des zones différentes peut améliorer la séparation des zones et des systèmes qui contribuent à l'exécution d'une fonction de l'installation.
b) Les ressources numériques ne sont pas toutes placées sous la responsabilité du même service.
c) Certaines ressources numériques sont isolées, ou bien plusieurs ressources numériques qui font partie du même système fonctionnel se trouvent sur un réseau isolé.
d) Des systèmes redondants et distincts qui exécutent la même fonction d'une installation doivent être placés dans des zones différentes.
e) La réglementation exige une séparation des ressources numériques.

5.21. Entre systèmes de zones différentes, seuls les connexions réseau et les échanges locaux de données (via des supports amovibles ou des appareils mobiles, par exemple) qui sont essentiels devraient être effectués. Lorsqu'une connexion réseau entre zones est indispensable, elle devrait être établie depuis la zone où le niveau de sécurité informatique est le plus strict vers celle dont le niveau de sécurité est le moins contraignant. Des restrictions peuvent être appliquées à l'aide de mesures de contrôle technique (filtrage, par exemple) ou de contrôle administratif (règles concernant l'usage de supports amovibles pour un système particulier, par exemple). Il faudrait consigner la liste des connexions réseau et les méthodes qui sont autorisées pour les échanges de données sans connexion.

5.22. Chaque zone ne peut comprendre que des systèmes (et des ressources numériques) ayant le même niveau de sécurité informatique. Une zone se voit attribuer le niveau de sécurité informatique des systèmes qu'elle comprend. Un niveau de sécurité informatique donné peut et devrait s'appliquer à différentes zones. Dans certains cas, il peut cependant être difficile de répartir dans plusieurs zones des systèmes auxquels des niveaux de sécurité informatique différents ont été attribués. Certains systèmes peuvent alors faire partie d'une zone dont le niveau de sécurité informatique est plus strict que celui qui leur a été attribué.

5.23. Il ne faudrait autoriser les communications qu'entre les zones ayant le même niveau de sécurité informatique ou des niveaux adjacents. Les communications entre les zones qui ont des niveaux de sécurité informatique différents ne devraient passer que par des points d'entrée de zone bien précis (points d'entrées qui filtrent les connexions entre les zones de niveau de sécurité 2 et 3, par exemple). Il faudrait définir des mesures de sécurité pour tous les points d'entrée de manière efficace et cohérente afin que l'architecture globale soit sécurisée. Il faudrait mettre en place des contrôles spécifiques à tous les points d'entrée, par exemple sur le contenu des données qui entrent ou qui sortent (plage autorisée pour les valeurs des paramètres, par exemple) ou sous forme de signature numérique des données. Les points d'entrée devraient également faire l'objet d'une surveillance particulière dans le journal d'événements.

Recensement des ressources numériques

5.24. Lors du recensement des ressources numériques d'un système, il conviendrait de consulter les éléments suivants :

a) base de données sur les ressources des systèmes (où figurent tous les composants numériques) ;
b) liste des logiciels et des microprogrammes ;
c) liste des informations sensibles qui concernent le système [5] ;
d) réseau des systèmes et schémas de l'architecture ;
e) documents de conception de l'installation, comme le rapport de sûreté ou les rapports d'essai ;
f) schémas des flux de données ;
g) liste des comptes utilisateurs, des comptes système et des privilèges qui leur sont associés ;
h) procédures relatives au système concerné.

5.25. La liste des ressources numériques peut comprendre les identifiants de ces ressources, des spécifications techniques et des données essentielles, des descriptions de leurs interfaces, des références aux évaluations du risque pour l'installation et ses systèmes, et le nom des responsables auxquels ces ressources ont été confiées.

5.26. Il faudrait tenir à jour et réexaminer régulièrement la liste des ressources numériques pendant la durée de vie de l'installation. Il faudrait également la réexaminer et la mettre à jour au besoin lorsqu' une évaluation du risque est menée pour un système.

5.27. Les ressources numériques qui sont également des ressources d'informations sensibles devraient être considérées comme des RNS. Dans le cadre de l'analyse des ressources numériques, il faudrait également recenser et prendre en compte les ressources numériques qui peuvent contribuer à produire un effet néfaste sur la fonction d'une RNS, afin de déterminer s'il faudrait les considérer comme des RNS, conformément au PSI .

5.28. La liste des RNS devrait être classée comme information sensible et protégée en conséquence.

Élaboration de l'architecture de sécurité informatique pour un système, y compris l'analyse des ressources numériques

5.29. L'exploitant devrait déterminer quelles tâches et quelles activités sont nécessaires pour que la sécurité informatique soit assurée dans l'installation. Ces tâches et ces activités devraient être associées à un niveau de sécurité informatique et aux mesures de sécurité informatique correspondantes. L'exploitant devrait veiller à ce que les moyens et les capacités nécessaires pour accomplir ces tâches et ces activités soient disponibles.

5.30. Dans le cadre de la GRSI pour un système, il faudrait recenser toutes les RNS. Pour l'analyse de menaces ou de types d'attaques particuliers, il est parfois également nécessaire d'examiner les ressources numériques qui ne sont pas des RNS lorsque leur compromission pourrait porter atteinte à une RNS. Il faudrait estimer l'ampleur du travail que représente l'évaluation du risque pour un système afin que les systèmes auxquels a été attribué le niveau de sécurité informatique le plus strict soient soumis à l'évaluation la plus rigoureuse.

5.31. D'une façon générale, le même niveau de sécurité informatique devrait être attribué aux systèmes qui exécutent la même fonction, qu'il s'agisse de systèmes indépendants, variés ou redondants. Il est fortement déconseillé d'attribuer un niveau de sécurité informatique moins contraignant à de tels systèmes, et cette attribution ne peut être envisagée qu'au cas par cas, à condition d'être justifiée par une raison précise et par une analyse des risques pour la sécurité.

5.32. Dans le cadre de l'analyse d'une RNS, il faudrait prendre en compte les informations qui concernent le matériel, les microprogrammes et les logiciels de la RNS en question. Ces informations peuvent servir d'élément d'entrée pour une analyse de la vulnérabilité. Cette dernière peut conduire à recommander de repérer, de désactiver ou de supprimer des services, des points d'accès ou des interfaces qui ne sont pas nécessaires pour le système (ou le réseau) de la RNS

concernée, afin de réduire la surface d'attaque (c'est-à-dire de renforcer la sécurité du système ; voir par. A.64).

5.33. Il faudrait analyser et classer par catégories les interfaces de chaque système (et de ses ressources numériques) au regard de la limite de zone. Les catégories suivantes peuvent être utilisées :

a) Communications internes considérées comme fiables : Cette catégorie comprend les communications établies entre les systèmes ou en leur sein, à l'intérieur d'une zone ou entre les ressources numériques d'un système, y compris les communications internes avec les appareils qui se trouvent à la limite d'une zone (pare-feu ou *data diodes,* par exemple). Aucune mesure de sécurité informatique ne peut permettre de surveiller ou de protéger efficacement ce type de communications contre une cyberattaque.
b) Communications externes autorisées : Cette catégorie comprend les communications entre zones via des chemins autorisés et des appareils situés à la limite d'une zone. En principe, ce type de communications est établi entre des systèmes distincts qui exécutent des fonctions différentes. Les mesures de sécurité informatique qui prennent la forme d'appareils situés aux limites de zone permettent de garantir que toutes les voies de communication, qu'elles soient numériques ou analogiques, sont sans cesse surveillées et que celles qui sont autorisées sont les seules à pouvoir être utilisées.
c) Communications interdites possibles : Cette catégorie comprend les communications interdites entre zones, par exemple à l'aide de câbles réseau, de connexions sans fil ou de supports amovibles. Ce type de communications interdites peut concerner des systèmes ou des ressources numériques qui se trouvent dans des zones différentes, mais qui sont proches physiquement ou logiquement, par exemple des systèmes qui sont situés dans la même zone, sans qu'il n'y ait de barrière physique pour contrôler les accès correspondants.

5.34. Il faudrait attribuer le même niveau de sécurité informatique, à savoir celui de la zone, à toutes les ressources numériques d'une zone qui utilisent des voies de communication internes considérées comme fiables.

5.35. Il faudrait attribuer aux appareils situés à la limite d'une zone un niveau de sécurité informatique équivalent au niveau le plus élevé (le plus strict) qui est appliqué au matériel qu'ils sont censés protéger. Un pare-feu installé entre deux zones ayant des niveaux de sécurité informatique différents peut par exemple être relié par une voie de communication interne considérée comme fiable à la zone

à laquelle le niveau de sécurité informatique le plus élevé a été attribué, mais seulement par une voie de communication externe autorisée à l'autre zone.

5.36. Une borne de détection des logiciels malveillants ou un antivirus qui servent à contrôler le contenu des supports amovibles et des appareils mobiles avant qu'ils n'entrent dans une zone ou n'en sortent, constituent un autre exemple d'appareil situé à la limite d'une zone. Une telle borne se voit attribuer le plus haut niveau de sécurité informatique qui est appliqué aux objets situés dans la zone qu'elle est censée protéger[38]. En pareil cas, l'exploitant doit veiller à ce que la borne ne permette pas de compromettre plusieurs systèmes situés dans des zones différentes (parce qu'elle est exposée à une vulnérabilité commune qui peut être exploitée pour compromettre plusieurs systèmes, par exemple).

5.37. Toutes les ressources numériques, notamment les RNS, qui sont connectées via une voie de communication interne considérée comme fiable, devraient être conformes aux exigences générales de l'ASID. Il faut mettre en place des mesures de sécurité informatique supplémentaires pour les communications externes autorisées [voir par. 5.33 b)].

5.38. Des RNS peuvent être installées à proximité (logique ou physique) d'autres RNS si des mesures de sécurité informatique ont été mises en place pour que les systèmes correspondants ne puissent pas utiliser de voies de communication interdites. Ces mesures ne peuvent être que des mesures de contrôle administratif. Les RNS se voient généralement attribuer un niveau de sécurité informatique élevé (niveau 1 à 3, par exemple).

5.39. Les ressources numériques qui ne sont pas autorisées à communiquer avec une RNS ne devraient pas pouvoir se trouver à proximité logique ou physique de la RNS concernée lorsque des voies de communication interdites existent. L'ASID devrait permettre d'élaborer et de maintenir des mesures de sécurité informatique vigoureuses afin d'éliminer de telles voies, ou prévoir des mesures compensatoires pour qu'elles puissent plus difficilement être utilisées.

5.40. Les ressources numériques auxquelles aucun niveau de sécurité informatique n'a été attribué ne devraient jamais se trouver à proximité d'une RNS. Le matériel et les appareils mobiles personnels d'un vendeur qui n'ont pas fait l'objet d'une

[38] Ce type de borne ne convient pas toujours pour la protection des systèmes de niveau 1 ou 2, car il est parfois difficile d'appliquer des exigences de sécurité informatique à une borne isolée. En outre, une borne qui détecte des logiciels malveillants uniquement à l'aide de listes noires ou de signatures ne peut pas assurer une forte protection.

évaluation et auxquels aucun niveau de sécurité informatique n'a été attribué devraient par exemple être considérés comme des appareils potentiellement malveillants pour les RNS et ne devraient pas se trouver à proximité logique ou physique de ce type de ressources.

5.41. Dans le cadre de l'analyse des ressources, il faudrait évaluer les effets des scénarios de cyberattaque crédibles sur le système concerné, ainsi que le risque pour l'installation. Il faudrait aussi tenir compte de la possibilité qu'une cyberattaque puisse se produire à n'importe quelle étape de la vie de l'installation ou de ses systèmes.

5.42. Les cyberattaques peuvent porter atteinte à un seul système ou à plusieurs systèmes, et peuvent être lancées parallèlement à d'autres formes d'actes malveillants qui occasionnent des dommages matériels. Il faudrait donc faire figurer la liste des relations possibles qui sont propres à un composant particulier dans le rapport d'évaluation, et évaluer ces relations.

5.43. Dans le cadre de l'évaluation, il faudrait examiner les actes malveillants qui permettraient de modifier les signaux de processus, les données de configuration du matériel ou les logiciels.

5.44. Lorsque l'on analyse les ressources, il faudrait déterminer où sont stockées les informations et par quels chemins elles circulent dans le système concerné (et dans ses ressources numériques). Il faudrait aussi recenser et justifier les mesures qui ont été mises en place pour protéger les flux de données et les communications indispensables et pour détecter les vulnérabilités qui pourraient subsister. L'analyse peut être étayée par :

a) l'analyse ou le test de l'efficacité des mesures de sécurité ;
b) la détermination de l'état actuel des mesures, y compris les points qui pourraient être améliorés ;
c) le fait de soumettre des logiciels à une évaluation de la vulnérabilité pour les systèmes concernés.

5.45. On peut prendre pour exemple le transfert d'un logiciel (code source ou code exécutable, par exemple) d'un environnement de développement vers un système de sécurité. En l'absence de mesures de sécurité informatique, le compilateur (matériel et logiciel) est affecté à la même zone que le système de sécurité lui-même (et se voit attribuer le même niveau de sécurité informatique), puisqu'il n'y a pas de limites. En revanche, si des mesures de sécurité sont appliquées à la limite située entre le compilateur et le système – par exemple, un test de l'intégrité des

données et une détection des vulnérabilités dans le code issu du compilateur –, le compilateur peut être placé dans une zone distincte et se voir attribuer un niveau de sécurité différent de celui du système lui-même. Les mesures qui sont appliquées au code produit par le compilateur contribuent à protéger le système. On leur attribue donc le même niveau de sécurité qu'au système qu'elles protègent.

5.46. Dans le cadre de l'analyse des ressources numériques, il faudrait établir une liste et une description des mesures de sécurité informatique particulières qui sont mises en œuvre pour chaque système. Ces mesures devraient être une combinaison de mesures de contrôle technique, de contrôle administratif et de contrôle physique.

5.47. L'analyse des ressources numériques devrait donner une idée qualitative ou quantitative du seuil de risque acceptable.

Vérification de l'évaluation des risques liés à la sécurité informatique pour un système

5.48. L'exploitant devrait vérifier et valider l'évaluation des risques liés à la sécurité informatique pour chaque système, conformément au cadre de l'évaluation. S'agissant de la vérification des résultats de la GRSI pour un système, on peut utiliser les méthodes d'évaluation qui sont décrites dans le paragraphe 4.98 concernant la GRSI pour l'installation.

Définition et élaboration des scénarios pour un système

5.49. La menace de référence ou l'énoncé de la menace nationaux servent de base à l'élaboration de scénarios crédibles qui tiennent compte des motivations, des capacités et des intentions des adversaires potentiels, ainsi que des occasions dont ils peuvent profiter (notamment pour les adversaires qui utilisent des techniques informatiques).

5.50. L'exploitant devrait élaborer des scénarios crédibles pour chaque système en s'appuyant sur la caractérisation de la menace afin de valider les mesures de sécurité informatique qui protègent le système. Ces scénarios devraient comprendre une série d'actions que pourrait entreprendre l'adversaire et qui pourrait entraîner la compromission de RNS.

5.51. Les scénarios devraient prendre en compte des techniques et des modes d'attaque courants. Ces derniers peuvent notamment être les suivants :

a) ingénierie sociale, y compris les attaques par hameçonnage ;
b) courriels malveillants ;
c) sites web malveillants ;
d) infection de supports amovibles par des logiciels malveillants ;
e) compromission de matériel d'inspection et de maintenance ;
f) accès à distance ;
g) recours à des initiés (volontaires ou involontaires) ;
h) compromission de la chaîne d'approvisionnement.

5.52. Les scénarios devraient être compatibles avec la menace de référence ou l'énoncé de la menace nationaux qui concernent l'installation afin de déterminer quelles RNS sont exposées aux attaques envisagées. Il peut être utile de commencer l'élaboration des scénarios par les cas les plus probables ou par ceux qui ont les conséquences les plus graves.

5.53. Les scénarios devraient être élaborés avec les objectifs suivants (par ordre d'importance) :

a) déterminer les scénarios où entrent en jeu des RNS et qui ont les conséquences les plus graves ;
b) déterminer les scénarios les plus probables où entrent en jeu des ressources numériques, notamment des RNS.

5.54. Dans le cadre des méthodes d'évaluation (par. 4.98), il faudrait utiliser des scénarios crédibles (par. 4.116 à 4.125) afin de contrôler l'efficacité des mesures de sécurité informatique qui ont été mises en œuvre.

5.55. L'exploitant devrait vérifier que les ressources numériques, notamment les RNS, sont convenablement protégées contre les adversaires recensés dans la menace de référence ou l'énoncé de la menace nationaux qui concernent l'installation.

Rapport sur la gestion des risques liés à la sécurité informatique pour un système

5.56. Les résultats de la GRSI pour un système devraient être consignés dans un rapport qui comprend :

a) un recensement de toutes les RNS, y compris de tous les composants matériels et logiciels de chaque RNS, dans la mesure du possible ;
b) un recensement des ressources numériques qui se trouvent sur une voie de communication connectée à une RNS, qui peuvent être reliées à une telle voie, qui sont utilisées par elle ou qui peuvent y accéder ; ces ressources peuvent comprendre des composants de systèmes auxquels un niveau de sécurité informatique a été attribué ;
c) un recensement des vulnérabilités, des faiblesses ou des défauts des systèmes ou des composants qui sont connus, par exemple des problèmes d'approvisionnement éventuels (fourniture de pièces contrefaites ou non conformes, par exemple), et des actions ou des omissions qui peuvent compromettre la sécurité ;
d) un recensement des mesures de contrôle technique, de contrôle administratif et de contrôle physique ;
e) des recommandations pour la mise en œuvre de contre-mesures ;
f) des recommandations pour l'amélioration des contre-mesures (c'est-à-dire des propositions de mesures de contrôle technique, de contrôle administratif et de contrôle physique supplémentaires) ;
g) un recensement des lacunes qui touchent la documentation ou les archives de l'installation ;
h) une classification des informations sensibles ;
i) les listes de contrôle des accès pour le personnel et les services ;
j) des mesures correctives à appliquer lorsque la situation se dégrade ;
k) une évaluation du risque résiduel pour le système concerné ;
l) un recensement et une description des autres indicateurs qui facilitent l'évaluation de la sécurité informatique (moyenne des temps de bon fonctionnement, temps moyen de réparation, temps moyen de détection, temps moyen de remise en état ou indicateurs de qualité de la sécurité, par exemple).

5.57. Le rapport de la GRSI pour un système devrait être classé comme information sensible et protégé en conséquence.

6. CONSIDÉRATIONS RELATIVES À LA GESTION DES RISQUES LIÉS À LA SÉCURITÉ INFORMATIQUE POUR UNE INSTALLATION OU UN SYSTÈME AUX DIFFÉRENTES ÉTAPES DE LA VIE DE L'INSTALLATION CONCERNÉE

6.1. La présente section donne des orientations concernant les différentes étapes de la vie d'une installation.

PLANIFICATION

6.2. L'exploitant devrait examiner les plans qu'il a établis pour l'installation au regard des règlements édictés par l'autorité compétente, et déterminer quelles questions doivent être traitées pour que les prescriptions réglementaires soient respectées.

6.3. L'exploitant devrait s'assurer qu'il dispose d'une méthode formalisée lui permettant d'effectuer une GRSI détaillée pour son installation.

6.4. L'exploitant devrait mener la GRSI pour l'installation selon les modalités qui figurent dans la section 4.

6.5. L'exploitant devrait vérifier que, si l'ASID peut être mise en place telle qu'elle a été définie, le risque résiduel ne dépassera pas les niveaux acceptables.

6.6. L'exploitant devrait planifier le développement des compétences nécessaires pour la sécurité informatique à toutes les étapes de la vie de l'installation.

6.7. La planification peut comprendre des activités qui sont menées en dehors du site prévu pour l'installation. L'exploitant devrait mettre en place des mesures de sécurité informatique pour les informations qui sont utilisées dans le cadre de ces activités, ainsi que pour les autres données d'entrée et les résultats de la planification qui sont des informations sensibles ou dépendent de ressources d'informations sensibles.

CHOIX DU SITE

6.8. L'exploitant devrait prendre en considération la sécurité informatique lors du choix du site de l'installation, car certaines activités qui contribuent à la sécurité informatique ne peuvent être menées que pour le site concerné, et non à distance ou de manière générale (création de réseaux isolés, accès pour les équipes qui interviennent en cas d'incident informatique et recherche des compétences en sécurité informatique dans la population active locale, par exemple).

6.9. Lorsqu'il détermine l'emplacement des gros appareils sur le site prévu, l'exploitant devrait tenir compte du fait que des mesures de contrôle physique devront être mises en place pour compléter les mesures de sécurité informatique.

6.10. Pour le choix du site, l'exploitant devrait vérifier s'il existe une infrastructure locale à l'appui des mesures de sécurité informatique (réseaux de communications d'urgence, par exemple).

CONCEPTION

6.11. L'exploitant devrait se servir des résultats de la GRSI pour l'installation qui a été menée lors de la planification afin que la conception de l'installation permette que les exigences de sécurité informatique qui sont applicables aux fonctions de l'installation (et sont définies dans l'ASID et dans le PSI) soient respectées lorsque les systèmes seront constitués. Il devrait procéder ainsi pour la conception d'une nouvelle installation et pour la modification d'une conception à des fins de rénovation ou de modification en phase d'exploitation.

6.12. Lors de la conception, il faudrait tenir compte des exigences de sécurité informatique qui s'imposent en raison des dépendances entre fonctions qui ont été répertoriées dans le cadre de la GRSI pour l'installation.

6.13. Les exigences de sécurité informatique devraient être suffisamment détaillées pour que des décisions relatives à la conception puissent être prises, pour que la conception puisse être contrôlée et pour que les modifications apportées à celle-ci puissent être évaluées.

6.14. L'exploitant devrait mener une GRSI pour chaque système, y compris en contrôlant la conception des mesures de sécurité informatique à chaque étape.

6.15. Lors de la conception, il faudrait étudier comment un initié peut accéder physiquement ou à distance aux RNS des zones vitales.

6.16. L'exploitant devrait définir des critères de validation de la sécurité informatique pour la phase de mise en service. Les systèmes qui exécutent des fonctions auxquelles le niveau de sécurité informatique le plus élevé a été attribué devraient être validés de manière indépendante.

6.17. Les personnes qui ont des connaissances en sécurité informatique et qui travaillent dans les différentes branches de l'organisme exploitant devraient participer à la conception afin que :

a) les exigences de sécurité informatique appropriées soient prises en compte ;
b) les modifications qui sont apportées à la conception ne dégradent pas la sécurité informatique, mais l'améliorent ;
c) les modifications, telles qu'elles sont effectuées, soient conformes aux exigences de sécurité informatique qui ont été définies ;
d) la sécurité informatique soit prise en compte lorsque l'efficacité est évaluée.

6.18. Dans le cadre de la conception, il faudrait rédiger les instructions nécessaires à l'application des exigences de sécurité informatique. Il faudrait conserver les informations relatives à la conception, tels les rapports d'analyse, afin qu'elles puissent être consultées ultérieurement par les personnes qui seront autorisées à se servir de la conception.

6.19. Les documents de conception pouvant contenir des informations sensibles en matière de sécurité informatique, ils devraient tous être classés conformément au système de classification des informations et protégés en conséquence.

6.20. L'exploitant devrait veiller à ce que toutes les exigences de sécurité informatique qui doivent être respectées par les vendeurs, les sous-traitants et les fournisseurs figurent dans les contrats correspondants[39] [19]. Les vendeurs, les sous-traitants et les fournisseurs devraient par obligation avoir mis en place des systèmes de gestion de la sécurité informatique et des environnements de développement sécurisés, et appliquer le principe de la sécurité dès la conception aux RNS qu'ils fabriquent ou qu'ils fournissent.

[39] La norme ISO/IEC 15408 [18] (« Critères communs »), qui a été élaborée par l'Organisation internationale de normalisation et par la Commission électrotechnique internationale, fait partie des outils qui peuvent contribuer à déterminer quelles sont les exigences de sécurité.

CONSTRUCTION

6.21. L'exploitant devrait veiller à ce que des mesures de contrôle physique, de contrôle administratif et de contrôle technique soient mises en place pendant la phase de construction, afin de maintenir les mesures de prévention et de protection qui sont prévues par le PSI et par l'ASID. Si des portes qui ferment à clef doivent par exemple être installées aux limites d'une enceinte, les serrures devraient être installées et fixées sous surveillance avant que des RNS ne soient installées dans l'enceinte, ou des mesures compensatoires appropriées devraient être mises en place.

6.22. L'exploitant devrait veiller à ce que les activités de sécurité informatique suivantes soient menées conformément au PSI et à l'ASID en phase de construction :

a) activités d'assurance (c'est-à-dire les essais, les évaluations et les vérifications) ;
b) utilisation de zones de stockage temporaire, soumises à un contrôle des procédures et de la sécurité, pour vérifier que les RNS n'ont pas été manipulées frauduleusement ;
c) gestion du personnel et vérification des produits qui sont livrés par les vendeurs, les sous-traitants et les fournisseurs (qu'ils travaillent sur le site ou à distance), de la fabrication à l'installation ;
d) évaluation et gestion de la chaîne d'approvisionnement ; dans ce cadre, il faudrait s'assurer que la procédure d'achat concernée est intégralement appliquée et n'a pas été modifiée frauduleusement.

MISE EN SERVICE

6.23. L'exploitant devrait intégrer le test des mesures de sécurité informatique dans les essais de réception des systèmes qui sont livrés dans l'installation par le fournisseur.

6.24. L'exploitant devrait mener des activités de configuration et de test lors de l'intégration des systèmes dans l'ASID (voir fig. 7) afin de respecter les

exigences de sécurité informatique. Les activités suivantes devraient par exemple être menées :

a) Les mots de passe et les méthodes d'authentification secondaires devraient être modifiés pour les ressources numériques, conformément aux procédures approuvées.
b) Les comptes des ressources numériques qui ont été utilisés pour le développement et la construction devraient être supprimés, et des mesures de contrôle technique devraient être mises en place.
c) Les outils d'appui aux systèmes (matériel et logiciels) devraient être soumis à des tests et à une évaluation à l'aide de mesures de sécurité informatique appropriées.

6.25. L'exploitant devrait valider les mesures de sécurité informatique par des essais. Les mesures de sécurité informatique et les mesures de protection physique devraient être validées conjointement pour assurer une bonne intégration.

6.26. En cas de conflit entre les mesures de sûreté et les mesures de sécurité, les mesures qui visent à garantir la sûreté devraient être maintenues et l'exploitant devrait chercher une solution pour satisfaire aux exigences de sécurité informatique. Tant qu'une solution de ce type n'a pas été adoptée, des mesures de sécurité informatique compensatoires devraient être mises en œuvre pour ramener le risque à un niveau satisfaisant et devraient être appuyées par une justification argumentée et par une analyse des risques pour la sécurité. Les mesures compensatoires ne devraient pas être constituées uniquement de mesures de contrôle administratif sur une longue période. L'absence de solution en matière de sécurité ne devrait jamais être acceptée.

6.27. L'examen et l'approbation de la partie du PSI qui est applicable et des documents connexes (qui sont nécessaires pour le fonctionnement des systèmes) devraient être achevés avant la phase d'exploitation.

EXPLOITATION

6.28. L'exploitant devrait confier à une personne (qui peut au besoin bénéficier de l'appui d'autres personnes ayant les compétences et les connaissances nécessaires) une responsabilité permanente concernant les modifications de la conception, la gestion, la maintenance et la conduite des opérations pour tout le PSI.

6.29. L'exploitant devrait tenir à jour des documents qui expliquent comment les mesures de sécurité informatique sont mises en œuvre conformément au PSI, à l'ASID et aux prescriptions d'origine externe.

6.30. L'exploitant devrait s'assurer que les exigences relatives à l'exploitation sont compatibles avec le niveau de sécurité informatique des différents systèmes et de leurs ressources numériques. Il peut par exemple être nécessaire de tenir compte des points suivants :

a) Les restrictions d'accès, les contrôles d'accès et les modalités de surveillance ne sont pas toujours les mêmes pour des appareils auxquels des niveaux de sécurité informatique différents ont été attribués.
b) Différents niveaux d'habilitation peuvent être exigés pour les membres du personnel qui travaillent sur différents systèmes, en fonction du niveau de sécurité informatique qui leur a été attribué.
c) Les tâches peuvent être réparties.

6.31. Les actions qui sont exercées sur les systèmes dans le cadre d'une évaluation de la vulnérabilité peuvent provoquer une instabilité de la centrale ou des processus et ne devraient donc être envisagées qu'avec des bancs d'essai ou des systèmes inutilisés, pendant les essais de réception en usine ou les longs arrêts programmés.

Maintenance

6.32. Les paragraphes suivants s'appliquent à la maintenance de courte durée et régulière en phase d'exploitation. La question de la maintenance de longue durée (à des fins de rénovation, de remplacement de systèmes ou de réparation, par exemple) est traitée dans les paragraphes qui sont consacrés à la conception, à la construction et à la cessation de l'exploitation.

6.33. L'exploitant devrait veiller à ce que les activités de maintenance soient compatibles avec le niveau de sécurité informatique du système ou de la ressource numérique qui fait l'objet d'une maintenance. Ainsi, outre les aspects généraux qui sont énumérés au paragraphe 6.30 et concernent la phase d'exploitation, il faudrait tenir compte des points suivants :

a) Il faudrait dresser la liste des activités de maintenance autorisées.
b) Il faudrait répertorier et contrôler les accès qui sont nécessaires pour la maintenance.
c) L'utilisation du matériel de maintenance peut être limitée à une certaine zone de sécurité informatique (ou à une ressource numérique ou à un système

particuliers) ou uniquement aux systèmes auxquels un certain niveau de sécurité informatique a été attribué.

d) Des environnements de maintenance sécurisés peuvent être nécessaires pour certains systèmes ou certaines ressources numériques.

6.34. Les systèmes peuvent être exposés à un risque plus élevé pendant une opération de maintenance, car des mesures de sécurité informatique peuvent alors être supprimées ou désactivées. En outre, des chemins supplémentaires peuvent être accessibles pendant une telle période, parce qu'il peut par exemple être nécessaire d'activer des interfaces pour la télémaintenance, ou d'utiliser des supports amovibles pour configurer ou mettre à jour des logiciels.

6.35. L'exploitant devrait mettre en place des mesures compensatoires adéquates lorsque les mesures de sécurité informatique habituelles sont supprimées ou désactivées. Exemples de points à prendre en considération :

a) Des mesures compensatoires devraient permettre d'assurer la protection physique lorsque l'on ouvre un appareil.

b) Il faudrait déterminer à l'avance si des interfaces distantes sont nécessaires (et justifiées) pour la maintenance, et des mesures de sécurité informatique appropriées devraient être appliquées à ces interfaces, conformément au PSI.

c) Il faudrait contrôler et surveiller l'utilisation des outils informatiques (appareils de mesure, de test et d'étalonnage) afin de s'assurer que ces outils ne sont pas compromis par une cyberattaque et ne peuvent être exploités pour compromettre les systèmes pour lesquels ils sont utilisés. Il faudrait protéger les équipements informatiques qui peuvent être temporairement connectés au système – matériel de test ou de configuration, par exemple – contre les logiciels malveillants et les transferts non autorisés de données. Il faudrait limiter le plus possible l'utilisation de matériel externe à cette fin. Il faudrait inspecter tous les appareils de ce type avant de les introduire dans l'installation.

d) Avant d'installer un logiciel dans un système, il faudrait le contrôler pour s'assurer qu'il n'est pas infecté par un logiciel malveillant. Dans ce cadre, il peut être nécessaire de vérifier que le logiciel n'a pas été modifié frauduleusement et qu'il est authentique, par exemple par un contrôle de sa signature, elle-même issue d'un hachage cryptographique.

e) Des mesures de sûreté (vérification parallèle par une deuxième personne, par exemple) peuvent également être appliquées à des fins de sécurité.

CESSATION DE L'EXPLOITATION

6.36. Lors de la cessation de l'exploitation, des modifications de grande ampleur peuvent être effectuées en parallèle et concerner plusieurs systèmes.

6.37. L'exploitant devrait envisager d'appliquer des mesures compensatoires pour faire face à tout risque résultant d'une modification ou d'une dégradation de systèmes de sécurité qui ont été provoquées par des changements apportés à l'environnement ou à la structure. Dans ce cadre, il peut accorder une grande importance aux mesures de contrôle administratif et s'appuyer davantage sur les vendeurs, les sous-traitants et les fournisseurs pour mettre en œuvre de telles mesures.

6.38. Exemples de changements pour lesquels des mesures compensatoires peuvent être appliquées :

a) Modification ou neutralisation de l'architecture et des mesures de sécurité informatique pour que des modifications puissent être effectuées.
b) Fluctuations des effectifs, y compris le cas où de nouveaux membres du personnel se rendent sur le site pour mener des activités où entrent en jeu des ressources numériques, y compris des RNS. Dans ce type de situation, il peut être nécessaire de mettre en place des contrôles d'habilitation supplémentaires ou d'autres mesures pour pouvoir faire face à la menace interne.
c) Remplacement de composants dans des proportions importantes, qui impose des conditions d'installations sécurisées, un entreposage sécurisé et des mesures supplémentaires pour la manipulation et l'aseptisation sécurisée des RNS qui sont remplacées.

DÉCLASSEMENT

6.39. Lorsque des ressources numériques sont déclassées, il faudrait évaluer et consigner les conséquences de ce déclassement pour la sécurité informatique (y compris la rupture d'intégration avec d'autres ressources numériques qui se trouvent en dehors de l'installation). Si le déclassement d'un système ou d'une ressource numérique rend les mesures de sécurité informatique moins efficaces, l'exploitant devrait mettre en place des mesures compensatoires.

6.40. Lorsque la liste des fonctions de l'installation évolue, un niveau de sécurité informatique différent peut être attribué aux ressources numériques qui contribuent

à l'exécution de ces fonctions, ou il peut ne leur être attribué aucun niveau. Il peut alors être nécessaire de modifier les mesures de sécurité informatique qui sont appliquées à de telles ressources numériques.

6.41. L'exploitant devrait veiller à la destruction sécurisée de toutes les ressources numériques qui contiennent des informations sensibles ne pouvant être déclassées de manière sécurisée lorsque ces ressources sont déclassées.

7. ÉLÉMENTS DU PROGRAMME DE SÉCURITÉ INFORMATIQUE

EXIGENCES DE SÉCURITÉ INFORMATIQUE

7.1. La politique et le programme de sécurité informatique devraient servir de référence pour les exigences de sécurité informatique qui sont définies dans le cadre de la GRSI pour l'installation et de la GRSI pour ses systèmes (voir respectivement les sections 4 et 5), compte tenu des différentes étapes de la vie de l'installation (section 6).

7.2. La direction et les cadres devraient considérer que la sécurité informatique dans les installations nucléaires est une question transversale, qui exige des connaissances, un savoir-faire et des compétences spécialisées.

7.3. La direction a la responsabilité générale de la sécurité informatique dans une installation nucléaire, et doit connaître et comprendre la cybermenace et les éventuelles conséquences dommageables d'une cyberattaque pour la sécurité nucléaire.

7.4. La direction devrait veiller à ce que toutes les relations de l'exploitant avec d'autres entités et tous les processus internes se déroulent conformément aux prescriptions juridiques et réglementaires qui touchent à la sécurité de l'information et à la sécurité informatique.

7.5. Les cadres devraient faire connaître les principes et les valeurs de la culture de sécurité nucléaire qui concernent la sécurité informatique. À ce titre, ils devraient notamment faire comprendre que des adversaires ayant des cybercompétences représentent une menace crédible, et que de tels adversaires

(y compris les menaces internes) peuvent prendre pour cible des installations nucléaires en lançant une cyberattaque ou une attaque combinée.

Politique de sécurité informatique

7.6. La politique de sécurité informatique fixe les grands objectifs d'une organisation dans ce domaine. Elle devrait commencer par expliquer clairement pourquoi elle est mise en place, devrait définir la question à traiter et les objectifs, et devrait présenter les conséquences qui pourraient apparaître si elle n'est pas respectée. Elle devrait aussi être conforme à la politique de sécurité informatique nationale et aux prescriptions réglementaires applicables. La politique de sécurité informatique devrait être applicable et réalisable, et devrait comprendre des indicateurs mesurables et contrôlables.

7.7. La politique de sécurité informatique de l'exploitant devrait tenir compte des résultats de la GRSI pour l'installation (voir section 4). Elle devrait exiger la protection des ressources numériques, notamment des RNS, contre les compromissions qui résultent des cyberattaques. Les parties de cette politique où figurent les exigences correspondantes devraient être claires et concises. La question de la mise en œuvre des exigences est traitée en détail dans le PSI.

7.8. La direction devrait approuver et faire appliquer la politique de sécurité informatique. Le nom de l'organisme ou de la personne responsable de cette politique et du PSI devrait figurer dans la politique de sécurité informatique.

7.9. La politique de sécurité informatique devrait faire partie de la politique de sécurité générale de l'installation et devrait être coordonnée avec les autres responsabilités relatives à la sécurité. Lors de l'élaboration de cette politique, il faut prendre en compte ses effets sur le plan juridique et en matière de ressources humaines.

7.10. Les mesures disciplinaires et les sanctions encourues par les membres du personnel qui ne respectent pas les exigences énoncées dans la politique de sécurité informatique peuvent figurer dans cette politique.

7.11. La politique de sécurité informatique devrait être prise en compte dans le PSI et dans ses éléments secondaires qui contribuent à l'application des mesures de sécurité informatique.

7.12. La politique de sécurité informatique doit définir des indicateurs clairs qui seront utilisés pour montrer que tous les aspects des règles sont respectés et que chaque aspect est mis en œuvre de manière satisfaisante.

Programme de sécurité informatique

7.13. Le PSI précise comment les objectifs qui sont fixés dans la politique de sécurité informatique sont atteints. Il définit les rôles, les responsabilités, les processus et les procédures pour la mise en œuvre de la politique de sécurité informatique au sein de l'organisation. Un PSI peut s'appliquer à une installation (y compris aux bâtiments et équipements associés) ou à une organisation (y compris à l'ensemble de ses sites et de ses services).

7.14. Le PSI devrait être élaboré, testé et tenu à jour dans le cadre du plan général de sécurité de l'installation.

7.15. Le PSI devrait tenir compte des résultats de la GRSI pour l'installation (section 4). Des membres du personnel qui jouent un rôle dans la sécurité informatique, la protection physique, la sûreté, l'exploitation ou les technologies de l'information peuvent participer à l'élaboration du PSI. Ce dernier est présenté schématiquement sur la figure 8.

7.16. Le PSI devrait être examiné et actualisé : a) périodiquement pour tenir compte de l'évolution des techniques et des menaces et b) en cas d'incident de sécurité informatique ou d'autre événement de sécurité nucléaire.

Éléments du programme de sécurité informatique

7.17. La référence [7] décrit les éléments d'un PSI qui sont généralement applicables aux organisations soumises au régime de sécurité nucléaire. Les paragraphes 7.18 à 7.20 donnent plus de précisions sur les différents éléments d'un PSI pour une installation nucléaire.

7.18. Le PSI devrait notamment expliquer comment remédier aux vulnérabilités des systèmes, appliquer les mesures de sécurité informatique, analyser les risques et mener des activités d'assurance pour que les risques liés à la sécurité informatique restent à un niveau acceptable.

7.19. Les éléments du PSI devraient être adaptés et appliqués aux différentes étapes de la vie d'une installation et aux différentes phases de la vie de chaque

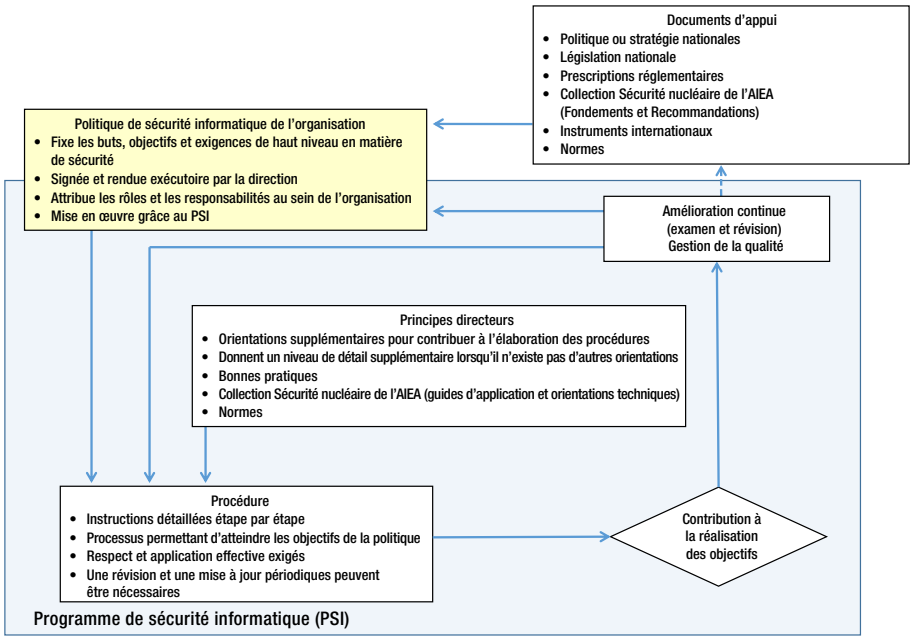

FIG. 8. Caractéristiques générales d'un programme de sécurité informatique classique.

système. Les caractéristiques particulières de mise en œuvre dans ces différents cas devraient figurer dans le PSI.

7.20. L'exploitant devrait adapter le PSI à l'installation concernée, mais il est souhaitable que, au minimum, les thèmes suivants y figurent :

a) Organisation et responsabilités :
   i) organigrammes ;
   ii) personnes responsables et responsabilités en matière de communication d'informations (voir par. A.3 à A.13 de l'appendice) ;
   iii) procédure périodique d'examen et d'approbation ;
   iv) interfaces avec d'autres programmes, comme les ressources humaines, les aspects de la sécurité qui concernent le personnel, la protection physique ou la formation (voir par. A.15 à A.38 de l'appendice).
b) Gestion des risques, des vulnérabilités et du respect des règles :
   i) GRSI pour l'installation et ses résultats (voir section 4) ;

ii) GRSI pour les systèmes et leurs résultats (voir section 5), y compris la classification et le recensement des ressources numériques[40], notamment des RNS ;
iii) fréquence de l'examen et de la réévaluation du plan de sécurité ;
iv) activités d'autoévaluation ;
v) procédures de contrôle, et détection et correction des défauts ;
vi) méthode d'évaluation de la vulnérabilité et du risque, et occasions de l'appliquer ou de la réappliquer ;
vii) respect de la législation et de la réglementation.

c) Conception et gestion de la sécurité :
i) architecture fondamentale de sécurité (c'est-à-dire l'ASID) ;
ii) approches fondamentales de la conception de la sécurité (c'est-à-dire les niveaux et les zones de sécurité informatique) ;
iii) mesures de sécurité informatique minimales pour chaque niveau de sécurité ;
iv) élaboration des exigences de sécurité informatique pour les vendeurs, les sous-traitants et les fournisseurs, y compris dans le cadre des contrats de maintenance ;
v) considérations de sécurité pour les étapes concernées de la vie de l'installation (voir section 6).

d) Gestion des ressources numériques :
i) caractéristiques des ressources numériques (identification, niveau de sécurité informatique, zone, emplacement et conséquences) ;
ii) gestion de la configuration (matériel, système d'exploitation, microprogrammes, applications logicielles, état des appareils et configurations correspondantes) ;
iii) flux de données et schémas des réseaux, où figurent toutes les connexions à des systèmes externes ;
iv) informations communiquées par les fournisseurs concernant les ressources.

e) Procédures de sécurité :
i) gestion des incidents de sécurité ;
ii) continuité des opérations ;
iii) sauvegarde, restauration et récupération de systèmes ;
iv) chaîne d'approvisionnement ;
v) contrôle des accès ;
vi) gestion informatique ;

[40] Les ressources numériques comprennent les mesures de contrôle technique qui reposent sur des technologies numériques.

vii) sécurité de la plateforme et des applications (renforcement de la sécurité des systèmes, par exemple) ;
viii) surveillance des systèmes, y compris la journalisation.

f) Gestion du personnel :
i) habilitation ;
ii) sensibilisation et formation ;
iii) qualification du personnel ;
iv) signalement des problèmes de sécurité, y compris la protection des agents qui signalent ce type de problèmes ;
v) cessation d'emploi ou transfert.

7.21. On trouvera de plus amples informations sur les différents éléments du PSI dans des normes internationales [19–21].

RÔLES ET RESPONSABILITÉS AU SEIN DE L'ORGANISATION

7.22. L'exploitant devrait définir les rôles et les responsabilités en matière de sécurité informatique au sein de l'organisation.

7.23. Les cadres devraient veiller à ce que tous les membres du personnel sachent qui, dans l'organisation, est responsable du pilotage du PSI dans les domaines qui concernent leur travail. Les agents qui ont des responsabilités en matière de sécurité informatique doivent être formés sur les éléments et les exigences qui figurent dans le PSI.

7.24. Dans la mesure du possible, la gestion de la sécurité informatique devrait être intégrée dans le système de gestion en vigueur dans l'installation (voir par. 7.30 à 7.34). Pour les installations existantes, le système de gestion décrit déjà les rôles et les responsabilités qui sont bien définis, et ceux-ci devraient être adaptés pour tenir compte de la sécurité informatique.

7.25. Les membres du personnel qui ont des responsabilités importantes en matière de sécurité informatique ne devraient pas être en conflit d'intérêts pour d'autres fonctions au sein de l'organisation ou pour d'autres tâches. Les cadres devraient mettre en place des politiques et des procédures pour éviter ou atténuer les conflits d'intérêts éventuels.

7.26. L'exploitant devrait s'assurer que les personnes et les organisations qui mènent des activités d'évaluation et de vérification essentielles sont dûment qualifiées et indépendantes.

7.27. La sécurité informatique exige une coopération entre des agents qui exercent différents rôles et travaillent dans différents services. L'exploitant devrait mettre en place un cadre formel pour permettre une coopération interdisciplinaire.

7.28. L'exploitant doit recenser les relations internes ou externes qui concernent le PSI. Il s'agit notamment des relations suivantes :

a) relations habituelles entre l'exploitant de l'installation et les autorités compétentes (organisme de réglementation, forces de l'ordre, services de renseignement ou services de sécurité, par exemple) ;
b) signalement aux autorités compétentes et relations avec les forces d'intervention en cas d'incident de sécurité ;
c) relations avec l'équipe d'intervention sur site ;
d) relations publiques ;
e) relations avec les vendeurs, les sous-traitants et les fournisseurs, y compris les différents maillons de la chaîne d'approvisionnement.

7.29. L'exploitant devrait gérer les risques dans un cadre formel (c'est-à-dire dans le cadre de la GRSI pour l'installation et ses systèmes) qui permet d'évaluer et de gérer les risques et les vulnérabilités qui concernent l'installation. L'exploitant devrait exploiter les résultats obtenus pour son système de gestion.

Système de gestion

7.30. Le système de gestion devrait prendre en compte la sécurité informatique, la protection physique, la sûreté, la santé, l'environnement, la qualité et les aspects financiers.

7.31. Il devrait y avoir des interfaces formelles et bien établies entre le système de gestion et la GRSI pour l'installation et ses systèmes.

7.32. Il faudrait définir et gérer les objectifs de sécurité informatique et de sécurité de l'information dans le cadre du système de gestion, comme pour d'autres objectifs opérationnels.

7.33. Il faudrait examiner le système de gestion pour garantir qu'il est complet et conforme aux politiques de sécurité de l'installation. Il faudrait aussi l'examiner régulièrement et l'adapter lorsque l'installation ou l'environnement évoluent. La figure 3 de la référence [22] présente schématiquement le processus d'amélioration continue des systèmes de gestion.

7.34. Il faudrait examiner les éléments du PSI (y compris la GRSI pour l'installation et ses systèmes) et intégrer les dispositions nécessaires à la sécurité informatique dans le système de gestion.

Indicateurs de sécurité informatique

7.35. Les indicateurs de sécurité informatique peuvent être utiles aux responsables de la sécurité pour évaluer la maturité du système de gestion, pour mesurer le risque associé aux cyberattaques qui pourraient compromettre des RNS, pour estimer l'efficacité des différentes parties de leurs programmes de sécurité, pour évaluer la sécurité d'un système, d'une méthode ou d'un produit particuliers et pour apprécier la capacité des membres du personnel à régler les questions de sécurité qui relèvent de leur responsabilité.

7.36. Les indicateurs devraient appuyer les décisions qui concernent le niveau de risque acceptable et contribuer à établir un registre des risques.

7.37. Il faudrait mener une analyse afin de déterminer quels paramètres peuvent être exploités pour gérer efficacement le PSI, et afin de définir les indicateurs correspondants. Parmi les indicateurs qui peuvent être utiles, on peut citer le temps moyen de remise en état (après une cyberattaque), le nombre d'incidents de sécurité informatique, le nombre de restaurations de RNS (qui peuvent être effectuées à plusieurs reprises), la liste des points à traiter en matière de sécurité et les informations de suivi des vulnérabilités (système de notation des vulnérabilités communes, efficacité des mesures d'atténuation, temps de déploiement de dispositifs de contrôle et déploiement de correctifs, par exemple).

7.38. Le système de gestion de l'organisation devrait prendre en compte de tels indicateurs.

CONCEPTION ET GESTION DE LA SÉCURITÉ

7.39. La sécurité pour l'installation et ses systèmes est conçue dans le cadre de la GRSI pour l'installation et ses systèmes (voir respectivement les sections 4 et 5). Un exemple du résultat obtenu, à savoir l'ASID et les mesures applicables à chaque niveau de sécurité informatique, est présenté dans la section 8.

Exigences de sécurité informatique

7.40. Avant d'apporter des modifications à l'installation et à ses systèmes, il faudrait les analyser pour déterminer leurs effets possibles sur la sécurité afin de pouvoir gérer les risques.

7.41. Lorsque l'on détermine quelles sont les données d'entrée de la conception, il faudrait prendre en considération la sécurité informatique. Ces données d'entrée sont notamment les suivantes :

a) exigences fonctionnelles ;
b) exigences en matière d'interface ;
c) exigences relatives à l'exploitation ;
d) emplacement du matériel ;
e) considérations environnementales ;
f) codes et normes à appliquer ;
g) considérations contractuelles ;
h) considérations relatives à la chaîne d'approvisionnement ;
i) logistique (coordination d'opérations complexes où entrent en jeu de nombreuses personnes, de nombreuses installations ou de nombreux produits, par exemple) ;
j) expérience d'exploitation antérieure ;
k) introduction de nouvelles technologies ;
l) prise en compte des facteurs humains ;
m) exigences de conception pour chaque discipline technique (notamment pour la sécurité informatique) ;
n) considérations relatives à la fabrication ;
o) mise en place ;
p) mise en service ;
q) déclassement ;
r) considérations financières.

GESTION DES RESSOURCES NUMÉRIQUES

7.42. L'exploitant devrait consigner la liste des caractéristiques de chaque ressource numérique qui ont de l'importance pour la sécurité informatique. Ces caractéristiques peuvent comprendre :

a) l'identifiant et l'emplacement des ressources ;
b) la configuration des ressources ;

c) leurs fonctions et leurs modes de fonctionnement ;
d) les interconnexions, y compris pour l'alimentation électrique ;
e) les flux de données, qu'ils soient internes ou externes ;
f) les procédures d'établissement des communications, la fréquence des communications et les protocoles correspondants ;
g) l'analyse des groupes d'utilisateurs ;
h) les responsables (des données et des systèmes informatisés) ;
i) les niveaux et les zones de sécurité informatique, et les conséquences des défaillances qui ont été évaluées.

7.43. Dans le cadre de la gestion des ressources numériques, il faudrait prendre en compte l'état des appareils qui appliquent des mesures de contrôle technique et utilisent des techniques numériques. Les personnes qui mènent les activités de sécurité informatique et les activités de protection physique peuvent être conjointement responsables des mesures, des procédures et des systèmes de sécurité intégrés. Un tel contrôle conjoint peut comprendre le contrôle des équipements qui servent à protéger le matériel informatique (salles, portes, clefs, serrures, caméras, détecteurs de mouvement ou indicateurs de manipulation frauduleuse, par exemple).

Gestion de la configuration

7.44. La gestion de la configuration vise à disposer de données détaillées et actualisées sur les composants logiciels et matériels qui ont été installés, et sur la manière dont ils ont été configurés. Elle devrait notamment permettre d'obtenir les informations qui sont nécessaires pour :

a) déterminer quelles sont les mesures de sécurité informatique requises ;
b) vérifier que les mesures de sécurité informatique sont correctement mises en œuvre et paramétrées ;
c) gérer les changements tout au long de la durée de vie des systèmes ;
d) faciliter les évaluations de la sécurité informatique ;
e) comprendre les raisons des modifications qui sont apportées aux mesures de sécurité informatique.

7.45. La gestion de la configuration comprend la gestion du changement. La sécurité informatique devrait être prise en compte dans le cadre de la gestion du changement afin que tous les changements soient évalués du point de vue de la sécurité informatique avant d'être engagés. Ainsi, des examens appropriés sont effectués et leurs résultats sont consignés avant que ne soient appliquées des procédures permettant de contourner ou de modifier des mesures de sécurité

informatique qui ont été mises en place, ou d'en réduire l'efficacité. Des changements de personnel peuvent aussi exiger des modifications qui concernent la sécurité informatique (annulation et gestion d'un compte, par exemple).

PROCÉDURES DE SÉCURITÉ

7.46. L'exploitant devrait élaborer des procédures de sécurité afin de faciliter la conception et la gestion de la sécurité informatique de l'installation et de ses systèmes. Dans le cadre de l'élaboration de ces procédures, l'exploitant devrait envisager d'appliquer la règle des deux personnes ou de séparer les tâches, en tenant compte du modèle de confiance pertinent et du niveau de sécurité informatique qui a été attribué à la zone ou aux zones concernées par la procédure.

7.47. Les procédures qui contiennent des instructions détaillées sur la manière de désactiver ou de contourner des mesures de sécurité informatique devraient être établies de telle manière que le déroulement des activités correspondantes est enregistré**.** De telles procédures peuvent aussi contenir des instructions relatives à l'application de mesures de sécurité informatique compensatoires ou autres lorsqu'une mesure de sécurité minimale est neutralisée.

7.48. De telles procédures peuvent être de nouvelles procédures autonomes, ou être rattachées à des procédures existantes qui répondent à un ou plusieurs objectifs relatifs à la sûreté, à la sécurité ou à l'organisation.

GESTION DU PERSONNEL

7.49. La gestion du personnel comprend les dispositions nécessaires à la mise en place d'un niveau d'habilitation suffisant, au respect d'un engagement de confidentialité, à la définition des compétences requises et, si nécessaire, à l'application de sanctions ou à la cessation d'emploi.

7.50. Il faudrait coordonner les activités de sécurité informatique et les activités de sécurité relatives aux membres du personnel afin de se protéger contre les menaces internes. Un niveau d'habilitation plus élevé peut en particulier être nécessaire pour les agents qui ont des responsabilités importantes en matière de sécurité (administrateurs système et membres de l'équipe de sécurité, par exemple). Des orientations supplémentaires sur la protection contre les menaces internes figurent dans la référence [6].

7.51. Le PSI devrait prévoir des activités de formation et de sensibilisation, afin de développer et de maintenir les compétences et les qualifications du personnel et de l'organisation qui sont nécessaires à la sécurité informatique.

8. EXEMPLE D'UTILISATION D'UNE ARCHITECTURE DE SÉCURITÉ INFORMATIQUE DÉFENSIVE ET MESURES DE SÉCURITÉ INFORMATIQUE CORRESPONDANTES

8.1. Un exemple d'utilisation d'une ASID à cinq niveaux de sécurité informatique dans une centrale nucléaire est présenté ci-dessous. Il ne s'agit que d'une application possible de l'approche graduée. Le choix exact des niveaux, de l'ASID et des mesures de sécurité informatique devrait être déterminé par une analyse spécifique de l'installation et de son environnement.

EXEMPLE D'UTILISATION D'UNE ARCHITECTURE DE SÉCURITÉ INFORMATIQUE DÉFENSIVE

8.2. Lorsqu'il utilise une ASID, l'exploitant devrait envisager de limiter les éléments dynamiques des réseaux et des systèmes pour rendre leur comportement plus prévisible. Cette meilleure prévisibilité peut faciliter la mise en œuvre de mesures de sécurité informatique efficaces.

8.3. Les zones auxquelles a été attribué le niveau de sécurité informatique le plus strict ne devraient être reliées à des zones ayant un niveau de sécurité moins contraignant que par des voies de communication unidirectionnelles, déterministes et à sécurité intégrée. Les transmissions de données correspondantes devraient s'effectuer depuis la zone où le niveau de sécurité informatique est le plus strict vers celle dont le niveau de sécurité est le moins contraignant[41]. Il est fortement recommandé d'éviter les exceptions. Celles-ci peuvent être envisagées

[41] À l'exception des zones où des fonctions gèrent uniquement des informations sensibles : dans ce cas, le sens est inversé. Des informations sensibles peuvent être transmises à des réseaux qui sont soumis à des restrictions, mais ne peuvent venir de tels réseaux.

uniquement au cas par cas, à condition d'être largement justifiées et étayées par une analyse des risques pour la sécurité[42].

8.4. Les appareils numériques ou les voies de communication qui sont utilisés pour les activités de surveillance, de maintenance ou de remise en état ne devraient pas permettre de contourner les mesures de sécurité informatique qui servent à protéger les voies de communication entre appareils ayant des niveaux de sécurité informatique différents.

8.5. Les systèmes auxquels le niveau de sécurité informatique le plus strict a été attribué devraient être installés dans les limites de la zone la plus sûre[43].

8.6. Les communications de données entre les systèmes de l'installation et le centre d'urgence (sur le site ou hors du site) devraient être protégées par des mesures de sécurité informatique.

DÉCOUPLAGE ENTRE LES ZONES DE SÉCURITÉ INFORMATIQUE

8.7. Les mesures de sécurité informatique qui assurent un découplage logique et physique entre des zones dépendent des exigences qui ont été fixées pour les niveaux de sécurité informatique des zones concernées. Afin de maintenir une défense en profondeur, il ne faudrait pas autoriser de liaison directe entre plusieurs zones.

8.8. Les mesures de contrôle technique qui préservent la sécurité aux limites de zones devraient permettre de résister à une cyberattaque et de donner l'alerte en cas de compromission présumée ou d'activité malveillante.

CONNECTIVITÉ EXTERNE

8.9. Lorsqu'une connectivité externe existe**,** il conviendrait d'assurer la sécurité à l'aide d'une approche graduée. Une telle connectivité devrait satisfaire aux

---

[42] Certains États Membres n'autorisent aucune exception pour les installations à haut risque ou à très haut risque. Pour d'autres types d'installations, l'autorité compétente peut laisser la question de l'utilisation de chemins bidirectionnels à la discrétion de l'exploitant.

[43] Les communications sans fil posent des problèmes lorsqu'elles sont utilisées dans des systèmes auxquels le niveau de sécurité le plus strict a été attribué, car il est difficile de mettre en place un périmètre sécurisé pour ce type de communications.

exigences qui concernent la protection de la confidentialité, de l'intégrité et de la disponibilité des informations sensibles, conformément au niveau de sécurité qui a été attribué à la zone concernée.

8.10. Il faudrait appliquer des restrictions d'accès appropriées (notamment une surveillance des accès) afin d'assurer une protection selon une approche graduée, car les connexions externes peuvent être exploitées pour compromettre des systèmes de l'installation.

8.11. Exemples de systèmes accessibles de l'extérieur :

a) systèmes de contrôle radiologique de l'environnement ;
b) systèmes d'automatisation et de contrôle des bâtiments ;
c) systèmes de protection contre l'incendie ;
d) systèmes de communication avec les centres d'urgence ;
e) systèmes d'accès à distance pour les vendeurs (lorsqu'un tel accès est autorisé) ;
f) appareils de terrain situés à l'extérieur du périmètre de sécurité ;
g) systèmes de contrôle des visiteurs.

8.12. La figure 9 donne un exemple d'utilisation d'une ASID. Y sont représentés les niveaux, les zones, les systèmes et les ressources numériques. Cet exemple reprend les orientations qui figurent dans la section 3.

EXEMPLES D'EXIGENCES

8.13. Des exemples d'exigences de sécurité qui sont appliqués à chaque niveau de sécurité informatique sont présentés aux paragraphes 8.16 à 8.21. Le choix exact des niveaux et des exigences de sécurité correspondantes devrait être déterminé par une analyse spécifique de l'installation et de son environnement.

RESSOURCES NUMÉRIQUES AUXQUELLES AUCUN NIVEAU DE SÉCURITÉ INFORMATIQUE N'A ÉTÉ ATTRIBUÉ

8.14. Il existe deux types de ressources numériques auxquelles aucun niveau de sécurité informatique n'a été attribué :

a) Le matériel prohibé ou à usage restreint (les restrictions imposées à l'exploitant ne lui permettent pas d'évaluer la sécurité de telles ressources

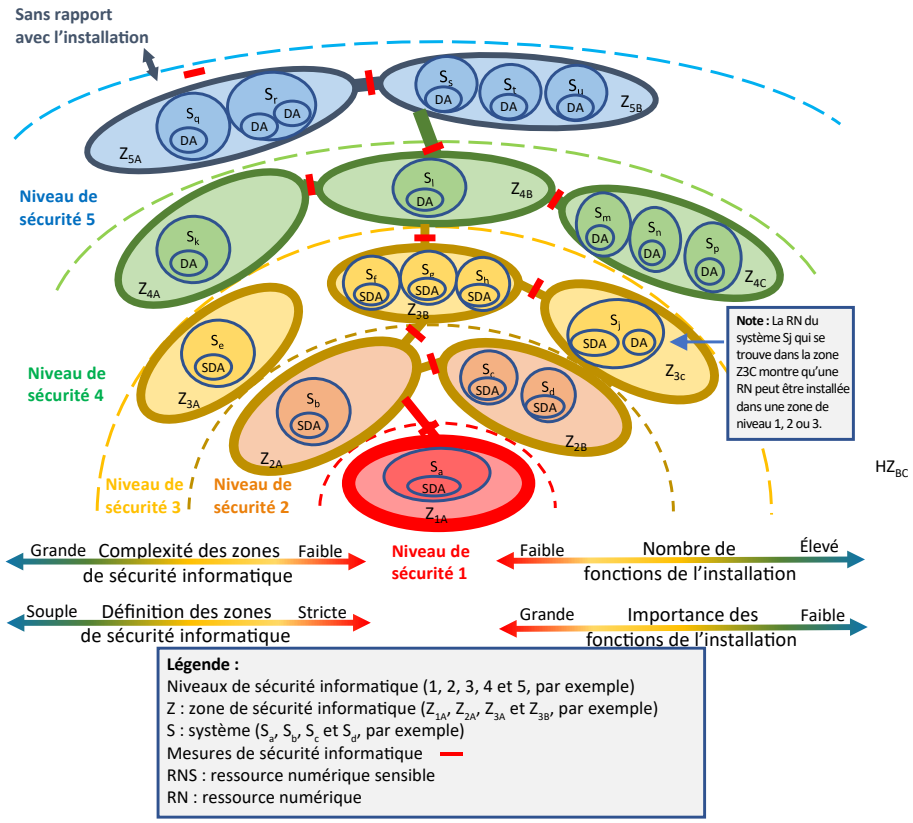

FIG. 9. Exemple d'utilisation d'une architecture de sécurité informatique défensive.

numériques). De telles restrictions peuvent être dues aux conditions de licence ou à des dispositions juridiques, réglementaires ou contractuelles qui interdisent à l'exploitant d'inspecter ou de modifier le matériel (matériel utilisé pour les garanties, par exemple).

b) Le matériel imprévu, qui peut être introduit dans l'installation sans que l'exploitant n'en ait fait la demande ou n'ait préalablement donné son accord. Ce type de matériel est considéré comme un article de « contrebande » tant qu'aucune évaluation des risques liés à la sécurité informatique n'a été effectuée.

8.15. L'exploitant peut imposer des restrictions à l'utilisation de ressources auxquelles aucun niveau de sécurité informatique n'a été attribué, tant qu'elles n'ont pas été évaluées, qu'elles ne se sont pas vu attribuer le niveau de sécurité informatique approprié et que les mesures de sécurité informatique nécessaires

n'ont pas été mises en place. Ainsi, les appareils auxquels aucun niveau de sécurité informatique n'a été attribué ne devraient pas être placés à proximité de systèmes dont le niveau de sécurité informatique est intermédiaire, élevé ou très élevé.

EXIGENCES GÉNÉRALES

8.16. Pour les systèmes et les niveaux concernés, les exigences générales suivantes sont appliquées :

a) Toutes les mesures d'ordre technique ou physique, ou qui portent sur le personnel ou l'organisation, et qui concernent les systèmes et les réseaux, sont élaborées et mises en œuvre de manière systématique et conformément à des procédures et à des processus qui ont été approuvés.
b) Des politiques et des pratiques sont définies pour chaque niveau de sécurité informatique.
c) Les utilisateurs sont tenus de respecter les politiques de sécurité et les procédures d'exploitation qui concernent la sécurité.
d) Les membres du personnel qui ont le droit d'accéder aux systèmes sont suffisamment qualifiés et expérimentés, et sont habilités si nécessaire.
e) Les utilisateurs et les administrateurs n'ont accès qu'aux fonctions des systèmes dont ils ont besoin dans le cadre de leur travail. On évite d'accorder de nombreux droits d'accès à une seule personne.
f) La fonctionnalité et les interfaces des systèmes sont aussi limitées que possible afin de réduire la vulnérabilité globale.
g) Des dispositifs appropriés de contrôle d'accès et d'authentification des utilisateurs sont mis en place.
h) Des mesures de protection contre l'infection par des logiciels malveillants et la propagation de tels logiciels sont mises en place.
i) Des procédures de journalisation et de surveillance sont mises en place en matière de sécurité, y compris pour des interventions appropriées.
j) Les vulnérabilités des applications et des systèmes sont surveillées, et des mesures appropriées sont prises.
k) La pertinence et l'efficacité des mesures sont examinées périodiquement.
l) Des évaluations de la vulnérabilité des systèmes sont effectuées périodiquement.
m) Les supports amovibles sont contrôlés conformément aux procédures d'exploitation qui concernent la sécurité. Il est interdit de connecter un appareil personnel à un système ou à un réseau.
n) Les ressources numériques font l'objet d'une maintenance rigoureuse et les mesures de sécurité informatique correspondantes sont strictement

maintenues à l'aide des procédures de gestion du changement qui sont en vigueur.

o) Des procédures de sauvegarde et de restauration appropriées sont mises en place.

p) Un seul niveau de sécurité informatique est attribué à un appareil donné.

q) L'accès physique aux composants et aux systèmes, y compris aux appareils, est limité selon les fonctions qu'ils exécutent.

r) Des mesures destinées à prévenir l'introduction non autorisée de systèmes dans une zone de sécurité informatique sont mises en place.

s) Seuls les utilisateurs autorisés et qualifiés peuvent apporter des modifications aux systèmes.

EXIGENCES APPLICABLES AU NIVEAU DE SÉCURITÉ 1

8.17. Outre les exigences générales, des exigences relatives aux mesures de prévention et de protection sont appliquées aux systèmes qui sont essentiels pour l'installation et qui requièrent le niveau de sécurité le plus élevé (systèmes de protection des réacteurs, par exemple). Ces exigences peuvent notamment être les suivantes :

a) Les systèmes sont conçus et mis en place de telle manière qu'ils peuvent faire l'objet d'une vérification et de tests concernant les attaques qui pourraient être lancées par des adversaires.

b) Aucun flux de données provenant d'un système auquel un faible niveau de sécurité a été attribué ne peut pénétrer dans un système de niveau 1 lorsque l'intégrité et la disponibilité constituent des priorités. Seules les communications vers l'extérieur sont possibles. Il est fortement recommandé d'éviter les exceptions. Celles-ci peuvent être envisagées uniquement au cas par cas, à condition d'être largement justifiées et étayées par une analyse des risques pour la sécurité[44].

c) Aucune télémaintenance n'est autorisée.

d) Les accès physiques et logiques aux systèmes sont strictement contrôlés, surveillés et enregistrés.

e) Le nombre de membres du personnel ayant accès aux systèmes est limité au strict minimum.

f) La règle des deux personnes est appliquée pour empêcher qu'une menace interne ne commette un acte non autorisé.

[44] Certains États Membres n'autorisent aucune exception.

g) Toutes les activités et tous les événements qui peuvent être des événements de sécurité sont enregistrés et surveillés.
h) La connexion de supports de stockage externes est approuvée et vérifiée au cas par cas.
i) Des procédures organisationnelles et administratives rigoureuses sont appliquées pour toutes les modifications, notamment pour la maintenance du matériel et pour les mises à jour et les modifications des logiciels.

EXIGENCES APPLICABLES AU NIVEAU DE SÉCURITÉ 2

8.18. Outre les exigences générales, des exigences relatives aux mesures de prévention et de protection devraient être appliquées pour les systèmes qui requièrent un niveau de sécurité élevé, tels les systèmes de contrôle opérationnel. Ces exigences peuvent notamment être les suivantes :

a) Seuls les flux de données unidirectionnels vers l'extérieur sont autorisés des systèmes de niveau 2 vers les systèmes de niveau 3. Seuls les messages d'acquittement et les messages de synchronisation nécessaires peuvent être acceptés dans le sens opposé (vers l'intérieur) [pour le protocole TCP/IP (protocole de contrôle de transmission/protocole Internet), par exemple].
b) La télémaintenance n'est pas autorisée.
c) Le nombre de membres du personnel qui ont accès aux systèmes est maintenu au minimum et une nette distinction est établie entre les utilisateurs et le personnel administratif.
d) Les accès physiques et logiques aux systèmes sont strictement contrôlés et enregistrés.
e) On évite d'accorder un accès administrateur depuis les autres niveaux de sécurité informatique. Si cela n'est pas possible, un tel accès est strictement contrôlé (par la règle des deux personnes et une authentification à deux facteurs, par exemple).
f) Toutes les mesures raisonnables sont prises pour garantir l'intégrité et la disponibilité des systèmes.

EXIGENCES APPLICABLES AU NIVEAU DE SÉCURITÉ 3

8.19. Outre les exigences générales, les exigences relatives aux mesures de prévention et de protection devraient être appliquées aux systèmes temps réel qui ne sont pas nécessaires pour l'exploitation (systèmes de supervision de processus qui se trouvent dans une salle de commande, par exemple), si, pour tous

les systèmes de ce type, les conséquences d'une compromission sont de gravité moyenne pour diverses cybermenaces. Ces exigences peuvent notamment être les suivantes :

a) L'accès à Internet depuis un système de niveau 3 est interdit.
b) L'enregistrement des données et les pistes de vérification sont surveillés pour les ressources essentielles.
c) Des passerelles de sécurité sont mises en place pour empêcher les connexions non contrôlées depuis les systèmes de niveau 4 et pour n'autoriser qu'une activité précise et limitée.
d) Les connexions physiques aux systèmes sont contrôlées.
e) Les accès physiques et logiques aux systèmes sont contrôlés et enregistrés.
f) La télémaintenance n'est autorisée qu'au cas par cas et à condition d'être rigoureusement contrôlée. L'ordinateur distant est utilisé conformément à une politique de sécurité qui a été définie par contrat.
g) Les fonctions des systèmes auxquelles les utilisateurs peuvent accéder sont soumises à des mécanismes de contrôle des accès et à la règle du « besoin d'en connaître ». Toute exception à cette règle est soigneusement examinée et une protection est assurée par d'autres moyens (contrôle des accès physiques, par exemple).
h) On évite d'accorder un accès administrateur depuis les autres niveaux de sécurité informatique dans la mesure du possible. Si cela n'est pas possible, un tel accès est strictement contrôlé (par une authentification à deux facteurs, par exemple).

EXIGENCES APPLICABLES AU NIVEAU DE SÉCURITÉ 4

8.20. Outre les exigences générales, les exigences relatives aux mesures de sécurité informatique devraient être appliquées aux systèmes de gestion des données techniques qui sont 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 travail, commande de travail, étiquetage et gestion de la documentation, par exemple), si ces systèmes doivent avoir un niveau de sécurité informatique intermédiaire. Ces exigences peuvent notamment être les suivantes :

a) L'accès à Internet depuis un système de niveau 4 est interdit.
b) Des passerelles de sécurité sont mises en place pour empêcher les communications interdites qui passent par des réseaux d'entreprises externes

ou de l'installation qui sont fiables et autorisés, et pour permettre de mener des activités précises qui sont autorisées.

c) Les connexions physiques aux systèmes sont contrôlées.

d) La télémaintenance est autorisée mais contrôlée. L'ordinateur distant est utilisé conformément à une politique de sécurité qui a été définie par contrat.

e) Les fonctions des systèmes auxquelles les utilisateurs peuvent accéder sont soumises à des mécanismes de contrôle des accès. Toute exception à cette règle est soigneusement examinée et une protection est assurée par d'autres moyens.

f) L'accès à distance depuis l'extérieur est autorisé pour certains services et pour les utilisateurs autorisés, à condition que des mécanismes appropriés de contrôle d'accès aient été mis en place.

EXIGENCES APPLICABLES AU NIVEAU DE SÉCURITÉ 5

8.21. Des exigences qui imposent des mesures de sécurité informatique devraient être appliquées aux systèmes qui n'ont pas d'importance directe pour le contrôle technique ou l'exploitation (systèmes de bureautique, par exemple), si de tels systèmes ne requièrent qu'un faible niveau de sécurité informatique. Ces exigences peuvent notamment être les suivantes :

a) Le niveau de sécurité informatique ne descend pas au-dessous d'un niveau de protection minimale, qui est défini en fonction des dernières connaissances disponibles.

b) Seuls les utilisateurs autorisés et qualifiés peuvent apporter des modifications aux systèmes.

c) L'accès à Internet depuis un système de niveau 5 est autorisé, à condition que des mesures de prévention et de protection adéquates soient appliquées.

d) L'accès à distance depuis l'extérieur est accordé aux utilisateurs autorisés, à condition que des mesures appropriées aient été mises en place.

e) La connexion physique d'appareils externes à des systèmes et à des réseaux fait l'objet d'un contrôle technique. Ces interfaces de systèmes plus importants sont caractérisées et évaluées de manière indépendante afin de vérifier qu'elles sont conformes à l'architecture de sécurité informatique.

Appendice

EXTRAITS D'UN PROGRAMME DE SÉCURITÉ INFORMATIQUE

A.1. Le présent appendice donne un exemple de certains éléments du PSI qui peuvent être utilisés dans le cadre d'une approche de la sécurité informatique fondée sur les résultats. Un exploitant peut être amené à modifier ces éléments pour tenir compte de circonstances qui sont propres à l'organisation ou à l'installation, mais les exemples couvrent tous les types d'informations dont l'exploitant a besoin pour élaborer et mettre en œuvre un PSI efficace.

A.2. L'exploitant devrait rendre obligatoires ces éléments ou des éléments similaires pour faciliter la compréhension entre les services de l'organisation, les vendeurs, les sous-traitants, les fournisseurs et les autorités compétentes. Il peut être nécessaire d'adapter les éléments aux caractéristiques de l'organisme exploitant et de l'installation afin d'améliorer la compréhension.

ORGANISATION ET RESPONSABILITÉS AU SEIN DE L'INSTALLATION

Direction

A.3. La direction de l'installation établit une politique de sécurité informatique et met en place des processus et des mécanismes de soutien pour garantir la mise en œuvre de cette politique. À cette fin, elle devrait :

a) assumer la responsabilité générale de tous les aspects de la sécurité informatique ;
b) définir les objectifs de sécurité pour l'installation ;
c) s'assurer du respect des lois et des règlements applicables ;
d) appeler durablement l'attention sur la menace de sécurité nucléaire actuelle et sur les évolutions correspondantes ;
e) fixer le degré d'acceptation du risque dans l'installation ;
f) attribuer des responsabilités organisationnelles en matière de sécurité informatique ;
g) assurer une communication adéquate entre les membres du personnel qui sont responsables des différents aspects de la sécurité nucléaire ;
h) veiller au respect de la politique de sécurité informatique ;

i) fournir des ressources adéquates pour pouvoir mettre en œuvre durablement le PSI.
j) veiller à ce que la politique et les procédures de sécurité informatique soient régulièrement réexaminées et mises à jour ;
k) appuyer les programmes de formation et de sensibilisation.

Spécialiste de la sécurité informatique

A.4. L'exploitant devrait attribuer la responsabilité générale de la sécurité informatique dans l'installation à une seule personne ou à un groupe. Dans la présente publication, on utilise le titre de « spécialiste de la sécurité informatique » pour définir ce rôle[45].

A.5. Le spécialiste de la sécurité informatique devrait coordonner étroitement les activités dans toute l'installation, mais en agissant de manière indépendante. Il devrait avoir des rapports hiérarchiques clairs, simples et directs avec la direction, car la sécurité informatique peut concerner presque toutes les activités de l'installation.

A.6. Il faudrait clairement définir et coordonner les rôles en matière de sécurité informatique dans les différents services de l'organisation, afin d'éviter les lacunes ou les conflits et pour que les mesures de sécurité informatique soient appliquées de manière cohérente. Ce point est particulièrement important lorsque le rôle de spécialiste de la sécurité informatique est confié à un groupe plutôt qu'à une seule personne : le spécialiste de la sécurité informatique devrait être l'unique responsable chargé de régler les questions qui concernent toute l'organisation et de résoudre les conflits qui pourraient survenir.

A.7. Le spécialiste 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, ainsi qu'une connaissance de la sûreté nucléaire et de la gestion de projets. Il devrait aussi être capable d'intégrer des personnes qui exercent des disciplines différentes dans une équipe efficace.

[45] Dans d'autres situations, le titulaire de cette fonction peut être appelé « responsable de la sécurité informatique », « responsable en chef de la sécurité de l'information », « responsable de la sécurité des technologies de l'information » ou « responsable de la sécurité de l'information », ou la fonction peut être confiée à plusieurs personnes.

A.8. Le spécialiste de la sécurité informatique devrait avoir la responsabilité et le pouvoir de gérer le PSI.

A.9. Les responsabilités particulières qui incombent généralement au spécialiste de la sécurité informatique sont les suivantes :

a) conseiller la direction sur la sécurité informatique ;
b) diriger l'équipe de sécurité informatique ;
c) promouvoir la sécurité informatique dans l'organisation, en proposant notamment des améliorations si nécessaire ;
d) coordonner et contrôler le développement des activités relatives à la sécurité informatique (application de la politique de sécurité informatique, de directives et d'orientations particulières**,** des procédures et des mesures de sécurité, par exemple) ;
e) coopérer avec les personnes chargées de la protection physique et avec d'autres membres du personnel qui sont responsables de la sécurité et de la sûreté afin de prévoir et de définir des mesures de sécurité informatique, y compris des mesures permettant d'intervenir en cas d'incident de sécurité informatique ;
f) recenser les systèmes qui sont essentiels à la sécurité informatique dans l'installation (c'est-à-dire ceux qui permettent d'appliquer des mesures de sécurité informatique minimales). Les responsables de ressources devraient connaître le rôle de leur matériel dans la sécurité informatique ;
g) conduire une évaluation périodique des risques liés à la sécurité informatique, indépendamment du personnel d'exploitation ;
h) mener des inspections, des vérifications et des examens réguliers des mesures de sécurité informatique minimales et communiquer des rapports d'étape à la direction ;
i) élaborer et organiser une formation sur la sécurité informatique pour le personnel concerné, et mettre en place une qualification professionnelle ;
j) préparer et diriger les interventions en cas d'incident de sécurité informatique, et notamment coopérer avec les membres du personnel interne et externe qui participent à l'intervention ;
k) enquêter sur les incidents de sécurité informatique et élaborer des mesures correctives à appliquer à la suite de tels incidents ;
l) participer à l'évaluation de la sécurité générale de l'installation ;
m) participer à l'analyse des besoins pour les nouveaux systèmes informatiques**.**

Équipe de sécurité informatique

A.10. L'exploitant devrait désigner les membres du personnel qui feront partie de l'équipe de sécurité informatique. Celle-ci peut être stable ou peut comprendre temporairement des personnes qui ont une compétence spécialisée si nécessaire. L'équipe aide le spécialiste de la sécurité informatique à s'acquitter de ses responsabilités : ce spécialiste doit avoir accès à des compétences dans tous les domaines qui ont un rapport avec la sécurité informatique, notamment la sûreté des installations, l'exploitation des centrales, la protection physique et les aspects de la sécurité qui concernent le personnel.

A.11. Les membres de l'équipe de sécurité informatique devraient être chargés de promouvoir la sécurité informatique dans le service où ils travaillent.

A.12. Les activités de l'équipe de sécurité informatique comprennent la surveillance active des ressources numériques, notamment des RNS, pour détecter tout signe possible de cyberattaque, et la coordination des interventions en cas d'incident de sécurité informatique. Elles peuvent aussi comprendre l'affectation de personnel au centre des opérations de sécurité, qui permet de surveiller et d'évaluer les incidents de sécurité informatique potentiels, et d'entreprendre et d'appuyer les activités d'intervention, pour lesquelles le concours d'autres organisations pourrait également être nécessaire.

Autres responsabilités de la hiérarchie

A.13. À différents niveaux de l'organisation, les responsables devraient veiller à ce qu'une attention appropriée soit accordée à la sécurité informatique dans leur domaine de responsabilité. Les activités que doivent généralement mener les responsables dans leur domaine sont les suivantes :

a) comprendre l'importance et le rôle de la sécurité informatique pour la sécurité nucléaire ;
b) agir conformément aux exigences et aux processus qui ont été définis dans le PSI ;
c) fournir des exigences relatives à l'exploitation et un retour d'information à la direction de la sécurité informatique, et résoudre les contradictions qui existent entre les exigences relatives à l'exploitation, les exigences de sécurité et les exigences de sûreté ;
d) signaler à la direction toute situation qui pourrait conduire à modifier le niveau de sécurité informatique, notamment les changements qui concernent le personnel, le matériel ou les processus ;

e) veiller à ce que le personnel soit suffisamment formé et au fait des questions de sécurité informatique pertinentes dans le cadre de ses fonctions ;
f) veiller à ce que les vendeurs, les sous-traitants et les fournisseurs qui travaillent pour eux respectent les exigences et les processus qui figurent dans le PSI ;
g) suivre, surveiller et signaler les incidents de sécurité informatique, et intervenir si un tel incident se produit ;
h) appliquer les mesures de sécurité informatique.

Responsabilités individuelles

A.14. Chaque membre d'une organisation devrait être responsable de l'exécution de ses propres tâches, conformément au PSI. En particulier, chacun doit :

a) comprendre l'importance et le rôle de la sécurité informatique pour la sécurité nucléaire ;
b) comprendre la politique de l'organisation en matière de sécurité informatique ;
c) connaître les procédures de sécurité informatique propres à son poste ;
d) agir dans les limites prévues par la politique de sécurité informatique ;
e) signaler aux responsables tout changement qui pourrait porter atteinte à la sécurité informatique ;
f) signaler aux responsables ou aux points de contact concernés tout incident ou tout incident possible qui compromettrait la sécurité informatique ;
g) assister à une formation initiale sur la sécurité informatique, et suivre régulièrement des remises à niveau dans ce domaine.

Responsabilités transversales

A.15. La sécurité informatique est un domaine transversal qui a une incidence sur de nombreuses activités et de nombreux services différents et qui en subit l'influence. Pour être efficace, elle requiert une coordination et une coopération étroites entre les différents services. Les paragraphes A.16 à A.38 exposent certaines responsabilités des services, ainsi que des questions transversales.

Protection physique

A.16. Le plan de sécurité du site et le PSI jouent un rôle essentiel dans l'élaboration d'un plan de sécurité complet pour l'installation, et doivent donc

se compléter. Les RNS sont protégées par des exigences relatives au contrôle des accès physique, et la compromission de systèmes informatiques peut entraîner la dégradation ou la perte des fonctions de protection physique. En outre, des adversaires peuvent chercher à attaquer une installation en lançant de manière coordonnée une cyberattaque et une attaque physique (c'est-à-dire une attaque combinée).

A.17. Si les services qui sont responsables du plan de sécurité du site et du PSI sont différents, ils devraient communiquer et coordonner leurs efforts afin d'assurer la cohérence entre les plans pendant le processus d'élaboration et d'examen.

A.18. L'exploitant devrait attribuer des responsabilités et des rôles adaptés au personnel chargé de la protection physique dans le cadre de l'élaboration, de la mise en œuvre et de la maintenance du PSI. Ces responsabilités et ces rôles peuvent être les suivants :

a) veiller à ce que les accès aux RNS soient uniquement des accès autorisés ;
b) détecter les supports amovibles et les appareils mobiles interdits qui entrent dans l'installation ;
c) détecter les enlèvements non autorisés d'informations ou de ressources d'informations qui se trouvent dans l'installation ;
d) s'assurer que les politiques qui concernent les supports amovibles ou des appareils mobiles qui sont autorisés dans l'installation sont appliquées (rechercher les logiciels malveillants avant toute entrée dans l'installation, par exemple) ;
e) signaler les incidents de sécurité informatique (détection de logiciels malveillants ou enlèvement non autorisé de ressources d'informations, par exemple), conformément à la procédure d'intervention prévue en cas d'incident ;
f) évaluer les pratiques en matière de sécurité de l'information (contrôles documentaires, contrôles portant sur les salles et les meubles fermés à clef, mise en place de normes pour les appareils qui protègent physiquement les ressources d'informations, contrôle des accès et surveillance, par exemple) ;
g) appuyer l'intervention en cas d'incident de sécurité informatique qui a un rapport avec le système de protection physique.

Technologies de l'information

A.19. Dans une installation nucléaire, le personnel informatique effectue des tâches d'assistance, d'administration et de gestion. Ces tâches peuvent comprendre des activités où entrent en jeu des ressources numériques qui sont

utilisées pour élaborer et stocker les procédures d'exploitation et de maintenance, les instructions de travail, les systèmes de gestion de la configuration, les documents de conception et les manuels d'exploitation.

A.20. Le PSI devrait recenser clairement les ressources numériques et les réseaux correspondants dont le personnel informatique est responsable. Le personnel informatique devrait surveiller les ressources numériques concernées et les réseaux correspondants**,** et signaler les incidents de sécurité informatique à la direction et au spécialiste de la sécurité informatique, conformément au plan d'intervention en cas d'incident.

A.21. Le personnel informatique devrait prendre des mesures pour que les incidents de sécurité informatique qui concernent des ressources numériques (qui ne sont pas des RNS) et des réseaux ne portent pas atteinte à des RNS.

Personnel technique

A.22. Il devrait y avoir des procédures formelles pour assurer la coordination entre le service technique et d'autres services compétents afin que les mesures relatives à la sécurité et à la sûreté nucléaires soient conçues et mises en œuvre de manière intégrée, conformément aux exigences qui figurent dans le PSI. Le personnel technique devrait être conscient que la sûreté nucléaire, la protection physique et la sécurité informatique sont des domaines distincts pour lesquels l'appui d'experts dûment qualifiés dans ces différents domaines est nécessaire.

A.23. Le personnel technique devrait présenter des éléments qui montrent l'efficacité de l'architecture de sécurité informatique (c'est-à-dire de l'ASID) et qui peuvent être comparés aux résultats attendus à la suite de la GRSI pour l'installation et ses systèmes.

A.24. Le personnel technique devrait piloter ou appuyer la GRSI pour les systèmes dont il est responsable.

A.25. Le personnel technique devrait donner des orientations aux vendeurs, aux sous-traitants et aux fournisseurs concernant les exigences de sécurité informatique pour les systèmes de l'installation. Il est chargé d'examiner les conceptions élaborées par les vendeurs afin de s'assurer qu'ils respectent les exigences de sécurité informatique. Il devrait demander aux vendeurs de confirmer que les produits qui ont été livrés à l'installation ont été mis au point dans un environnement sécurisé. Le personnel technique devrait aussi établir et appliquer une procédure d'examen de la documentation technique des produits,

de réception des produits sur site et de test de ces produits afin de garantir le respect des exigences de sécurité informatique.

A.26. Le personnel technique devrait veiller à ce que des activités de suivi de la performance soient mises en place afin de s'assurer que les mesures de sécurité informatique restent efficaces.

Exploitation

A.27. Le PSI devrait recenser les systèmes et les réseaux de l'installation dont le personnel d'exploitation est responsable. Le personnel d'exploitation doit faire en sorte que les exigences qui s'appliquent à ces systèmes et qui figurent dans le PSI soient respectées.

A.28. Le personnel d'exploitation devrait veiller à ce que l'ASID et les mesures de sécurité informatique qui relèvent de sa responsabilité soient conservées et restent efficaces.

A.29. Le personnel d'exploitation devrait veiller à ce que des procédures soient mises en place pour détecter les incidents de sécurité informatique et pour déclencher des interventions concernant les systèmes et les réseaux qui relèvent de sa responsabilité.

A.30. Le personnel d'exploitation devrait inciter tout le personnel à être attentif aux situations afin que seuls les supports amovibles et les appareils mobiles autorisés soient utilisés dans l'installation.

Organisation des achats et de la chaîne d'approvisionnement

A.31. Les produits achetés devraient répondre aux spécifications qui ont été définies pour le matériel, les appareils ou les composants. Ces spécifications devraient comprendre des exigences de sécurité informatique appropriées.

A.32. Dans le cadre des achats, il faudrait effectuer des contrôles afin de vérifier que les RNS qui ont été mises au point ou fournies par les vendeurs et les fournisseurs intègrent des mesures de sécurité informatique qui sont conformes au niveau de sécurité informatique qui a été attribué aux RNS concernées.

A.33. Les acheteurs devraient comprendre qu'il est important de définir des exigences de sécurité informatique propres aux achats. Des accords juridiques,

par exemple des licences ou des contrats, devraient être conclus avec les vendeurs, les sous-traitants et les fournisseurs pour faire appliquer de telles exigences.

A.34. Les acheteurs et le personnel technique peuvent ignorer qu'un appareil multi-usage sera considéré comme une RNS si l'exploitant s'en sert pour un usage particulier. Il faudrait alors tenir compte de la possibilité qu'un tel appareil puisse être utilisé comme RNS une fois acheté, et des exigences de sécurité informatique appropriées devraient être appliquées.

A.35. Les acheteurs devraient collaborer avec le personnel technique afin que les exigences de sécurité informatiques soient imposées par contrat aux vendeurs, aux sous-traitants ou aux fournisseurs, et que les conceptions qui sont soumises par les vendeurs, les sous-traitants ou les fournisseurs respectent les exigences de sécurité informatiques. Les acheteurs devraient également informer le personnel technique lorsqu'un vendeur, un sous-traitant ou un fournisseur de RNS ne peut probablement ou absolument plus fournir d'assistance.

A.36. Les acheteurs devraient envisager d'évaluer les vendeurs, les sous-traitants et les fournisseurs avant de conclure un contrat. Dans ce cadre, ils peuvent analyser les procédures qui sont appliquées par le vendeur, le sous-traitant ou le fournisseur concernés pour concevoir, mettre au point, tester et assembler une RNS, ou fournir une assistance sur cette ressource, ou peuvent évaluer la formation et l'expérience du vendeur, du sous-traitant ou du fournisseur concernant la conception de RNS ayant le niveau de sécurité informatique requis. Cette démarche peut aussi permettre a) de déterminer si les vendeurs, les sous-traitants ou les fournisseurs principaux ont mis en place des mesures de sécurité afin d'évaluer correctement la fiabilité de leurs vendeurs, de leurs sous-traitants et de leurs fournisseurs, et b) de vérifier la provenance des RNS, des composants de RNS, des logiciels et des mises à jour qui ont été livrés à l'exploitant.

A.37. Les acheteurs devraient veiller à ce que tous les vendeurs, tous les sous-traitants et tous les fournisseurs de RNS disposent de procédures pour avertir l'exploitant en cas d'incident qui concerne la chaîne d'approvisionnement et qui pourrait porter atteinte à une RNS (compromission de composants d'une RNS, de techniques utilisées par une RNS, de processus de développement ou d'informations sensibles, par exemple).

A.38. Les acheteurs devraient veiller à ce que les vendeurs, les sous-traitants et les fournisseurs de RNS disposent d'un circuit de distribution fiable pour la livraison de RNS, de composants de RNS, de logiciels et de mises à jour à l'exploitant.

GESTION DES RISQUES, DES VULNÉRABILITÉS ET DU RESPECT DES RÈGLES

Relations externes relatives à la gestion du risque

A.39. Dans le cadre de la gestion du risque, il faudrait analyser les relations externes (c'est-à-dire les relations avec les vendeurs, les sous-traitants et les fournisseurs). Les responsabilités relatives au respect des exigences qui découlent de la GRSI pour un système devraient être définies par contrat.

A.40. L'exploitant devrait contrôler et inspecter les activités concernées des vendeurs, des sous-traitants et des fournisseurs afin de s'assurer que les exigences de sécurité informatique qui figurent dans le PSI sont respectées. Les contrats qui sont conclus avec les vendeurs, les sous-traitants et les fournisseurs devraient permettre à l'exploitant d'exécuter cette tâche.

A.41. Dans le cadre de la gestion des risques, l'exploitant devrait tenir compte des prescriptions réglementaires et des autres prescriptions externes qui ont une incidence sur la sécurité informatique. Il devrait permettre aux autorités compétentes d'assurer un contrôle et de mener des inspections concernant les mesures qui ont été prises pour respecter ces prescriptions.

Activités d'assurance en sécurité informatique

A.42. Les activités d'assurance en sécurité informatique devraient être menées pendant toute la durée de vie de l'installation, selon les modalités décrites dans les sections 4 et 5. Les activités d'assurance effectuées dépendent du stade où se trouve l'installation. La référence [8] donne des précisions sur les activités d'assurance qui sont applicables aux systèmes de contrôle-commande.

A.43. Dans le cadre de ce type d'activités, l'exploitant peut effectuer des évaluations (y compris des vérifications), des examens, des exercices et des tests[46].

A.44. L'exploitant devrait vérifier que le PSI est conforme à sa politique de sécurité informatique (des évaluations de la sécurité informatique peuvent par exemple être menées pour vérifier que les exigences de sécurité informatique qui découlent de la politique de l'exploitant sont respectées). Dans ce cadre, plusieurs évaluations complémentaires peuvent être nécessaires pour examiner

[46] Les exercices et les tests peuvent aussi servir pour d'autres éléments du PSI, comme les procédures de sécurité ou la gestion du personnel.

différents éléments du PSI et leur mise en œuvre. Les résultats des évaluations comprennent une liste des lacunes et des bonnes pratiques, ainsi que des suggestions d'améliorations.

A.45. Les activités d'assurance devraient servir de guide pour l'amélioration continue du PSI. À cette fin, elles devraient être reproductibles et fiables, et devraient être menées régulièrement et à chaque fois qu'un incident de sécurité informatique se produit ou que la menace évolue.

A.46. Les activités d'assurance devraient comprendre une évaluation de l'efficacité de l'organisation et des mesures qui ont été mises en place pour que la sécurité informatique soit effective et efficace.

A.47. Les activités d'assurance peuvent être menées par un groupe interne ou externe. La sécurité informatique peut par exemple être évaluée par une équipe interne à titre d'auto-évaluation. Si l'évaluation est effectuée par un groupe externe, son résultat doit être contrôlé en interne.

A.48. Les activités d'assurance internes ou externes devraient être complétées par des évaluations indépendantes, qui sont menées par des tiers. Les évaluateurs indépendants doivent pouvoir interroger les membres du personnel concernés et avoir accès aux documents et au matériel nécessaires. Ils peuvent faire partie du personnel de l'organisme exploitant, mais doivent être indépendants des personnes qui exécutent, vérifient ou supervisent les travaux évalués.

A.49. Il faudrait déterminer si les évaluateurs indépendants ou externes sont fiables avant de les autoriser à accéder aux informations ou à l'installation, car les activités d'assurance exigent souvent de consulter des informations sensibles sur la sécurité informatique. On trouvera de plus amples informations sur les enquêtes de sécurité dans la référence [6].

A.50. Les procédures applicables aux évaluations indépendantes devraient prévoir des restrictions pertinentes à l'enlèvement, à l'utilisation, à la conservation et à la distribution des informations sensibles, et devraient imposer de supprimer ce type d'informations lorsqu'elles ne sont plus nécessaires.

A.51. Il faudrait développer et maintenir les capacités à mener des activités d'assurance, afin de pouvoir faire face à l'évolution des techniques et de la cybermenace. Ces capacités sont nécessaires pour les membres du personnel qui sont chargés des activités d'assurance, mais aussi pour l'autorité compétente, qui peut être amenée à examiner les résultats de ces activités.

Cadre de l'évaluation

A.52. L'exploitant devrait déterminer quelles fonctions et quels aspects de la sécurité seront évalués.

A.53. Le cadre de l'évaluation devrait être adapté au stade où se trouve l'installation. Ainsi, une évaluation complète de la sécurité informatique peut être nécessaire à certaines étapes, tandis qu'à d'autres étapes, une évaluation de certaines fonctions ou de certains aspects de la sécurité pourrait être plus judicieuse. (On trouvera une liste d'activités d'évaluation pour différentes étapes de la vie d'un système de contrôle-commande dans la référence [8].)

Techniques d'évaluation

A.54. L'équipe d'évaluation devrait utiliser les techniques suivantes, le cas échéant, pour acquérir les informations dont elle a besoin pour formuler ses conclusions et ses recommandations :

a) examen des documents et des dossiers (législation, réglementation et dossiers de l'installation, par exemple) ;
b) entretiens avec des membres du personnel des organisations concernées (personnel de l'autorité compétente, personnel d'exploitation de l'installation et représentants d'autres organisations, par exemple) ;
c) observation directe de l'organisation, de ses pratiques et de ses systèmes, ainsi que de l'application des mesures de sécurité informatique.

Élaboration du rapport d'évaluation

A.55. Dans le cadre de l'évaluation, la collecte des données consiste à consigner les observations et les données pertinentes qui ont été recueillies lors de l'examen des documents et des dossiers, au cours des entretiens avec les membres du personnel et pendant l'observation directe. Les observations peuvent être pertinentes à titre individuel, mais peuvent aussi faire collectivement apparaître une tendance dans l'installation ou dans l'organisation, et il pourrait être nécessaire d'infléchir cette tendance. L'exploitant devrait donc répertorier les observations qui semblent confirmer des tendances ou des problèmes récurrents.

A.56. Il faudrait analyser les observations par comparaison avec des règles à respecter, comme la réglementation nationale, les procédures de l'organisation ou les normes du secteur, selon le cas. Un enseignement est tiré si une prescription réglementaire ou une procédure interne n'est pas respectée. Les références qui

sont utilisées pour tirer un enseignement devraient être définies clairement et être approuvées pendant la préparation de l'évaluation.

A.57 Les observations ne permettent pas toujours de tirer des enseignements, et les enseignements n'ont pas tous un aspect négatif : ils mettent parfois en évidence des bonnes pratiques, des pratiques organisationnelles ou des procédures constituant une méthode efficace et généralement nouvelle qui permet d'atteindre les objectifs de sécurité. Les bonnes pratiques qui pourraient être adoptées par d'autres organisations pour améliorer la sécurité informatique en leur sein peuvent être répertoriées et signalées.

A.58. Outre les enseignements et les bonnes pratiques, l'équipe d'évaluation peut formuler des recommandations et des propositions dans le rapport d'évaluation où figurent les enseignements.

A.59. S'il y a lieu, les recommandations donnent la marche à suivre pour respecter les prescriptions juridiques et réglementaires ou les normes internationales (obligations conventionnelles, par exemple). En principe, elles n'expliquent pas comment corriger un problème, mais se contentent de mettre en évidence un problème qui doit être corrigé.

A.60. Les propositions donnent des informations complémentaires sur certains enseignements, et portent notamment sur des mesures de redressement ou d'atténuation. Ces informations ne proviennent pas nécessairement des orientations relatives à la réglementation, et découlent souvent des normes techniques et des bonnes pratiques du secteur concerné.

Exemple de méthode d'évaluation

A.61. On trouvera un exemple de méthode d'évaluation dans la référence [23]. Il permet de procéder à une évaluation interdomaines des fonctionnalités et de la sécurité informatique d'une installation. Il contribue ainsi à prendre en compte les processus et les systèmes qui exécutent des fonctions de l'installation concernée, telles les opérations, la sûreté, la sécurité ou la préparation et la conduite des interventions d'urgence.

Plan de gestion de la configuration

A.62. Les mesures de sécurité informatique qui protègent les RNS devraient être gérées dans le cadre d'un plan de gestion de la configuration. Ce plan devrait être élaboré et mis en œuvre par l'exploitant, et devrait :

a) attribuer les rôles et les responsabilités appropriés, et définir les processus et les procédures de gestion de la configuration ;
b) décrire en détail la configuration des RNS et leurs liens d'interdépendance ;
c) déterminer à partir de quelle étape de la mise au point du système la gestion de la configuration doit s'appliquer aux RNS ;
d) définir un moyen d'identification des RNS et une procédure pour la gestion des mesures de sécurité informatique qui permettent de les protéger.

Configuration de référence

A.63. Une configuration de référence des RNS devrait être gérée dans le cadre du contrôle de la configuration. La configuration de référence devrait être mise à jour au besoin pour tenir compte des performances du système et, par exemple, pour renforcer la sécurité des systèmes ou tenir compte des effets des modifications sur la sécurité informatique.

Renforcement de la sécurité des systèmes

A.64. L'exploitant devrait envisager de mettre en place une procédure systématique pour renforcer la sécurité des RNS. Le renforcement de la sécurité d'un système consiste à appliquer un ensemble de mesures de contrôle administratif et technique pour diminuer le risque d'exposition des composants d'un système informatique aux cyberattaques et pour désactiver les composants matériels ou logiciels qui ne sont pas nécessaires au fonctionnement ou à la maintenance du système concerné. Les composants matériels et les logiciels qui sont généralement retirés ou désactivés sont les suivants :

a) interfaces ou protocoles réseau inutilisés (y compris les pilotes de périphériques) ;
b) périphériques inutilisés (y compris les pilotes de périphériques) ;
c) gestion des supports amovibles ;
d) communications filaires ou sans fil interdites ;

e) services de messagerie qui n'ont pas de rapport avec les fonctions exécutées par le système concerné ;
f) services et applications fournis par des médias sociaux ;
g) serveurs ou clients pour des services inutilisés ;
h) compilateurs installés sur des postes de travail et des serveurs, sauf ceux qui sont utilisés pour la mise au point du système ;
i) compilateurs pour des langages informatiques qui ne sont pas utilisés par le système de contrôle ;
j) protocoles réseau et protocoles de communication inutilisés ;
k) fonctions d'administration, de diagnostic et de gestion du réseau et du système qui ne sont pas utilisées ;
l) sauvegarde des fichiers, des bases de données et des programmes qui ont été utilisés pendant la mise au point du système ;
m) données et fichiers de configuration qui ne sont pas utilisés ;
n) programmes et macrocommandes qui ont été fournis à titre d'exemple ;
o) utilitaires de traitement de texte qui ne sont pas utilisés ;
p) extensions d'applications qui ne sont pas utiles (pour des navigateurs, par exemple) ;
q) jeux.

A.65. Le renforcement de la sécurité devrait être obligatoire pour les RNS qui utilisent des composants disponibles dans le commerce, et seules les fonctionnalités de ces composants qui sont nécessaires à l'exécution des fonctions des RNS (ou du système concerné) devraient être conservées.

A.66. Le renforcement de la sécurité devrait avoir pour but de réduire la quantité de données qui doivent être surveillées et analysées pour déterminer si la ressource numérique ou le système qui est protégé est en sécurité. Il peut également aider l'exploitant à mieux comprendre le comportement normal et les fonctionnalités du système concerné.

A.67. Pour renforcer la sécurité, on peut utiliser des outils qui permettent de garantir que seules les versions approuvées des programmes informatiques autorisés peuvent s'exécuter sur la RNS concernée. Les dossiers sur le renforcement de la sécurité devraient comprendre la documentation fournie avec les bibliothèques qui sont utilisées par les outils en question.

A.68. Pour le renforcement de la sécurité, il faudrait utiliser uniquement des mécanismes de mise à jour sécurisés et fiables. Il faudrait évaluer ces mécanismes de mise à jour afin de s'assurer qu'ils présentent un risque très faible ou nul d'être utilisés pour attaquer le système qui est mis à jour. Dans ce cadre, il faudrait

par exemple vérifier que chaque mise à jour de système est identifiée par une signature cryptée du vendeur autorisé.

Considérations sur les mises à jour de logiciels

A.69. Les vendeurs fournissent des mises à jour de sécurité, généralement sous forme de correctifs, afin de remédier aux vulnérabilités qui ont été détectées dans leurs systèmes. Comme les modifications des systèmes de sûreté s'effectuent selon des procédures coûteuses en ressources, il n'est pas toujours possible d'installer immédiatement un correctif, de sorte que le système concerné peut être exposé à un risque pendant un certain temps.

A.70. L'exploitant devrait demander au vendeur la liste des composants logiciels qui sont utilisés dans les systèmes, ainsi que les mises à jour de logiciels applicables (notamment des correctifs de sécurité), ou dresser lui-même cette liste.

A.71. L'exploitant devrait avoir établi une procédure formelle pour s'assurer que les mises à jour de sécurité informatique qui concernent le matériel et les composants sont évaluées afin de déterminer leur applicabilité et leur effet et, tout particulièrement, si une installation immédiate est nécessaire pour réduire la vulnérabilité correspondante. L'exploitant devrait installer la mise à jour ou mettre en place des mesures compensatoires efficaces afin d'empêcher que la vulnérabilité en question ne soit exploitée.

A.72. L'exploitant devrait définir et mettre en œuvre des mesures de sécurité informatique qui permettent d'assurer une solide sécurité afin que les mises à jour et les vulnérabilités auxquelles elles remédient puissent être évaluées sans que ces vulnérabilités soient exploitées pendant l'évaluation et l'installation. Ainsi, le renforcement de la sécurité d'un système peut permettre de réduire le nombre de mises à jour de sécurité qui doivent être évaluées et installées, car il n'est pas nécessaire d'installer les mises à jour qui ne portent que sur des fonctionnalités supprimées ou désactivées.

PROCÉDURES DE SÉCURITÉ

Surveillance des systèmes

A.73. Chaque système qui est pris en compte par le PSI devrait se voir attribuer un responsable (par exemple un ingénieur spécialiste du système en question), qui est chargé de surveiller ce système.

A.74. La surveillance d'un système devrait comprendre la surveillance de l'état et de l'efficacité des mesures de sécurité informatique.

A.75. Le responsable d'un système devrait être chargé de faire en sorte que les supports de récupération et les informations sur la configuration soient à jour, et que le plan de remise en état du système concerné soit tenu à jour et puisse être exécuté si nécessaire (par exemple dans le cadre d'exercices réguliers).

Contrôle des changements apportés à la configuration

A.76. Il faudrait contrôler les changements qui sont apportés à la configuration des RNS, l'analyse de leurs conséquences pour la sécurité étant expressément prise en compte. Un cadre ou le responsable du système concerné devrait approuver les changements à apporter à la configuration d'une RNS avant qu'ils ne soient mis en œuvre. Cette approbation devrait être consignée de manière formelle.

A.77. Le spécialiste de la sécurité informatique devrait examiner les activités associées à la modification de la configuration d'une RNS. Il faudrait consigner, conserver et réexaminer les modifications qui sont apportées à la configuration des RNS.

A.78. Le spécialiste de la sécurité informatique devrait assumer la responsabilité générale de la supervision du contrôle des modifications de la configuration qui concernent des RNS, mais peut déléguer cette responsabilité aux responsables des ressources. Il devrait adopter des dispositions afin que la supervision soit efficacement assurée et coordonnée.

Exercices de sécurité informatique

A.79. En pratique, le suivi constant de l'efficacité du PSI devrait comprendre une évaluation de ses composantes grâce à des exercices.

A.80. Les exercices qui portent sur la sécurité de l'information et sur la sécurité informatique peuvent allier évaluation et formation. Dans le cadre des exercices, il faudrait aussi simuler des scénarios dans lesquels des attaques combinées (cyberattaques et attaque physiques coordonnées) sont lancées.

A.81. Le système de gestion de la sécurité de l'information et de la sécurité informatique peut faire l'objet d'exercices gradués en fonction du rôle et du niveau hiérarchique du personnel concerné. Les exercices permettent d'évaluer avec

quelle efficacité les processus opérationnels et les communications fonctionnent en cas d'incident de sécurité informatique. Ils permettent également de former les membres du personnel qui participent à la gestion et à l'intervention, quelle que soit leur position hiérarchique.

A.82. L'exploitant devrait prendre en considération les avantages des exercices suivants :

a) exercices qui portent sur les procédures de sécurité et visent à évaluer dans quelle mesure ces procédures permettent d'atteindre les objectifs du PSI ;
b) exercices qui sont destinés à entraîner le personnel à appliquer les procédures de sécurité, et qui visent donc à mieux faire connaître ces procédures, l'objet des tâches qui les composent et les interventions en cas d'incident de sécurité informatique.

Tests d'intrusion

A.83. L'exploitant devrait déterminer s'il doit effectuer des tests d'intrusion (qui simulent des cyberattaques réelles contre des systèmes réels) dans le cadre de l'évaluation de la sécurité informatique d'un système ou d'une ressource numérique, en tenant compte des aspects juridiques, de la sûreté, de la sécurité et de la capacité de l'exploitant à éviter ou à annuler les effets néfastes que ces tests pourraient avoir sur la ressource numérique ou le système concernés. Les limites à l'utilisation des tests d'intrusion pour les systèmes de contrôle-commande sont décrites dans la référence [8].

A.84. La méthode précise qui est employée pour une cyberattaque dépendant fortement de la configuration exacte du système attaqué, un système testé doit être aussi proche que possible du système réel. Des procédures de sauvegarde et de restauration complètes devraient être en vigueur pour remettre le système dans un état stable connu si un test d'évaluation crée une situation anormale.

A.85. Le calendrier, le budget et les objectifs des tests, les produits attendus, le matériel et les logiciels à utiliser, les moyens nécessaires, les règles de fonctionnement et une procédure de remise en état devraient figurer dans un plan de tests.

A.86. Les techniques de tests peuvent notamment être les suivantes :

a) Le *fingerprinting*, qui consiste à détecter et à quantifier toutes les communications établies entre les composants d'un système ou en leur sein, et à analyser les effets de ces communications sur les RNS sur lesquelles portent les tests. Cette technique permet d'obtenir les résultats suivants :
   i) fonctionnement de base du réseau ;
   ii) diagramme précis du réseau ;
   iii) détection des périphériques non autorisés et des communications malveillantes ;
   iv) vérification du fait que les appareils qui assurent une protection aux limites de zone fonctionnent comme prévu ;
   v) mise en évidence de moyens permettant de mieux définir les zones et de mieux protéger le périmètre.

b) Les tests à données aléatoires, qui visent à déceler des anomalies ou des vulnérabilités dans un composant ou un système par injection automatique d'une grande variété de données afin de déterminer quels types de données et quels lieux d'injection pourraient être utilisés à des fins malveillantes. Ils peuvent permettre de détecter les faiblesses des logiciels, et donner des indications sur la solidité d'un système.

A.87. Des indicateurs de sécurité informatique peuvent servir de référence pour évaluer les vulnérabilités. Des indicateurs bien choisis et fréquemment utilisés (système de notation des vulnérabilités communes, par exemple) peuvent permettre de comparer les vulnérabilités entre différents systèmes. L'exploitant devrait déterminer par quels moyens les vulnérabilités détectées pourraient être utilisées, et devrait prendre des mesures pour empêcher qu'elles ne soient exploitées. Il devrait envisager de signaler toutes les vulnérabilités afin qu'elles soient ajoutées dans une base de données nationale des vulnérabilités.

Intervention en cas d'incident de sécurité informatique

A.88. Le personnel qui est chargé de la sécurité informatique devrait être tenu de signaler tous les incidents de sécurité informatique présumés, conformément au plan d'intervention en cas d'incident. L'exploitant devrait envisager d'organiser des formations de sensibilisation spécialisées pour les membres du personnel qui occupent un poste essentiel sans lien direct avec la sécurité informatique, mais qui pourraient subir les conséquences des failles de sécurité informatique.

A.89. L'exploitant devrait disposer d'un plan d'urgence pour détecter les incidents de sécurité informatique qui peuvent porter atteinte aux RNS (et tous les autres événements de sécurité nucléaire qui donnent lieu à un incident de sécurité informatique), et intervenir si un tel incident se produit. Ce plan devrait

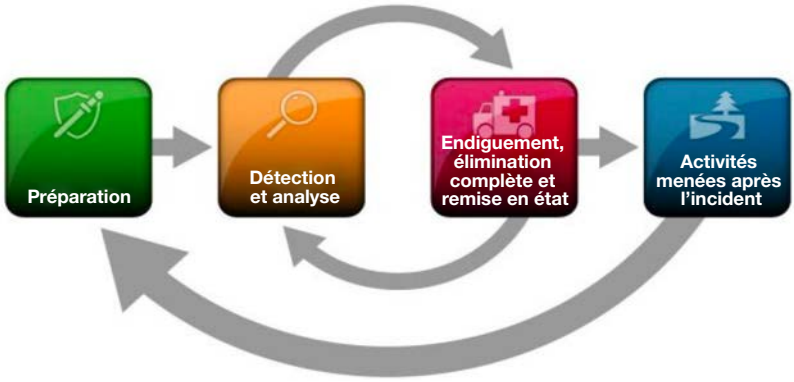

FIG. 10. Intervention en cas d'incident de sécurité informatique (repris de la référence [24], avec l'aimable autorisation du NIST).

contenir des procédures permettant de déterminer l'emplacement et la nature de la menace, de prévenir tout acte malveillant ou d'en atténuer les conséquences, d'informer les autorités compétentes et de rétablir la situation.

A.90. Une intervention en cas d'incident est un ensemble d'activités (voir fig. 10), et chacune d'entre elles devrait être étudiée.

A.91. Lors d'un incident de sécurité informatique, la confidentialité, l'intégrité ou la disponibilité des données traitées, stockées ou transmises par un système informatique peuvent être compromises. Lors d'un tel incident, une politique de sécurité informatique explicite ou implicite, une règle d'utilisation ou une pratique de sécurité informatique habituelle peuvent aussi ne pas avoir été respectées. Certains événements défavorables (inondation, incendie, coupure d'électricité ou canicule, par exemple) peuvent provoquer l'arrêt d'un système, mais ne résultent pas d'un acte malveillant et ne sont donc pas considérés comme des incidents de sécurité informatique.

A.92. Un incident de sécurité informatique peut devenir un incident lié à la sécurité de l'information ou une atteinte à la sécurité de l'information si des informations sensibles ont certainement ou probablement été compromises. On trouvera des exemples d'informations qui peuvent être sensibles pour une installation nucléaire dans la référence [5].

A.93. L'exploitant devrait constituer une équipe locale d'intervention face aux incidents de sécurité informatique, qui sera chargée d'intervenir si un

incident de sécurité informatique se produit dans l'installation. La taille, la composition et les compétences de cette équipe dépendront de la nature et de l'infrastructure informatique de l'organisation concernée, mais des personnes ayant des compétences en sécurité nucléaire, en sûreté nucléaire, en préparation et en conduite des interventions d'urgence, et en sécurité informatique, devraient en faire partie. Cette équipe peut être composée des mêmes personnes que l'équipe de sécurité informatique, ou certaines personnes peuvent faire partie des deux équipes.

A.94. Une équipe d'intervention informatique d'urgence est un service technique qui fournit des moyens d'assistance et d'intervention lorsqu'un incident de sécurité informatique se produit. Elle peut exister à différents niveaux (à l'échelle nationale ou locale, ou d'un secteur industriel, par exemple). L'équipe d'intervention informatique d'urgence peut être disponible en complément des moyens d'intervention dont dispose un organisme exploitant qui fait face à un incident de sécurité informatique. Pour la planification des activités d'intervention de l'organisme exploitant, il faudrait prendre en compte la capacité de cette équipe à intervenir en période de crise.

A.95. L'exploitant devrait veiller à ce que chaque membre de l'équipe d'intervention informatique d'urgence qui jouerait un rôle en cas d'intervention et tous les membres de l'équipe d'intervention face aux incidents de sécurité informatique participent à des exercices. Il faudrait tenir compte des contacts qui auront lieu entre l'équipe d'intervention informatique d'urgence et l'équipe d'intervention face aux incidents de sécurité informatique, y compris dans le cadre des activités préparatoires (accord préalable donné aux membres de l'équipe d'intervention informatique d'urgence pour qu'ils puissent accéder à certaines zones de l'installation, par exemple). Les exercices devraient permettre de tester les éléments essentiels qui sont échangés entre les autorités compétentes, l'équipe d'intervention informatique d'urgence, l'équipe d'intervention face aux incidents de sécurité informatique et le personnel d'exploitation sur site, qui sont représentés sur la figure 11.

Phases d'une intervention en cas d'incident de sécurité informatique

Préparation

A.96. La planification des actions en phase de préparation consiste notamment à élaborer une stratégie qui guidera les processus opérationnels en cas d'intervention face à un incident de sécurité informatique, à définir les rôles et les responsabilités de tous ceux qui participent à ce type d'intervention, à rédiger des

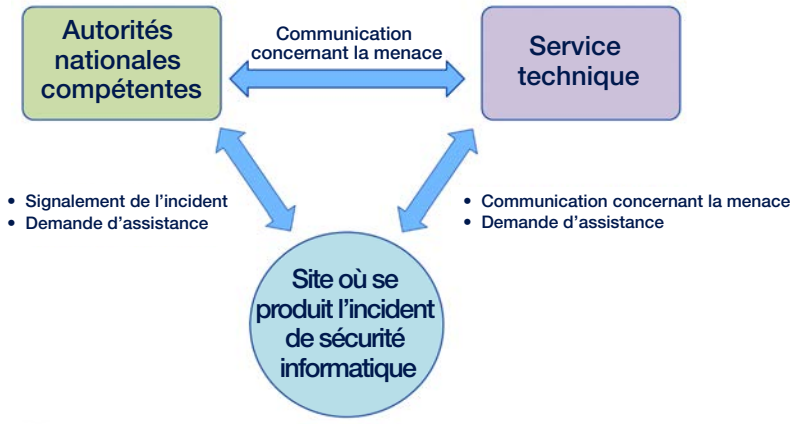

FIG. 11. Relations entre les différents acteurs en cas d'intervention faisant suite à un incident de sécurité informatique.

procédures conformes à la stratégie et à répertorier les ressources disponibles pour une telle intervention. Il faudrait définir clairement les exigences et les critères à appliquer en cas d'intervention face à un incident de sécurité informatique. Le plan d'intervention devrait être approuvé par la direction.

Détection et analyse

A.97. En phase de détection et d'analyse, l'équipe d'intervention face aux incidents de sécurité informatique devrait être responsable de la caractérisation technique de l'incident. Dans le cadre des activités de détection, il faut notamment veiller à ce que les données soient suffisamment surveillées pour faciliter la détection grâce à la collecte et à la conservation des informations relatives à de possibles incidents. L'équipe d'intervention face aux incidents de sécurité informatique peut se placer dans un cadre de tests et d'évaluation spécifique pour analyser les incidents sans perturber de systèmes qui fonctionnent ni modifier d'éléments de preuve potentiels.

A.98. Les activités d'analyse peuvent dépasser les compétences de cette équipe, et la caractérisation technique initiale de l'incident et certains aspects de l'analyse peuvent exiger des moyens importants. Les priorités de l'analyse sont généralement les suivantes :

a) déterminer les effets possibles de l'incident de sécurité informatique sur la sécurité nucléaire, la sûreté et la préparation et la conduite des

interventions d'urgence, et définir les actions à mener pour assurer la sûreté de l'installation ;

b) déterminer l'ampleur de l'incident afin d'envisager une intervention appropriée ;

c) déterminer quel préjudice l'incident peut causer (perte d'informations, dommages matériels dans l'installation et perception du public) ;

d) pour cet incident, déterminer quelles sont l'intention immédiate de l'adversaire et les futures menaces possibles, y compris la possibilité que les effets de l'incident soient exploités dans le cadre d'une attaque ultérieure ;

e) déterminer la cause profonde de l'incident et définir les mesures à prendre pour prévenir les futurs incidents de nature similaire ou en atténuer les effets ;

f) découvrir quel est l'adversaire et établir son profil, y compris les techniques et les outils utilisés, ainsi que les vulnérabilités exploitées par l'adversaire.

Atténuation (endiguement, élimination complète et remise en état)

A.99. Les actions d'atténuation visent à endiguer l'incident de sécurité informatique, à supprimer tous les logiciels malveillants ou à corriger tous les dysfonctionnements ou toutes les configurations incorrectes sur les systèmes touchés, à rétablir les fonctions des systèmes et à récupérer toutes les données, à l'aide de mesures compensatoires si nécessaire. Même si les composants ou les systèmes qui sont compromis n'exécutent pas de fonction cruciale de sûreté ou de sécurité, il faut les contrôler et les remettre en état pour empêcher que l'attaque n'atteigne un composant ou un système qui exécute une fonction de ce type. Les activités d'atténuation se poursuivent et évoluent à mesure que des informations sont recueillies et analysées pendant la phase de détection et d'analyse.

A.100. Lorsqu'il étudie comment endiguer un incident de sécurité informatique, l'exploitant devrait être conscient que plusieurs composants ou plusieurs systèmes peuvent apparaître comme compromis à la suite de l'enquête sur l'incident en question. Si l'un des composants ou des systèmes compromis exécute une fonction cruciale de sûreté ou de sécurité – qui contribue par exemple à la protection de RNS, à la sûreté d'exploitation de l'installation ou à la protection de matières nucléaires ou d'autres matières radioactives –, il faut mettre en œuvre des mesures compensatoires pour pouvoir exécuter cette fonction tant que le composant ou le système concernés n'ont pas été remis en état.

A.101. Les mesures de remise en état peuvent notamment être les suivantes : remplacement à l'identique (utilisation d'un pare-feu de secours, par exemple) ; séparation entre les structures, les systèmes et les composants de sûreté et le

composant ou le système qui est compromis ; mesures temporaires, comme l'affectation d'un gardien pour contrôler l'accès à la partie concernée de l'installation afin de remplacer un système numérique de contrôle de l'accès. Les mesures de remise en état doivent permettre de remplacer la fonction touchée, mais pas nécessairement le composant ou le système qui est compromis.

Activités menées après l'incident

A.102. Dernière phase de l'intervention, les activités menées après l'incident consistent à mettre en œuvre des mesures qui visent à empêcher qu'un incident de sécurité informatique similaire ne se reproduise, qui permettront de détecter rapidement ce type d'incidents ou qui permettront d'en limiter autant que possible les conséquences. Pendant cette phase, des enseignements peuvent être tirés au sein de l'organisation, et, s'il y a lieu, des informations sur les menaces et les enseignements tirés peuvent être communiquées à toutes les personnes qui interviennent en cas d'incident de sécurité informatique, afin d'empêcher qu'une attaque similaire ne puisse réussir dans une autre installation. Les conclusions qui sont tirées après un incident peuvent permettre d'élaborer de nouvelles mesures de sécurité pour empêcher une réinfection par des logiciels malveillants, et peuvent contribuer à mettre à jour les caractéristiques de la menace et des vulnérabilités. Les autres activités qui peuvent être menées après un incident sont les suivantes : évaluer l'efficacité du PSI ; déterminer quelles formations permettraient de remédier aux insuffisances du personnel en matière d'intervention ; déterminer quelles ressources étaient nécessaires pour régler l'incident, à titre de préparation aux futurs incidents.

Communication externe

A.103. Au cours d'une intervention à la suite d'un incident de sécurité informatique, il peut être obligatoire ou souhaitable de communiquer des informations aux autorités compétentes (ou à d'autres organisations) dans certaines situations. Ces communications permettent à toute personne qui doit être renseignée sur un incident de sécurité informatique d'obtenir régulièrement des informations. Comme les personnes qui interviennent en cas d'incident seront probablement très occupées, l'exploitant doit examiner attentivement la question de la fréquence des communications et du niveau de détails fourni. Il peut envisager de désigner un point de contact unique pour la communication sur les incidents de sécurité informatique et pour les demandes d'informations qui sont soumises par des organismes externes.

Planification des activités

A.104. La planification des activités devrait permettre que les exigences de sécurité informatique à respecter pour l'exécution et la vérification des activités soient définies et planifiées.

A.105. Il faudrait définir les qualifications que doivent posséder le personnel et les sous-traitants en matière de sécurité informatique pour les activités à mener, et ces qualifications devraient être prises en compte lors de la planification. Chaque organisation responsable est tenue de signaler tous les incidents de sécurité informatique présumés, conformément au plan d'intervention en cas d'incident.

A.106. Lorsque des instructions de travail sont rédigées, les exigences de sécurité informatique doivent être prises en compte. Ces instructions peuvent notamment concerner les actions suivantes :

a) suppression de mesures de sécurité informatique (à des fins de maintenance) ;
b) application de mesures compensatoires ou autres (tant que les mesures habituelles sont désactivées) ;
c) remise en place de mesures de sécurité informatique (après une maintenance) ;
d) vérification du fait que les mesures de sécurité informatique ont été correctement rétablies.

A.107. Les instructions de maintenance devraient comprendre les instructions relatives à la configuration des paramètres de sécurité sur les appareils.

A.108. Si la maintenance exige de retirer un appareil qui n'est plus nécessaire, l'appareil en question devrait être aseptisé ou détruit de manière sécurisée.

A.109. Il faudrait répertorier les achats nécessaires en matière de sécurité informatique et les faire figurer dans le plan de travail.

CONNAISSANCE ET FORMATION

A.110. Même si les ordinateurs sont utilisés pour de nombreux aspects de la vie professionnelle et personnelle, les personnes connaissent généralement mal les techniques utilisées, les cybermenaces, les mesures de sécurité informatique et les effets possibles d'une compromission. Une sensibilisation à la sécurité informatique et une formation dans ce domaine sont nécessaires pour tous

les membres du personnel, ainsi que pour tous les sous-traitants qui ont des responsabilités en matière de sécurité nucléaire.

A.111. Les erreurs humaines provoquent ou contribuent à provoquer des incidents de sécurité informatique. Quelle que soit leur position hiérarchique, les membres du personnel doivent connaître la sécurité informatique, dont l'importance doit être régulièrement soulignée.

A.112. La conscience de l'importance de la sécurité informatique peut contribuer à la sécurité informatique pour les raisons suivantes :

a) elle permet de comprendre que la sécurité informatique contribue non seulement à la sécurité nucléaire de l'installation, mais aussi à sa sûreté ;
b) les aspects essentiels de la culture de sécurité sont compris de la même manière au sein de l'organisation ;
c) cette conscience favorise l'observation et l'accompagnement professionnel de collègues, le signalement des incidents potentiels de sécurité informatique ou de sécurité de l'information, et la compréhension des situations ;
d) elle permet de comprendre qu'une cyberattaque peut porter atteinte simultanément à plusieurs mesures de sécurité ou de sûreté, ce qui affaiblit la défense en profondeur ;
e) elle permet de résoudre les conflits qui peuvent apparaître entre les objectifs de la sûreté et les objectifs de la sécurité ;
f) elle permet de connaître et de favoriser les bonnes pratiques en matière de sécurité informatique ;
g) elle permet de mieux comprendre comment des personnes peuvent contribuer à provoquer des incidents de sécurité informatique par inadvertance.

A.113. Les indicateurs suivants peuvent être utilisés pour évaluer la sensibilisation à la sécurité informatique au sein de l'organisation :

a) les exigences de sécurité informatique sont clairement consignées et bien comprises par le personnel ;
b) des procédures et des protocoles clairs et efficaces existent pour l'utilisation des systèmes informatiques, tant à l'intérieur qu'à l'extérieur de l'organisation ;
c) le personnel connaît et comprend l'importance des mesures de sécurité informatique qui figurent dans le PSI ;
d) les systèmes informatiques restent sécurisés et utilisés conformément aux normes de sécurité informatique et aux procédures approuvées ;

e) le non-respect des procédures de sécurité informatique est considéré comme grave et regrettable ;
f) les résultats des observations, des évaluations, des tests et des exercices sont positifs (les tests montrent que les membres du personnel ne répondent pas aux courriels d'hameçonnage, par exemple) ;
g) les cadres s'engagent pleinement en faveur des initiatives relatives à la sécurité, qu'elles concernent des systèmes informatiques ou d'autres systèmes, et appuient de telles initiatives.

A.114. L'objectif d'un programme de formation en sécurité informatique est de faire en sorte que les membres du personnel et les sous-traitants possèdent les connaissances et les compétences nécessaires pour accomplir leur travail conformément aux exigences et aux procédures de sécurité informatique de l'installation. La formation à la sécurité informatique devrait être prise en compte par un système de gestion des formations déjà utilisé.

A.115. L'exploitant devrait disposer d'un programme de formation composé des éléments suivants :

a) programme de formation en sécurité informatique, qui doit avoir été suivi avec succès pour pouvoir accéder aux systèmes informatiques ; la formation devrait être à la mesure du niveau de sécurité informatique des systèmes auxquels les personnes auront accès ;
b) formation et qualification spéciales pour les personnes qui ont des responsabilités importantes en matière de sécurité (spécialiste de la sécurité informatique, équipe de sécurité informatique, autres responsables de la sécurité, chefs de projet, administrateurs réseau, ingénieurs système, concepteurs, techniciens, personnel chargé de la gestion des documents, personnel affecté aux projets, acheteurs, sous-traitants et membres de la direction, par exemple) ;
c) supports de formation mis à jour régulièrement pour tenir compte des procédures et des mesures nouvelles qui sont mises en place pour faire face aux nouvelles menaces ;
d) formation suivie régulièrement afin que le personnel connaisse bien les dernières procédures et les nouvelles menaces ;
e) obligation faite au personnel de reconnaître qu'il comprend ses responsabilités en matière de sécurité informatique ;
f) évaluations pratiques des connaissances du personnel sur ses responsabilités en matière de sécurité informatique.

A.116. Il faudrait utiliser différentes méthodes de formation, comme l'apprentissage en ligne, les formations en présentiel, les exercices pratiques et les forums de discussion[47]. Des organismes externes, notamment l'AIEA, peuvent fournir des supports à l'appui de ces activités.

A.117. Le programme de formation devrait comprendre a) des indicateurs qui permettent d'évaluer la sensibilisation à la sécurité informatique et l'efficacité de la formation et b) des procédures pour l'amélioration continue, des remises à niveau régulières du personnel et la mise à jour des formations, au besoin.

EXEMPLE DE PROCESSUS POUR LA PLANIFICATION DES INTERVENTIONS FAISANT SUITE À UN INCIDENT DE SÉCURITÉ INFORMATIQUE

A.118. On trouvera un exemple de processus pour la planification des interventions faisant suite à un incident de sécurité informatique dans la référence [25].

[47] Les forums de discussion peuvent être à l'origine de fuites qui peuvent aider l'adversaire. Il est donc déconseillé de mettre des informations sur des forums de discussion qui sont accessibles à tous.

RÉFÉRENCES

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

[2] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Recommandations de sécurité nucléaire sur la protection physique des matières nucléaires et des installations nucléaires (INFCIRC/225/Révision 5), nº 13 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2012).

[3] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Recommandations de sécurité nucléaire relatives aux matières radioactives et aux installations associées, nº 14 de la collection Sécurité nucléaire de l'AIEA , AIEA, Vienne (2012).

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

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

[6] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Mesures de prévention et de protection contre les menaces internes, nº 8-G (Rev. 1) de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2021).

[7] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Sécurité informatique pour la sécurité nucléaire, nº 42-G de la Collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2022).

[8] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Sécurité informatique des systèmes de contrôle-commande dans les installations nucléaires, nº 33-T de la collection Sécurité nucléaires de l'AIEA, AIEA, Vienne (2023).

[9] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Évaluation de la menace contre la sécurité nucléaire nationale, menaces de référence et énoncés de la menace représentative, nº 10-G (Rev. 1) de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2022).

[10] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, La sécurité tout au long de la durée de vie d'une installation nucléaire, nº 35-G de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2021).

[11] ORGANISATION INTERNATIONALE DE NORMALISATION, 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 27000:2018, ISO, Genève (2018).
[12] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Glossaire de sûreté de l'AIEA - Terminologie employée en sûreté nucléaire et en radioprotection, Édition 2018, AIEA, Vienne (2021).
[13] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Sûreté des centrales nucléaires : conception, nº SSR-2/1 (Rev. 1) de la collection Normes de sûreté de l'AIEA, AIEA, Vienne (2017).
[14] ORGANISATION INTERNATIONALE DE NORMALISATION, COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE, Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information, ISO/CEI 27005:2018, ISO, Genève (2018).
[15] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Protection physique des matières nucléaires et des installations nucléaires (Guide d'application de la publication INFCIRC/225/Révision 5), nº 27-G de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2019).
[16] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Identification des zones vitales des installations nucléaires, nº 16 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2015).
[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA Safety Standards Series No. SSG-30, IAEA, Vienna (2014).
[18] ORGANISATION INTERNATIONALE DE NORMALISATION, COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE, Technologies de l'information – Techniques de sécurité – Critères d'évaluation pour la sécurité TI, ISO/CEI 15408:2009, ISO, Genève (2009).
[19] ORGANISATION INTERNATIONALE DE NORMALISATION, COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE, Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences, ISO/CEI 27001:2013, ISO, Genève (2013).
[20] COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE, Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande – Exigences relatives aux programmes de sécurité applicables aux systèmes programmés, IEC 62645:2014, IEC, Genève (2014).
[21] ORGANISATION INTERNATIONALE DE NORMALISATION, 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 27002:2013, ISO, Genève (2013).
[22] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Nuclear Installations, IAEA Safety Standards Series No. GS-G-3.5, IAEA, Vienna (2009).

[23] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Conduite des évaluations de la sécurité informatique dans les installations nucléaires, AIEA, Vienne (2018).
[24] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Computer Security Incident Handling Guide, NIST SP 800-61, Rev. 2, NIST, Gaithersburg (2012).
[25] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Incident Response Planning at Nuclear Facilities, IAEA, Vienna (2016).

Annexe I

SCÉNARIOS D'ATTAQUE POSSIBLES CONTRE DES SYSTÈMES D'INSTALLATIONS NUCLÉAIRES

I–1. La présente annexe donne des exemples de moyens par lesquels des adversaires pourraient exploiter des vulnérabilités de systèmes qui exécutent des fonctions cruciales d'une installation. Il ne s'agit toutefois que d'exemples, et les exploitants doivent faire preuve de créativité en matière de sécurité informatique afin d'imaginer comment leurs adversaires pourraient agir et comment les mesures de sécurité informatique pourraient contrecarrer leurs actions.

I–2. Les exemples sont le fruit de discussions avec des experts des États Membres. Ils ne visent pas à donner une liste exhaustive des possibilités ou une recette pour une attaque d'installation nucléaire, mais constituent un point de départ pour les exploitants et les États Membres qui élaborent des plans pour faire face à des cybermenaces qui sont dynamiques et évoluent rapidement.

I–3. Une cyberattaque coordonnée peut comprendre plusieurs phases :

a) choix de la cible ou des cibles ;
b) reconnaissance ;
c) accès aux systèmes concernés ou compromission de ces systèmes ;
d) lancement de l'attaque ;
e) dissimulation des preuves relatives à l'attaque et à l'adversaire.

I–4. Les adversaires utiliseront tout ou partie des tactiques présentées, et il convient d'en tenir compte lorsque l'on établit des profils de cybermenaces propres aux systèmes de contrôle-commande et à d'autres ressources numériques sensibles (RNS) d'une installation nucléaire. Ces tactiques sont utilisées dans les scénarios qui sont décrits dans la présente annexe. Ces scénarios montrent des types d'attaques courants qui ont été proposés par des experts en sécurité informatique qui connaissent le secteur nucléaire.

I–5. Les types de menaces sont présentés dans la référence [I-1].

SCÉNARIO I : COMPROMISSION D'UN OUTIL D'ASSISTANCE, CE QUI PERMET À L'ADVERSAIRE D'ACCÉDER À DES SYSTÈMES OPÉRATIONNELS ESSENTIELS

I–6. But de l'attaque : accéder à des informations nucléaires et à des ressources numériques au moyen d'un chemin fiable qui est utilisé par les vendeurs pour fournir une assistance.

I–7. Description : l'attaque est initialement dirigée contre le portail d'accès en ligne par lequel les vendeurs ont accès à des informations sensibles et aux RNS de l'installation pour pouvoir fournir une assistance. L'adversaire compromet le portail et, par élévation des privilèges, devient administrateur de la base de données et modifie l'adresse électronique renseignée pour l'un des vendeurs. Ce vendeur a accès à distance à des informations opérationnelles essentielles concernant l'installation et certaines RNS. L'adversaire utilise alors la fonction « mot de passe oublié » du portail, qui envoie un lien vers une page permettant de changer le mot de passe à l'adresse électronique de l'adversaire. Celui-ci ouvre cette page pour modifier le mot de passe du vendeur et se connecte au portail sous l'identité du vendeur autorisé. Une fois connecté, l'adversaire a accès à toutes les informations du portail et à toutes les RNS auxquelles le vendeur a accès. Il commence alors à modifier les réglages et les paramètres de fonctionnement des RNS, ce qui provoque une instabilité de fonctionnement, puis l'arrêt de l'installation.

SCÉNARIO II : EXPLOITATION DES MÉCANISMES D'APPROBATION TRANSITIVE ENTRE UN SERVEUR DU RÉSEAU PÉRIMÉTRIQUE QUI EST UTILISÉ POUR PUBLIER DES INFORMATIONS, ET LES RNS INTERNES

I–8. But de l'attaque : accéder aux RNS et aux systèmes internes.

I–9. Description :

1) À l'aide d'outils en libre accès et de moteurs de recherche, l'adversaire localise le serveur du réseau périmétrique[1] qui est utilisé pour publier sur Internet des informations sur la production d'isotopes radioactifs qui sont

[1] Ce type de réseau sert de « tampon » entre les systèmes internes fiables et les systèmes accessibles au public qui ne sont pas fiables, comme Internet. Il est parfois appelé « zone démilitarisée ».

issues de systèmes internes fiables. Ce serveur se trouve sur le réseau périmétrique, mais les données qu'il contient proviennent d'un serveur de base de données master qui se trouve sur le même réseau que le système de contrôle d'une installation qui produit des isotopes radioactifs. Le serveur de la base de données master recueille des informations qui proviennent de l'environnement de production interne et les envoie à la base de données qui se trouve sur le réseau périmétrique. Le réseau périmétrique est séparé du réseau de production par un pare-feu, qui contient une liste de contrôle des accès afin que seule la base de données qui se trouve sur le serveur du réseau périmétrique puisse communiquer avec la base de données master.

2) L'adversaire exploite une vulnérabilité pour obtenir un accès administrateur au serveur situé sur le réseau périmétrique, et prend le contrôle de la voie de communication qui relie ce serveur et le serveur de la base de données master, qui se trouve sur le réseau du système de contrôle. Le pare-feu est configuré de telle manière qu'il autorise les communications entre le réseau périmétrique et la base de données master (c'est-à-dire qu'il établit une « approbation transitive » entre les réseaux), de sorte que l'adversaire, qui contrôle le serveur du réseau périmétrique, peut se connecter directement à la base de données master.
3) L'adversaire utilise la connexion à la base de données master pour effectuer une reconnaissance et savoir combien de ressources du système de contrôle se trouvent sur le même réseau. Comme aucune mesure de sécurité ne protège ce réseau, l'adversaire peut prendre le contrôle des RNS et compromettre les appareils qui contrôlent la production, la gestion, le transport, l'entreposage et l'inventaire des isotopes.

SCÉNARIO III : INFECTION DES SYSTÈMES DE CONTRÔLE-COMMANDE D'UNE CENTRALE NUCLÉAIRE PAR UN LOGICIEL MALVEILLANT

I–10. But de l'attaque : forcer l'exploitant à arrêter une centrale nucléaire.

I–11. Description :

1) Un ingénieur en poste dans une centrale nucléaire travaille à domicile sur un ordinateur portable qui est utilisé pour régler les machines et optimiser la centrale, mettre à jour les programmes de performance et paramétrer les logiciels qui sont utilisés pour la surveillance de la sûreté.
2) À son domicile, l'ingénieur utilise cet ordinateur pour accéder au site web d'un vendeur et obtenir une mise à jour logicielle pour les systèmes de

contrôle-commande, qui jouent un rôle essentiel dans le fonctionnement de la centrale. Pendant le téléchargement de la mise à jour, il se connecte à un compte bancaire, consulte le site web de l'entreprise et utilise des médias sociaux, et un logiciel malveillant est téléchargé sur l'ordinateur. Ce logiciel malveillant est nouveau et n'est pas détecté par l'antivirus de l'ordinateur.

3) Comme la politique de l'entreprise lui interdit d'apporter l'ordinateur dans la centrale, l'ingénieur copie la mise à jour téléchargée sur une clef USB qu'il compte utiliser pour mettre à jour les logiciels des ressources concernées. Cependant, le logiciel malveillant effectue également une copie de lui-même sur la clef USB et, lorsque l'ingénieur utilise cette clef pour installer la mise à jour via un poste de travail de la centrale, le logiciel malveillant effectue une copie de lui-même sur le système de la centrale. L'exploitant a supposé que les mesures de protection physique qui sont en vigueur empêcheraient un ordinateur non autorisé de se connecter au réseau du système de contrôle, et la possibilité d'une infection au moyen de supports amovibles n'a pas été envisagée.

4) Une fois que le logiciel malveillant a infecté le poste de travail, il effectue des copies de lui-même et contamine d'autres composants connectés dans la centrale. Comme l'exploitant n'a pas mis en place de mesures de sécurité informatique à l'échelle de la centrale et qu'aucun antivirus n'a été installé sur les systèmes essentiels, le logiciel malveillant infecte les ressources numériques cruciales présentes sur le réseau, ce qui provoque des défaillances et oblige l'exploitant à arrêter la centrale.

SCÉNARIO IV : OBTENTION D'INFORMATIONS SENSIBLES SUR LE FONCTIONNEMENT D'UNE CENTRALE NUCLÉAIRE DIRECTEMENT À PARTIR D'APPAREILS QUI ONT ÉTÉ DÉCLASSÉS DE MANIÈRE INAPPROPRIÉE

I–12. But de l'attaque : recueillir suffisamment d'informations pour pouvoir préparer une attaque précise contre la centrale concernée.

I–13. Description :

1) Un adversaire recueille des informations sur les médias sociaux et des éléments qui montrent qu'une installation nucléaire va acheter un système de contrôle en remplacement d'un ancien système. En outre, l'exploitant a l'intention de vendre les anciens appareils pour financer en partie l'achat du nouveau système de contrôle.

2) L'installation n'ayant pas établi de procédure formelle de déclassement en matière de sécurité de l'information, un système qui a été utilisé pour exécuter des actions cruciales de contrôle-commande est vendu sans que les informations qui y sont stockées ne soient examinées ou supprimées. L'adversaire achète ce système et découvre des fichiers de projet à jour, des diagrammes de réseau, des noms d'utilisateur et des mots de passe, ainsi que d'autres données qui lui permettent de comprendre tout le fonctionnement de l'installation nucléaire.
3) L'adversaire exploite ces informations pour concevoir un plan d'attaque de certaines RNS qui sont utilisées dans l'installation et pour créer des courriels convaincants dans le cadre d'une campagne d'hameçonnage. Enfin, il utilise à la fois les informations obtenues grâce au système acheté et celles qui ont été fournies à leur insu par les victimes de la campagne d'hameçonnage pour lancer une attaque combinée contre l'installation.

SCÉNARIO V : INGÉNIERIE SOCIALE STRATÉGIQUE CONTRE UN AGENT DE SÉCURITÉ D'UNE INSTALLATION

I–14. But de l'attaque : obtenir par ingénierie sociale des informations d'un agent de sécurité d'une installation à l'appui d'une attaque.

I–15. Description :

1) Un adversaire mène une campagne d'ingénierie sociale contre un agent de sécurité d'une installation en utilisant l'hameçonnage, la reconnaissance des lieux et des informations publiques, notamment les traces laissées par l'agent sur les médias sociaux.
2) Sous une fausse identité, l'adversaire exploite ces informations pour commencer à communiquer directement avec l'agent de sécurité, qui en vient progressivement à lui faire confiance, car il le prend pour un autre. À mesure que la correspondance se poursuit, l'adversaire commence à ajouter des pièces jointes crédibles qui sont en réalité des logiciels malveillants. Lorsque ces logiciels sont activés, ils ouvrent secrètement une voie de communication vers l'ordinateur de l'adversaire et lui envoient certains fichiers qui se trouvent sur l'ordinateur de l'agent de sécurité. Grâce à ces informations, l'adversaire peut concevoir des plans précis et détaillés pour attaquer les systèmes de protection physique de la centrale et intercepter des matières nucléaires en cours de transport.

RÉFÉRENCE POUR L'ANNEXE I

[I–1] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Sécurité informatique pour la sécurité nucléaire, n° 42-G de la Collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2022).

Annexe II

EXEMPLE D'ATTRIBUTION DE NIVEAUX DE SÉCURITÉ INFORMATIQUE DANS UNE CENTRALE NUCLÉAIRE

II–1. Un niveau de sécurité informatique est attribué à un système (ou à la zone où se trouve un système) en fonction des conséquences possibles qu'une attaque contre le système concerné aurait pour la sûreté, la sécurité et le fonctionnement de l'installation : moins les conséquences sont acceptables, plus le niveau de sécurité informatique est strict.

II–2. Pour éviter les analyses au cas par cas de chaque système et de toutes les conséquences possibles, des critères peuvent être établis pour faciliter l'attribution des niveaux de sécurité informatique.

II–3. L'une des considérations fondamentales est la classe de sûreté du système examiné. Il n'y a toutefois pas de correspondance automatique entre les niveaux de sécurité informatique et les classes de sûreté. Un niveau de sécurité strict est nécessaire pour un système important pour la sûreté, mais un niveau contraignant peut également être nécessaire pour un système sans classe de sûreté qui joue un rôle critique dans la prévention de conséquences potentielles graves pour la sécurité.

II–4. Exemples de critères généraux pour une approche graduée des niveaux de sécurité informatique :

1) Le niveau de sécurité informatique 1 est attribué aux systèmes numériques de la centrale pour lesquels une atteinte à l'intégrité ou à la disponibilité peut avoir des conséquences radiologiques pour la population en dehors du site. Il s'agit du critère qui est appliqué pour les systèmes de classe de sûreté 1E/F1A (qui correspondent aux systèmes contribuant à l'exécution de fonctions de catégorie A dans la classification de sûreté de la Commission électrotechnique internationale [II-1]).
2) Le niveau de sécurité informatique 2 est attribué aux systèmes numériques de la centrale pour lesquels une atteinte à l'intégrité ou à la disponibilité peut dégrader un ou plusieurs des éléments suivants :
   i) gestion d'une situation d'urgence ;
   ii) sûreté de la centrale en fonctionnement normal ;
   iii) principal processus nucléaire ;
   iv) protection physique de la centrale.

3) Le niveau de sécurité informatique 3 est attribué aux systèmes numériques de la centrale pour lesquels une atteinte à l'intégrité ou à la disponibilité n'a pas de conséquences radiologiques ni d'effets néfastes sur la sûreté ou la protection physique, mais peut avoir d'autres effets importants. Ces systèmes peuvent notamment comprendre des ressources numériques qui facilitent l'exploitation ou la maintenance de la centrale, ainsi que des systèmes qui peuvent avoir un effet sur la production d'électricité.
4) Le niveau de sécurité informatique 4 est attribué aux systèmes numériques de la centrale pour lesquels une atteinte à l'intégrité ou à la disponibilité n'a pas d'effet à court terme sur le fonctionnement de la centrale, mais peut en avoir à plus long terme.
5) Le niveau de sécurité informatique 5 est attribué aux systèmes numériques de la centrale pour lesquels une atteinte à l'intégrité ou à la disponibilité n'a aucun effet sur la sûreté, sur la disponibilité de la centrale et sur le fonctionnement de l'installation.

II–5. En dehors de ces critères généraux, on peut dresser une liste de fonctions types d'une installation ou de types de systèmes pour chaque niveau de sécurité informatique. Cette liste peut simplifier l'attribution des niveaux de sécurité informatique aux systèmes.

II–6. Les niveaux de sécurité informatique sont définis par les conséquences possibles d'une compromission des systèmes informatiques (voir réf. [II-2]). Dans bien des cas, les informations acquises ou calculées par un système numérique peuvent également être obtenues à l'aide d'outils analogiques ou par une personne. Le niveau de sécurité informatique peut alors être moins strict (et donc moins restrictif pour le fonctionnement normal).

II–7. Lorsque plusieurs ressources numériques différentes sont utilisées pour la même fonction, un système doit être considéré comme le système principal contribuant à l'exécution de cette fonction et se voir attribuer un niveau de sécurité informatique en fonction des conséquences de sa compromission.

RÉFÉRENCES POUR L'ANNEXE II

[II–1] COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE, Centrales nucléaires de puissance : Instrumentation et contrôle-commande importants pour la sûreté – Classification des fonctions d'instrumentation et de contrôle-commande, IEC 61513:2011, IEC, Genève (2011).

[II–2] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems — Requirements for Security Programmes for Computer-Based Systems, IEC 62645:2014, IEC, Geneva (2014).

Annexe III

EXEMPLE D'APPLICATION DU PRINCIPE DES NIVEAUX ET DES ZONES DE SÉCURITÉ INFORMATIQUE

GÉNÉRALITÉS

III–1. La présente annexe donne un exemple d'application des niveaux et des zones de sécurité informatique. Le tableau III-1 contient une liste des systèmes qui sont présentés dans cet exemple et montre la correspondance qui existe entre les niveaux de sécurité informatique et les zones physiques et logiques qui sont utilisées dans cet exemple.

III–2. Pour les systèmes simples, qui sont composés d'un petit nombre de ressources situées à un emplacement bien défini, il est facile d'appliquer des niveaux de sécurité informatique et de définir des zones physiques et logiques. Le problème est plus difficile pour les systèmes complexes qui sont présents dans toute l'installation et pour les zones physiques qui contiennent des systèmes auxquels des niveaux de sécurité différents doivent être attribués, comme la salle de commande principale.

SALLE DE COMMANDE PRINCIPALE

III–3. Il y a généralement des commandes pour de nombreuses catégories de systèmes soumis à des exigences de sécurité différentes (systèmes de sûreté, chaudière nucléaire, systèmes électriques, systèmes auxiliaires et systèmes informatiques, par exemple) dans la salle de commande principale. Les interfaces homme-machine de tous les systèmes de l'installation se trouvent complètement ou en partie dans la salle de commande principale. Ces systèmes et les interfaces homme-machine utilisent généralement des ressources numériques pour remplir leurs fonctions.

III–4. Dans les installations anciennes, cette situation complique l'application des niveaux de sécurité informatique pour plusieurs raisons :

a) Les anciens pupitres comprennent généralement des commandes pour plusieurs systèmes, surtout pour la partie non nucléaire de la centrale et pour les systèmes auxiliaires. Ce regroupement peut rendre plus difficiles l'isolation et la séparation des systèmes. Dans certains cas, les fonctions de

l'installation qui sont exécutées par des systèmes auxquels des niveaux de sécurité informatique différents ont été attribués peuvent être regroupées sur un seul pupitre, auquel le niveau de sécurité le plus strict doit être appliqué.

b) Selon le principe des niveaux et des zones de sécurité informatique, les ressources numériques qui se trouvent dans les limites physiques de la salle de commande principale et des salles des appareils se verraient attribuer des niveaux de sécurité différents. Par exemple, un système de protection d'un réacteur peut se voir attribuer le niveau le plus strict (niveau de sécurité 1, par exemple), tandis qu'un ordinateur personnel qui permet à un agent d'accéder à une messagerie électronique peut se voir attribuer le niveau le moins contraignant (niveau de sécurité 5, par exemple).

c) Les membres du personnel qui mènent des activités autorisées sur un système situé dans la salle de commande principale peuvent avoir accès à d'autres appareils situés dans cette salle.

III–5. L'exemple suivant vise à exposer les solutions possibles pour résoudre les problèmes décrits ci-dessus sur le plan de la sécurité informatique, compte tenu des notions qui sont présentées sur la figure 1 du corps du texte.

III–6. Il est difficile de définir des zones de sécurité informatique dans la salle de commande principale (et pour les systèmes de protection physique et de protection contre l'incendie), car les fonctions de l'installation doivent être surveillées et gérées de manière centralisée. La notion de zone de sécurité informatique permet d'établir des limites physiques ou logiques, ce qui peut contribuer à lever ces limitations. Ces relations sont représentées sur la figure III-1.

III–7. On suppose que la salle de commande principale (et les salles de la zone protégée qui contiennent des appareils électroniques) est classée comme zone vitale et protégée en conséquence. Le sabotage d'un appareil situé dans la salle de contrôle principale peut donc avoir des conséquences radiologiques inacceptables.

III–8. Le tableau III-1 donne un exemple de systèmes pour lesquels une surveillance, des communications ou une action depuis la salle de commande principale sont nécessaires.

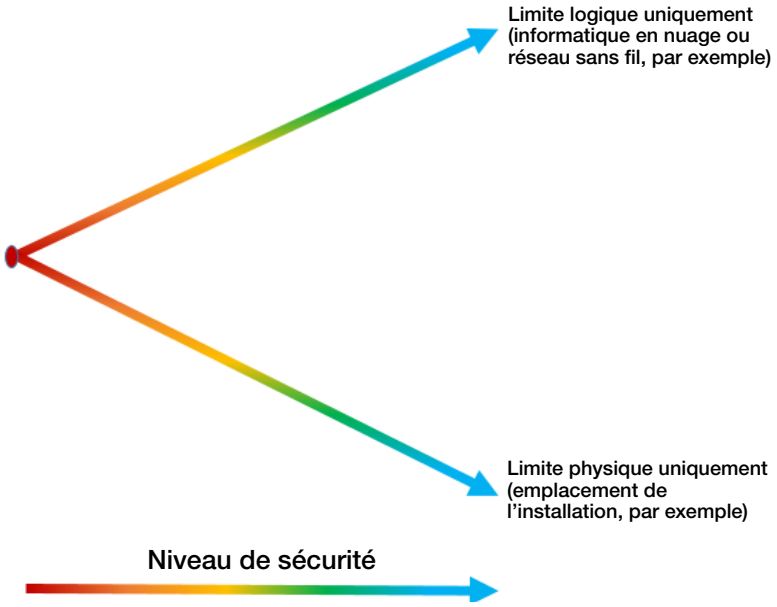

FIG. III-1. Exigences applicables aux limites physiques et logiques des zones en fonction du niveau de sécurité informatique.

TABLEAU III-1. LISTE DE SYSTÈMES : EXEMPLE D'APPLICATION DU PRINCIPE DES NIVEAUX ET DES ZONES DE SÉCURITÉ INFORMATIQUE

Système	Fonction la plus importante	NSI	Limite logique	Limite physique
Système de protection du réacteur	Prévenir les conditions accidentelles	1	Réseau interne spécifique découplé à l'aide d'une *data diode*	Matériel situé dans une seule zone vitale
			Pas de connectivité externe	Mesure de sécurité informatique (*data diode*) située dans une zone vitale

TABLEAU III-1. LISTE DE SYSTÈMES : EXEMPLE D'APPLICATION DU PRINCIPE DES NIVEAUX ET DES ZONES DE SÉCURITÉ INFORMATIQUE (suite)

Système	Fonction la plus importante	NSI	Limite logique	Limite physique
Système de limitation du réacteur	Maîtriser la réactivité	2	Réseaux spécifiques, découplés à l'aide d'une *data diode*, d'un pare-feu ou d'autres dispositifs de sécurité	Matériel situé dans une ou plusieurs zones vitales Les câbles réseau, le matériel et les dispositifs de routage qui se trouvent en dehors des zones vitales sont physiquement renforcés (par une gaine sécurisée et par des tableaux, par exemple)
Système d'information sur les processus	Alerter les agents et leur donner des informations sur l'environnement et l'état de l'installation	3	Réseaux connectés à l'IHM Note : Il peut s'agir d'un pupitre distinct ou supplémentaire de la salle de commande principale	Matériel et réseaux situés dans la zone protégée ou dans les zones vitales
Systèmes d'automatisation de l'exploitation	Contrôler les systèmes qui se trouvent dans la partie non nucléaire de la centrale	3	Réseaux connectés à l'IHM Note : Il peut s'agir d'un pupitre distinct ou supplémentaire de la salle de commande principale, ou le pupitre peut faire partie d'un système d'information sur les processus	Matériel et réseaux situés dans la zone protégée ou dans les zones vitales

TABLEAU III-1. LISTE DE SYSTÈMES : EXEMPLE D'APPLICATION DU PRINCIPE DES NIVEAUX ET DES ZONES DE SÉCURITÉ INFORMATIQUE (suite)

Système	Fonction la plus importante	NSI	Limite logique	Limite physique
Bureautique	Exécuter des fonctions pour le personnel	4	Aucune connexion logique (filaire, sans fil ou interface avec un support amovible) n'est autorisée avec une zone (ou un système) de niveau 1, 2 ou 3	Autorisée dans la zone d'accès limitée, la zone protégée et les zones vitales
Systèmes de télécommunication	Appeler les forces d'intervention ou d'autres services externes si nécessaire	4	Aucune connexion logique (filaire, sans fil ou interface avec un support amovible) n'est autorisée avec une zone de niveau 1, 2 ou 3	Autorisés à tous les endroits nécessaires pour les objectifs de l'exploitant
Appareils informatiques mobiles personnels	Aucune fonction nécessaire ; utilisation uniquement par dérogation	5	Uniquement autorisés sur les réseaux de niveau 5 Ne peuvent être utilisés à proximité d'une zone de niveau 1, 2 ou 3	Interdits dans les zones vitales

Note : IHM : interface homme-machine ; NSI : niveau de sécurité informatique.

ZONES SITUÉES EN DEHORS DE LA SALLE DE COMMANDE PRINCIPALE ET SURVEILLÉES DEPUIS CETTE SALLE

Système de protection du réacteur (niveau de sécurité informatique 1)

III–9. Dans le tableau III-1, le niveau de sécurité informatique le plus contraignant (niveau 1) exige que les limites logique et physique des zones de sécurité informatique concernées soient définies de manière stricte et que ces limites ne débordent pas les unes sur les autres. Le réseau spécifique peut

par exemple être limité à des emplacements situés dans la zone vitale (ou son équivalent).

III–10. Les accès physiques et logiques aux zones auxquelles le niveau de sécurité informatique 1 a été attribué doivent être strictement contrôlés. Les accès physiques peuvent être contrôlés à l'aide d'une barrière solide munie d'un dispositif de contrôle des accès et de détection d'intrusions pour répondre aux prescriptions qui figurent dans la référence [III-1], et les accès logiques peuvent être contrôlés au moyen d'une voie de communication unidirectionnelle et à sécurité intégrée (*data diode*, par exemple), conformément aux orientations de la présente publication et de la référence [III–2].

III–11. Les systèmes qui exécutent la fonction de l'installation consistant à prévenir les conditions accidentelles (système de protection d'un réacteur, par exemple) se voient généralement attribuer le niveau de sécurité informatique le plus strict. Le matériel qui assure cette fonction sera situé dans une zone vitale proche du réacteur, mais sera surveillé par l'intermédiaire d'une interface homme-machine dans la salle de commande principale. Cette situation peut poser un problème pour le découpage en zones de sécurité informatique, car l'interconnexion entre le système de protection du réacteur et l'interface homme-machine pourrait se situer en dehors des zones vitales (dans la zone protégée, par exemple), ce qui ne serait pas conforme à l'exigence de sécurité physique.

III–12. L'une des solutions possibles consiste à séparer la fonction de surveillance de la fonction de prévention des conditions accidentelles. Elle permet une séparation logique, au moyen d'une *data diode*, entre les ressources numériques qui se trouvent dans la zone vitale et préviennent les conditions accidentelles, et celles qui se trouvent en dehors de la zone vitale et qui sont utilisées pour la surveillance dans la salle de commande principale. Elle ne sera efficace que si la fonction de prévention des conditions accidentelles est indépendante et n'exige aucune information ou action extérieures aux systèmes qui exécutent cette fonction.

III–13. Les ressources numériques qui préviennent les conditions accidentelles se verront attribuer le niveau de sécurité informatique le plus strict (niveau 1), compte tenu de la fonction qu'elles remplissent. Elles se trouveront dans une zone vitale située à l'extérieur de la salle de commande principale. Les ressources numériques qui surveillent le système de protection du réacteur (pupitre du système de protection du réacteur qui se trouve dans la salle de commande principale, par exemple) se verront attribuer le niveau de sécurité 2 (ou un niveau plus élevé).

ZONES SITUÉES EN DEHORS DE LA SALLE DE COMMANDE PRINCIPALE ET GÉRÉES DEPUIS CETTE SALLE

Système de limitation du réacteur (niveau de sécurité informatique 2)

III–14. D'après le tableau III-1, les ressources numériques qui exécutent des fonctions auxquelles a été attribué le niveau de sécurité 2 doivent se trouver dans une zone vitale, et leurs accès physiques et logiques doivent être strictement contrôlés. Pour des questions opérationnelles, la fonction de maîtrise de la réactivité doit toutefois être associée à des commandes situées dans la salle de commande principale (instructions destinées à augmenter ou à diminuer la puissance, par exemple).

III–15. Le matériel est situé dans des zones vitales et l'infrastructure du réseau (câblage, commutateurs et tableaux) est renforcée lorsqu'elle se trouve dans des zones moins sécurisées (si les câbles passent par la zone protégée, par exemple). Des commandes étant nécessaires (c'est-à-dire des communications en provenance de la salle de commande principale et destinées au matériel), il n'est pas possible de mettre en place une *data diode* pour contrôler les accès logiques.

III–16. L'une des solutions possibles consiste à établir une isolation physique et logique entre la zone où se trouvent le réseau et les ressources numériques qui sont utilisés pour ces communications et les zones auxquelles un niveau de sécurité plus faible (niveau 3 à 5) a été attribué. Il est ainsi possible de séparer logiquement d'autres systèmes auxquels un niveau plus faible a été attribué. Cette solution ne sera efficace que si la fonction de prévention des conditions accidentelles est indépendante et n'exige aucune information ou action extérieures aux systèmes qui exécutent cette fonction.

III–17. Le même raisonnement et la même solution peuvent être appliqués au système d'information sur les processus et aux systèmes d'automatisation de l'exploitation, auxquels le niveau de sécurité informatique 3 a été attribué.

ZONES OU APPAREILS QUI DISPOSENT D'UNE CONNECTIVITÉ EXTERNE

Bureautique et systèmes de télécommunication (niveau de sécurité informatique 4 ou 5)

III–18. D'après le tableau III-1, la bureautique et les systèmes de télécommunication assurent des fonctions nécessaires qui exigent une connectivité externe. Celle-ci permet aux agents d'accéder aux informations et aux ressources dont ils peuvent avoir besoin lors de certains événements et dans certaines conditions.

III–19. Les connexions externes à Internet et à d'autres services, réseaux et appareils peuvent accroître les risques, sauf si des mesures sont mises en place pour garantir que des informations ne puissent être échangées entre ces sources externes et les systèmes qui exécutent des fonctions auxquelles un niveau de sécurité plus élevé a été attribué. Des mesures rigoureuses sont nécessaires pour supprimer ou restreindre l'accès aux interfaces avec un support amovible, aux connexions filaires, aux connexions sans fil et aux autres moyens par lesquels des informations peuvent être échangées avec les ressources numériques qui disposent d'une connectivité externe, ainsi que pour définir des zones de sécurité informatique étroitement délimitées pour ces ressources numériques, et dotées de solides mécanismes de découplage. La séparation des zones de sécurité dans la salle de commande principale est étudiée plus en détail aux paragraphes III-21 à III-27.

Appareils informatiques mobiles personnels (auxquels aucun niveau de sécurité n'a été attribué)

III–20. On suppose que la sécurité des appareils informatiques mobiles et des logiciels personnels n'a pas été renforcée et que des informations peuvent être échangées avec les ressources numériques auxquelles un niveau de sécurité a été attribué et qui se trouvent à proximité. Les appareils informatiques mobiles personnels ne sont donc pas autorisés dans la salle de commande principale (et dans les salles des appareils).

SÉPARATION DES ZONES DE SÉCURITÉ DANS LA SALLE DE COMMANDE PRINCIPALE

III–21. Comme l'explique le paragraphe III-13, les ressources numériques exécutent souvent plusieurs fonctions, qui exigent des niveaux de sécurité informatique différents, et ces ressources numériques se trouvent généralement dans la salle de commande principale. Cette proximité accroît le risque de compromission des ressources numériques par cyberattaque.

III–22. Cela est particulièrement vrai si aucune mesure de contrôle physique n'a été mise en place pour protéger l'accès aux ressources numériques et les interfaces entre ces ressources. En pareil cas, un initié qui peut accéder logiquement ou physiquement à la zone de la salle de commande principale a toute latitude pour compromettre les ressources numériques de cette zone.

III–23. Les ressources (et les systèmes) numériques qui se trouvent dans la salle de commande principale exécutent des fonctions qui nécessitent souvent des informations communiquées par d'autres ressources numériques ou des actions qui doivent être entreprises par le personnel d'exploitation. Si le système de protection du réacteur a été logiquement et physiquement séparé de la salle de commande principale comme dans l'exemple présenté ci-dessus (par exemple par une *data diode* pour la surveillance), les autres fonctions de sûreté principales à prendre en compte sont la maîtrise de la réactivité et l'évacuation de la chaleur du cœur.

III–24. Les systèmes qui exécutent ces fonctions de sûreté se voient généralement attribuer le niveau de sécurité informatique 2. D'après le tableau III-1, le niveau de sécurité informatique 2 exige des limites de zone strictes, mais celles-ci peuvent être une combinaison de limites physiques et de limites logiques.

III–25. Le placement des ressources numériques de la salle de commande principale dans différentes zones est rendu plus difficile par le fait que des fonctions informatiques d'appui (courrier électronique, Internet et gestion des activités, par exemple) sont nécessaires pour aider les agents dans la salle de contrôle principale. L'installation de ressources numériques pour exécuter ces fonctions peut créer une situation dans laquelle des systèmes auxquels un niveau de sécurité compris entre 2 et 5 a été attribué sont mis à la disposition des mêmes agents dans la salle de commande principale, alors que l'exigence de séparer les ressources numériques qui exécutent des fonctions auxquelles des niveaux de sécurité différents ont été attribués doit être respectée.

III–26. Dans cet exemple, les solutions suivantes peuvent être adoptées :

a) Les réseaux logiques ne sont jamais connectés directement et utilisent toujours de solides mécanismes de découplage. Les réseaux de niveau de sécurité 2 ne s'étendent pas au-delà de la salle de commande principale (et des salles des appareils associées qui se trouvent dans la zone protégée) sans que de tels mécanismes n'aient été mis en place.
b) Les réseaux logiques sont clairement séparés et définis, et la responsabilité de leur gestion peut être confiée à des services différents (service informatique et service technique, par exemple).
c) Des mesures de contrôle physique peuvent être mises en place pour créer des sous-zones dans la salle de commande principale. Elles peuvent prendre la forme de tableaux fermés à clef, de dispositifs de blocage des interfaces pour supports amovibles (bloqueurs de port, par exemple), de gaines sécurisées ou de zones d'accès limité dans la salle de commande principale.

III–27. Compte tenu des solutions proposées ci-dessus, plusieurs niveaux de sécurité informatique pourraient exister dans une même zone physique (dans la salle de commande principale, par exemple) grâce à des contrôles logiques et à des contrôles physiques. Par la mise en place de mesures de sécurité informatique supplémentaires, la salle de commande principale peut cependant être divisée en sous-zones auxquelles sont attribués des niveaux de sécurité différents.

RÉFÉRENCES POUR L'ANNEXE III

[III–1] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Recommandations de sécurité nucléaire sur la protection physique des matières nucléaires et des installations nucléaires (INFCIRC/225/Révision 5), n° 13 de la collection Sécurité nucléaire de l'AIEA , AIEA, Vienne (2011).

[III–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).

GLOSSAIRE

architecture de sécurité informatique défensive. Configuration de systèmes informatiques conforme à des exigences, des contraintes et des mesures de conception qui doivent être imposées pendant toute la durée de vie d'un système, de sorte que les systèmes qui exécutent une fonction répertoriée d'une installation et importante pour la sûreté ou la sécurité de l'installation en question, et auxquels est attribué un niveau de sécurité informatique à l'échelle de l'installation soient suffisamment protégés.

attaque combinée. Acte malveillant consistant dans le lancement coordonné d'une cyberattaque et d'une attaque physique.

cyberattaque. Acte malveillant destiné à empêcher d'avoir accès à une cible particulière ou à la voler, la modifier ou la détruire par accès non autorisé à un système informatique sensible (ou par des actions dans un tel système).

détection. Processus d'un système de protection physique qui commence avec la perception d'un acte potentiellement malveillant ou d'un autre acte non autorisé et qui s'achève avec l'évaluation de la cause de l'alarme.

énoncé de la menace. Description des agresseurs crédibles (y compris de leurs attributs et caractéristiques) sous la forme d'une menace de référence ou d'un énoncé de la menace représentative, élaborée sur la base de l'évaluation nationale de la menace contre la sécurité nucléaire.

évaluation de la menace. Évaluation des menaces – effectuée à partir des informations fournies par les services de renseignement et les forces de l'ordre et des informations en libre accès – qui décrit les motivations, les intentions et les capacités de ces menaces.

événement de sécurité nucléaire. Événement ayant des incidences potentielles ou effectives sur la sécurité nucléaire auxquelles il faut remédier.

fonction d'une installation. Ensemble coordonné d'actions, de processus et d'opérations qui sont associés à une installation nucléaire. Il peut notamment servir à exécuter des fonctions importantes pour la sûreté nucléaire, la sécurité nucléaire, la comptabilité et le contrôle des matières nucléaires ou la gestion des informations sensibles, ou qui ont un rapport avec l'un de

ces domaines. Les fonctions d'une installation comprennent également les fonctions opérationnelles et administratives (ou organisationnelles).

gestion des risques liés à la sécurité informatique Évaluation et gestion des risques associés à de possibles cyberattaques qui pourraient dégrader la sûreté ou la sécurité nucléaires. La gestion des risques liés à la sécurité informatique s'effectue à l'échelle d'une installation ou d'un système.

incident de sécurité informatique. Incident qui nuit ou peut nuire à la confidentialité, à l'intégrité, ou à la disponibilité d'un système informatique (y compris les données qu'il contient), ou qui constitue une violation des règles de sécurité ou présente un risque imminent de violation de ces règles.

information sensible. Information, sous quelque forme que ce soit, y compris les logiciels, dont la divulgation, la modification, l'altération, la destruction, ou le refus d'utilisation non autorisés pourrait compromettre la sécurité nucléaire.

initié. Toute personne bénéficiant d'un accès autorisé à des installations associées ou des activités associées ou à des informations sensibles ou des ressources d'informations sensibles, qui pourrait commettre un acte criminel ou des actes non autorisés délibérés mettant en jeu ou visant des matières nucléaires, d'autres matières radioactives, des installations associées ou des activités associées, ou d'autres actes que l'État considère comme nuisant à la sécurité nucléaire, ou en faciliter la commission.

menace de référence. Attributs et caractéristiques d'initiés et/ou d'agresseurs externes potentiels susceptibles de tenter un enlèvement non autorisé ou un acte de sabotage contre lesquels un système de protection physique est conçu et évalué.

mesures de contrôle administratif. Règles, procédures et pratiques définissant les actions autorisées, nécessaires ou interdites qui visent à protéger les systèmes informatiques et qui contiennent des instructions concernant les actions du personnel, des vendeurs, des sous-traitants et des fournisseurs.

mesures de contrôle physique. Barrières physiques qui protègent les appareils de mesure, les systèmes informatiques et les ressources auxiliaires contre les dommages matériels et empêchent les accès physiques non autorisés.

mesures de contrôle technique. Matériel ou logiciel utilisé pour prévenir et détecter les intrusions ou les autres actes malveillants, en atténuer les conséquences et procéder à la remise en état.

mesures de sécurité informatique. Mesures destinées à prévenir, détecter ou retarder, contrer et atténuer les conséquences d'actes malveillants ou d'autres actes qui pourraient compromettre la sécurité informatique.

mesures de sécurité nucléaire. Mesures visant soit à empêcher une menace contre la sécurité nucléaire d'accomplir des actes criminels ou des actes non autorisés délibérés qui mettent en jeu ou visent des matières nucléaires, d'autres matières radioactives, des installations associées ou des activités associées, soit à détecter des événements de sécurité nucléaire ou à intervenir en cas de tels événements.

niveau de sécurité informatique. Degré de protection requis pour répondre aux besoins de sécurité informatique concernant une fonction relative à la sécurité nucléaire, à la sûreté nucléaire, à la comptabilité et au contrôle des matières nucléaires ou à la gestion des informations sensibles.

programme de sécurité informatique. Plan appliqué pour mettre en œuvre la stratégie de sécurité informatique, où sont définis les rôles, les responsabilités et les procédures au sein d'un organisme. Il décrit précisément les moyens d'atteindre les objectifs de sécurité informatique et fait partie du plan général de sécurité (ou s'y rattache).

régime de sécurité nucléaire. Régime comprenant :

— le cadre législatif et réglementaire et les systèmes et mesures d'ordre administratif régissant la sécurité nucléaire des matières nucléaires, des autres matières radioactives, des installations associées et des activités associées ;
— les établissements et organismes de l'État chargés d'assurer la mise en œuvre du cadre législatif et réglementaire et des systèmes administratifs de sécurité nucléaire ;
— des systèmes de sécurité nucléaire et des mesures de sécurité nucléaire pour la prévention des événements de sécurité nucléaire, leur détection et les interventions correspondantes.

ressources d'informations sensibles. Tout équipement ou composant utilisé pour entreposer, traiter, contrôler ou transmettre des informations sensibles.

Les ressources d'informations sensibles comprennent les systèmes de contrôle, les réseaux, les systèmes d'information et tout autre support électronique ou physique.

ressources numériques sensibles Ressources d'informations sensibles qui sont des systèmes informatiques (ou en font partie).

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

sécurité informatique. Partie de la sécurité de l'information qui concerne la protection des systèmes informatiques.

système de sécurité nucléaire. Ensemble intégré de mesures de sécurité nucléaire.

systèmes informatiques. Dispositifs techniques qui produisent, traitent, calculent, communiquent ou stockent des données numériques, y donnent accès, ou assurent, fournissent ou contrôlent des services qui utilisent de telles données. Ces dispositifs peuvent être physiques ou virtuels. Ils peuvent comprendre des ordinateurs de bureau, des ordinateurs portables, des tablettes et d'autres ordinateurs personnels, des smartphones, des ordinateurs centraux, des serveurs, des ordinateurs virtuels, des logiciels, des bases de données, des supports amovibles, des appareils de contrôle-commande numérique, des automates programmables, des imprimantes, des dispositifs réseau et des composants et des dispositifs embarqués.

zone de sécurité informatique. Ensemble de systèmes ayant des limites physiques ou logiques communes – et défini si nécessaire à l'aide de critères supplémentaires – auquel est attribué un seul niveau de sécurité informatique afin de simplifier la gestion, la communication et l'application des mesures de sécurité informatique.

IAEA
Agence internationale de l'énergie atomique

Nº 26

OÙ COMMANDER ?

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

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

AMÉRIQUE DU NORD

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

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

RESTE DU MONDE

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

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

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

Commandes individuelles :
www.eurospanbookstore.com/iaea

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

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

Unité de la promotion et de la vente
Agence internationale de l'énergie atomique
Centre international de Vienne, B.P. 100, 1400 Vienne (Autriche)
Téléphone : +43 1 2600 22529 ou 22530 • Télécopie : +43 1 26007 22529
Courriel : sales.publications@iaea.org • Site web : https://www.iaea.org/fr/publications

La présente publication contient des orientations sur la manière d'établir, d'améliorer, de développer, de mettre en œuvre, de maintenir et de préserver la sécurité informatique dans une installation nucléaire. Elle porte sur l'utilisation d'approches fondées sur les risques pour mettre en place et améliorer les règles et les programmes de sécurité informatique, décrit l'intégration de la sécurité informatique dans le système de gestion d'une installation et présente une méthode systématique pour déterminer quelles sont les fonctions de l'installation et les mesures de sécurité informatique appropriées qui protègent l'installation des cyberattaques, conformément à l'évaluation de la menace ou à la menace de référence. La présente publication prend en compte toutes les ressources numériques associées à une installation nucléaire et est applicable à tous les stades de la durée de vie d'une installation nucléaire.

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE