Norme internationale

ISO/IEC 27019

Deuxième édition
2024-10

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information pour l'industrie des opérateurs de l'énergie

Information security, cybersecurity and privacy protection — Information security controls for the energy utility industry

Numéro de référence
ISO/IEC 27019:2024(fr)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos ..... **vi**
Introduction ..... **vii**
1 Domaine d'application **1**
2 Références normatives **2**
3 Termes, définitions et abréviations **2**
3.1 Termes et définitions 2
3.2 Abréviations 4
4 Structure du présent document **4**
5 Mesures de sécurité organisationnelles **4**
5.1 Politiques de sécurité de l'information 4
5.2 Fonctions et responsabilités liées à la sécurité de l'information 4
5.3 Séparation des tâches 5
5.4 Responsabilités de la direction 5
5.5 Contacts avec les autorités 5
5.6 Contacts avec des groupes d'intérêt spécifiques 5
5.7 Renseignements sur les menaces 6
5.8 Sécurité de l'information dans la gestion de projet 6
5.9 Inventaire des informations et autres actifs associés 6
5.10 Utilisation correcte des informations et autres actifs associés 7
5.11 Restitution des actifs 7
5.12 Classification des informations 7
5.13 Marquage des informations 7
5.14 Transfert des informations 7
5.15 Contrôle d'accès 7
5.16 Gestion des identités 8
5.17 Informations d'authentification 8
5.18 Droits d'accès 9
5.19 Sécurité de l'information dans les relations avec les fournisseurs 9
5.20 Prise en compte de la sécurité de l'information dans les accords conclus avec les fournisseurs 9
5.21 Gestion de la sécurité de l'information dans la chaîne d'approvisionnement TIC 10
5.22 Surveillance, révision et gestion des changements des services fournisseurs 10
5.23 Sécurité de l'information dans l'utilisation de services en nuage 10
5.24 Planification et préparation de la gestion des incidents de sécurité de l'information 10
5.25 Évaluation des événements de sécurité de l'information et prise de décision 10
5.26 Réponse aux incidents liés à la sécurité de l'information 10
5.27 Tirer des enseignements des incidents de sécurité de l'information 10
5.28 Recueil de preuves 10
5.29 Sécurité de l'information pendant une perturbation 10
5.30 Préparation des TIC pour la continuité d'activité 11
5.31 Exigences légales, statutaires, réglementaires et contractuelles 11
5.32 Droits de propriété intellectuelle 11
5.33 Protection des enregistrements 11
5.34 Protection de la vie privée et des DCP 11
5.35 Revue indépendante de la sécurité de l'information 11
5.36 Conformité aux politiques, règles et normes de sécurité de l'information 11
5.37 Procédures d'exploitation documentées 11
5.38 ENR – Identification des risques relatifs aux tiers 12
5.39 ENR – La sécurité avec les clients 12
6 Mesures de sécurité applicables aux personnes **13**
6.1 Présélection 13
6.2 Conditions générales d'embauche 13
6.3 Sensibilisation, apprentissage et formation à la sécurité de l'information 14

6.4 Processus disciplinaire 14
6.5 Responsabilités après la fin ou le changement d'un emploi 14
6.6 Accords de confidentialité ou de non-divulgation 14
6.7 Travail à distance 14
6.8 Déclaration des événements de sécurité de l'information 14

7 Mesures de sécurité physique 15
7.1 Périmètres de sécurité physique 15
7.2 Les entrées physiques 15
7.3 Sécurisation des bureaux, des salles et des équipements 15
7.4 Surveillance de la sécurité physique 15
7.5 Protection contre les menaces physiques et environnementales 15
7.6 Travail dans les zones sécurisées 15
7.7 Bureau vide et écran vide 15
7.8 Emplacement et protection du matériel 16
7.9 Sécurité des actifs hors des locaux 16
7.10 Supports de stockage 16
7.11 Services généraux 17
7.12 Sécurité du câblage 17
7.13 Maintenance du matériel 17
7.14 Élimination ou recyclage sécurisé(e) du matériel 17
7.15 ENR – Sécurisation des centres de contrôle 17
7.16 ENR – Sécurisation des salles d'équipements 19
7.17 ENR – Sécurisation des sites périphériques 20
7.18 ENR – Systèmes de contrôle et de communication interconnectés 21

8 Mesures de sécurité technologiques 22
8.1 Terminaux finaux des utilisateurs 22
8.2 Droits d'accès privilégiés 22
8.3 Restriction d'accès à l'information 22
8.4 Accès aux codes source 22
8.5 Authentification sécurisée 23
8.6 Dimensionnement 23
8.7 Protection contre les programmes malveillants 23
8.8 Gestion des vulnérabilités techniques 23
8.9 Gestion des configurations 24
8.10 Suppression des informations 24
8.11 Masquage des données 24
8.12 Prévention de la fuite de données 24
8.13 Sauvegarde des informations 24
8.14 Redondance des moyens de traitement de l'information 24
8.15 Journalisation 24
8.16 Activités de surveillance 25
8.17 Synchronisation des horloges 25
8.18 Utilisation de programmes utilitaires à privilèges 25
8.19 Installation de logiciels sur des systèmes en exploitation 25
8.20 Sécurité des réseaux 26
8.21 Sécurité des services réseau 26
8.22 Cloisonnement des réseaux 26
8.23 Filtrage web 26
8.24 Utilisation de la cryptographie 26
8.25 Cycle de vie de développement sécurisé 26
8.26 Exigences de sécurité des applications 26
8.27 Principes d'ingénierie et d'architecture des systèmes sécurisés 26
8.28 Codage sécurisé 27
8.29 Tests de sécurité dans le développement et l'acceptation 27
8.30 Développement externalisé 27
8.31 Séparation des environnements de développement, de test et opérationnels 27
8.32 Gestion des changements 27
8.33 Informations de test 27

8.34 Protection des systèmes d'information pendant les tests d'audit 27
8.35 ENR – Traitement des systèmes existants 28
8.36 ENR – Intégrité et disponibilité des fonctions de sûreté 28
8.37 ENR – Sécurisation des communications de données de contrôle des processus 29
8.38 ENR – Connexion logique des systèmes de contrôle des processus externes 30
8.39 ENR – Moindre fonctionnalité 31
8.40 ENR – Communication d'urgence 31

Annexe A (informative) **Référencement des mesures de sécurité spécifiques à l'industrie des opérateurs de l'énergie** **33**

Annexe B (informative) **Correspondance entre le présent document et la première édition (ISO/IEC 27019:2017)** **35**

Bibliographie **45**

Avant-propos

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC, participent également aux travaux.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents ~~ISO~~. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives ou www.iec.ch/members_experts/refdocs).

L'ISO et l'IEC attirent l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'ISO et l'IEC ne prennent pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, L'ISO et l'IEC n'avaient pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse www.iso.org/brevets et https://patents.iec.ch. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié tout ou partie de tels droits de propriété.

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir www.iso.org/iso/avant-propos. Pour l'IEC, voir www.iec.ch/understanding-standards.

Le présent document a été élaboré par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

Cette deuxième édition annule et remplace la première édition (ISO/IEC 27019:2017), qui a fait l'objet d'une révision technique.

Les principales modifications sont les suivantes:

— l'alignement des mesures de sécurité sur les thèmes organisationnels, humains, physiques et technologiques couverts par l'ISO/IEC 27002:2022;

— les «Recommandations» et les «Informations supplémentaires» des Article 5 à 8 ont été mises à jour afin d'éviter les redondances avec l'ISO/IEC 27002:2022;

— des attributs ont été ajoutés aux mesures de sécurité spécifiques au présent document.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/members.html et www.iec.ch/national-committees.

Introduction

0.1 Historique et contexte

Le présent document fournit des recommandations basées sur l'ISO/IEC 27002:2022 pour le management de la sécurité de l'information appliqué aux systèmes de contrôle des processus utilisés dans l'industrie des opérateurs de l'énergie. L'objectif du présent document est d'étendre le contenu de l'ISO/IEC 27002:2022 au domaine des systèmes de contrôle des processus et des technologies d'automatisation pour l'industrie de l'énergie.

Outre les objectifs et mesures de sécurité présentés dans l'ISO/IEC 27002:2022, les systèmes de contrôle des processus utilisés par les opérateurs de l'énergie et les fournisseurs d'énergie sont soumis à d'autres exigences spécifiques. Par rapport aux environnements des technologies de l'information et de la communication (TIC) classiques (par exemple la bureautique ou les systèmes de négociation d'énergie), il existe des différences fondamentales et substantielles concernant le développement, le fonctionnement, la réparation, la maintenance et l'exploitation des systèmes de contrôle des processus. De plus, la technologie des processus mentionnée dans le présent document peut représenter des composants qui font partie intégrante des infrastructures critiques. Ceux-ci sont donc indispensables au fonctionnement sécurisé et fiable de ces infrastructures. Il convient que ces distinctions et caractéristiques soient dûment prises en considération par les processus de management pour les systèmes de contrôle des processus, et elles justifient une attention spéciale au sein de la norme ISO/IEC 27001 et des normes associées.

Sur le plan de la conception et de la fonction, les systèmes de contrôle des processus utilisés par l'industrie des opérateurs de l'énergie sont en fait des systèmes de traitement de l'information. Ils collectent des données des processus et supervisent l'état des processus physiques à l'aide de capteurs. Les systèmes traitent ensuite ces données et génèrent en sortie des données de commande qui régulent des actions à l'aide d'actionneurs. Le contrôle et la régulation sont automatiques, mais une intervention manuelle par le personnel d'exploitation est également possible. Les informations et les systèmes de traitement de l'information constituent ainsi une partie essentielle des processus opérationnels au sein des opérateurs de l'énergie. Il est important que des mesures de sécurité appropriées soient appliquées de la même manière que pour d'autres unités de l'organisation.

Les composants logiciels et matériels (par exemple: les automates programmables) basés sur les technologies TIC standard sont de plus en plus utilisés dans des environnements de contrôle des processus, et sont également traités dans le présent document. De plus, les systèmes de contrôle des processus dans l'industrie des opérateurs de l'énergie sont de plus en plus interconnectés entre eux pour former des systèmes complexes. Il convient de prendre en compte les risques associés à cette tendance dans l'appréciation des risques.

Les informations et les systèmes de traitement de l'information dans les environnements de contrôle des processus sont de plus exposés à un nombre croissant de menaces et de vulnérabilités.

Une sécurité de l'information efficace dans le domaine du contrôle des processus au sein de l'industrie des opérateurs de l'énergie peut être obtenue par l'établissement, la mise en œuvre, la surveillance, la révision, et le cas échéant, l'amélioration des mesures de sécurité applicables énoncées dans le présent document, afin d'atteindre les objectifs métier et de sécurité spécifiques de l'organisation. Il importe à ce stade d'apporter une attention particulière au rôle spécial joué par les opérateurs de l'énergie dans la société, et à la nécessité économique d'une fourniture d'énergie sécurisée et fiable. En définitive, la réussite globale de la cybersécurité des industries énergétiques repose sur les efforts menés collaborativement par toutes les parties prenantes (vendeurs, fournisseurs, clients, etc.).

0.2 Considérations de sécurité pour les systèmes de contrôle des processus utilisés par les opérateurs de l'énergie

L'exigence pour un cadre de sécurité de l'information général et global pour le domaine du contrôle des processus au sein de l'industrie des opérateurs de l'énergie se fonde sur plusieurs exigences de base:

a) les clients s'attendent à une fourniture d'énergie sécurisée et fiable;

b) un fonctionnement sûr, fiable et sécurisé des systèmes de fourniture d'énergie est requis par les exigences légales;

c) les fournisseurs d'énergie ont besoin de la sécurité de l'information afin de protéger leurs intérêts commerciaux, de répondre aux besoins des clients et de se conformer aux réglementations légales.

0.3 Exigences de sécurité de l'information

Il est essentiel que les opérateurs de l'énergie identifient leurs exigences de sécurité. Il existe trois principales sources en matière d'exigences de sécurité:

a) l'appréciation du risque de l'organisation, prenant en compte l'ensemble de sa stratégie et objectifs métier. Cela peut être facilité ou appuyé par une appréciation du risque de sécurité de l'information. Il convient que cela aboutisse à la détermination des mesures de sécurité nécessaires assurant que les risques résiduels pour l'organisation correspondent à ses critères d'acceptation des risques;

b) il est attendu que les exigences légales, statutaires, réglementaires et contractuelles auxquelles l'organisation et ses parties intéressées (partenaires commerciaux, fournisseurs de services, etc.) se conforment ainsi que leur environnement socioculturel;

c) l'ensemble des principes, objectifs et exigences métier pour toutes les étapes du cycle de vie de l'information que l'organisation a développé pour appuyer son fonctionnement.

NOTE Il est important que les opérateurs de l'énergie s'assurent que les exigences de sécurité des systèmes de contrôle des processus soient analysées et prises en compte de manière adéquate dans les politiques de sécurité de l'information. L'analyse des exigences et objectifs de sécurité de l'information inclut la prise en compte de tous les critères pertinents pour la fourniture et l'acheminement sécurisés d'énergie, tels que:

— déficience de la sécurité de la fourniture d'énergie;

— restriction du flux énergétique;

— proportion de la population concernée;

— danger de dommage corporel;

— effets sur d'autres infrastructures critiques;

— effets sur la protection des données privées;

— impacts financiers.

0.4 Détermination des mesures de sécurité

Une fois que les risques et les exigences de sécurité ont été identifiés et que des décisions ont été prises sur la manière de gérer les risques, des mesures de sécurité appropriées sont choisies et mises en œuvre pour s'assurer que les risques sont réduits à un niveau acceptable.

En plus des mesures de sécurité assurées par un système de management de la sécurité de l'information complet, le présent document fournit une assistance supplémentaire et des mesures de sécurité spécifiques au secteur pour les systèmes de contrôle des processus utilisés par l'industrie des opérateurs de l'énergie, qui prennent en considération les exigences particulières de ces environnements. Si nécessaire, d'autres mesures de sécurité peuvent être développées pour répondre à des exigences particulières. Le choix des mesures de sécurité dépend des décisions prises par l'organisation sur la base de ses propres critères d'acceptation des risques, des options disponibles pour faire face au risque, et de l'approche générale de l'organisation pour la gestion des risques.

NOTE Des lois nationales et internationales, des ordonnances légales et des réglementations peuvent s'appliquer.

0.5 Public

Le présent document est destiné aux personnes responsables de l'exploitation des systèmes de contrôle des processus utilisés par les opérateurs de l'énergie, les responsables de la sécurité de l'information, les fournisseurs, les intégrateurs de systèmes et les auditeurs. Pour ce groupe cible, le présent document détaille

les mesures de sécurité fondamentales conformément aux objectifs de l'ISO/IEC 27002:2022 et définit les mesures spécifiques pour les systèmes de contrôle des processus de l'industrie des opérateurs de l'énergie, leurs systèmes support et l'infrastructure associée.

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information pour l'industrie des opérateurs de l'énergie

1 Domaine d'application

Le présent document fournit des mesures de sécurité de l'information pour l'industrie des opérateurs de l'énergie basées sur l'ISO/IEC 27002:2022 permettant de contrôler et de surveiller la production, le transport, le stockage et la distribution de l'électricité, du gaz, du pétrole et de la chaleur, ainsi que pour le contrôle des processus support associés. Cela inclut en particulier:

— les technologies de contrôle, de surveillance et d'automatisation des processus, centralisées et distribuées, et les systèmes d'information utilisés pour leur exploitation, tels que les dispositifs de programmation et de paramétrage;

— les contrôleurs numériques et les composants d'automatisation tels que les dispositifs de contrôle et de terrain ou les automates programmables (PLC, programmable logic controllers), y compris les capteurs et actionneurs numériques;

— tous les autres systèmes informatiques utilisés pour prendre en charge le domaine du contrôle des processus, par exemple pour les tâches de visualisation de données supplémentaires et à des fins de contrôle, de surveillance, d'archivage de données, de journalisation d'historiques, de génération de rapports et de documentation;

— les technologies de communication utilisées dans le domaine du contrôle des processus, par exemple les réseaux, la télémétrie, les applications de téléconduite et les technologies de contrôle à distance;

— les composants d'infrastructures de compteurs avancées (ICA), tels que les compteurs intelligents;

— les dispositifs de mesure, destinés par exemple à mesurer les valeurs d'émission;

— les systèmes de protection et de sûreté numériques, tels que les relais de protection, les automates programmables de sûreté (PLC) ou les régulateurs d'urgence;

— les systèmes de management de l'énergie, par exemple, pour la production d'énergie décentralisée (DER, distributed energy resources), les infrastructures de recharge électrique et chez les particuliers, les bâtiments d'habitation ou les installations de clients industriels;

— les composants distribués d'environnements de réseaux intelligents, par exemple dans les réseaux électriques, chez les particuliers, dans les bâtiments d'habitation ou dans les installations de clients industriels;

— tous les logiciels, firmwares et applications installés sur les systèmes mentionnés ci-dessus, par exemple les applications de systèmes de gestion de la distribution (DMS, distribution management system) ou les systèmes de gestion des coupures (OMS, outage management systems);

— tous les locaux hébergeant les équipements et les systèmes mentionnés ci-dessus;

— les systèmes de maintenance à distance pour les systèmes mentionnés ci-dessus.

Le présent document ne s'applique pas au domaine du contrôle des processus des installations nucléaires. Ce domaine est couvert par l'IEC 63096.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO/IEC 27002:2022, *Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information*

3 Termes, définitions et abréviations

3.1 Termes et définitions

Pour les besoins du présent document, les termes et les définitions de l'ISO/IEC 27002 ainsi que les suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia: disponible à l'adresse https://www.electropedia.org/

3.1.1
blackout
coupure étendue du courant électrique

3.1.2
redémarrage à froid
redémarrage d'un système électrique après un blackout total ou partiel grâce à des ressources énergétiques internes ou externes

3.1.3
centre de réponse aux incidents de sécurité informatique
CSIRT
équipe d'experts en sécurité qui prennent en charge la gestion des incidents de sécurité de l'information

3.1.4
actif critique
actif qui peut avoir un impact direct sur la production, le transport, le stockage et la distribution de l'électricité, du gaz, du pétrole et de la chaleur

3.1.5
infrastructure critique
ensemble d'organisations et d'installations essentielles au fonctionnement de la société et de l'économie dans leur ensemble

Note 1 à l'article: Une défaillance ou un dysfonctionnement de ces organisations et installations peut avoir pour résultat des insuffisances prolongées d'approvisionnement, un impact significatif sur la sécurité publique et d'autres répercussions de grande ampleur.

3.1.6
débogage
action qui consiste à analyser des dysfonctionnements de systèmes informatiques

3.1.7
système de distribution
réseau de distribution pour l'acheminement de l'énergie électrique à l'aide d'un réseau à haute, moyenne ou basse tension, ou un réseau de distribution local ou régional pour le transport du gaz, du pétrole ou de la chaleur

3.1.8
système de management de l'énergie
équipement ou infrastructure permettant de surveiller, mesurer et contrôler la consommation d'énergie chez les particuliers, dans les bâtiments d'habitation ou dans les installations de clients industriels

Note 1 à l'article: Le terme «système de management de l'énergie» sert aussi couramment à désigner un ensemble d'applications utilisées par les opérateurs d'un réseau de transport d'électricité pour surveiller, contrôler et optimiser les performances du système de production et/ou de transport.

3.1.9
fourniture d'énergie
processus de production ou stockage de l'énergie pour livraison aux clients et exploitation d'un réseau de fourniture d'énergie

3.1.10
opérateur de l'énergie
entité légale ou personne qui fournit de l'énergie sous forme d'électricité, de gaz, de pétrole ou de chaleur à d'autres parties, à un réseau de distribution d'énergie ou à un complexe de stockage

3.1.11
interface homme-machine
IHM
interface utilisateur pour l'exploitation et la surveillance d'un *système de contrôle des processus* (3.1.13) ou d'une centrale

3.1.12
maintenance
mesures utilisées dans le domaine de la *fourniture d'énergie* (3.1.9) normalement liées à l'inspection, à l'élimination de défauts et à l'amélioration

3.1.13
système de contrôle des processus
système servant à contrôler et à surveiller la production, le transport, le stockage et la distribution de l'électricité, du gaz, du pétrole et de la chaleur, incluant le contrôle des processus support associés

Note 1 à l'article: Les systèmes de contrôle des processus sont souvent appelés de manière plus générale systèmes de contrôle industriels. Dans le présent document, les termes «système de contrôle des processus» et «système de contrôle industriel» se limitent aux technologies et aux composants utilisés dans l'industrie des opérateurs de l'énergie.

3.1.14
sûreté
absence de risque intolérable

[SOURCE: Guide ISO/IEC 51:2014, 3.14]

3.1.15
système de sûreté
système et composant nécessaires à assurer la *sûreté* (3.1.14)

3.1.16
système de supervision, de contrôle et d'acquisition de données
SCADA
système de contrôle des processus (3.1.13) généralement utilisé pour contrôler les actifs dispersés utilisant l'acquisition de données et des commandes de supervision centralisées

3.1.17
réseaux intelligents
système électrique qui utilise les technologies d'échange d'informations et de contrôle, le traitement distribué et les capteurs et actionneurs associés

Note 1 à l'article: Les technologies de réseaux intelligents sont utilisées à des fins telles que:

— l'intégration du comportement et des actions des utilisateurs du réseau et autres parties prenantes;

— la livraison efficace d'une fourniture d'électricité durable, économique et sécurisée.

3.1.18
système de transport
réseau de transport pour l'acheminement de l'énergie électrique à l'aide d'un réseau à haute tension ou à très haute tension, ou réseau de transport de gaz naturel à l'aide d'un réseau de canalisations à haute pression (gazoducs)

3.2 Abréviations

CSIRT	Centre de réponse aux incidents de sécurité informatique [*Computer security incident response team*]
IHM	Interface homme-machine
SCADA	Système de supervision, de contrôle et d'acquisition de données [*Supervisory control and data acquisition*]
TIC	Technologies de l'information et de la communication

4 Structure du présent document

La structure du présent document est la même que celle de l'ISO/IEC 27002:2022, avec les éléments suivants:

— les mesures de sécurité de l'ISO/IEC 27002, qui restent inchangées;

— des mesures de sécurité avec des recommandations supplémentaires et des informations supplémentaires spécifiques à l'industrie des opérateurs de l'énergie;

— de nouvelles mesures de sécurité non incluses dans l'ISO/IEC 27002:2022, qui comportent le préfixe ENR.

Le Tableau A.1 présente les mesures de sécurité spécifiques liées à l'énergie, qui peuvent être prises en compte lors de la mise en œuvre de l'ISO/IEC 27001:2022 en plus des mesures de sécurité de l'ISO/IEC 27001:2022.

Le Tableau B.1 indique la correspondance entre les mesures de sécurité indiquées dans les Articles 5 à 8 et celles de l'ISO/IEC 27019:2017[1)]. Le Tableau B.2 indique la correspondance entre les mesures de sécurité spécifiées dans l'édition précédente (ISO/IEC 27019:2017) et celles du présent document.

5 Mesures de sécurité organisationnelles

5.1 Politiques de sécurité de l'information

Il n'y a aucune information supplémentaire spécifique à l'industrie des opérateurs de l'énergie pour l'ISO/IEC 27002:2022, 5.1.

5.2 Fonctions et responsabilités liées à la sécurité de l'information

Parmi les recommandations supplémentaires spécifiques à l'industrie des opérateurs de l'énergie pour l'ISO/IEC 27002:2022, 5.2, on peut citer:

Il convient d'informer les ingénieurs de systèmes de contrôle, les ingénieurs de télécommunications et autres personnels pertinents de leurs fonctions et responsabilités, en particulier en ce qui concerne les aspects liés à la sécurité de l'information des systèmes de contrôle des processus.

1) Annulée.