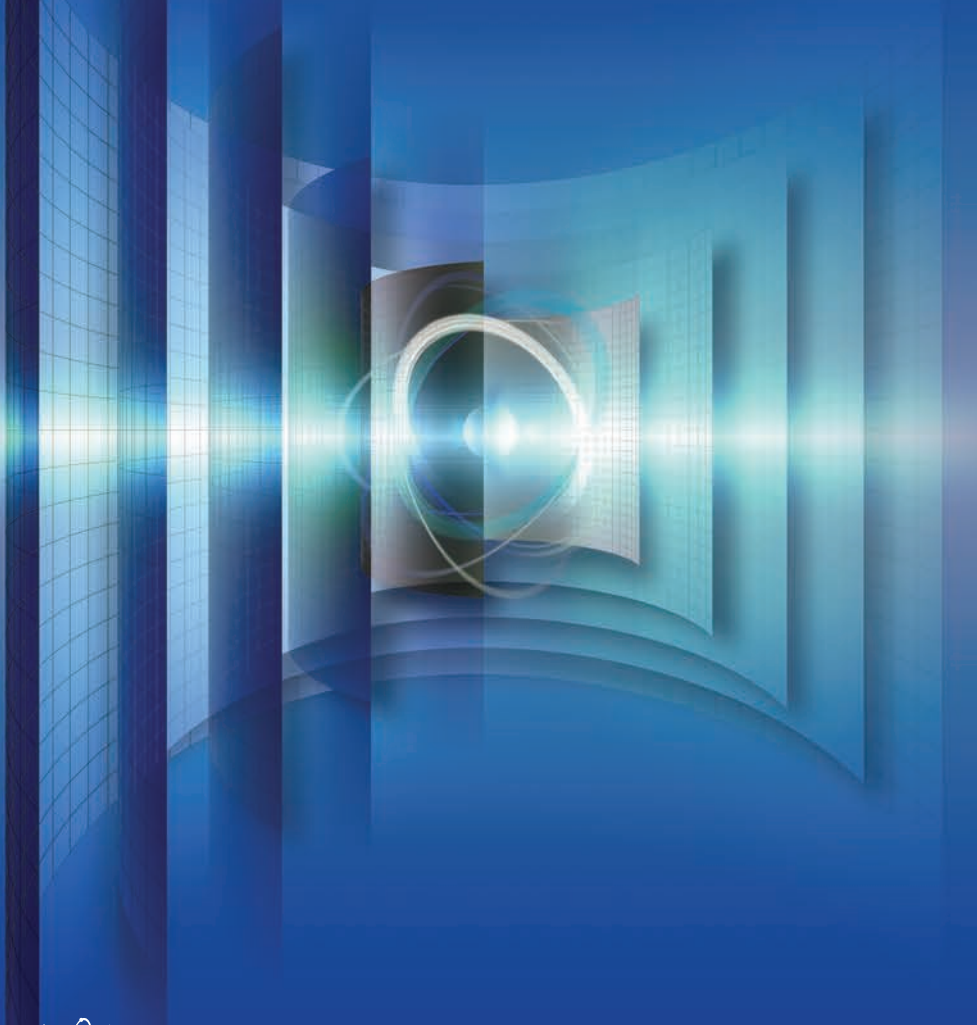
Collection Sécurité nucléaire de l'AIEA n° 33-T

Orientations techniques

Sécurité informatique des systèmes de contrôle-commande dans 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 **collection Sécurité nucléaire de l'AIEA**. Ces publications sont conformes aux instruments internationaux relatifs à la sécurité nucléaire, notamment à la Convention sur la protection physique des matières nucléaires telle qu'amendée, à la Convention internationale pour la répression des actes de terrorisme nucléaire, aux résolutions 1373 et 1540 du Conseil de sécurité des Nations Unies et au Code de conduite sur la sûreté et la sécurité des sources radioactives, et elles les complètent.

CATÉGORIES DANS LA COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA

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

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

RÉDACTION ET EXAMEN

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

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

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

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

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

SÉCURITÉ INFORMATIQUE DES SYSTÈMES DE CONTRÔLE-COMMANDE DANS 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
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 33-T

SÉCURITÉ INFORMATIQUE DES SYSTÈMES DE CONTRÔLE-COMMANDE DANS LES INSTALLATIONS NUCLÉAIRES

ORIENTATIONS TECHNIQUES

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE, 2023

DROIT D'AUTEUR

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

Imprimé par l'AIEA en Autriche
Décembre 2023
STI/PUB/1787

SÉCURITÉ INFORMATIQUE
DES SYSTÈMES DE CONTRÔLE-COMMANDE
DANS LES INSTALLATIONS NUCLÉAIRES
AIEA, VIENNE, 2023
STI/PUB/1787
ISBN 978–92–0–228923–9 (imprimé)
ISBN 978–92–0–228623–8 (pdf)
ISSN 2520–6931

AVANT-PROPOS

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

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

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

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

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

NOTE DE L'ÉDITEUR

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

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

Les appendices sont réputés faire partie intégrante de la publication. 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. Les systèmes de contrôle-commande jouent un rôle essentiel pour garantir l'exploitation sûre des installations nucléaires. Au fur et à mesure de leur évolution et de l'amélioration de leur performance, les technologies numériques sont de plus en plus souvent incorporées et intégrées dans les systèmes de contrôle-commande[1]. Les nouvelles installations nucléaires et les conceptions modernes d'installations nucléaires utilisent des systèmes numériques de contrôle-commande largement intégrés pour traiter efficacement et simultanément de grandes quantités de données de processus tout en nécessitant moins d'interaction et d'intervention humaines que les systèmes de contrôle-commande précédents. Les technologies numériques sont également souvent introduites dans les systèmes de contrôle-commande lors de la modernisation d'installations existantes. Toutefois, l'application des technologies numériques aux systèmes de contrôle-commande a rendu ces derniers vulnérables aux cyberattaques.

1.2. Une cyberattaque est un acte malveillant perpétré par des personnes ou des organismes. Elle vise des informations sensibles ou des ressources d'informations sensibles dans l'intention de voler, de modifier une cible spécifiée, d'empêcher d'y avoir accès ou de détruire une cible spécifiée par un accès non autorisé à un système sensible (ou par des actes au sein un tel système). Les ressources d'informations sensibles comprennent les systèmes de contrôle, les réseaux, les systèmes d'information et tout autre support électronique ou physique. Des adversaires ont lancé des cyberattaques réussies contre des systèmes de contrôle-commande, comme la cyberattaque Stuxnet, qui a entraîné la destruction de matériel dans une installation nucléaire [1].

1.3. Les cyberattaques visant les systèmes de contrôle-commande peuvent compromettre la sûreté et la sécurité des installations nucléaires. Elles peuvent contribuer au sabotage ou aider à l'enlèvement non autorisé de matières nucléaires. Les effets des cyberattaques sur les systèmes de contrôle-commande liés à la sûreté peuvent entraîner de multiples conséquences, comme une perte temporaire de contrôle de processus ou des conséquences radiologiques inacceptables. La sensibilisation du public aux cyberattaques visant les systèmes

[1] Le terme « système de contrôle-commande » est employé dans le reste de la présente publication pour désigner les systèmes de contrôle-commande qui utilisent des technologies numériques, dépendent de ces technologies ou sont compatibles avec ces technologies.

de contrôle-commande peut également ébranler la confiance dans la sûreté et la sécurité des installations nucléaires.

1.4. La nécessité de protéger les systèmes informatiques (y compris les systèmes de contrôle-commande) est établie dans les Recommandations de sécurité nucléaire sur la protection physique des matières et des installations nucléaires (INFCIRC/225/Révision 5) [2], au paragraphe 4.10, qui dispose que :

> « [l]es systèmes informatisés utilisés pour la protection physique, la sûreté nucléaire et la comptabilité et le contrôle des matières nucléaires devraient être protégés contre la compromission (cyberattaque, manipulation ou falsification, par exemple) conformément à l'*évaluation de la menace* ou à la *menace de référence*. »

1.5. La publication intitulée *La sécurité informatique dans les installations nucléaires* (collection Sécurité nucléaire n° 17 de l'AIEA) [3], propose des orientations visant spécialement les installations nucléaires sur la mise en œuvre d'un programme de sécurité informatique afin d'étayer les orientations énoncées dans la référence [2]. La référence [3] donne également des précisions sur des termes clefs tels que « sécurité informatique », « sécurité de l'information » et « cybersécurité ». Les expressions « sécurité de l'information » et « cybersécurité » sont, aux fins de la présente publication, considérées comme des synonymes de sécurité informatique et ne seront pas employées ici.

1.6. Il doit être expressément tenu compte de la sécurité informatique à toutes les phases du cycle de vie d'un système de contrôle-commande. L'expression « cycle de vie » (par opposition à durée de vie) laisse entendre que la vie du système est véritablement cyclique (comme dans le cas du recyclage ou du retraitement), et notamment que des éléments de l'ancien système sont utilisés dans le nouveau système. La référence [4] contient une liste des activités menées habituellement dans le cadre du cycle de vie d'un système de contrôle-commande.

1.7. Dans le passé, la sécurité informatique n'a pas fait l'objet d'une attention particulière lors de la conception des systèmes de contrôle-commande dans les installations nucléaires, car les systèmes câblés ou analogiques étaient supposés invulnérables aux cyberattaques en raison de la rigidité de leur mise en œuvre, de l'isolement et de la séparation des systèmes, ainsi que de la quasi-absence de communications interactives, en particulier avec des réseaux ou des systèmes externes. Le passage à la technologie numérique a modifié la nature des systèmes de contrôle-commande dans les installations nucléaires en permettant

l'interconnexion des systèmes de contrôle-commande reprogrammables (à distance ou localement) et fonctionnant de manière distincte.

1.8. L'utilisation accrue de composants et de dispositifs numériques programmables à usages multiples a entraîné une réduction de la diversité des systèmes de contrôle-commande. Cela inclut l'utilisation d'éléments et d'approches communs dans toute une série d'applications industrielles (par exemple, les protocoles de communication). Les actes de malveillance[2] visant ces technologies courantes dans d'autres secteurs pourraient également avoir une incidence sur une installation nucléaire.

1.9. Les personnes autorisées, qu'elles se trouvent sur le site ou sur un site éloigné, qui ont un accès logique ou physique aux systèmes de contrôle-commande peuvent, en tant qu'agresseurs internes, constituer une menace pour la sûreté et la sécurité d'une installation nucléaire. Ces agresseurs internes peuvent être des salariés de l'installation ou du personnel employé par des vendeurs, des prestataires ou des fournisseurs, pouvant utiliser leur accès autorisé pour perpétrer des actes malveillants. Le besoin de protection des systèmes informatiques contre les menaces internes est reconnu dans la référence [5].

OBJECTIF

1.10. L'objectif de la présente publication est de proposer des orientations sur la sécurité informatique destinées à protéger les systèmes de contrôle-commande dans les installations nucléaires contre des actes malveillants qui pourraient empêcher ces systèmes de remplir leurs fonctions liées à la sûreté et à la sécurité. La présente publication est principalement consacrée à l'exploitation des installations nucléaires en toute sécurité, mais l'application de ces orientations peut également contribuer à l'amélioration de la sûreté et de la performance d'exploitation des installations nucléaires.

1.11. La présente publication s'adresse aux autorités compétentes, et notamment aux organismes de réglementation, ainsi qu'au personnel chargé de la gestion, de l'exploitation, de la maintenance et de l'ingénierie des installations nucléaires, aux vendeurs, prestataires et fournisseurs de systèmes de contrôle-commande, aux concepteurs de systèmes de contrôle-commande, aux laboratoires de

[2] Les actes de malveillance n'incluent pas les événements provoqués par une erreur humaine ou par des défaillances aléatoires de matériel ou de composants.

recherche et aux autres organismes s'intéressant à la sûreté et à la sécurité des installations nucléaires.

PORTÉE

1.12. La présente publication porte sur l'application de mesures de sécurité informatique aux systèmes de contrôle-commande qui assurent des fonctions de sûreté, de sécurité[3] ou des fonctions auxiliaires dans les installations nucléaires. Ces mesures ont pour but de protéger les systèmes de contrôle-commande contre des actes malveillants perpétrés par des personnes ou des organismes. La présente publication porte également sur l'application de ces mesures aux environnements de développement, de simulation et de maintenance de ces systèmes.

1.13. Les orientations proposées dans la présente publication s'appliquent aux systèmes de contrôle-commande dans les nouvelles installations nucléaires[4] et aux nouveaux systèmes de contrôle-commande dans les installations existantes. Ces orientations devraient être mises en œuvre dans toute la mesure du possible pour les anciens systèmes de contrôle-commande dans les installations existantes, y compris les systèmes qui n'utilisent pas les technologies numériques.

1.14. Bien qu'ils ne soient pas expressément abordés dans la présente publication, d'autres systèmes en interface et systèmes de technologies de l'information et de la communication (TIC) comme le système de contrôle des activités et le système de communication, peuvent entraîner des risques pour le(s) système(s) de contrôle-commande. Il faut tenir compte de ces risques lors de la conception et de la mise en œuvre des mesures de sécurité informatique destinées aux systèmes de contrôle-commande dans une installation. Les mesures de sécurité informatique destinées à ces systèmes peuvent être différentes de celles qui sont appliquées aux systèmes de contrôle-commande et doivent être évaluées et adaptées de manière appropriée.

1.15. La présente publication ne propose pas d'orientations détaillées sur les considérations de sûreté relatives aux systèmes de contrôle-commande. On trouvera des orientations de cet ordre dans les références [4, 6]. En outre, la présente publication ne définit ni ne modifie les termes techniques employés

---

[3] Les systèmes assurant des fonctions de sécurité sont notamment les systèmes utilisés pour la protection physique et la comptabilité et le contrôle des matières nucléaires.

[4] Une nouvelle installation est une installation qui n'est pas encore parvenue à l'étape de la mise en service.

dans les normes de sûreté de l'AIEA et dans d'autres publications de l'AIEA relatives à la sûreté. Ces termes sont mis en avant dans la présente publication, lorsqu'ils sont employés, et leurs définitions figurent dans le Glossaire de sûreté de l'AIEA [7].

STRUCTURE

1.16. À la suite de cette introduction, la présente publication est divisée en quatre sections. La section 2 présente une vue d'ensemble des systèmes de contrôle-commande utilisés dans les installations nucléaires et du rôle de la sécurité informatique dans la protection de ces systèmes contre les cyberattaques. La section 3 présente la relation entre la sécurité informatique et la sûreté des systèmes de contrôle-commande. La section 4 présente les orientations sur la sécurité informatique qui doivent être appliquées au cours des différentes phases du cycle de vie des systèmes de contrôle-commande, y compris pendant le déclassement d'une installation.

2. CONCEPTS CLÉS POUR LA SÉCURITÉ INFORMATIQUE DES SYSTÈMES DE CONTRÔLE-COMMANDE

2.1. Les systèmes de contrôle-commande dans les installations nucléaires permettent de suivre et contrôler les processus et le matériel. Ces systèmes sont notamment les suivants :

a) les systèmes SCADA (contrôle et acquisition de données) ;
b) les systèmes de commande répartis ;
c) les systèmes de contrôle numérique centralisés ;
d) les systèmes de contrôle composés de contrôleurs logiques programmables ;
e) les micro-contrôleurs et les appareils « intelligents » ;
f) les systèmes utilisant des dispositifs logiques programmés (par exemple des réseaux de portes programmables par l'utilisateur, des dispositifs logiques programmables complexes et des circuits intégrés à application spécifique).

Les systèmes similaires qui contrôlent les installations industrielles sont souvent appelés « systèmes de contrôle industriel ».

2.2. Les systèmes de contrôle-commande sont conçus pour assurer un comportement sûr, sécurisé, fiable et déterministe de l'installation nucléaire en fonctionnement normal ou anormal[5]. Les considérations et les mesures relatives à la conception destinées à améliorer la sûreté peuvent également être bénéfiques pour la sécurité. Par exemple, les mesures relatives à la conception telles que la performance déterministe, les méthodes permettant d'éviter, de détecter et de tolérer les défaillances, la gestion de la configuration, la vérification et la validation indépendantes et d'autres méthodes d'essai avancées peuvent assurer une certaine défense contre des tentatives malveillantes visant à modifier le comportement des systèmes de contrôle-commande.

2.3. La conception de l'architecture globale de contrôle-commande dans les installations nucléaires intègre des concepts qui peuvent contribuer à la sécurité informatique en atténuant les effets d'un dysfonctionnement intentionnel ou accidentel[6], tels que l'indépendance, la redondance, la défense en profondeur en matière de sûreté et la diversité[7]. L'expression « défense en profondeur en matière de sûreté » est employée dans la présente publication pour désigner la défense en profondeur définie dans le Glossaire de sûreté de l'AIEA [7], afin de la distinguer de l'application du concept similaire, mais axé sur la sécurité, de « défense en profondeur » (défini dans les Fondements de la sécurité nucléaire [8]) dans la mise en œuvre des mesures de sécurité informatique, décrite à la section 4.

2.4. La mise en œuvre de ces concepts dans l'architecture globale de contrôle-commande d'une installation et d'autres mesures relatives à la conception devraient être évaluées afin de déterminer leur contribution à la sécurité informatique. Par exemple, la diversité de la conception ou de la technologie est de nature à réduire les vulnérabilités communes des principaux systèmes de sûreté ou de contrôle, mais elle peut ajouter des vulnérabilités propres à chaque système.

---

[5] Dans le Glossaire de sûreté de l'AIEA [7], l'expression « fonctionnement anormal » est synonyme d'« incident de fonctionnement prévu ». Pour la présente publication, le premier terme est considéré comme plus facile à comprendre.

[6] L'expression « dysfonctionnement » est employée dans le présent texte pour désigner des situations qui n'ont pas été examinées précédemment (c'est-à-dire qui ne sont pas des incidents de fonctionnement prévus), mais pour lesquelles le système de contrôle-commande ne fonctionne pas comme prévu.

[7] L'indépendance, la redondance, la défense en profondeur en matière de sûreté et la diversité renvoient ici à des concepts particuliers utilisés dans le Glossaire de sûreté de l'AIEA [7].

2.5. Les orientations figurant dans la présente publication s'appliquent à tous les systèmes de contrôle-commande associés à une installation nucléaire, sauf indication contraire.

SÉCURITÉ INFORMATIQUE DES SYSTÈMES DE CONTRÔLE-COMMANDE

2.6. Le paragraphe 2.2 de la référence [2] dispose ce qui suit :

> « Le régime national de protection physique[8] devrait essayer d'atteindre ces objectifs comme suit :
>
> — Prévention d'un *acte malveillant* par la dissuasion et la protection des informations sensibles ;
> — Lutte contre une tentative d'*acte malveillant* ou un *acte malveillant* grâce à un système intégré de *détection*, de retardement et d'intervention ;
> — Atténuation des conséquences d'un *acte malveillant*. »

2.7. La manière dont la prévention, la gestion et l'atténuation peuvent être appliquées à la sécurité informatique des systèmes de contrôle-commande est par exemple :

— La prévention : installation de dispositifs de fermeture en cas de panne de courant qui bloquent les communications non autorisées des données pour réduire la possibilité d'une cyberattaque visant le réseau qui pourrait avoir des conséquences néfastes sur le système de contrôle-commande.
— La gestion, y compris la détection, le retard et l'intervention : grâce à l'inspection des fichiers journaux des événements du système, l'exploitant peut détecter les signes avant-coureurs et prendre des mesures de protection avant le début d'un acte malveillant qui pourrait nuire à la sûreté ou à la sécurité d'une installation.
— L'atténuation et la remise en état : si l'on découvre qu'un système de contrôle-commande est infecté par un logiciel malveillant, une fois que la propagation du logiciel malveillant a été arrêtée, l'exploitant déterminera si des mesures compensatoires de contrôle (par exemple, la mise à jour

[8] Dans le passé, l'expression « protection physique » a été employée pour décrire ce que l'on appelle maintenant la sécurité nucléaire des matières nucléaires et des installations nucléaires.

des signatures antivirus, l'installation de systèmes de prévention ou de détection des intrusions ou l'amélioration de ces systèmes, ou les deux) sont nécessaires pour empêcher une nouvelle infection, procéder à une remise sur pied du système, vérifier l'efficacité des mesures compensatoires de contrôle, restaurer le système et le remettre en service, après avoir effectué une analyse détaillée de la sûreté et vérifier l'intégrité du système, le cas échéant.

2.8. La protection des systèmes de contrôle-commande contre la compromission repose parfois sur la présomption qu'une seule mesure préventive suffit, comme l'isolement des systèmes par rapport à d'autres réseaux. Toutefois, une telle présomption risque d'entraîner une application insuffisante des mesures de gestion et d'atténuation, de sorte que la défaillance de cette seule mesure de sécurité informatique pourrait entraîner la compromission du système protégé.

2.9. Un grand nombre d'approches, de méthodes, de techniques, de normes et de lignes directrices différentes en matière de sécurité informatique ont été élaborées pour les systèmes TIC généraux. Certaines d'entre elles ne sont pas directement applicables aux systèmes de contrôle-commande dans les installations nucléaires, qui ont des besoins spécifiques dans le domaine de la sécurité informatique qui ne sont pas les mêmes que les systèmes TIC.

2.10. Néanmoins, étant donné que la sécurité informatique des systèmes de contrôle-commande ne peut être totalement séparée de la sécurité informatique des systèmes TIC, les exploitants et les organismes de réglementation devraient élaborer des politiques, des prescriptions, des mesures et des pratiques en matière de sécurité informatique qui prennent en compte les systèmes de contrôle-commande et les systèmes TIC de manière intégrée.

2.11. De nombreux systèmes de contrôle-commande ont un cycle de vie de plusieurs dizaines d'années, y compris des périodes pendant lesquelles il se peut que le vendeur ne puisse pas fournir d'assistance ou que l'assistance fournie soit inadéquate pour satisfaire aux prescriptions en matière de sécurité informatique[9] applicables aux systèmes. Il s'agit notamment de l'assistance fournie par le vendeur d'origine et par des tiers associés. Par exemple, au fil du temps, il peut arriver que les programmes antivirus n'assurent pas une protection suffisante contre l'exploitation des vulnérabilités des systèmes de contrôle-commande, en

[9] Dans la présente publication, on entend par « prescriptions en matière de sécurité informatique » les prescriptions écrites spécifiques imposées par l'autorité compétente concernée ou par l'exploitant pour se conformer aux prescriptions réglementaires.

raison d'une perte de compatibilité matérielle ou logicielle ou de l'impossibilité de continuer à fournir des mises à jour des signatures.

2.12. Dans la plupart des applications, les systèmes de contrôle-commande fonctionnent en temps réel et leurs actions sont effectuées dans des intervalles de temps stricts. Dans les installations nucléaires, ces actions sont par exemple le contrôle des conditions normales de fonctionnement, les actions protectrices, les actions de limitation et la signalisation des alarmes aux exploitants. Les mesures de sécurité informatique ne devraient pas entraver, empêcher ou retarder l'exécution des actions opérationnelles ou des actions de sûreté nécessaires. Les mesures de sécurité informatique destinées aux systèmes modernes de contrôle-commande peuvent permettre de prévenir, de détecter, de retarder les actes malveillants, d'intervenir face à de tels actes et d'en atténuer les conséquences, mais il faut veiller à ce que les mesures d'intervention n'entravent pas les fonctions de sûreté accréditées ou que le système ne soit pas prévu par la base de conception[10].

2.13. Les mesures de sécurité informatique appliquées rétrospectivement ou pas suffisamment appliquées peuvent introduire un facteur de complexité supplémentaire dans la conception du système de contrôle-commande, ce qui peut accroître la probabilité d'une défaillance ou d'un dysfonctionnement de ce système.

2.14. L'élément essentiel 9 des Fondements de la sécurité nucléaire [8] définit l'utilisation d'approches tenant compte des risques pour allouer des ressources et dans le cadre de la conduite des activités liées à la sécurité nucléaire. Une conception élaborée dans le cadre d'une approche axée sur la connaissance du risque pour tenir compte des considérations relatives à la sécurité dès le début du processus de conception peut être plus simple et plus robuste grâce à l'intégration des caractéristiques de sécurité, à l'élimination des fonctionnalités non nécessaires (par exemple, l'accès à distance) ou à la sécurisation renforcée du système.

---

[10] La base de conception pour les constituants importants pour la sûreté doit comporter des spécifications concernant la capacité, la fiabilité et la fonctionnalité requises dans des conditions de fonctionnement pertinentes, dans des conditions accidentelles et dans des conditions résultant de dangers internes et externes pour satisfaire aux critères d'acceptation précis pendant la durée de vie utile de l'installation nucléaire. La base de conception est en outre définie dans le Glossaire de sûreté de l'AIEA [7]. La base de conception des systèmes de contrôle-commande est décrite plus en détail dans la section 3 de la référence [4].

MESURES DE SÉCURITÉ INFORMATIQUE

2.15. Les mesures de sécurité informatique permettent de prévenir, de détecter, de retarder les actes malveillants et d'intervenir face à de tels actes et d'en atténuer les conséquences. Les mesures de sécurité informatique permettent également de veiller à ce que des actes non malveillants ne dégradent pas la sécurité et n'augmentent pas la vulnérabilité des systèmes informatiques aux actes malveillants.

2.16. Les mesures de sécurité informatique qui s'attaquent aux vulnérabilités du système ou fournissent des couches de protection peuvent être classées dans l'une des trois catégories suivantes : les mesures de contrôle technique, les mesures de contrôle physique ou les mesures de contrôle administratif. Ces trois catégories devraient être prises en compte et une combinaison appropriée devrait être choisie lors de la mise en place d'une sécurité informatique intégrée pour les systèmes de contrôle-commande.

2.17. Les mesures de contrôle technique sont le matériel et/ou le logiciel permettant de prévenir et de détecter les intrusions ou les autres actes malveillants, d'en atténuer les conséquences et de procéder à la remise en état. Il conviendrait de tenir compte de la capacité des mesures de contrôle technique d'assurer une protection continue et automatique lors de l'évaluation de leur efficacité par rapport aux mesures de contrôle physique ou administratif.

2.18. Les mesures de contrôle physique sont des barrières physiques qui protègent les instruments, les systèmes informatiques et les ressources auxiliaires contre les dommages matériels et empêchent les accès physiques non autorisés. Les mesures de contrôle physique sont entre autres les verrous, les cages, les dispositifs antifraude, les salles d'isolement, les barrières et les gardes.

2.19. Les mesures de contrôle administratif sont les politiques, procédures et pratiques conçues pour protéger les systèmes informatiques en fournissant des instructions pour les actions des salariés et du personnel employé par des organismes tiers. Les mesures de contrôle administratif précisent ce que les salariés et le personnel employé par des organismes tiers peuvent faire, doivent faire ou ont interdiction de faire. Les mesures de contrôle administratif concernant les installations nucléaires sont notamment les mesures de contrôle opérationnel et les mesures de contrôle de gestion.

APPLICATION D'UNE APPROCHE GRADUÉE

2.20. L'exploitant devrait imposer des prescriptions en matière de sécurité informatique en se fondant sur une approche graduée qui tient compte du risque et prend en considération les éléments suivants :

— l'importance des fonctions du système de contrôle-commande tant pour la sûreté (c'est-à-dire la classification du point de vue de la sûreté) que la sécurité ;
— les menaces identifiées et évaluées pour l'installation ;
— l'attrait du système de contrôle-commande pour les adversaires potentiels ;
— les vulnérabilités du système de contrôle-commande ;
— l'environnement opérationnel ;
— les conséquences qui pourraient résulter directement ou indirectement d'une compromission du système.

Cette approche pourrait se fonder sur les résultats d'une évaluation des risques liés à la sécurité informatique.

2.21. Dans une approche graduée, les prescriptions en matière de sécurité informatique sont définies proportionnellement aux conséquences que pourrait avoir une attaque. Une compromission d'une fonction du système de contrôle-commande peut avoir les conséquence suivantes, allant des plus graves aux moins graves :

— La fonction est indéterminée. Les effets de la compromission entraînent une altération non observée de la conception ou de la fonction du système.
— La fonction se comporte de manière inattendue ou effectue des actions inattendues qui sont observables par l'exploitant.
— La fonction échoue.
— 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).

2.22. Les niveaux de sécurité informatique devraient être appliqués selon les indications figurant dans la présente publication aux systèmes de contrôle-commande afin de permettre la mise en œuvre d'une approche graduée de la sécurité informatique.

2.23. On trouvera dans la référence [3] un exemple de l'application d'une approche graduée utilisant des niveaux de sécurité[11]. Inversement, on trouvera dans la référence [9] un exemple de l'application d'une approche graduée relative à la sûreté.

NIVEAUX DE SÉCURITÉ INFORMATIQUE

2.24. Les niveaux de sécurité informatique et les classes de sûreté sont des concepts distincts mais liés. La classification du point de vue de la sûreté d'un constituant important pour la sûreté trouve ses fondements dans l'importance de sa fonction pour la sûreté ainsi que dans les conséquences que pourrait avoir sa défaillance.

2.25. Chaque fonction du système de contrôle-commande associée à une installation se voit généralement attribuer un niveau de sécurité informatique pour indiquer le degré de protection de la sécurité informatique dont elle a besoin. Chaque niveau nécessitera différentes séries de mesures de sécurité informatique pour satisfaire aux prescriptions en matière de sécurité informatique pertinentes. Les niveaux de sécurité sont souvent définis en fonction des objectifs de sécurité d'un organisme. On trouvera dans la référence [10] des renseignements complémentaires sur l'application des niveaux et des zones de sécurité.

2.26. Les sous-systèmes et composants des systèmes de contrôle-commande dont le dysfonctionnement pourrait compromettre la sûreté nucléaire (y compris l'atténuation des accidents), la sécurité nucléaire ainsi que la comptabilité et le contrôle des matières nucléaires sont recensés et se voient attribuer des niveaux de sécurité en fonction de leur contribution à la fonction du système de contrôle-commande.

2.27. L'exploitant attribue un niveau de sécurité à un système, un sous-système ou un composant de contrôle-commande en fonction des conséquences que pourrait avoir sa défaillance ou son dysfonctionnement, y compris un dysfonctionnement d'une manière qui diffère de sa conception ou des modes de défaillance concevables qui seraient définis dans une analyse de la sûreté de l'installation. Le niveau de sécurité informatique attribué à un système, sous-système ou composant de contrôle-commande est propre à ce système, sous-système ou composant et est indépendant de son environnement.

---

[11] On entend par « niveaux de sécurité » et par « zones de sécurité » tout au long de la présente publication les niveaux de sécurité informatique et les zones de sécurité informatique.

ZONES DE SÉCURITÉ INFORMATIQUE

2.28. Le concept de zone de sécurité implique le regroupement logique et/ou physique de systèmes informatiques qui sont soumis à prescriptions communes en matière de sécurité informatique, du fait des propriétés inhérentes aux systèmes ou de leurs connexions à d'autres systèmes. Tous les systèmes situés dans une seule zone sont protégés au même niveau de sécurité, à savoir le niveau attribué à la fonction du système de contrôle-commande ayant le niveau de sécurité le plus élevé dans la zone. Le regroupement des systèmes de contrôle-commande en zones de sécurité peut simplifier l'application et la gestion des mesures de sécurité informatique.

2.29. Les considérations relatives à la mise en œuvre des zones de sécurité devraient remplir les critères suivants :

— les systèmes appartenant à la même zone ont des besoins similaires pour ce qui est des mesures de sécurité informatique ;
— les systèmes appartenant à la même zone forment une zone constituant un espace fiable pour les communications internes entre ces systèmes (c'est-à-dire une zone constituant un espace fiable interne) ;
— chaque zone comprend des systèmes qui ont la même importance ou une importance comparable pour la sécurité et la sûreté de l'installation ou qui constituent un espace fiable interne ;
— les dispositions relatives à l'architecture de sûreté du système (par exemple, la redondance, la diversité, la séparation géographique et électrique, le critère de défaillance unique) sont maintenues ;
— des mesures de contrôle technique sont mises en œuvre aux limites des zones afin de restreindre le flux de données et la communication entre les systèmes situés dans des zones différentes (par exemple, un site distant) ou auxquels ont été attribués des niveaux de sécurité différents ;
— les supports amovibles, les appareils mobiles et autre matériel temporaire qui nécessitent un accès logique ou physique à un système ne sont utilisés qu'à l'intérieur d'une seule zone ou d'un ensemble défini de zones ;
— on peut diviser les zones en sous-zones pour améliorer la configuration.

2.30. Lorsque des zones de sécurité sont utilisées dans une installation, certains systèmes ou composants de contrôle-commande peuvent être attribués à une zone dont le niveau de sécurité est plus strict que leur propre niveau de sécurité inhérent. Par exemple, un dispositif de communication qui n'exécute que des fonctions de sûreté ou de sécurité de niveau inférieur peut se voir attribuer le même niveau de sécurité que le système de protection du réacteur, s'il est situé

dans la zone de sécurité du système de protection du réacteur. Cette attribution est due à la possibilité d'une utilisation malveillante du dispositif pour compromettre les composants du système de protection du réacteur, qui sont de la plus haute importance pour la sûreté. En outre, l'utilisation de la zone de sécurité du système de protection du réacteur permet de créer une zone constituant un espace fiable interne. Il ne sera donc pas nécessaire de mettre en œuvre des mesures de sécurité informatique supplémentaires entre les composants du système de protection du réacteur et le dispositif de communication.

3. APPROCHE DE LA SÉCURITÉ INFORMATIQUE DES SYSTÈMES DE CONTRÔLE-COMMANDE TENANT COMPTE DES RISQUES

3.1. Une approche de la sécurité informatique des systèmes de contrôle-commande tenant compte des risques peut faire appel à des évaluations du risque pour identifier les vulnérabilités d'une installation à une cyberattaque en lien avec ces systèmes et déterminer les conséquences qui pourraient résulter de l'exploitation fructueuse de ces vulnérabilités. Des mesures de sécurité informatique peuvent alors être mises en œuvre sur la base des résultats des évaluations du risque.

3.2. Les systèmes de contrôle-commande étant souvent essentiels pour la sûreté des installations, une bonne connaissance de la sûreté nucléaire peut aider à évaluer le risque, à élaborer des mesures de sécurité informatique pour le système de contrôle-commande, à évaluer les conflits potentiels entre la sûreté et la sécurité et à examiner les moyens de résoudre ces conflits. Par exemple, des adversaires pourraient saboter une installation en lançant une cyberattaque visant les systèmes de contrôle-commande d'une installation, ce qui pourrait avoir des conséquences pour la sûreté et la sécurité. Ces attaques pourraient provoquer des défaillances des systèmes de contrôle-commande ou les faire fonctionner d'une manière différente de celle qui est prévue ou des modes de défaillance analysés. Les actes malveillants peuvent avoir une incidence sur un seul ou sur plusieurs systèmes de contrôle-commande. Par exemple, les actes malveillants peuvent contourner les multiples niveaux de défense en profondeur pour la

sûreté ou provoquer leur défaillance simultanée[12]. Les actes malveillants peuvent également allier des cyberattaques à des éléments d'attaque physique.

3.3. Une sécurité informatique inadéquate ou un système de contrôle-commande compromis peut mettre en péril la sûreté d'une installation. Par exemple, si un système de contrôle-commande est compromis, un adversaire peut obtenir des données qui fournissent les informations critiques nécessaires pour planifier une attaque ou modifier des données qui facilitent le sabotage des systèmes de l'installation ou l'enlèvement non autorisé de matières nucléaires. Il se pourrait aussi qu'une cyberattaque entraînant un sabotage déclenche un accident ou dégrade la performance d'une fonction de sûreté. Une telle attaque pourrait également entraîner une perte de disponibilité du système.

3.4. Les cyberattaques visant les systèmes de contrôle-commande pourraient également avoir des conséquences qui permettent l'enlèvement non autorisé de matières nucléaires d'une installation. Les systèmes de contrôle-commande remplissant des fonctions de protection physique ou de comptabilité et de contrôle des matières nucléaires peuvent faire l'objet de cyberattaques, ce qui pourrait mettre une installation dans une situation dont le plan de sécurité du site n'a pas tenu compte. Un acte malveillant pourrait également allier une cyberattaque visant ces systèmes à des éléments d'attaque physique, l'objectif étant l'enlèvement de matières nucléaires sans autorisation.

3.5. Par conséquent, les mesures de sécurité informatique destinées aux systèmes de contrôle-commande doivent chercher des moyens de lutter à la fois contre les cyberattaques qui provoquent directement un sabotage et celles qui recueillent des informations susceptibles de faciliter le sabotage de l'installation nucléaire ou l'enlèvement non autorisé de matières nucléaires.

INTERFACE AVEC LA GESTION DES RISQUES LIÉS À LA SÉCURITÉ INFORMATIQUE DE L'INSTALLATION

3.6. L'exploitant devrait mettre en place un processus de gestion des risques liés à la sécurité informatique de l'installation visant à mettre en œuvre la sécurité informatique destiné à protéger les fonctions exécutées par les systèmes de contrôle-commande. Ce processus permet de recenser les vulnérabilités

[12] Les cinq niveaux de défense en profondeur pour la sûreté nucléaire sont présentés dans le détail dans la référence [7].

de l'installation[13] à une cyberattaque et de déterminer les conséquences d'une compromission d'une ou de plusieurs fonctions exécutées par les systèmes de contrôle-commande qui a atteint son but (ce qui peut inclure l'exploitation des vulnérabilités).

3.7. Les résultats des processus de gestion des risques liés à la sécurité informatique de l'installation devraient être notamment un recensement des fonctions de l'installation exécutées par les systèmes de contrôle-commande, y compris les systèmes auxiliaires et complémentaires qui, s'ils sont compromis, pourraient nuire à la sûreté, à la sécurité des matières nucléaires ou à la gestion des accidents. L'analyse de la sûreté de l'installation peut servir de base à la gestion des risques liés à la sécurité informatique d'une installation, mais cette analyse ne suffit pas à elle seule, car elle ne tient pas compte de tous les dysfonctionnements. Des dysfonctionnements dus à des cyberattaques pourraient mettre l'installation dans des conditions dont l'analyse de la sûreté n'a pas tenu compte.

3.8. Les résultats des processus de gestion des risques liés à la sécurité informatique de l'installation devraient répertorier les conséquences potentielles liées à la sûreté nucléaire, à la sécurité nucléaire et à la comptabilité et au contrôle des matières nucléaires résultant de la compromission d'un système en raison d'une cyberattaque visant les systèmes de contrôle-commande. Lors de l'analyse des conséquences d'une attaque visant un système de contrôle-commande, il conviendrait d'envisager que l'attaque puisse être un élément d'une attaque plus vaste visant plusieurs systèmes de contrôle-commande ou d'une cyberattaque et d'une attaque physique confondues. Cette analyse pourrait ensuite permettre d'attribuer les niveaux de sécurité appropriés aux différents systèmes et composants de contrôle-commande en fonction des conséquences que pourrait avoir leur défaillance ou leur dysfonctionnement.

3.9. Les niveaux de sécurité attribués aux systèmes de contrôle-commande peuvent être associés à une liste hiérarchique de conséquences potentielles pour la sécurité ou la sûreté. Par exemple, les états de la centrale, les conséquences du sabotage, le classement par catégories des matières nucléaires ou une combinaison de ces éléments pourraient être utilisés, comme dans les exemples figurant aux paragraphes 3.10–3.13 et 3.15.

3.10. Pour des raisons de sûreté, les états de la centrale pourraient permettre d'indiquer les conséquences que pourrait avoir sur la sûreté une cyberattaque

[13] La hiérarchie et les définitions des états de la centrale sont présentées dans le Glossaire de sûreté [7], sauf indication contraire.

visant les systèmes de contrôle-commande. Par exemple, les états de la centrale pourraient être associés à des niveaux de sécurité pour les systèmes de contrôle-commande, classés en ordre croissant, allant de la situation ayant les conséquences les moins graves à la situation ayant les conséquences les plus graves comme suit :

1) Le fonctionnement normal : une cyberattaque visant les systèmes de contrôle-commande ne peut pas faire fonctionner l'installation en dehors des limites et conditions spécifiées pour un fonctionnement normal.
2) L'incident de fonctionnement prévu : une cyberattaque visant les systèmes de contrôle-commande peut entraîner un écart de l'état de la centrale par rapport au fonctionnement normal d'une manière qui est prévue, mais qui, grâce aux dispositions appropriées prises lors de la conception, ne cause pas de dommages notables à des constituants importants pour la sûreté ou ne dégénère pas en conditions accidentelles.
3) L'accident de dimensionnement[14] : une cyberattaque visant les systèmes de contrôle-commande peut provoquer des conditions accidentelles qui restent dans les limites du dimensionnement de l'installation et pour lesquelles les dommages causés aux matières nucléaires (ou autres matières radioactives) et le rejet de matières radioactives restent dans des limites autorisées.
4) Les conditions hors dimensionnement : une cyberattaque visant les systèmes de contrôle-commande peut provoquer des conditions accidentelles qui ne sont pas considérées comme des accidents de dimensionnement, mais dont il est tenu compte dans le processus de conception de l'installation conformément aux méthodes de type « meilleure estimation » et dans lesquelles les rejets de matières radioactives sont maintenus dans des limites acceptables. Les conditions hors dimensionnement pourraient comprendre les conditions accidentelles graves.

3.11. Les conséquences du sabotage des fonctions exécutées par les systèmes de contrôle-commande pourraient également être associées à des niveaux de sécurité. Une telle approche supposerait que l'État définisse le seuil des conséquences radiologiques inacceptables, comme le recommande le paragraphe 3.44 de la référence [2]. La définition d'un seuil des conséquences radiologiques inacceptables peut être fondée sur des critères quantitatifs ou qualitatifs, qui peuvent être exprimés en termes de rejets de radionucléides (par exemple, un rejet dépassant une certaine quantité définie), de doses (par exemple, un rejet entraînant une dose de rayonnement dépassant une certaine valeur identifiée

[14] La hiérarchie et le texte qui y était joint pour l'accident de dimensionnement et les conditions additionnelles de dimensionnement sont tirés de la référence [7].

pour une personne située en un point identifié, généralement hors du site) ou de conditions de l'installation (par exemple, un sabotage pouvant entraîner un endommagement significatif du réacteur). Comme indiqué aux paragraphes 3.94 et 3.95 de la référence [11] :

> « les cibles dont le sabotage pourrait provoquer un rejet radioactif substantiel qui porterait sensiblement atteinte à la population et à l'environnement à l'extérieur de l'installation nucléaire doivent bénéficier de la plus haute protection possible. Dans la référence…[2], ce type d'événement est qualifié de situation ayant de graves conséquences radiologiques. »
>
> « L'État devrait définir le seuil de ces graves conséquences radiologiques. »

3.12. On trouvera dans la référence [11] un exemple de liste hiérarchique des conséquences que pourrait avoir un sabotage et résumées pour les fonctions du système de contrôle-commande, classées en ordre croissant, allant des conséquences les moins graves aux conséquences les plus graves comme suit :

— Les conséquences radiologiques en-dessous du seuil des conséquences radiologiques inacceptables : les cibles dont les conséquences sont peu importantes nécessitent donc un faible niveau de protection.
— Les conséquences radiologiques inacceptables peuvent être classées en trois catégories, allant des conséquences les moins graves aux conséquences les plus graves :
  - Niveau de conséquence C : un sabotage pourrait donner lieu à des doses aux personnes sur le site qui justifient une action protectrice urgente visant à réduire au minimum les effets sanitaires sur le site.
  - Niveau de conséquence B : un sabotage pourrait donner lieu à des doses ou à une contamination hors du site qui justifient une action protectrice urgente visant à réduire au minimum les effets sur la santé hors du site (peut également être considéré comme ayant des conséquences radiologiques graves).
  - Niveau de conséquence A : un sabotage pourrait être à l'origine d'effets déterministes graves sur la santé hors du site (pourrait être également considéré comme ayant des conséquences radiologiques graves).

3.13. Les niveaux de sécurité pourraient également être associés à la possibilité de l'enlèvement non autorisé de matières nucléaires. Les conséquences que pourraient avoir les cyberattaques visant les systèmes de contrôle-commande exécutant des fonctions de protection physique ou des fonctions de comptabilité et de contrôle des matières nucléaires pourraient être associées à des niveaux

de sécurité en fonction de la catégorie des matières pouvant faire l'objet d'un enlèvement non autorisé. Le tableau I de la référence [2] définit les critères de catégorisation des matières nucléaires et recense en outre les mesures recommandées pour la protection physique en fonction de cette catégorisation.

3.14. Il n'existe actuellement aucun consensus international sur un modèle applicable à une hiérarchie totalement intégrée de toutes les conséquences pour la sûreté et la sécurité découlant d'accidents et d'événements de sécurité nucléaire engendrés par des cyberattaques. Toutefois, l'exploitant ou l'État devrait établir une telle hiérarchie au niveau national.

3.15. Il conviendra peut-être de tenir compte également d'autres conséquences, telles que la perte de réputation, lors de l'évaluation des conséquences cumulées d'une cyberattaque visant les systèmes de contrôle-commande d'une installation. On trouvera dans la référence [12] une liste des conséquences possibles.

3.16. Les tactiques et les techniques des adversaires évoluent constamment et les installations nucléaires devraient favoriser une culture de sécurité nucléaire qui examine en permanence les risques liés à la sécurité informatique et permet l'adaptabilité du programme de sécurité informatique de l'installation. On trouvera d'autres explications sur la culture de sécurité nucléaire dans la référence [13].

3.17. La configuration du système et les activités associées aux systèmes de contrôle-commande améliorés grâce au matériel numérique devraient être analysées afin de repérer les modifications apportées aux voies logiques et physiques susceptibles d'ouvrir des possibilités pouvant être exploitées par un adversaire. Ces activités associées aux systèmes de contrôle-commande sont notamment les activités de maintenance temporaire, les processus d'achat, l'assistance fournie par le vendeur, la communication avec les appareils de terrain et les mises à jour manuelles du logiciel.

3.18. La gestion des risques liés à la sécurité informatique de l'installation est un processus itératif et cyclique qui pourrait inclure une analyse initiale, une identification et une évaluation de la menace, une définition des niveaux de sécurité, un examen périodique et une analyse actualisée. Un processus d'acceptation devrait être défini pour examiner et vérifier les résultats des analyses nouvelles ou actualisées.

3.19. S'agissant des nouvelles installations, la gestion des risques liés à la sécurité informatique de l'installation devrait être assurée dans le cadre du processus de conception et acceptée avant l'achèvement de la phase initiale de mise en service.

3.20. En ce qui concerne les installations existantes, les éléments d'entrée de la gestion nouvelle ou actualisée des risques liés à la sécurité informatique de l'installation peuvent être notamment une analyse de la sûreté, des éléments détaillés de la sûreté et de l'architecture des processus, ainsi que des résultats de la gestion des risques liés à la sécurité informatique de l'installation précédemment acceptés.

INTERFACE AVEC LA GESTION DES RISQUES LIÉS À LA SÉCURITÉ INFORMATIQUE DU SYSTÈME

3.21. La gestion des risques liés à la sécurité informatique du système devrait utiliser les résultats de la gestion des risques liés à la sécurité informatique de l'installation (s'ils sont disponibles) et les documents concernant la base de la conception des systèmes de contrôle-commande comme éléments d'entrée pour déterminer le risque que posent pour la sécurité les cyberattaques visant un ou plusieurs systèmes, sous-systèmes ou composants de contrôle-commande. Les risques liés à la sécurité informatique pour les systèmes de contrôle-commande qui ont fait l'objet d'une évaluation devraient être analysés et étayés par des documents.

3.22. L'exploitant devrait attribuer les rôles et responsabilités tout au long du cycle de vie du système de contrôle-commande pour l'évaluation et la gestion des risques liés à la sécurité informatique du système de contrôle-commande. La sécurité informatique nécessite des efforts ciblés de la part d'organismes et d'équipes pluridisciplinaires. Par exemple, l'exploitant peut créer des groupes de travail chargés de gérer les processus et activités de sécurité informatique et d'obtenir les autorisations.

3.23. L'exploitant devrait tenir un inventaire du système de contrôle-commande, notamment du logiciel, des sous-systèmes et des composants, qui est mis à jour et conservé tout au long du cycle de vie du système. L'exploitant devrait utiliser cet inventaire lorsqu'il assure la gestion des risques liés à la sécurité informatique du système.

3.24. Il conviendrait d'évaluer les composants du système de contrôle-commande et de leur attribuer le niveau de sécurité approprié sur la base de la

gestion des risques liés à la sécurité informatique du système. En ce qui concerne ces composants, il conviendrait de recenser les conséquences pour la sûreté et la sécurité qui pourraient résulter d'un dysfonctionnement ou d'une compromission. Si des zones de sécurité sont mises en place dans l'installation, il faudrait attribuer et identifier la zone de sécurité.

3.25. Lorsque l'exploitant assure la gestion des risques liés à la sécurité informatique du système, il devrait envisager la possibilité d'une cyberattaque à chaque phase du cycle de vie du système de contrôle-commande. L'exploitant devrait également tenir compte, dans son évaluation, du fait que les cyberattaques peuvent avoir une incidence sur un système ou sur plusieurs systèmes et qu'elles peuvent être utilisées parallèlement à d'autres formes d'actes malveillants occasionnant des dommages matériels. Il devrait être aussi tenu compte des actes malveillants susceptibles de modifier les signaux du processus, les données de configuration du matériel ou le logiciel dans la gestion des risques liés à la sécurité informatique du système.

3.26. En outre, tous les moyens d'attaque susceptibles d'être employés pour injecter un programme malveillant ou des données malveillantes dans le système de contrôle-commande devraient être pris en considération dans la gestion des risques liés à la sécurité informatique du système. Par exemple, un programme malveillant pourrait être introduit dans le système de contrôle-commande par des connexions de communication, des produits et services fournis ou des appareils portables temporairement connectés au matériel cible.

3.27. La gestion des risques liés à la sécurité informatique du système devrait déterminer la probabilité que chaque conséquence potentielle associée au système de contrôle-commande se produise, en utilisant comme éléments d'entrée les éléments suivants : la disponibilité de moyens d'attaque spécifiques qui pourraient être employés pour injecter un programme malveillant ou des données malveillantes dans le système de contrôle-commande ; l'application et l'efficacité des mesures de sécurité informatique ; les capacités de la menace ; et d'autres informations associées.

3.28. La gestion des risques liés à la sécurité informatique du système est un processus itératif et cyclique qui, à l'instar de la gestion des risques liés à la sécurité informatique de l'installation, suppose une analyse initiale, la mise en œuvre de mesures de sécurité informatique, un examen périodique et une analyse actualisée. Il conviendrait d'envisager le réexamen de la gestion des risques liés

à la sécurité informatique du système lorsque l'une des situations suivantes se produit :

— La gestion des risques pour la sécurité informatique de l'installation ou l'analyse de la sûreté de l'installation est révisée.
— Des modifications sont apportées au système.
— Des événements ou des incidents de sécurité pertinents se produisent.
— Des menaces ou vulnérabilités nouvelles ou ayant évolué ont été détectées.

3.29. La gestion des risques liés à la sécurité informatique du système devrait permettre de recenser les actes ou omissions d'origine humaine qui pourraient compromettre la sécurité.

ATTRIBUTION DES MESURES DE SÉCURITÉ INFORMATIQUE

3.30. Les orientations figurant aux paragraphes 3.31–3.34 s'appliquent à tous les systèmes, sous-systèmes et composants de contrôle-commande auxquels il est possible d'appliquer une approche graduée conformément au niveau de sécurité qui leur a été attribué.

3.31. Chaque système, sous-système ou composant de contrôle-commande devrait se voir attribuer un niveau de sécurité en fonction des conséquences que pourrait avoir sa défaillance ou son dysfonctionnement, tant pour la sûreté que pour la sécurité.

3.32. L'application de mesures de sécurité informatique à chaque système de contrôle-commande devrait être déterminée par le niveau de sécurité qui lui a été attribué ou par le niveau de sécurité de la zone de sécurité dans laquelle il est situé, le niveau le plus strict étant appliqué.

3.33. Il conviendrait de recenser et de définir les prescriptions en matière de sécurité informatique pour chaque niveau de sécurité. L'efficacité des mesures mettant en œuvre ces prescriptions devrait être évaluée pour faire en sorte de prévoir une protection suffisante pour les systèmes de contrôle-commande auxquels a été attribué chaque niveau de sécurité.

3.34. Si les mesures de sécurité informatique ne peuvent pas assurer une protection suffisante des systèmes de contrôle-commande à chaque niveau de sécurité, il conviendrait d'envisager des mesures supplémentaires ou des mesures de substitution, par exemple des caractéristiques de protection physique au

niveau de l'installation, des fonctions électroniques indépendantes, une nouvelle conception du système ou des mesures administratives qui éliminent certaines vulnérabilités ou réduisent les conséquences d'un dysfonctionnement.

INTERFACES ENTRE LA SÛRETÉ ET LA SÉCURITÉ

3.35. Comme il est indiqué au paragraphe 1.2 de la référence [8],

> « La sécurité et la sûreté nucléaires ont toutes deux pour but de protéger les personnes, les biens, la société et l'environnement. Les mesures de sécurité et de sûreté doivent être conçues et appliquées de manière intégrée afin de créer une synergie entre ces deux domaines et aussi de façon telle que les mesures de sécurité ne compromettent pas la sûreté et que les mesures de sûreté ne compromettent pas la sécurité. »

On trouvera dans les références [4 et 6] d'autres indications sur les considérations de sûreté relatives aux systèmes de contrôle-commande.

3.36. Le bien-fondé d'une mesure de sécurité informatique donnée dépendra des considérations de sûreté, de sécurité et des considérations opérationnelles. La contribution du personnel chargé de la sûreté, de la sécurité et de l'exploitation est nécessaire pour attribuer des mesures de sécurité informatique aux systèmes de contrôle-commande. Les mesures de sécurité informatique ne peuvent être définies indépendamment des préoccupations en matière de sûreté et les caractéristiques de sûreté ne peuvent être définies indépendamment des préoccupations en matière de sécurité. Par exemple, pour des raisons de sûreté, il se pourrait que certaines fonctions de sécurité (par exemple, la collecte des dossiers de vérification ou la génération d'alarmes de sécurité) doivent être mises en œuvre dans des systèmes distincts qui peuvent contrôler le système de contrôle-commande, mais qui n'ont pas d'effets négatifs sur la capacité du système d'exécuter ses fonctions essentielles. À défaut, les examens de sécurité actifs effectués uniquement lorsque les systèmes de contrôle-commande ne sont pas en service pourraient permettre d'atteindre les objectifs de sécurité tout en limitant l'impact sur les systèmes opérationnels.

3.37. Des mesures de sécurité informatique mal conçues pourraient introduire des modes de défaillance potentiels dans le système, augmenter la probabilité d'un fonctionnement intempestif et remettre en question la capacité du système d'exécuter de manière fiable sa fonction de sûreté. Par exemple, une mise en œuvre mal conçue d'un système de détection d'un logiciel malveillant ou d'un

virus dans le système de contrôle-commande pourrait accroître la complexité du système de contrôle-commande, augmenter la latence du système de contrôle-commande et avoir pour effet de rendre le système de contrôle-commande vulnérable à l'exploitation. Toutefois, une mesure de contrôle technique bien conçue, qui permet de s'assurer que seul un logiciel vérifié et validé est autorisé à tourner sur un système de contrôle-commande, pourrait améliorer la capacité de ce système d'exécuter de manière fiable sa fonction de sûreté, tout en offrant des avantages notables sur le plan de la sécurité.

3.38. De nombreuses fonctions qui sont conçues pour être intégrées dans les systèmes de contrôle-commande pour des raisons de sûreté peuvent également présenter des avantages sur le plan de la sécurité. On peut citer à cet égard la vérification de la validité, de l'authenticité et de l'intégrité des données reçues avant qu'elles ne soient utilisées dans une fonction du système de contrôle-commande.

3.39. Il peut arriver qu'une mesure de sécurité informatique ne puisse pas être mise en œuvre conformément au niveau de sécurité attribué à un système de contrôle-commande, par exemple par suite de conflits avec des fonctions de sûreté essentielles, mais ces exceptions devraient être analysées et justifiées de manière approfondie.

3.40. L'ensemble des mesures de sécurité informatique du système de contrôle-commande devrait fonctionner de concert et empêcher les points de défaillance unique (ou ne pas en introduire).

3.41. La stratégie de sûreté peut avoir un effet négatif sur la sécurité. Par exemple, la conception à des fins de sûreté suppose souvent de répartir les fonctions entre différents sous-systèmes (ou processeurs) afin d'isoler les effets d'une défaillance et de prévoir des systèmes redondants et présentant une grande diversité afin qu'une défaillance unique ne compromette pas des fonctions importantes. Ces stratégies entraînent une augmentation du nombre de sous-systèmes dans les systèmes de contrôle-commande, ce qui accroît du même coup le nombre de cibles visées par une cyberattaque. Il conviendrait donc de prendre des mesures visant à réduire le risque qu'une cyberattaque entraîne une perte de diversité ou de redondance du système. Les mesures de sécurité informatique ne devraient pas introduire de nouvelles vulnérabilités susceptibles d'entraîner des défaillances de cause commune entre ces systèmes redondants et diversifiés.

CONSIDÉRATIONS DE SÛRETÉ RELATIVES AUX MESURES DE SÉCURITÉ INFORMATIQUE

3.42. Les orientations figurant aux paragraphes 3.43–3.52 s'appliquent à tous les systèmes de contrôle-commande importants pour la sûreté.

3.43. La mise en œuvre des mesures de sécurité informatique ne devrait pas compromettre les fonctions essentielles de sûreté et la performance du système de contrôle-commande.

3.44. Ni le fonctionnement normal ni le fonctionnement anormal d'une mesure de sécurité informatique ne devrait avoir d'effets négatifs sur la capacité d'un système de contrôle-commande de remplir sa fonction de sûreté.

3.45. L'exploitant devrait identifier, documenter et prendre en considération dans les analyses de risques du système les modes de défaillance des mesures de sécurité informatique et la manière dont ces modes de défaillance auraient une incidence sur les fonctions du système de contrôle-commande

3.46. Les mesures de sécurité informatique qui protègent l'interface homme-système ne devraient pas porter atteinte à la capacité de l'exploitant de maintenir la sûreté de l'installation. L'exploitant devrait également tenir compte des effets négatifs tels que l'interception et la modification des données de processus envoyées à l'interface homme-système (arnaque, par exemple) dans le but d'empêcher ou de retarder l'actionnement par l'exploitant d'une fonction de sûreté (par exemple, déclenchement manuel).

3.47. Les mesures de sécurité informatique qui ne peuvent pas être intégrées sur le plan pratique dans le système de contrôle-commande devraient être mises en œuvre indépendamment du système de contrôle-commande. Des mesures de contrôle administratif supplémentaires peuvent être nécessaires pour utiliser et maintenir ces dispositifs distincts.

3.48. Des mesures de sécurité informatique intégrées dans les systèmes de contrôle-commande devraient être élaborées conformément aux orientations relatives aux systèmes de gestion figurant dans la référence [14] ou à un autre système de gestion équivalent et être qualifiées au même niveau que le système dans lequel sont intégrées les mesures de sécurité informatique.

3.49. En cas de conflit entre la sûreté et la sécurité, les considérations relatives à la conception dont il est tenu compte pour garantir la sûreté devraient être

maintenues, à condition que l'exploitant recherche une solution compatible pour satisfaire aux prescriptions en matière de sécurité informatique. Des mesures compensatoires de sécurité informatique devraient être mises en œuvre pour ramener le risque à un niveau acceptable et être appuyées par une justification argumentée et une analyse des risques pour la sécurité. Les mesures mises en œuvre ne devraient pas reposer uniquement sur des mesures de contrôle administratif pendant une période prolongée. L'absence de solution de sécurité ne devrait jamais être acceptée.

3.50. La responsabilité première de la conception, du choix et de la mise en œuvre des mesures de sécurité informatique devrait être clairement attribuée par l'exploitant, mais elle devrait s'exercer dans le cadre d'une collaboration entre le personnel chargé des activités relatives à la conception, à la maintenance, à la sûreté et à la sécurité du système de contrôle-commande.

3.51. L'analyse de la conception du système de contrôle-commande devrait démontrer que les mesures de sécurité informatique intégrées au système de contrôle-commande et celles qui sont mises en œuvre en tant que dispositifs distincts n'auront pas d'incidence négative sur les fonctions de sûreté accréditées des systèmes et composants importants pour la sûreté.

3.52. Le maintien des mesures de sécurité informatique ne devrait pas avoir d'effets négatifs sur la disponibilité des systèmes de contrôle-commande.

4. LA SÉCURITÉ INFORMATIQUE DANS LE CYCLE DE VIE DU SYSTÈME DE CONTRÔLE-COMMANDE

4.1. La conception des systèmes de contrôle-commande pour les installations nucléaires devrait être gérée dans le cadre du système intégré de gestion de l'installation[15] pour que toutes les prescriptions en matière de sécurité

[15] Conformément à la référence [7], le système de gestion est un « Ensemble d'éléments interdépendants ou interactifs (système) qui sert à établir les politiques et les objectifs et permet d'atteindre les objectifs de façon efficiente et efficace ». Dans la présente publication, ces éléments sont notamment la structure organisationnelle, la culture organisationnelle, les politiques et les processus, y compris ceux qui permettent de trouver et d'allouer les ressources (par exemple, personnel, matériel, infrastructure et environnement de travail) pour le développement des systèmes de contrôle-commande.

informatique soient prises en considération et mises en œuvre dans toutes les phases du cycle de vie du système de contrôle-commande et que ces prescriptions soient respectées dans la conception finale. La référence [14] établit les Prescriptions générales de sûreté applicables aux systèmes de gestion des installations nucléaires. En outre, dans la référence [8], le paragraphe 3.12 a) fait référence à l'importance des systèmes de gestion intégrés pour la sécurité nucléaire. La référence [3] traite plus en détail la relation globale entre les systèmes de gestion et la sécurité informatique.

4.2. Le paragraphe 2.13 de la référence [4] dispose ce qui suit :

> « Dans les systèmes numériques de contrôle-commande, la démonstration que le produit final est adapté à son objectif dépend fortement, mais pas exclusivement, de l'utilisation d'un processus de développement de qualité qui prévoit une spécification et une mise en œuvre disciplinées des prescriptions de conception. »

Il est ajouté au paragraphe 2.14 ce qui suit :

> « Dans le domaine de l'énergie nucléaire ainsi que dans d'autres domaines critiques pour la sûreté, comme l'aérospatiale, des processus de développement ont été appliqués et sont généralement représentés comme des modèles de cycle de vie, qui décrivent les activités de développement de systèmes électroniques et les relations entre ces activités. ... En règle générale, les activités relatives à une étape de développement donnée sont regroupées dans la même phase du cycle de vie ».

Il conviendrait de tenir compte de la sécurité informatique à toutes les phases du cycle de vie du système de contrôle-commande.

4.3. Comme il est indiqué au paragraphe 2.17 de la référence [4],

> « Trois niveaux fondamentaux des cycles de vie sont nécessaires pour décrire le développement des systèmes de contrôle-commande :
>
> — un cycle de vie global de l'architecture de contrôle-commande[16] ;
> — un ou plusieurs cycles de vie des systèmes de contrôle-commande ;

[16] Selon la définition du paragraphe 3.10 de la référence [4] ; « l'architecture globale de contrôle-commande est la structure organisationnelle des systèmes de contrôle-commande de la centrale. »

— un ou plusieurs cycles de vie des composants : les cycles de vie des composants sont généralement gérés dans le cadre du dévelop-pement de la plate-forme et indépendamment du niveau de l'architecture globale et des différents cycles de vie du système. Les cycles de vie des composants des systèmes numériques sont généralement structurés en cycles de vie distincts pour le développement du matériel et du logiciel. »

4.4. La définition des modèles de cycle de vie et les activités regroupées dans chaque phase du cycle de vie sont généralement déterminées par les développeurs et les exploitants d'un système, mais la définition et la mise en œuvre devraient être une initiative pluridisciplinaire portant sur de nombreux autres domaines, notamment la sécurité informatique. En règle générale, la principale responsabilité des systèmes de contrôle-commande incombe aux développeurs jusqu'à ce que les systèmes soient transférés à l'organisme exploitant aux fins de l'installation, de l'intégration et de la mise en service.

4.5. Étant donné que le cycle de vie des systèmes de contrôle-commande peut s'étendre sur plusieurs décennies, différents organismes peuvent jouer le rôle de développeurs ou d'autres rôles au cours du cycle de vie d'un système. Par exemple, il n'est pas rare qu'un vendeur se charge du développement initial et que l'acheteur apporte ultérieurement des modifications, surtout si celles-ci sont d'importance secondaire. Le fait que ces modifications soient mises au point par des organismes différents n'élimine pas la nécessité de mettre en œuvre des mesures de sécurité informatique dans toutes les phases du cycle de vie du système de contrôle-commande.

4.6. Dès que possible, la sécurité informatique devrait être planifiée de manière cohérente pour tous les cycles de vie de l'architecture, du système et des composants du système de contrôle-commande. Cette planification devrait spécifier les mesures de sécurité informatique qui doivent être appliquées à chaque phase pour protéger l'architecture, les systèmes et les composants de contrôle-commande contre des cyberattaques susceptibles de compromettre des fonctions importantes pour la sûreté. Il conviendrait d'envisager la possibilité de modifier les fonctions de sûreté ou les mesures de sécurité informatique au cours des phases ultérieures.

4.7. Le processus de développement du système de contrôle-commande devrait s'efforcer de réduire au minimum les vulnérabilités et les faiblesses potentielles de la sécurité informatique et d'identifier les vulnérabilités et les

faiblesses potentielles résiduelles à chaque phase du cycle de vie du système de contrôle-commande.

4.8. Bien que les modèles de cycle de vie puissent être organisés de nombreuses manières, les phases du cycle de vie théorique sont utilisées dans la présente publication comme cadre pour décrire les aspects de la sécurité informatique à prendre en considération au cours du cycle de vie du système de contrôle-commande. Ces phases sont les suivantes :

— la planification des processus ;
— la base de conception ;
— l'architecture globale et la répartition fonctionnelle du système de contrôle-commande ;
— la définition des prescriptions applicables au système de contrôle-commande ;
— le choix de constituants préalablement mis au point ;
— la conception détaillée et la mise en œuvre ;
— l'intégration du système ;
— la validation du système ;
— l'installation, l'intégration et la mise en service ;
— l'exploitation et la maintenance;
— la modification ;
— le déclassement.

4.9. Outre ces phases, le cycle de vie du système de contrôle-commande comporte également de nombreuses activités communes à toutes les phases du cycle de vie. Les activités courantes qui sont importantes pour la sécurité informatique sont les suivantes :

— l'assurance de la qualité ;
— la gestion de la configuration ;
— la vérification et la validation[17] ;

[17] Le Glossaire de sûreté de l'AIEA [7] définit à la fois la vérification et la validation. La vérification du système informatique est « Le *processus* consistant à garantir qu'une phase du cycle de vie du *système* satisfait aux prescriptions imposées par la phase précédente. » La validation du système informatique est « le *processus* consistant à tester et à évaluer le *système* informatique intégré (matériel et logiciel) afin de garantir sa conformité aux prescriptions fonctionnelles, aux prescriptions relatives aux performances et aux prescriptions concernant les interfaces. »

— l'évaluation de la sécurité ;
— la documentation.

4.10. Les prescriptions en matière de sécurité informatique et les activités pour chaque phase du cycle de vie devraient être à la mesure des conséquences résultant d'un accès, d'une utilisation, d'une divulgation, d'une manipulation, d'une perturbation ou d'une destruction non autorisés ou inappropriés du système de contrôle-commande. Il faudrait également envisager la possibilité de compromission d'un système, d'une structure d'appui ou d'informations qui pourraient compromettre la sûreté ou la sécurité.

4.11. Le reste de cette section est divisée en plusieurs sous-sections qui passent en revue les orientations générales sur la sécurité informatique qui s'appliquent à toutes les phases du cycle de vie et les orientations sur la sécurité qui sont propres à chaque phase du cycle de vie. Dans cet examen de la question, les phases ne sont examinées qu'une seule fois, mais les orientations devraient être appliquées au cycle de vie dans lequel la phase a lieu.

ORIENTATIONS GÉNÉRALES POUR LA SÉCURITÉ INFORMATIQUE

4.12. La politique de sécurité informatique d'une installation nucléaire précise les objectifs généraux de sécurité informatique de l'installation. S'agissant de la planification de la sécurité informatique de l'installation et du système, ces objectifs sont spécifiés dans la politique en termes clairs, précis et, si possible, mesurables. Les objectifs de l'installation sont transposés en objectifs du système. On trouvera dans la référence [3] d'autres orientations sur la sécurité informatique dans les installations nucléaires.

4.13. La politique de sécurité informatique devrait comporter des éléments relatifs à la sécurité des systèmes de contrôle-commande et, par conséquent, la politique devrait s'appliquer aux organismes chargés des activités dans le cycle de vie du système de contrôle-commande. Parmi ces organismes figurent notamment les exploitants, les vendeurs, les prestataires et les fournisseurs qui conçoivent, mettent en œuvre et achètent des systèmes, des logiciels et des composants de contrôle-commande.

4.14. Chaque organisme chargé des activités du cycle de vie du système de contrôle-commande devrait recenser et consigner par écrit les normes et procédures conformes aux politiques de sécurité applicables afin de veiller à

ce que le matériel, les logiciels et les microprogrammes réduisent au minimum l'existence de codes non documentés (par exemple, le codage de porte dérobée), de programmes malveillants (par exemple, les intrusions, les virus, les vers informatiques, les chevaux de Troie et les bombes programmées) et d'autres fonctions ou applications non désirées, non nécessaires ou non documentées, en vue de limiter au minimum le nombre de possibilités de cyberattaque.

4.15. La politique de sécurité informatique, le programme de sécurité informatique, les normes associées et les procédures applicables devraient porter sur chaque phase du cycle de vie du système de contrôle-commande afin de protéger les systèmes de contrôle-commande de l'installation contre toute compromission.

4.16. Les politiques, le programme, les normes et procédures de sécurité informatique, ainsi que toutes les mesures de sécurité informatique, devraient satisfaire aux prescriptions réglementaires et aux prescriptions en matière de sécurité informatique.

4.17. Les politiques, normes et procédures de sécurité informatique peuvent figurer dans le programme de sécurité du système de contrôle-commande d'un organisme ou être incorporées dans les plans du cycle de vie du système de contrôle-commande. Dans la pratique, une approche mixte est souvent adoptée.

ASPECTS DE LA POLITIQUE DE SÉCURITÉ INFORMATIQUE LIÉS AUX SYSTÈMES DE CONTRÔLE-COMMANDE

4.18. La politique de sécurité informatique des installations nucléaires devrait décrire l'application d'une approche graduée à la mise en œuvre des mesures de sécurité informatique pour les systèmes de contrôle-commande. L'approche graduée devrait être appliquée en fonction de l'importance pour la sûreté et la sécurité de chaque fonction du système de contrôle-commande (par exemple, en fonction du niveau de sécurité attribué à chaque système). Le personnel d'encadrement devrait définir et appliquer des objectifs clairs pour la politique de sécurité informatique qui soient cohérents avec les objectifs généraux de sûreté et de sécurité de l'installation et s'intéresser tout particulièrement à la sécurité des systèmes de contrôle-commande. On trouvera dans la référence [3] plus d'informations sur des aspects généraux à prendre en considération dans une politique et un programme de sécurité informatique.

4.19. La politique de sécurité informatique devrait inclure des éléments importants pour les systèmes de contrôle-commande, tels que :

— le contrôle des accès, y compris le contrôle physique et logique des accès, et l'utilisation des privilèges minimum ;
— la gestion de la configuration et des ressources, y compris la gestion des mots de passe, la gestion des mises à jour correctives, l'utilisation du système, la sécurisation renforcée du système, le contrôle de la configuration, les restrictions d'utilisation des appareils mobiles et des supports amovibles, les appareils et réseaux sans fil et l'accès à distance ;
— les activités de vérification de l'intégrité du système et des composants ;
— les processus d'achat ;
— la gestion des risques et de la menace, y compris les processus de collecte, d'analyse, de documentation et de mise en commun avec d'autres personnes qui ont besoin d'être informées des vulnérabilités, des faiblesses et des menaces, et d'agir en conséquence) ;
— l'intervention en cas d'incidents et la remise en état ;
— la vérification et les évaluations.

4.20. La politique de sécurité informatique devrait attribuer les rôles et les responsabilités aux organismes ou aux personnes qui exercent des activités relatives au cycle de vie du système de contrôle-commande.

PROGRAMME DE SÉCURITÉ INFORMATIQUE

4.21. Chaque organisme chargé de la mise en œuvre des activités du cycle de vie des systèmes de contrôle-commande devrait élaborer et mettre en œuvre un programme de sécurité informatique intégré ou distinct pour les systèmes de contrôle-commande.

4.22. Le programme de sécurité informatique devrait définir les rôles et les responsabilités pour chaque phase du cycle de vie du système de contrôle-commande pour chaque système de contrôle-commande.

4.23. Le programme de sécurité informatique devrait préciser que les organismes responsables appliquent le concept de défense en profondeur et définir les mesures de sécurité informatique destinées aux systèmes de contrôle-commande en fonction du niveau de sécurité qui leur a été attribué.

4.24. Le programme de sécurité informatique devrait spécifier la mise en œuvre de mesures de sécurité informatique destinées à protéger contre les actes malveillants commis par des agresseurs internes et la manipulation du système de contrôle-commande (y compris son intégrité) à chaque phase du cycle de vie du système de contrôle-commande.

4.25. Le programme de sécurité informatique devrait préciser que l'accès aux systèmes, composants, logiciels, données de configuration et outils de contrôle-commande est contrôlé pendant toutes les phases du cycle de vie du système de contrôle-commande. Le principe du privilège minimum et le besoin de disposer d'informations sont des exemples de pratiques de contrôle des accès.

4.26. Le programme de sécurité informatique devrait assurer la confidentialité des mesures de sécurité informatique, y compris la protection des documents correspondants, conformément au niveau de sécurité des systèmes de contrôle-commande dont il est question dans les documents.

4.27. Le programme de sécurité informatique devrait s'attaquer aux vulnérabilités et aux faiblesses potentielles en matière de sécurité informatique pour chaque phase du cycle de vie du système de contrôle-commande.

4.28. Le programme de sécurité informatique devrait définir le processus permettant de classer comme informations sensibles et compartimentées les informations relatives à la sécurité du système de contrôle-commande, telles que des détails concernant les vulnérabilités constatées dans les systèmes de contrôle-commande de l'installation ou les défenses spécifiques utilisées pour protéger les systèmes[18]. Dans la référence [8], une information sensible est définie comme une « [I]nformation, quelle que soit sa forme (logiciel compris), dont la divulgation non autorisée, la modification, l'altération, la destruction ou le refus d'utilisation pourrait compromettre la sécurité nucléaire ».

4.29. Les installations nucléaires et les organismes associés sont vivement encouragés à échanger d'autres informations non sensibles sur les vulnérabilités afin que les installations soient mieux préparées au cas où des informations sur les vulnérabilités des systèmes de contrôle-commande seraient diffusées et échangées entre des adversaires potentiels. On trouvera dans la référence [15] des orientations sur la sécurité de l'information nucléaire.

---

[18] On entend par « compartimentation » la division de l'information en plusieurs parties contrôlées indépendamment qui a pour but d'empêcher les agresseurs internes de rassembler toutes les informations nécessaires pour tenter de commettre un acte malveillant.

4.30. Le programme de sécurité informatique pour les systèmes de contrôle-commande devrait préciser qu'il est nécessaire d'effectuer des examens et des évaluations périodiques de la sécurité informatique et de les documenter à chaque phase du cycle de vie.

4.31. Le programme de sécurité informatique devrait spécifier les mesures de sécurité informatique qui assurent un environnement sécurisé propice aux activités de développement.

4.32. En ce qui concerne les anciens systèmes de contrôle-commande, il est possible d'accorder un rôle plus important aux mesures de contrôle administratif et à l'isolement que pour les systèmes contemporains. Le programme de sécurité informatique devrait définir et soutenir les mesures compensatoires supplémentaires de sécurité informatique qui sont nécessaires pour assurer la sécurité informatique des anciens systèmes de contrôle-commande.

ENVIRONNEMENT DE DÉVELOPPEMENT SÉCURISÉ

4.33. Les orientations figurant aux paragraphes 4.34–4.40 s'appliquent au développement de tous les systèmes, sous-systèmes et composants de contrôle-commande auxquels il est possible d'appliquer une approche graduée conformément au niveau de sécurité qui leur a été attribué.

4.34. Le système de contrôle-commande devrait être développé dans un environnement de développement sécurisé. Cela s'applique aux sites internes et externes. L'attribution d'un niveau de sécurité à cet environnement devrait tenir compte du niveau de sécurité du système dans l'environnement cible, du niveau de sécurité des autres systèmes développés ou stockés dans l'environnement de développement commun et des outils de développement. Les mesures de sécurité informatique de l'environnement devraient être évaluées pour confirmer leur conformité aux dispositions relatives au niveau de sécurité attribué.

4.35. L'environnement de développement sécurisé devrait inclure des mesures de contrôle administratif, telles que le contrôle de la configuration et la gestion des ressources.

4.36. Des mesures de contrôle physique devraient être utilisées pour contrôler les accès aux environnements de développement sécurisés.

4.37. Il conviendrait de vérifier le matériel d'essai et le matériel auxiliaire utilisés dans les environnements de développement du système de contrôle-commande pour confirmer que leur utilisation ne donne pas la possibilité d'introduire des programmes malveillants ou des données malveillantes dans l'environnement de développement sécurisé.

4.38. Il faudrait mettre en place des mesures de sécurité informatique pour contrôler le mouvement des données et des dispositifs pour toutes les phases de développement, afin que des programmes malveillants ou des données malveillantes ne soient pas introduits dans des environnements de développement sécurisés et de protéger les informations sensibles associées aux systèmes de contrôle-commande. Ces mesures de sécurité informatique devraient être notamment des mesures de contrôle administratif et technique (restrictions d'utilisation et procédures de contrôle des supports amovibles et des appareils mobiles par exemple). L'environnement de développement sécurisé devrait être considéré comme un environnement distinct, physiquement et logiquement indépendant de l'environnement opérationnel et de l'environnement économique.

4.39. Il faudrait mettre en œuvre des mesures de sécurité informatique pour protéger l'intégrité de l'environnement de développement sécurisé ainsi que des données d'entrée et de sortie de la conception (données, fichiers de configuration, mises à jour du logiciel et correctifs logiciels, par exemple) pendant les transferts entre l'environnement de développement sécurisé et l'environnement cible. Parmi ces mesures, on pourrait citer les systèmes automatisés de configuration des ressources dont l'avantage sur le plan de la sécurité pour l'environnement de développement sécurisé et l'environnement cible a été confirmé par une analyse.

4.40. Les outils de tiers ou de vendeurs utilisés pour le développement de systèmes de contrôle-commande devraient être testés, validés et protégés pour tenir compte du niveau de sécurité attribué à l'environnement de développement.

PLANS D'URGENCE

4.41. Les organismes qui mettent en œuvre une ou plusieurs activités du cycle de vie du système de contrôle-commande devraient élaborer des plans et procédures d'urgence visant à empêcher l'escalade et la progression d'un comportement anormal et à procéder à la remise en état après des incidents de sécurité informatique. Ces plans et procédures d'urgence devraient être examinés, faire périodiquement l'objet d'exercices et être mis à jour lorsque des anomalies ont été constatées.

4.42. L'exploitant devrait élaborer un plan d'intervention en cas d'incident de sécurité informatique axé sur des procédures permettant de définir et de repérer un comportement anormal ou suspect détecté sur les systèmes de contrôle-commande et les systèmes associés et d'intervenir en pareil cas.

4.43. Le plan d'intervention en cas d'incident de sécurité informatique devrait englober la collecte d'informations et les prescriptions prévues par la loi pour la conservation des preuves lors d'incidents de sécurité en vue d'étayer la phase d'analyse.

4.44. Le plan d'intervention en cas d'incident de sécurité informatique devrait affecter du personnel à l'équipe d'intervention en cas d'incident de sécurité informatique de l'installation. Cette équipe devrait être disponible dans l'installation pour intervenir en cas d'incident de sécurité informatique identifié. Le personnel affecté peut inclure notamment des experts connaissant tout particulièrement les systèmes de contrôle-commande ou des personnes possédant des compétences dans le domaine de la sécurité informatique.

4.45. Parmi les copies de sauvegarde et de restauration du système de contrôle-commande qui sont particulièrement importantes pour les plans et procédures d'urgence, il faudrait notamment citer le logiciel, les données essentielles et les fichiers de configuration. Ces copies devraient être stockées dans un lieu physique distinct de l'emplacement de la source afin de se prémunir contre toute défaillance de cause commune. Il conviendrait de prendre des mesures de sécurité informatique pour protéger ces copies contre le vol, la manipulation frauduleuse, l'effacement ou la destruction.

VENDEURS, PRESTATAIRES ET FOURNISSEURS DE SYSTÈMES DE CONTRÔLE-COMMANDE

4.46. Aux paragraphes 4.47–4.53, on entend par « vendeurs », « prestataires » et « fournisseurs » ceux qui fournissent à l'installation nucléaire le matériel numérique, le logiciel et les services destinés aux systèmes de contrôle-commande auxquels une approche graduée de la sécurité informatique est appliquée conformément au niveau de sécurité attribué au système. L'exploitant devrait veiller à l'application des orientations figurant aux paragraphes 4.47–4.53 dans le cadre de l'exécution d'un contrat avec les vendeurs, les prestataires ou les fournisseurs en question.

4.47. Les vendeurs et les vendeurs intermédiaires devraient avoir mis en place des processus de sécurité informatique solides et vérifiables.

4.48. Les vendeurs, les prestataires et les fournisseurs devraient satisfaire à toutes les prescriptions en matière de sécurité informatique applicables. Ils doivent, entre autres, appliquer les mesures de sécurité informatique spécifiées par l'exploitant, lors de l'assistance fournie sur place ou sur le lieu de travail du vendeur, du prestataire ou du fournisseur, ainsi que pendant le transit ou le stockage des biens achetés.

4.49. Le vendeur, le prestataire ou le fournisseur devrait avoir mis en place un processus de gestion de la sécurité informatique.

4.50. Les prescriptions en matière de sécurité informatique applicables sur les sites où un vendeur, un prestataire ou un fournisseur accomplit des tâches concernant les systèmes de contrôle-commande devraient être clairement spécifiées par contrat par l'exploitant en fonction du niveau de sécurité attribué au système, au sous-système ou au composant.

4.51. Un processus devrait permettre à l'exploitant et au vendeur, au prestataire ou au fournisseur de porter à leur connaissance réciproque les vulnérabilités et de coordonner les activités d'intervention et d'atténuation.

4.52. Le vendeur, le prestataire ou le fournisseur devrait démontrer qu'il dispose d'un mécanisme crédible pour être informé des vulnérabilités, les évaluer et les signaler à l'installation nucléaire pendant toute la durée de prestation de services contractuels. Cet aspect à prendre en considération peut être prolongé au-delà d'une période de garantie habituelle afin de soutenir le cycle de vie du matériel installé. Dans ces cas, il faudrait inclure le mécanisme pour la période prolongée dans les obligations contractuelles convenues par les vendeurs, les prestataires ou les fournisseurs.

4.53. Il conviendrait de procéder à une vérification et à une évaluation des vendeurs, des prestataires ou des fournisseurs chargés de la conception, du développement, de l'intégration et de la maintenance du contrôle-commande et de communiquer les résultats à l'exploitant.

FORMATION À LA SÉCURITÉ INFORMATIQUE

4.54. L'ensemble du personnel effectuant des tâches relatives aux systèmes de contrôle-commande, notamment des tâches en lien avec des informations sensibles associées à ces systèmes, devrait bénéficier d'une formation périodique à la sensibilisation à la sécurité informatique et aux procédures en la matière.

4.55. Tout le personnel qui a un accès physique ou logique aux systèmes de contrôle-commande devrait posséder les compétences requises en adéquation avec ses responsabilités en matière de sécurité informatique et bénéficier d'une formation spécialisée à la sécurité des systèmes de contrôle-commande en fonction de son rôle et de ses responsabilités afin de maintenir ses compétences.

4.56. Tout le personnel qui a un accès physique ou logique aux systèmes de contrôle-commande devrait atteindre un niveau de compétence approprié à son rôle pour appuyer les tâches de sécurité informatique et reconnaître les incidents potentiels de sécurité informatique. Ces personnes peuvent être informées de l'incidence des modifications apportées au système de contrôle-commande ou aux mesures de sécurité informatique associées auxquelles elles ont accès.

4.57. Le personnel recensé comme faisant partie de l'équipe d'intervention en cas d'incident de sécurité informatique devrait être formé à l'identification d'un incident de sécurité informatique et à l'intervention en cas de tels incidents. Il faudra peut-être pour cela utiliser un banc d'essai pour les systèmes de contrôle-commande en tant que composant du programme de formation à la sécurité du système de contrôle-commande.

4.58. Le personnel chargé de l'ingénierie, de l'exploitation et de la maintenance devrait être formé pour assurer le maintien des fonctions de sûreté et de sécurité du système de contrôle-commande.

4.59. Le personnel chargé de la conception du système de contrôle-commande devrait bénéficier d'une formation à la conception et à la programmation sécurisées des systèmes de contrôle-commande des installations nucléaires (par exemple, comment prendre en considération la sécurité dans la conception du logiciel).

ÉLÉMENTS COMMUNS DE TOUTES LES PHASES DU CYCLE DE VIE

4.60. Dans la plupart des cas, les prescriptions de sûreté relatives au système de gestion [14] et les orientations générales figurant dans les guides de sûreté associés [16, 17] donnent des indications suffisantes pour les activités du système de gestion liées à la sécurité informatique dans toutes les phases du cycle de vie du système de contrôle-commande. Il existe toutefois quelques domaines dans lesquels des indications plus précises sont nécessaires.

Systèmes de gestion

4.61. Les orientations figurant aux paragraphes 4.62–4.70 s'appliquent à tous les organismes qui effectuent une ou plusieurs activités du cycle de vie relatives aux systèmes de contrôle-commande auxquels une approche graduée de la sécurité informatique est appliquée conformément au niveau de sécurité attribué au système.

4.62. Les prescriptions de sûreté 6–8 applicables aux systèmes de gestion figurant aux paragraphes 4.8–4.20 de la référence [14] devraient être consultées lors de la rédaction des prescriptions réglementaires et/ou applicables à la sécurité informatique relatives aux systèmes de gestion.

4.63. Chaque organisme chargé du développement, du déploiement, de l'exploitation, de la maintenance ou de la mise hors service des systèmes ou des composants de contrôle-commande devrait tenir compte de la sécurité informatique des systèmes de contrôle-commande dans son système de gestion intégré.

4.64. Le système de gestion intégré de l'installation devrait appuyer les processus et procédures de sécurité informatique.

4.65. Les activités du cycle de vie devraient être menées dans le cadre d'un système de gestion prévoyant des dispositions adéquates relatives la sécurité des systèmes et composants de contrôle-commande.

4.66. Il conviendrait de mettre en place des processus et procédures vérifiables pour confirmer que les systèmes, sous-systèmes et composants de contrôle-commande qui jouent un rôle important dans le maintien de la sécurité informatique continuent à remplir leurs fonctions de sécurité tout au long de leur durée de vie opérationnelle.

4.67. Il faudrait prévoir d'examiner la sécurité des systèmes de contrôle-commande (par exemple, des inspections de la configuration) tout au long du cycle de vie du système de contrôle-commande afin de démontrer que les procédures de sécurité ont été suivies et que le niveau d'exécution requis a été atteint (par exemple, qu'aucun composant supplémentaire n'a été ajouté).

4.68. Il conviendrait de procéder à des inspections indépendantes[19] afin de vérifier que les processus et procédures de sécurité informatique sont mis en œuvre conformément au plan d'assurance de la qualité de l'exploitant.

4.69. Des dossiers détaillés des activités du cycle de vie devraient être produits et conservés de manière à permettre à tout moment de les examiner et de les comparer avec les prescriptions en matière de sécurité informatique. Ces dossiers devraient inclure tous les incidents de sécurité informatique et les mesures d'intervention ou d'urgence prises à la suite de ces incidents.

4.70. Les personnes autorisées ayant un accès logique ou physique privilégié aux systèmes de contrôle-commande devraient faire l'objet d'une évaluation de leur fiabilité, bénéficier d'une formation à la sécurité informatique et leur comportement devrait être soumis à observation conformément au programme d'atténuation des risques liés aux agresseurs internes de l'installation ou à un programme équivalent (voir la référence [5]).

Examens de la sécurité informatique et audits de sécurité informatique

4.71. Les orientations figurant aux paragraphes 4.72–4.77 s'appliquent à tous les organismes qui effectuent une ou plusieurs activités du cycle de vie relatives aux systèmes de contrôle-commande auxquels une approche graduée de la sécurité informatique est appliquée conformément au niveau de sécurité attribué au système.

4.72. Des examens de la sécurité informatique et des audits de sécurité informatique des systèmes de contrôle-commande et des activités associées devraient être effectués régulièrement pour s'assurer de la conformité avec les règlements, la politique de sécurité informatique et les bonnes pratiques de sécurité des systèmes de contrôle-commande.

[19] Le terme « indépendant » signifie que l'inspection est effectuée par une personne ou par un organisme différent de la partie faisant l'objet de l'examen.

4.73. Les examens de la sécurité informatique des systèmes de contrôle-commande devraient être indépendants et effectués par des évaluateurs internes et/ou externes qualifiés.

4.74. Des politiques et procédures, y compris les rôles et les responsabilités pour la réalisation de ces examens, devraient être définies et documentées.

4.75. Les examens de la sécurité informatique des systèmes de contrôle-commande devraient permettre de vérifier la mise en œuvre et l'efficacité des mesures de sécurité informatique qui leur sont associées.

4.76. Les tests d'évaluation intrusifs ne devraient pas viser les systèmes de contrôle-commande opérationnels. Les tests d'évaluation intrusifs supposent de tenter d'exploiter une vulnérabilité (par exemple, comme dans les tests de pénétration) susceptible de modifier les conditions de fonctionnement ou la configuration du système de contrôle-commande non prévue par sa base de conception. L'exploitant devrait envisager d'utiliser des méthodes contrôlées pour effectuer des tests sans charge utile même si l'installation est dans une condition qui empêche les conséquences radiologiques inacceptables, par exemple si l'installation est en état de mise à l'arrêt ou de déchargement du combustible. La réalisation et l'exécution de ces tests devraient être abordées dans les politiques et procédures de l'installation. Ces tests devraient être conçus spécifiquement pour chaque système. L'équipe d'intervention en cas d'incidents de sécurité informatique devrait prendre part aux tests d'évaluation intrusifs.

4.77. Il conviendrait d'archiver, de conserver et de protéger les dossiers relatifs aux examens de la sécurité informatique et aux données d'analyse associées tout au long du cycle de vie du système de contrôle-commande.

Gestion de la configuration de la sécurité informatique

4.78. Les orientations figurant aux paragraphes 4.79–4.87 s'appliquent à tous les systèmes, sous-systèmes et composants de contrôle-commande auxquels un niveau de sécurité a été attribué.

4.79. Les activités de contrôle de la configuration logicielle peuvent contribuer à la prévention et à la détection des incidents de sécurité informatique, bien qu'elles n'aient pas pour but premier de viser des objectifs spécifiques en matière de sécurité nucléaire. Il conviendrait d'analyser et de confirmer les avantages obtenus en matière de sécurité informatique grâce à l'exécution de ces activités avant de s'en attribuer le mérite. Par exemple, un incident de sécurité informatique

pourrait être détecté grâce à ces activités, mais le délai de déclenchement de l'intervention en cas de détection d'un incident serait probablement insuffisant pour protéger le système, par rapport au délai d'intervention dans un système de sécurité informatique qui incorpore des mesures de sécurité informatique en couches avec des éléments d'intervention automatique.

4.80. Les modifications non gérées de la configuration logicielle sont une source importante de nouvelles vulnérabilités et de situations imprévisibles. Généralement, le système de gestion de la configuration utilisé pour les systèmes de contrôle-commande est un système générique qui gère également de nombreux autres types de systèmes. Néanmoins, le système de gestion de la configuration devrait être utilisé de manière à incorporer la connaissance des systèmes de contrôle-commande et de leurs mesures de sécurité informatique.

4.81. La gestion de la configuration dépend de la gestion du changement, qui est un processus garantissant l'utilisation de processus de conception approuvés et une vérification et une validation appropriées en cas de modification apportée à un système informatique. Elle prévoit également le contrôle des documents qui appuient ces processus. Le paragraphe 5.26 de la publication intitulée *Application of the Management System for Facilities and Activities*, (n° GS-G-3.1 de la collection Normes de sûreté de l'AIEA [16]) dispose ce qui suit :

> « Les types de documents devant être contrôlés devraient inclure notamment, mais non exclusivement, les documents qui définissent le système de management, les prescriptions en matière de sûreté, les instructions de travail, les rapports d'évaluation, les dessins, les fichiers de données, les spécifications, les codes informatiques, les commandes et les documents connexes, ainsi que les documents des fournisseurs. »

4.82. Les mesures de sécurité informatique destinées aux systèmes de contrôle-commande utilisant le processus de gestion de la configuration de l'installation devraient être cohérentes avec les prescriptions relatives au contrôle de la configuration de l'installation applicables au système de contrôle-commande associé.

4.83. La gestion de la configuration devrait être assurée pour les mesures de sécurité informatique associées aux systèmes de contrôle-commande tout au long de leur cycle de vie.

4.84. La gestion de la configuration des mesures de sécurité informatique associées aux systèmes de contrôle-commande devrait comprendre notamment des

techniques et des procédures permettant d'analyser les effets des changements de configuration, d'approuver les changements de configuration, de veiller à ce que les versions du logiciel soient combinées correctement, d'autoriser l'utilisation des documents de conception et du logiciel et d'établir et de conserver un fichier classant par ordre chronologique les changements de configuration (par exemple, les versions des outils logiciels utilisées à un moment donné de la conception).

4.85. L'identification, le stockage et l'utilisation des composants de contrôle-commande et les mesures de contrôle technique associées devraient être protégés contre toute compromission.

4.86. Les documents de configuration des mesures de sécurité informatique associées aux systèmes de contrôle-commande devraient être conservés et protégés contre tout accès non autorisé ou toute compromission. Ces informations devraient être classées comme sensibles et l'accès à ces informations devrait être limité aux personnes qui ont besoin d'en avoir connaissance.

4.87. Des mesures de contrôle technique visant à limiter l'accès et à garantir l'intégrité devraient être appliquées au logiciel et aux fichiers de configuration pendant le développement, le transport, l'installation et l'exploitation.

Vérification et validation

4.88. Les orientations figurant aux paragraphes 4.89–4.94 s'appliquent à tous les systèmes, sous-systèmes et composants de contrôle-commande auxquels un niveau de sécurité a été attribué.

4.89. Chaque phase du processus de développement du système de contrôle-commande utilise les informations recueillies au cours des phases précédentes et fournit des résultats qui serviront de base aux phases ultérieures. Il conviendrait de procéder à la vérification après la conclusion d'une phase du processus de développement et avant le passage à la phase suivante du processus de développement et la vérification devrait comporter une évaluation des mesures de sécurité informatique.

4.90. Avant l'achèvement de la phase de mise en service du processus de développement du système de contrôle-commande, il conviendrait de valider le système de contrôle-commande pour veiller à ce que les prescriptions en matière de sécurité informatique soient satisfaites tout en continuant aussi à respecter les prescriptions fonctionnelles, les prescriptions relatives aux performances et les prescriptions concernant les interfaces. Le but est de déterminer avec un degré

d'assurance élevé que le système fonctionnera comme il se doit. La validation des mesures de sécurité informatique devrait être effectuée par des équipes, des personnes ou des groupes indépendants des concepteurs et des développeurs. L'étendue de la validation indépendante et le degré d'indépendance, par exemple, devraient être adaptés au niveau de sécurité attribué au système ou au composant concerné, que la validation soit effectuée par des employés du vendeur, du prestataire ou du fournisseur ou par des experts externes indépendants du vendeur, du prestataire ou du fournisseur.

4.91. Les activités de vérification et de validation devraient démontrer que le système de contrôle-commande satisfait aux prescriptions pertinentes en matière de sécurité informatique.

4.92. L'exploitant devrait vérifier et valider chaque mesure de contrôle technique afin de confirmer qu'elle assure au système de contrôle-commande la protection prévue et qu'elle ne réduit pas la fiabilité de ses fonctions de sûreté ou de sécurité.

4.93. Les mesures de sécurité informatique devraient être vérifiées et validées et les efforts consentis devraient correspondre au niveau de sécurité attribué au système de contrôle-commande associé ou à la classification aux fins de la sûreté du système de contrôle-commande, le niveau le plus strict étant appliqué.

4.94. Les activités de vérification et de validation devraient permettre de recenser, de constater et de documenter les vulnérabilités, faiblesses ou autres anomalies détectées, ainsi que leur résolution. Compte tenu de la taille et de la complexité de la plupart des systèmes informatiques modernes, il peut être difficile de faire en sorte que les résultats de ces activités soient exhaustifs ou qu'ils permettent de mettre au jour toutes les anomalies. Par exemple, les outils automatisés permettant d'effectuer des examens de code logiciel dépendent de la plateforme et du langage de programmation utilisés et peuvent n'avoir que partiellement atteint leur objectif. En outre, il est possible que certains systèmes d'exploitation, le code machine et les fonctions de bibliothèque pouvant être appelées, qui peuvent contenir des vulnérabilités susceptibles d'être exploitées, ne puissent pas être analysés.

Évaluations de la sécurité informatique

4.95. Les orientations figurant aux paragraphes 4.96–4.100 s'appliquent à tous les systèmes, sous-systèmes et composants de contrôle-commande auxquels un niveau de sécurité a été attribué.

4.96. Il conviendrait d'effectuer des évaluations de la sécurité informatique pour chaque phase du cycle de vie du système de contrôle-commande afin de recenser les menaces potentielles ainsi que les vulnérabilités et les faiblesses.

4.97. Il faudrait contrôler les informations à l'intention du public ou les informations provenant de sources librement accessibles, ainsi que les sources des vendeurs, des prestataires ou des fournisseurs et les sources des experts afin de repérer rapidement les changements dans le paysage de la menace et les nouvelles vulnérabilités.

4.98. Il conviendrait d'évaluer les menaces et les vulnérabilités nouvelles ou ayant évolué pour analyser leur incidence potentielle sur la sécurité informatique du système de contrôle-commande. Des mesures correctives (par exemple la modification des caractéristiques de sécurité) devraient être prises si ces modifications pouvaient entraîner des violations potentielles de la sécurité ou des risques inacceptables pour l'installation.

4.99. Chaque organisme chargé du développement, du déploiement, de l'exploitation, de la maintenance ou du déclassement de systèmes ou de composants de contrôle-commande devrait procéder périodiquement à des évaluations de la sécurité informatique et à des audits de sécurité informatique.

4.100. Les résultats des évaluations de la sécurité informatique devraient permettre d'actualiser la gestion des risques liés à la sécurité informatique du système.

Documents

4.101. Les orientations figurant aux paragraphes 4.102–4.106 s'appliquent à tous les systèmes, sous-systèmes et composants de contrôle-commande auxquels un niveau de sécurité a été attribué.

4.102. Les documents relatifs à la sécurité informatique du système de contrôle-commande permettent d'éviter les ambiguïtés et facilitent le fonctionnement correct et sans erreur, la surveillance, le dépannage, la maintenance, les modifications futures et la modernisation du système, ainsi que la formation du personnel de l'installation et du personnel d'appui technique.

4.103. Des documents devraient être générés afin d'enregistrer suffisamment d'informations relatives à la sécurité informatique des systèmes de contrôle-commande pour démontrer que les mesures de sécurité informatique sont

conçues, mises en œuvre et maintenues de manière à atteindre le niveau de protection exigé, conformément au niveau de sécurité attribué.

4.104. Il conviendrait de définir des documents d'entrée et de sortie relatifs à la sécurité informatique pour les activités de chaque phase du cycle de vie du système de contrôle-commande.

4.105. Les documents devraient garantir la traçabilité des prescriptions en matière de sécurité informatique dans toutes les activités du cycle de vie du système de contrôle-commande. L'ajout, la modification et la suppression de mesures de sécurité informatique destinées aux systèmes de contrôle-commande devraient être enregistrés.

4.106. Les documents devraient être protégés contre la divulgation non autorisée, la manipulation frauduleuse et l'effacement et contre la destruction en fonction du niveau de sécurité attribué au système de contrôle-commande associé.

Base de conception

4.107. Les orientations figurant aux paragraphes 4.108–4.114 s'appliquent à tous les systèmes, sous-systèmes et composants de contrôle-commande auxquels il est possible d'appliquer une approche graduée conformément au niveau de sécurité qui leur a été attribué.

4.108. Le paragraphe 3.11 de la référence [4] dispose que « La base de conception définit les fonctions, les conditions et les prescriptions pour le contrôle-commande global et pour chaque système de contrôle-commande. » Ces informations permettent ensuite d'attribuer des prescriptions en matière de sécurité informatique à chaque système de contrôle-commande et aux systèmes de sécurité auxiliaires. La base de conception permet également d'établir des spécifications relatives à la conception, à la mise en œuvre, à la construction, aux tests et à la performance applicables aux mesures de sécurité informatique.

4.109. Il conviendrait d'utiliser la base de conception de l'architecture globale de contrôle-commande et de chaque système de contrôle-commande pour orienter la conception des mesures de sécurité informatique devant être mises en œuvre pour satisfaire aux prescriptions réglementaires en matière de sécurité informatique (y compris la menace de référence ou l'évaluation de la menace). On trouvera d'autres indications sur la menace de référence (y

compris les évaluations de la menace et les autres énoncés de la menace) dans la référence [18].

4.110. Il conviendrait de définir dans la base de conception les considérations relatives à la conception de la sécurité informatique pour les systèmes de contrôle-commande et les systèmes de sécurité auxiliaires.

4.111. Le niveau de protection devant être appliqué à chaque système de contrôle-commande devrait être défini dans la base de conception, conformément au niveau de sécurité attribué défini dans la gestion des risques liés à la sécurité informatique de l'installation et du système.

4.112. La base de conception devrait spécifier les prescriptions applicables aux mesures de sécurité informatique, y compris les mesures de contrôle technique, physique et administratif.

4.113. La base de conception devrait spécifier les prescriptions de sûreté qui permettent des activités de validation efficaces, en vue d'empêcher les mesures de sécurité informatique de nuire à la performance des systèmes de contrôle-commande en matière de sûreté.

4.114. La base de conception devrait être maintenue et périodiquement mise à jour pour tenir compte des modifications apportées aux prescriptions réglementaires en matière de sécurité informatique ou des risques.

Contrôle des accès

4.115. Les orientations figurant aux paragraphes 4.116–4.120 s'appliquent à tous les systèmes, sous-systèmes et composants de contrôle-commande auxquels il est possible d'appliquer une approche graduée conformément au niveau de sécurité qui leur a été attribué.

4.116. Il conviendrait de contrôler l'accès physique et logique aux systèmes de contrôle-commande pour empêcher tout accès non autorisé. L'accès privilégié aux systèmes de contrôle-commande devrait être strictement contrôlé pour que seul le personnel autorisé ait accès à la configuration, au logiciel et au matériel existants ou soit en mesure d'y apporter des modifications. Il est possible de restreindre cet accès selon la fonction du personnel autorisé, tant sur le plan de la durée que du nombre de systèmes auxquels il est possible d'avoir accès.

4.117. Il faudrait réduire le plus possible le nombre de points d'accès aux réseaux et aux dispositifs afin de limiter au minimum le nombre de moyens d'attaque potentiels.

4.118. Les communications numériques devraient être limitées aux utilisations autorisées et contrôlées pour détecter toute activité anormale. Il conviendrait de prendre des mesures appropriées en cas de détection d'une activité anormale.

4.119. S'agissant des systèmes de contrôle-commande auxquels est attribué le niveau de sécurité le plus strict, il faudrait envisager des méthodes d'authentification plurifactorielle, pour autant que ces méthodes soient compatibles avec les interactions entre le personnel de l'installation et le système de contrôle-commande en fonction du temps.

4.120. Des procédures de gestion et d'attribution des rôles et des droits d'accès pour les comptes système et les comptes utilisateurs devraient être élaborées et mises à jour périodiquement. Les procédures devraient tenir compte du principe du privilège minimum. Ce processus peut être référencé ou intégré dans le programme de sécurité informatique de l'installation et dans le système de gestion intégrée de l'installation.

Protection de la confidentialité des informations

4.121. Les orientations figurant aux paragraphes 4.122–4.125 s'appliquent à tous les systèmes, sous-systèmes et composants de contrôle-commande auxquels il est possible d'appliquer une approche graduée conformément au niveau de sécurité qui leur a été attribué.

4.122. Lorsque les mesures de protection physique et de sécurité informatique visant à protéger la confidentialité des informations sont insuffisantes, il se peut que des informations soient divulguées sans autorisation, ce qui pourrait compromettre la protection physique ou la sécurité informatique du système ou de l'installation. La publication n° 23-G de la collection Sécurité nucléaire de l'AIEA [15] dispose ce qui suit :

> « Les informations sont du savoir, quelle que soit la forme sous laquelle elles existent ou sont exprimées. Elles incluent les idées, les concepts, les événements, les processus, les pensées, les faits et les schémas. Les informations peuvent être enregistrées sur des supports tels que papier, pellicule et supports magnétiques ou optiques ou être conservées dans des systèmes électroniques. »

4.123. Les informations relatives aux systèmes de contrôle-commande devraient être répertoriées (par exemple, les bases de données, les fichiers et documents associés, les composantes des changements, les simulateurs) et, le cas échéant, classées comme informations sensibles et sécurisées par des mesures appropriées. On trouvera dans les références [12, 15] des informations supplémentaires sur les mesures recommandées pour protéger les informations sensibles.

4.124. Les mesures de sécurité informatique devraient permettre de protéger la confidentialité des informations associées aux systèmes de contrôle-commande, qui peuvent être notamment des informations sur la conception, la fabrication, l'installation et le fonctionnement des systèmes de contrôle-commande et du matériel associé.

4.125. L'exploitant devrait appliquer des mesures de contrôle technique, physique et administratif à des fins de prévention, de détection et d'intervention en cas de divulgation ou d'exfiltration non autorisées d'informations sensibles liées aux systèmes de contrôle-commande.

Contrôle de la sécurité

4.126. Les orientations figurant aux paragraphes 4.127–4.130 s'appliquent à tous les systèmes, sous-systèmes et composants de contrôle-commande auxquels il est possible d'appliquer une approche graduée conformément au niveau de sécurité qui leur a été attribué.

4.127. Les prescriptions en matière de sécurité informatique applicables au contrôle de la sécurité des systèmes de contrôle-commande devraient être spécifiées en fonction des niveaux de sécurité attribués aux systèmes.

4.128. Le contrôle des systèmes de contrôle-commande exigeant le niveau de sécurité le plus élevé ou un niveau de sécurité élevé devrait faire preuve d'indépendance[20] ou de diversité dans les mesures de sécurité informatique déployées pour détecter les compromissions ou les dysfonctionnements. Des interfaces utilisateur pour le contrôle de la sécurité, des indications de compromission, des instruments d'enregistrement et des alarmes devraient être prévus à des emplacements appropriés et être adaptés et suffisants pour faciliter le contrôle efficace de la sécurité informatique dans tous les états de l'installation.

[20] La séparation des systèmes de contrôle du système de contrôle-commande, qui permet la séparation des tâches, est un exemple d'indépendance.

4.129. Il conviendrait d'établir des prescriptions applicables au contrôle des mesures de contrôle technique ou physique afin de faciliter l'adoption des mesures de sûreté et de sécurité nécessaires.

4.130. Les systèmes de contrôle-commande et les mesures de sécurité informatique qui leur sont associées devraient être contrôlés et répertoriés de façon continue. L'analyse devrait permettre de repérer les accès ou les modifications non autorisés. Il faudrait protéger l'intégrité de ces dossiers.

Considérations relatives à l'architecture défensive globale de sécurité informatique

4.131. Les orientations figurant aux paragraphes 4.132–4.140 s'appliquent à tous les systèmes, sous-systèmes et composants de contrôle-commande auxquels un niveau de sécurité a été attribué.

4.132. L'exploitant devrait spécifier une architecture défensive globale pour la sécurité informatique des systèmes de contrôle-commande dans laquelle tous les systèmes de contrôle-commande se voient attribuer un niveau de sécurité et sont protégés conformément aux prescriptions applicables.

4.133. L'architecture défensive devrait permettre de faciliter et de maintenir la capacité de prévention, de détection, d'atténuation des cyberattaques des systèmes de contrôle-commande et de remise en état après une cyberattaque. L'architecture défensive comprend, mais non exclusivement, des limites logiques ou physiques formelles telles que les zones de sécurité dans lesquelles des mesures défensives sont déployées[21]. Lors de la mise en œuvre d'une architecture de ce type, les exploitants devraient envisager de limiter les éléments dynamiques des réseaux composites et de leurs différents systèmes afin d'accroître la détermination de leur comportement. Cette détermination accrue peut contribuer à la mise en œuvre de mesures de sécurité informatique efficaces pour la détection d'incidents potentiels en matière de sécurité informatique.

4.134. Des limites de sécurité informatique devraient être mises en œuvre entre les systèmes, sous-systèmes et composants de contrôle-commande ayant des niveaux de sécurité différents et qui sont protégés grâce à des mesures de sécurité informatique différentes. Les limites de sécurité informatique sont les limites

[21] Une architecture qui comprend une série de niveaux défensifs concentriques de sécurité croissante et qui prend en compte à la fois les composants matériels et logiciels est l'illustration d'une architecture défensive.

logiques et physiques d'un système ou d'un ensemble de systèmes ayant le même niveau de sécurité et elles peuvent donc être sécurisées par l'application de mesures défensives communes (par exemple, les zones de sécurité informatique).

4.135. Le flux de données devrait être contrôlé entre les zones de sécurité auxquelles différents niveaux de sécurité ont été attribués et entre les différents systèmes de contrôle-commande ayant le même niveau de sécurité sur la base d'une approche fondée sur le risque si l'on veut que l'architecture défensive reste efficace.

4.136. Les systèmes de contrôle-commande exigeant le niveau de sécurité le plus élevé (c'est-à-dire le niveau de sécurité le plus strict) ne devraient être connectés à des systèmes exigeant des niveaux de sécurité moins élevés (c'est-à-dire des niveaux de sécurité plus faibles) que par des voies de communication de données unidirectionnelles déterministes et sécurisées en cas de panne[22]. Ces voies d'acheminement des données devraient se limiter à la transmission de données depuis les dispositifs exigeant le niveau de sécurité le plus strict vers les dispositifs auxquels sont attribués des niveaux de sécurité plus faibles. Les exceptions sont fortement déconseillées et ne peuvent être envisagées qu'au strict cas par cas et à condition d'être largement justifiées et étayées par une analyse des risques liés à la sécurité[23].

4.137. Les dispositifs numériques ou les réseaux de communication utilisés pour les activités de contrôle, de maintenance et de remise en état ne devraient pas contourner les mesures de contrôle technique servant à protéger les voies de communication entre des dispositifs ayant des niveaux de sécurité différents.

4.138. Les systèmes auxquels est attribué le niveau de sécurité le plus strict devraient être installés dans les limites de la zone la plus sûre. Les fonctions de communication sans fil posent des problèmes lorsqu'elles sont mises en œuvre dans des systèmes de contrôle-commande auxquels est attribué le niveau de sécurité le plus strict, car il est difficile de mettre en place un périmètre sécurisé pour ces communications.

---

[22] L'accès à distance aux systèmes ayant le niveau de sécurité le plus strict n'est pas possible en raison de la limitation unidirectionnelle du trafic sortant depuis le système de contrôle-commande.

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

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

4.140. Les mesures de contrôle technique mises en œuvre dans chaque zone de sécurité ou à la limite de la zone de sécurité devraient faire appel à des technologies différentes de celles qui ont été mises en œuvre à des niveaux ou dans des limites de sécurité adjacents. Cela garantira l'utilisation de technologies très diverses pour protéger les systèmes de contrôle-commande.

Défense en profondeur contre la compromission

4.141. Les orientations figurant aux paragraphes 4.142–4.151 s'appliquent à tous les systèmes, sous-systèmes et composants de contrôle-commande auxquels il est possible d'appliquer une approche graduée conformément au niveau de sécurité qui leur a été attribué.

4.142. La défense en profondeur contre la compromission consiste à mettre en place de multiples couches défensives de mesures de sécurité informatique qui doivent être neutralisées ou contournées pour qu'une cyberattaque puisse se dérouler et compromettre un système de contrôle-commande. Par conséquent, la défense en profondeur est assurée non seulement par la mise en œuvre d'une multitude de couches défensives (par exemple, des zones de sécurité au sein d'une architecture de sécurité informatique défensive), mais aussi par l'instauration et le maintien d'un programme solide de mesures de sécurité informatique qui permettent d'évaluer, de prévenir, de détecter, de protéger et d'atténuer une attaque contre un système de contrôle-commande, d'intervenir en cas d'attaque et de procéder à une remise en état après une attaque. Par exemple, en cas d'échec de la prévention (violation d'une règle) ou si les mécanismes de protection sont contournés (par un nouveau virus qui n'est pas reconnu comme une cyberattaque, par exemple), il existe encore des mécanismes permettant de détecter toute modification non autorisée dans un système de contrôle-commande visé et d'intervenir.

4.143. Aucune défaillance unique au sein des couches défensives ou entre elles ne devrait rendre la sécurité informatique globale des systèmes de contrôle-commande invalide ou inefficace. Par exemple, l'exploitation d'une vulnérabilité critique à l'intérieur d'un dispositif de protection de réseau commun utilisé à deux emplacements logiquement liés mais physiquement séparés pourrait

faciliter une attaque contournant une multiplicité de couches de mesures de sécurité informatique.

4.144. Les systèmes de contrôle-commande et les composants numériques connexes devraient être conçus et exploités conformément au concept de défense en profondeur contre la compromission.

4.145. Le personnel devrait être chargé d'exécuter des actions de sécurité en complément des mesures de contrôle technique. Il conviendrait d'analyser et de justifier l'équilibre entre l'activité humaine et les mesures de contrôle technique.

4.146. Une approche systématique devrait être adoptée pour répertorier et consigner par écrit les actions humaines susceptibles de compromettre la sécurité des systèmes de contrôle-commande à chaque phase de leur cycle de vie.

4.147. Il faudrait adopter une approche fondée sur le risque pour définir la sécurisation appropriée des systèmes de contrôle-commande, y compris la mise en œuvre de mesures de contrôle technique et d'une défense en profondeur contre la compromission. Des couches de mesures de sécurité informatique permettant d'appliquer une défense en profondeur contre la compromission devraient être mises en œuvre conformément à la gestion des risques liés à la sécurité informatique de l'installation et du système.

4.148. Chaque couche défensive devrait être protégée contre les cyberattaques provenant des couches adjacentes.

4.149. Les mécanismes de protection permettant d'assurer l'isolement entre les couches défensives devraient atténuer les défaillances de cause commune.

4.150. Les couches défensives et les contre-mesures associées devraient empêcher ou retarder la progression des attaques.

4.151. Les couches défensives devraient être efficaces tout au long du cycle de vie du système de contrôle-commande et être prises en considération au moment de la conception, de la configuration, de la modification du système et de l'attribution des paramètres des composants du système.

Définition des prescriptions en matière de sécurité informatique

4.152. Les prescriptions en matière de sécurité informatique applicables à l'architecture défensive et aux différents systèmes et composants de contrôle-commande devraient être établies et consignées par écrit. Ces prescriptions applicables à l'architecture défensive devraient avoir pour origine la base de conception du contrôle-commande.

4.153. Les prescriptions en matière de sécurité informatique applicables aux systèmes, sous-systèmes et composants de contrôle-commande devraient tenir compte des prescriptions fonctionnelles et des prescriptions relatives à la performance, de la configuration du système, de la qualification, de l'ergonomie, des définitions de données et de la communication des données, de la documentation, de l'installation et de la mise en service, de l'exploitation et de la maintenance.

4.154. L'élaboration des prescriptions en matière de sécurité informatique applicables aux systèmes de contrôle-commande devrait tenir compte de la gestion des risques liés à la sécurité informatique de l'installation et du système. Les prescriptions en matière de sécurité informatique devraient être examinées et mises à jour en fonction des modifications apportées aux résultats de la gestion des risques liés à la sécurité informatique de l'installation et du système.

4.155. Les prescriptions en matière de sécurité informatique applicables à l'architecture défensive et les différents systèmes de contrôle-commande devraient respecter la conception de base établie pour l'architecture globale de contrôle-commande.

Sélection de constituants préalablement mis au point

4.156. Les orientations figurant aux paragraphes 4.157–4.164 s'appliquent à tous les systèmes, sous-systèmes et composants de contrôle-commande auxquels il est possible d'appliquer une approche graduée conformément au niveau qui leur a été attribué.

4.157. Parmi les constituants préalablement mis au point, on pourrait citer les dispositifs électroniques, le logiciel préalablement mis au point, les produits disponibles dans le commerce, les dispositifs numériques composés du matériel et du logiciel (y compris les microprogrammes), les dispositifs matériels configurés

à l'aide d'un langage de description du matériel ou les blocs fonctionnels préalablement mis au point.

4.158. Les constituants préalablement mis au point pourraient être notamment du matériel et des logiciels préalablement mis au point (y compris les microprogrammes) provenant d'organismes qui n'ont pas de programme de sécurité informatique approprié ou qui ne sont pas disposés à communiquer des éléments précis sur leur programme de sécurité informatique. Dans ces cas, il est nécessaire d'analyser les caractéristiques de sécurité informatique des constituants et de justifier leur utilisation dans les systèmes de contrôle-commande ou les systèmes auxiliaires.

4.159. Il est probable que les produits disponibles dans le commerce ou le logiciel préalablement mis au point fassent l'objet de droits exclusifs et leur code source n'est généralement pas disponible pour les activités de vérification approfondies. Par conséquent, il est probable qu'il n'existe pas de méthode fiable permettant à l'exploitant de déterminer de manière exhaustive les vulnérabilités de ces produits en matière de sécurité. Dans ces cas, des mesures compensatoires de sécurité informatique seront nécessaires, à moins que ces produits ne soient modifiés par le développeur de l'application.

4.160. Il conviendrait d'appliquer des mesures de sécurité informatique pour que les caractéristiques des produits disponibles dans le commerce ou les logiciels préalablement mis au point ne puissent pas empêcher les systèmes de contrôle-commande de respecter les prescriptions en matière de sécurité informatique. Par exemple, des orientations peuvent être formulées pour réduire le nombre de codes utilisés, empêcher les utilisateurs non autorisés d'avoir accès à des points d'entrée et éliminer les fonctionnalités non nécessaires, réduisant ainsi la surface d'attaque (c'est-à-dire la sécurisation renforcée du système). Toutefois, l'application de ces mesures de sécurité informatique n'offre qu'une protection limitée et l'exploitant devrait appliquer des mesures de sécurité informatique compensatoires supplémentaires.

4.161. Les composants ou le logiciel préalablement mis au point devraient être sélectionnés et configurés à l'aide d'un processus de qualification de la sécurité correspondant au niveau de sécurité du système de contrôle-commande.

4.162. L'utilisation des produits disponibles dans le commerce et du logiciel préalablement mis au point devrait être vérifiée pour que ces produits et ce logiciel respectent les prescriptions en matière de sécurité informatique applicables aux systèmes de contrôle-commande.

4.163. L'exploitant devrait déterminer les documents requis pour qualifier les produits disponibles dans le commerce. Il ne faudrait pas se fier aux mesures de contrôle technique dont l'efficacité ne peut être vérifiée.

4.164. Les fonctions ou services non nécessaires d'un produit disponible dans le commerce et ou d'un logiciel préalablement mis au point devraient être supprimés.

Conception et mise en œuvre du système de contrôle-commande

4.165. Les orientations figurant aux paragraphes 4.166–4.174 s'appliquent à tous les systèmes, sous-systèmes et composants de contrôle-commande auxquels il est possible d'appliquer une approche graduée conformément au niveau de sécurité qui leur a été attribué.

4.166. Dans la phase de mise en œuvre du système de contrôle-commande (matériel et logiciel intégrés), la conception du système est transformée en code, en structures de base de données et en représentations exécutables par la machine. La mise en œuvre porte sur la configuration et l'installation du matériel, le codage et les tests du logiciel, ainsi que la configuration et l'installation de communication (y compris, le cas échéant, l'incorporation d'un logiciel réutilisé et de produits disponibles dans le commerce).

4.167. Lors des phases de conception et de mise en œuvre du cycle de vie du système de contrôle-commande, il conviendrait de recenser les prescriptions en matière de sécurité informatique applicables aux systèmes de contrôle-commande et de vérifier leur mise en œuvre.

4.168. Il conviendrait de transposer les prescriptions recensées dans la spécification du système de contrôle-commande en constituants de conception spécifiques dans la description de la conception du système. Ces constituants de conception spécifiques devraient prévoir des dispositions devant être mises en œuvre dans le cadre de la conception du système de contrôle-commande ou par des mesures de sécurité informatique appliquées sur le plan externe au système de contrôle-commande.

4.169. Les constituants de conception de la sécurité informatique du système de contrôle-commande devraient porter sur le contrôle de l'accès physique et logique aux fonctions du système, l'utilisation des services du système de contrôle-commande et la communication de données avec d'autres systèmes.

4.170. L'accès physique et logique à un système de contrôle-commande devrait être contrôlé en fonction du niveau de sécurité attribué à ce système. Par exemple, des prescriptions en matière de sécurité informatique devront être appliquées aux systèmes auxquels est attribué le niveau de sécurité le plus strict aux fins du contrôle des accès plurifactoriel, tel que le contrôle des accès nécessitant à la fois la connaissance (par exemple d'un mot de passe), la possession (d'une clé, d'une carte à puce, par exemple) et des caractéristiques personnelles (par exemple les empreintes digitales).

4.171. Les systèmes de contrôle-commande devraient être conçus de manière à inclure des caractéristiques permettant de résister à la compromission ou de s'en protéger.

4.172. Les mesures relatives à la conception devraient assurer avec le plus de certitude possible que la sécurité d'un système auquel est attribué un niveau de sécurité donné n'est pas réduite par des connexions à des systèmes auxquels sont attribués des niveaux de sécurité moins élevés.

4.173. Il faudrait concevoir des combinaisons appropriées de mesures de contrôle administratif (par exemple, un programme de sécurité informatique) et de mesures de contrôle physique pour réduire la susceptibilité d'un système de contrôle-commande aux cyberattaques.

4.174. Il conviendrait de répartir et d'installer les composants des systèmes de contrôle-commande dans des installations qui sécurisent physiquement le matériel et ses communications réseau avec d'autres systèmes, par exemple en installant toutes les connexions de données pour les systèmes et les composants dans des enceintes dont la sécurité est garantie.

Intégration des systèmes de contrôle-commande

4.175. Les orientations figurant aux paragraphes 4.176–4.178 s'appliquent à tous les systèmes, sous-systèmes et composants de contrôle-commande.

4.176. L'intégration des systèmes de contrôle-commande est le processus qui consiste à fusionner le matériel et le logiciel du système de contrôle-commande (y compris les microprogrammes) en un seul système. Souvent, les vendeurs, les prestataires ou les fournisseurs procéderont à des tests d'intégration de chaque système qu'ils produisent ainsi que d'une combinaison de systèmes relevant de leur domaine de compétence avant l'expédition sur le site de l'installation.

Ces tests permettent de vérifier la bonne exécution des composants logiciel et l'interface appropriée entre les composants du système de contrôle-commande.

4.177. Il conviendrait de mettre en place au cours de la phase d'intégration du cycle de vie du système de contrôle-commande des mesures de contrôle technique intégrées et de les configurer conformément aux spécifications avant les tests.

4.178. Lors des tests d'intégration, le vendeur, le prestataire ou le fournisseur devrait confirmer que les mesures de sécurité informatique intégrées fonctionnent bien conformément aux spécifications et ne compromettent pas la capacité des systèmes de contrôle-commande d'exécuter leurs fonctions essentielles.

Validation du système

4.179. Les orientations figurant aux paragraphes 4.180–4.185 s'appliquent à tous les systèmes, sous-systèmes et composants de contrôle-commande auxquels un niveau de sécurité a été attribué.

4.180. Les activités de validation du système coïncident habituellement avec d'autres phases du cycle de vie. Une fois l'intégration du système achevée, une validation partielle du système est généralement effectuée, par exemple à l'aide d'entrées simulées. Les activités de validation se poursuivent généralement dans le cadre des phases d'installation, d'intégration des systèmes de contrôle-commande et de mise en service. La validation est considérée comme achevée lorsqu'un système passe en mode d'exploitation normale.

4.181. Il conviendrait de démontrer au cours de la validation de chaque système, sous-système et composant de contrôle-commande que les prescriptions en matière de sécurité informatique et les constituants de configuration sont mis en œuvre. Les tests des fonctions de sécurité ont pour objectif de veiller à ce que les prescriptions en matière de sécurité informatique applicables aux systèmes de contrôle-commande soient validées par l'exécution de tests d'intégration, de tests système et d'essais de réception, s'il y a lieu.

4.182. Il faudrait que les activités de validation du système permettent de confirmer l'efficacité des mesures de sécurité informatique et de vérifier si ces mesures ont des incidences potentielles, directes ou indirectes, sur les fonctions de sûreté.

4.183. Il conviendrait de démontrer que chaque mesure de contrôle technique mise en œuvre dans le système de contrôle-commande fonctionne conformément

à ce qui est prévu et n'accroît pas le risque de vulnérabilités en matière de sécurité ni ne réduit la fiabilité des fonctions de sûreté.

4.184. La validation des mesures de sécurité informatique des systèmes de contrôle-commande devrait prévoir une évaluation de la configuration du système (y compris toute la connectivité externe), des tests de qualification du logiciel, des tests de qualification du système et des essais d'acceptation du système en usine. La validation de ces mesures de sécurité informatique peut s'appuyer sur les tests du système de contrôle-commande qui permettent d'identifier les vulnérabilités potentielles ou de caractériser les comportements ou les actions inattendus.

4.185. Les tests de validation du système devraient être effectués dans un environnement sécurisé. Par exemple, les dispositifs de test (simulateurs ou émulateurs) devraient être sécurisés par des mesures de sécurité informatique. La rigueur des mesures de sécurité informatique devrait correspondre au niveau de sécurité attribué au système de contrôle-commande.

Installation, intégration globale et mise en service du système de contrôle-commande

4.186. Au cours de l'installation et de la mise en service, l'exploitant devrait procéder à un examen de réception au cours duquel est vérifiée l'exactitude des mesures de contrôle physiques et techniques dans l'environnement cible, tout en tenant compte de l'intégration globale du système de contrôle-commande[24].

4.187. L'installation du système de contrôle-commande, l'intégration globale du système de contrôle-commande et la mise en service devraient être effectuées dans un environnement sécurisé. L'attribution d'un niveau de sécurité à cet environnement devrait tenir compte du niveau de sécurité du système dans l'environnement cible et du niveau de sécurité des outils utilisés lors de l'installation et de la mise en service.

4.188. Il conviendrait de protéger l'environnement sécurisé par des mesures de sécurité informatique correspondant au niveau de sécurité attribué au système de contrôle-commande et aux processus de sécurité mis en œuvre pour effectuer l'installation et la mise en service. Dans certains cas, des mesures compensatoires

[24] Dans la présente publication, on entend par « intégration globale du système de contrôle-commande » l'intégration de tous les systèmes de contrôle-commande d'une installation et il ne faut pas confondre cette expression avec l'expression « intégration du système de contrôle-commande », dont il est question plus haut dans la présente publication.

de contrôle administratif et physique devraient être prévues pour contrôler l'accès à l'environnement sécurisé ainsi qu'au matériel et aux sources de données associés.

4.189. Le matériel utilisé dans l'environnement sécurisé devrait être vérifié afin de confirmer que leur utilisation ne donne pas la possibilité d'introduire des programmes malveillants ou des données malveillantes dans l'environnement ou dans les composants du système de contrôle-commande.

4.190. Il faudrait mettre en place des mesures de sécurité informatique visant à contrôler et suivre le mouvement des données et des ressources numériques à l'intérieur et à l'extérieur de l'environnement sécurisé.

Exploitation et maintenance

4.191. Les orientations figurant aux paragraphes 4.192–4.205 s'appliquent à tous les systèmes, sous-systèmes et composants de contrôle-commande auxquels il est possible d'appliquer une approche graduée conformément au niveau de sécurité qui leur a été attribué.

4.192. Les activités d'exploitation et de maintenance se poursuivent tout au long du cycle de vie du système de contrôle-commande et il en a déjà été question dans les sections ci-dessus portant sur la planification des processus et les activités communes à toutes les phases du cycle de vie. L'organisme d'exploitation devrait assumer l'entière responsabilité de la sécurité informatique dans le cadre du bon déroulement des activités d'exploitation et de maintenance lorsqu'il entre dans la phase d'exploitation et de maintenance d'un système.

4.193. Les activités de maintenance sont les activités exigées par l'exploitant pour maintenir les systèmes ou les composants en bonne condition de fonctionnement. Ces activités de maintenance devraient être étendues aux mesures de contrôle technique et physique assurant la sécurité informatique des systèmes de contrôle-commande et peuvent comprendre :

— la maintenance préventive ou les tests préventifs périodiques ;
— les actions visant à détecter, empêcher ou atténuer la dégradation des composants ;
— les actions visant à diagnostiquer, réparer, remette en état ou remplacer les composants défectueux par des composants identiques.

4.194. Il conviendrait d'appliquer des mesures de sécurité informatique aux activités d'exploitation et de maintenance pour que les composants et les systèmes ne soient pas compromis.

4.195. La phase d'exploitation implique l'utilisation du système de contrôle-commande par l'exploitant dans l'environnement opérationnel prévu. Pendant cette phase, l'exploitant devrait :

— vérifier que la sécurité du système de contrôle-commande est intacte au moyen de techniques telles que les tests et contrôles périodiques, l'examen des journaux système et le suivi en temps réel, si possible ;
— évaluer l'incidence des modifications apportées au système de contrôle-commande dans l'environnement opérationnel sur la sécurité du système de contrôle-commande ;
— évaluer l'effet de toute modification proposée sur la sécurité du système de contrôle-commande ;
— évaluer les procédures d'exploitation pour s'assurer qu'elles sont conformes à l'utilisation prévue ;
— analyser les risques pour la sécurité ayant des répercussions sur l'exploitant et le système ;
— évaluer les nouvelles contraintes de sécurité dans le système ;
— évaluer l'exactitude et la facilité d'utilisation des procédures ;
— réaliser périodiquement des auto-évaluations de la sécurité des systèmes informatiques et des audits de sécurité informatique, qui sont des éléments clefs d'un bon programme de sécurité ;
— évaluer les rapports d'incidents disponibles sur les nouvelles menaces et vulnérabilités.

4.196. Il conviendrait d'analyser les activités d'exploitation et de maintenance pour s'assurer que la mise en œuvre des mesures de sécurité informatique empêche l'introduction de logiciels malveillants dans le système de contrôle-commande.

4.197. Les activités de maintenance devraient être conformes aux prescriptions en matière de sécurité informatique applicables aux systèmes de contrôle-commande existants, à moins que des modifications ne soient apportées à ces prescriptions dans le cadre de l'activité de maintenance. Dans certains cas, il peut être nécessaire de supprimer ou de désactiver temporairement les mesures de sécurité informatique pour permettre l'exécution des tâches de maintenance requises. Pendant la période d'indisponibilité des mesures de sécurité informatique, le système présente un risque plus élevé et des mesures compensatoires devraient être mises en œuvre.

4.198. Les activités d'étalonnage, d'essai et de maintenance pourraient nécessiter l'utilisation de supports amovibles et d'appareils mobiles temporairement connectés aux systèmes et composants numériques de contrôle-commande. Les mesures de sécurité informatique pour ces activités devraient tenir compte :

— de l'application de mesures de contrôle administratif et technique efficaces aux fins d'une utilisation sûre et sécurisée des dispositifs numériques ;
— de la vérification de l'intégrité de tous les points de contrôle définis afin d'éviter qu'ils subissent des modifications indésirables et de les protéger contre de telles modifications ;
— du recours à du personnel qualifié (y compris des tiers) qui a été formé à l'exécution de ces activités sur la base des prescriptions en matière de sécurité informatique.

4.199. Les interfaces devraient être désactivées ou leur accès devrait être limité lorsqu'elles ne sont pas nécessaires ou non utilisées (par exemple, connexion des ordinateurs de maintenance et de développement).

4.200. Il conviendrait de mettre en place des mesures de sécurité informatique visant à empêcher tout accès non nécessaire ou non autorisé.

4.201. Des processus ou des applications de suivi devraient être mis en place pour vérifier la configuration actuelle du logiciel par rapport à des configurations connues.

4.202. L'accès à distance devrait être limité autant que possible. Lorsque l'accès à distance est nécessaire, il conviendrait de tenir compte du risque que représentent de telles connexions et de mettre en œuvre des mesures de sécurité informatique supplémentaires. Cette connectivité ne devrait être maintenue qu'aussi longtemps que cela sera nécessaire pour son objectif spécifique.

4.203. Les activités d'exploitation et de maintenance devraient être soumises à un contrôle strict dans le cadre de processus formels d'ordres de travaux et de procédures de maintenance. Par exemple, il faudrait envisager des mécanismes correcteurs, tels que la règle des deux personnes, pour des tâches telles que la modification de la configuration des systèmes de contrôle-commande opérationnels.

4.204. Les activités d'exploitation ne devraient pas nécessiter de modifier les mesures de sécurité informatique du système de contrôle-commande.

4.205. Les outils d'exploitation et de maintenance du système qui peuvent être utilisés pour compromettre le système de contrôle-commande devraient être protégés proportionnellement au niveau de sécurité du système de contrôle-commande associé. Par exemple, les outils utilisés sur un système auquel est attribué un niveau de sécurité plus strict ne devraient pas être utilisés sur un système auquel est attribué un niveau de sécurité plus faible.

Modification des systèmes de contrôle-commande

4.206. L'application de mesures de sécurité informatique aux anciens systèmes de contrôle-commande d'une installation nucléaire existante ne va pas toujours de soi. Par exemple, les difficultés suivantes sont susceptibles de survenir :

— Il n'est pas toujours possible de modifier l'architecture des anciens systèmes de contrôle-commande sans affecter leur comportement déterministe.
— Il se peut que les technologies existantes utilisées pour le stockage des programmes ou des données, les interfaces ou la communication ne permettent pas de modification.
— Il se peut que les structures et l'aménagement des installations existantes ne permettent pas de mettre en place des mesures de protection physique suffisantes.
— Les mesures de contrôle technique contemporaines qui assurent des fonctions de contrôle de la sécurité risquent de ne pas être compatibles avec les technologies appliquées dans les anciens systèmes de contrôle-commande.

4.207. Lors de la modernisation d'une installation nucléaire qui implique le remplacement des anciens systèmes de contrôle-commande par des systèmes de contrôle-commande modernes, l'exploitant devrait envisager la possibilité que les anciennes interfaces avec les systèmes d'origine de l'installation et d'autres systèmes devront être maintenues et que de nouvelles vulnérabilités et faiblesses risqueront d'être introduites en raison de la nouvelle technologie ou de la nouvelle conception.

4.208. Les modifications apportées aux systèmes de contrôle-commande changent le système ou les documents y afférents. Ces changements peuvent être classés comme suit :

— les changements ou les améliorations (aux fins de correction ou d'adaptation) ;

— la migration (c'est-à-dire le déplacement d'un système vers un nouvel environnement opérationnel) ;
— le remplacement (c'est-à-dire le retrait d'un appui actif de la part de l'organisme d'exploitation et de maintenance, le remplacement partiel ou total par un nouveau système, ou l'installation d'un système mis à niveau).

4.209. Les modifications du système de contrôle-commande peuvent résulter des prescriptions ou être spécifiées pour corriger des erreurs (correction), pour s'adapter à un changement d'environnement opérationnel (adaptation) ou pour tenir compte des demandes ou des améliorations supplémentaires de l'exploitant.

4.210. Lorsque des modifications sont apportées à un système de contrôle-commande, une évaluation de la sécurité du système de contrôle-commande modifié devrait être prévue, par exemple en actualisant la gestion des risques liés à la sécurité informatique du système.

4.211. Il conviendrait de prendre en considération la sécurité informatique dans le cadre du processus de gestion du changement. Il s'agit notamment des modifications apportées au logiciel et au matériel des systèmes de contrôle-commande.

4.212. Pour être sûr que des vulnérabilités n'ont pas été introduites dans l'environnement de l'installation par des modifications, l'exploitant devrait évaluer les modifications qu'il est proposé d'apporter au système de contrôle-commande, y compris leur incidence sur le programme de sécurité informatique et sur la sécurité du système de contrôle-commande existant, évaluer les anomalies découvertes pendant l'exploitation, évaluer les besoins de migration et évaluer les modifications apportées, notamment les activités de validation et de vérification.

4.213. Il conviendrait d'évaluer les mesures de sécurité informatique qui sont présentées aux paragraphes 4.206–4.212 ci-dessus et de les revoir pour tenir compte des prescriptions en matière de sécurité informatique découlant du processus de modification, le cas échéant.

4.214. Pendant la modification, les prescriptions en matière de sécurité informatique applicables aux systèmes de contrôle-commande existants devraient rester en vigueur, à moins qu'elles ne soient modifiées dans le cadre de l'activité de modification.

4.215. La gestion de la configuration des mesures de sécurité informatique devrait être mise en place pour empêcher l'introduction de logiciels non autorisés dans les systèmes de contrôle-commande.

4.216. Lors de la migration des systèmes, l'exploitant devrait vérifier que les systèmes qui ont fait l'objet d'une migration satisfont aux prescriptions en matière de sécurité informatique du système de contrôle-commande.

4.217. Les artefacts résultant du développement, de l'installation et des essais devraient être retirés du système et de ses fichiers de configuration avant la mise en service aux fins de l'exploitation.

4.218. Les modifications apportées aux systèmes de contrôle-commande devraient être traitées comme des processus de développement et être vérifiées et validées.

4.219. Toutes les modifications apportées au système de contrôle-commande et à ses composants, y compris le logiciel, le matériel et les configurations du système, devraient tenir compte des vulnérabilités en matière de sécurité et des menaces qui peuvent surgir non seulement pendant l'exécution de ces activités, mais aussi à la suite des modifications.

4.220. De nombreuses ressources numériques et composants associés, y compris les supports de stockage amovibles, ont la capacité de conserver les données numériques lorsqu'elles sont retirées d'un système. Parmi ces données numériques, on peut citer les données logiques préprogrammées ou les données résiduelles du système (relevés de capteurs, signaux de commande, données analytiques, trafic réseau, etc.). Ces données peuvent être extraites des composants jetés.

4.221. Des mesures de contrôle administratif et technique devraient être mises en place pour que les données restantes sur les composants jetés ne puissent pas être utilisées pour encourager la mise au point d'un exploit informatique. Il conviendrait de détruire les composants ou de supprimer les données en toute sécurité, à moins que les données résiduelles sur les composants devant être jetés aient été évaluées pour montrer qu'elles ne présentent pas un risque de compromission de la sécurité.

4.222. En ce qui concerne les modifications impliquant le remplacement des systèmes de contrôle-commande, l'exploitant devrait procéder au nettoyage des données, à la destruction des disques ou à l'écrasement complet pour être sûr

que les données ne peuvent pas être récupérées à partir du système de contrôle-commande remplacé lors de sa mise hors service.

DÉCLASSEMENT

4.223. Au cours de la phase de déclassement, avant que les matières nucléaires, les autres matières radioactives et les ressources d'informations sensibles n'aient été retirées de l'installation, l'exploitant devrait évaluer l'effet du remplacement des fonctions de sécurité du système de contrôle-commande existant ou de leur suppression de l'environnement opérationnel.

4.224. L'exploitant devrait inclure dans la portée de cette évaluation les effets de la suppression des fonctions de sécurité du système sur les interfaces des systèmes de sûreté et des systèmes non liés à la sûreté.

4.225. L'exploitant devrait consigner par écrit les méthodes qui permettront d'atténuer une modification des fonctions de sécurité du système de contrôle-commande (par exemple, le remplacement des fonctions de sécurité, l'isolation des autres systèmes de sûreté et les interactions avec l'exploitant ou la mise hors service des fonctions d'interface du système de contrôle-commande).

4.226. Tant que le déclassement d'une installation n'est pas achevé, les procédures de sécurité devraient conserver des éléments qui garantissent le nettoyage du matériel et des données.

RÉFÉRENCES

[1] ALBRIGHT, D., BRANNAN, P., WALROND, C., Stuxnet Malware and Natanz : Mise à jour du rapport de l'ISIS du 22 décembre 2010 (2011), http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/8

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

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

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna (2016).

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

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems and Software Important to Safety for Research Reactors, IAEA Safety Standards Series No. SSG-37, IAEA, Vienna (2015).

[7] 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).

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

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of a Graded Approach in the Application of the Safety Requirements for Research Reactors, IAEA Safety Standards Series No. SSG-22, IAEA, Vienna (2012).

[10] COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE, Nuclear Power Plants - Instrumentation and Control Systems - Requirements for Security Programmes for Computer-based Systems, IEC 62645:2014, IEC, Geneva (2014).

[11] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Protection physique des matières nucléaires et des installations nucléaires, publication nº 27-G de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2019).

[12] ORGANISATION INTERNATIONALE DE NORMALISATION, Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information, ISO/CEI 27005:2011, ISO, Genève (2011).

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

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and Management for Safety, IAEA Safety Standards Series No. GSR Part 2, IAEA, Vienna (2016).
[15] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Sécurité de l'information nucléaire, publication nº 23-G de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2017).
[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Management System for Facilities and Activities, IAEA Safety Standards Series No. GSG-3.1, IAEA, Vienna (2006).
[17] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Nuclear Installations, IAEA Safety Standards Series No. GS-G-3.5, IAEA, Vienna (2009).
[18] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Élaboration, utilisation et actualisation de la menace de référence, collection Sécurité nucléaire de l'AIEA nº 10, AIEA, Vienne (2012).

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

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 sécurité informatique représente un domaine sensible qui doit faire face à des vecteurs de menace accrue dans un environnement technologique dynamique. La sécurité informatique dans les installations nucléaires est rendue plus difficile encore en raison de l'intégration des systèmes de contrôle-commande dans le cadre de gestion de la sécurité informatique. La présente publication propose des orientations relatives à l'application de mesures de sécurité informatique aux systèmes de contrôle-commande dans les installations nucléaires, y compris la base technique et les méthodes permettant d'appliquer des mesures de sécurité informatique aux systèmes de contrôle-commande qui assurent la sûreté, la sécurité ou des fonctions auxiliaires dans les installations nucléaires. Ces mesures ont pour but de protéger les systèmes de contrôle-commande contre des actes malveillants perpétrés par des personnes ou des organismes. La présente publication porte également sur l'application de ces mesures aux environnements de développement, de simulation et de maintenance de ces systèmes.

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE