NORME INTERNATIONALE

ISO/IEC 27019

Première édition
2017-10

Technologies de l'information — Techniques de sécurité — Mesures de sécurité de l'information pour l'industrie des opérateurs de l'énergie

Information technology — Security techniques — Information security controls for the energy utility industry

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 27019:2017
https://standards.iteh.ai/catalog/standards/sist/7b2ffdff-c361-467c-a8c5-4c9f200f9cfa/iso-iec-27019-2017

Numéro de référence
ISO/IEC 27019:2017(F)

© ISO/IEC 2017

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27019:2017
https://standards.iteh.ai/catalog/standards/sist/7b2ffdff-c361-467c-a8c5-4c9f200f9cfa/iso-iec-27019-2017

DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2017

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos ..... **vii**

0 Introduction ..... **viii**

1 Domaine d'application **1**

2 Références normatives **2**

3 Termes et définitions **2**

4 Structure du document **4**
4.1 Généralités 4
4.2 Affinage des exigences de l'ISO/IEC 27001:2013 4
4.3 Recommandations spécifiques à l'industrie des opérateurs de l'énergie relatives à l'ISO/IEC 27002:2013 5

5 Politiques de sécurité de l'information **5**

6 Organisation de la sécurité de l'information **5**
6.1 Organisation interne 5
6.1.1 Fonctions et responsabilités liées à la sécurité de l'information 5
6.1.2 Séparation des tâches 5
6.1.3 Relations avec les autorités 5
6.1.4 Relations avec des groupes de travail spécialisés 6
6.1.5 La sécurité de l'information dans la gestion de projet 6
6.1.6 ENR – Identification des risques relatifs aux tiers 6
6.1.7 ENR – La sécurité avec les clients 7
6.2 Appareils mobiles et télétravail 7
6.2.1 Politique en matière d'appareils mobiles 7
6.2.2 Télétravail 8

7 La sécurité des ressources humaines **8**
7.1 Avant l'embauche 8
7.1.1 Sélection des candidats 8
7.1.2 Termes et conditions d'embauche 8
7.2 Pendant la durée du contrat 9
7.2.1 Responsabilités de la direction 9
7.2.2 Sensibilisation, apprentissage et formation à la sécurité de l'information 9
7.2.3 Processus disciplinaire 9
7.3 Rupture, terme ou modification du contrat de travail 9

8 Gestion des actifs **9**
8.1 Responsabilités relatives aux actifs 9
8.1.1 Inventaire des actifs 9
8.1.2 Propriété des actifs 10
8.1.3 Utilisation correcte des actifs 10
8.1.4 Restitution des actifs 10
8.2 Classification de l'information 10
8.2.1 Classification des informations 10
8.2.2 Marquage des informations 11
8.2.3 Manipulation des actifs 11
8.3 Manipulation des supports 11

9 Contrôle d'accès **11**
9.1 Exigences métier en matière de contrôle d'accès 11
9.1.1 Politique de contrôle d'accès 11
9.1.2 Accès aux réseaux et aux services en réseau 11
9.2 Gestion de l'accès utilisateur 12
9.2.1 Enregistrement et désinscription des utilisateurs 12
9.2.2 Maîtrise de la gestion des accès utilisateur 12
9.2.3 Gestion des privilèges d'accès 12

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27019:2017
https://standards.iteh.ai/catalog/standards/sist/7b2ffdff-c361-467c-a8c5-4c9f200f9cfa/iso-iec-27019-2017

9.2.4 Gestion des informations secrètes d'authentification des utilisateurs 12
9.2.5 Revue des droits d'accès utilisateur 12
9.2.6 Suppression ou adaptation des droits d'accès 12
9.3 Responsabilités des utilisateurs 12
9.3.1 Utilisation d'informations secrètes d'authentification 12
9.4 Contrôle de l'accès au système et aux applications 13
9.4.1 Restriction d'accès à l'information 13
9.4.2 Sécuriser les procédures de connexion 13
9.4.3 Système de gestion des mots de passe 13
9.4.4 Utilisation de programmes utilitaires à privilèges 13
9.4.5 Contrôle d'accès au code source des programmes 14

10 Cryptographie 14
10.1 Mesures cryptographiques 14
10.1.1 Politique d'utilisation des mesures cryptographiques 14
10.1.2 Gestion des clés 14

11 Sécurité physique et environnementale 14
11.1 Zones sécurisées 14
11.1.1 Périmètre de sécurité physique 14
11.1.2 Contrôles physiques des accès 14
11.1.3 Sécurisation des bureaux, des salles et des équipements 14
11.1.4 Protection contre les menaces extérieures et environnementales 15
11.1.5 Travail dans les zones sécurisées 15
11.1.6 Zones de livraison et de chargement 15
11.1.7 ENR – Sécurisation des centres de contrôle 15
11.1.8 ENR – Sécurisation des salles d'équipements 16
11.1.9 ENR – Sécurisation des sites périphériques 17
11.2 Matériels 18
11.2.1 Emplacement et protection du matériel 18
11.2.2 Services généraux 18
11.2.3 Sécurité du câblage 18
11.2.4 Maintenance du matériel 18
11.2.5 Sortie des actifs 18
11.2.6 Sécurité du matériel et des actifs hors des locaux 19
11.2.7 Mise au rebut ou recyclage sécurisé(e) du matériel 19
11.2.8 Matériel utilisateur laissé sans surveillance 19
11.2.9 Politique du bureau propre et de l'écran vide 19
11.3 ENR – Sécurité dans les locaux de tiers 19
11.3.1 ENR – Équipements situés dans les locaux d'autres opérateurs de l'énergie 19
11.3.2 ENR – Équipements situés dans les locaux du client 20
11.3.3 ENR – Systèmes de contrôle et de communication interconnectés 20

12 Sécurité liée à l'exploitation 21
12.1 Procédures et responsabilités liées à l'exploitation 21
12.1.1 Procédures d'exploitation documentées 21
12.1.2 Gestion des changements 21
12.1.3 Dimensionnement 21
12.1.4 Séparation des environnements de développement, de test et d'exploitation 21
12.2 Protection contre les logiciels malveillants 21
12.2.1 Mesures contre les logiciels malveillants 21
12.3 Sauvegarde 22
12.4 Journalisation et surveillance 22
12.4.1 Journalisation des événements 22
12.4.2 Protection de l'information journalisée 22
12.4.3 Journaux administrateur et opérateur 22
12.4.4 Synchronisation des horloges 22
12.5 Maîtrise des logiciels en exploitation 23
12.5.1 Installation de logiciels sur des systèmes en exploitation 23
12.6 Gestion des vulnérabilités techniques 23

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27019:2017
https://standards.iteh.ai/catalog/standards/sist/7b2ffdff-c361-467c-a8c5-4c9f200f9cfa/iso-iec-27019-2017

 © ISO/IEC 2017 – Tous droits réservés

12.6.1 Gestion des vulnérabilités techniques 23
12.6.2 Restrictions liées à l'installation de logiciels 23
12.7 Considérations sur l'audit du système d'information 23
12.8 ENR – Systèmes existants 24
12.8.1 ENR – Traitement des systèmes existants 24
12.9 ENR – Fonctions de sûreté 24
12.9.1 ENR – Intégrité et disponibilité des fonctions de sûreté 24

13 Sécurité des communications 25
13.1 Management de la sécurité des réseaux 25
13.1.1 Contrôle des réseaux 25
13.1.2 Sécurité des services de réseau 25
13.1.3 Cloisonnement des réseaux 25
13.1.4 ENR – Sécurisation des communications de données de contrôle des processus 25
13.1.5 ENR – Connexion logique des systèmes de contrôle des processus externes 26
13.2 Transfert de l'information 26

14 Acquisition, développement et maintenance des systèmes d'information 27
14.1 Exigences de sécurité applicables aux systèmes d'information 27
14.1.1 Analyse et spécification des exigences de sécurité de l'information 27
14.1.2 Sécurisation des services d'application sur les réseaux publics 27
14.1.3 Protection des transactions liées aux services d'application 27
14.2 Sécurité des processus de développement et d'assistance technique 27
14.2.1 Politique de développement sécurisé 27
14.2.2 Procédures de contrôle des changements apportés au système 27
14.2.3 Revue technique des applications après changement apporté à la plateforme d'exploitation 27
14.2.4 Restrictions relatives aux changements apportés aux progiciels 27
14.2.5 Principes d'ingénierie de la sécurité des systèmes 27
14.2.6 Environnement de développement sécurisé 27
14.2.7 Développement externalisé 28
14.2.8 Phase de test de la sécurité du système 28
14.2.9 Test de conformité du système 28
14.2.10 ENR – Moindre fonctionnalité 28
14.3 Données de test 28

15 Relations avec les fournisseurs 28
15.1 Sécurité de l'information dans les relations avec les fournisseurs 28
15.1.1 Politique de sécurité de l'information dans les relations avec les fournisseurs 28
15.1.2 La sécurité dans les accords conclus avec les fournisseurs 28
15.1.3 Chaîne d'approvisionnement informatique 29
15.2 Gestion de la prestation du service 29

16 Gestion des incidents liés à la sécurité de l'information 29
16.1 Gestion des incidents liés à la sécurité de l'information et améliorations 29
16.1.1 Responsabilités et procédures 29
16.1.2 Signalement des événements liés à la sécurité de l'information 29
16.1.3 Signalement des failles liées à la sécurité de l'information 29
16.1.4 Appréciation des événements liés à la sécurité de l'information et prise de décision 29
16.1.5 Réponse aux incidents liés à la sécurité de l'information 29
16.1.6 Tirer des enseignements des incidents liés à la sécurité de l'information 30
16.1.7 Recueil de preuves 30

17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité 30
17.1 Continuité de la sécurité de l'information 30
17.2 Redondances 30
17.2.1 Disponibilité des moyens de traitement de l'information 30
17.2.2 ENR – Communication d'urgence 30

18 Conformité 31

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27019:2017
https://standards.iteh.ai/catalog/standards/sist/7b2ffdff-c361-467c-a8c5-4c9f206bc1a/iso-iec-27019-2017

18.1 Conformité aux obligations légales et réglementaires 31
18.1.1 Identification de la législation et des exigences contractuelles applicables 31
18.1.2 Droits de propriété intellectuelle 32
18.1.3 Protection des enregistrements 32
18.1.4 Protection de la vie privée et protection des données à caractère personnel 32
18.1.5 Réglementation relative aux mesures cryptographiques 32
18.2 Revue de la sécurité de l'information 32
18.2.1 Revue indépendante de la sécurité de l'information 32
18.2.2 Conformité avec les politiques et les normes de sécurité 32
18.2.3 Examen de la conformité technique 32

Annexe A (normative) **Objectifs de sécurité et mesures de sécurité de référence spécifiques à l'industrie des opérateurs de l'énergie** **33**

Bibliographie **37**

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27019:2017
https://standards.iteh.ai/catalog/standards/sist/7b2ffdff-c361-467c-a8c5-4c9f200f9cfa/iso-iec-27019-2017

 © ISO/IEC 2017 – Tous droits réservés

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. Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte, l'ISO/IEC JTC 1.

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. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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 le lien suivant: www.iso.org/iso/fr/avant-propos.html.

ISO/IEC 27019:2017
https://standards.iteh.ai/catalog/standards/sist/7b2fddff-c361-467c-a8c5-4e91200f9cfa/iso-iec-27019-2017

Le présent document a été élaboré par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

Cette première édition annule et remplace la première édition (ISO/IEC/TR 27019:2013), qui a fait l'objet d'une révision technique.

Les principales modifications par rapport à l'édition précédente sont les suivantes:

— le champ d'application a été étendu au secteur de l'énergie pétrolière;

— le présent document, qui était un Rapport technique, est devenu une Norme internationale;

— l'édition précédente a été alignée sur l'ISO/IEC 27002:2005. La nouvelle structure a été alignée sur l'ISO/IEC 27002:2013;

— le titre a été modifié;

— le contenu technique a été révisé et mis à jour, le cas échéant, pour refléter les progrès technologiques actuels dans le secteur de l'énergie.

© ISO/IEC 2017 – Tous droits réservés

0 Introduction

0.1 Historique et contexte

Le présent document donne un ensemble de principes directeurs basés sur l'ISO/IEC 27002:2013 « Code de bonne pratique pour le management de la sécurité de l'information » 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'objet du présent document est d'étendre le contenu de l'ISO/IEC 27002:2013 au domaine des systèmes de contrôle des processus et de la technologie des automates, permettant ainsi à l'industrie des opérateurs de l'énergie de mettre en œuvre un système de management de la sécurité de l'information (ISMS) conforme à l'ISO/IEC 27001:2013 et qui puisse s'étendre du niveau métier à celui du contrôle des processus.

Outre les objectifs et mesures de sécurité présentés dans l'ISO/IEC 27002:2013, les systèmes de contrôle des processus utilisés par les opérateurs de l'énergie et les fournisseurs d'énergie sont sujets à d'autres exigences spécifiques. Par rapport aux environnements TIC classiques (comme 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 faire partie intégrante des infrastructures critiques. Ceux-ci sont donc indispensables au fonctionnement sécurisé et fiable de ces infrastructures. Ces distinctions et caractéristiques sont à prendre en considération par les processus de management pour les systèmes de contrôle des processus, et justifient une attention spéciale au sein de la série de normes ISO/IEC 27000.

Sur le plan de la conception et de la fonction, les systèmes de contrôle des processus utilisés par le secteur 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 régissent des actions à l'aide d'actionneurs. Le contrôle et les actions sont automatiques, mais une intervention manuelle par le personnel opérationnel 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 donc important que des mesures de protection appropriées soient appliquées de la même manière que pour les autres unités de l'organisation.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27019:2017
https://standards.iteh.ai/catalog/standards/sist/...

Les composants logiciels et matériels (par exemple les automates programmables) basés sur les technologies TIC standards 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 le secteur des opérateurs de l'énergie sont de plus en plus interconnectés entre eux pour former des systèmes complexes. Les risques associés à cette tendance sont à prendre en compte 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. Il est donc essentiel que, dans le domaine du contrôle des processus au sein de l'industrie des opérateurs de l'énergie, une sécurité de l'information adéquate soit réalisée par le biais de la mise en œuvre et de l'amélioration continue d'un système de management de la sécurité de l'information (ISMS) conformément à l'ISO/IEC 27001:2013.

Une sécurité de l'information efficace dans le domaine du contrôle des processus au sein du secteur des opérateurs de l'énergie peut être assurée par la mise en place, l'implémentation, la supervision, la révision, et le cas échéant, l'amélioration des mesures applicables énoncées dans le présent document, afin d'atteindre les objectifs métiers 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 est basée 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

 © ISO/IEC 2017 – Tous droits réservés

La condition pour une structure de sécurité de l'information générale et globale pour le domaine du contrôle des processus au sein de l'industrie des opérateurs de l'énergie est basée 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 et réglementaires;

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 liées à la sécurité de l'information

Il est essentiel que les opérateurs de l'énergie identifient leurs exigences de sécurité. Ces exigences proviennent de trois sources principales:

a) les résultats de l'appréciation des risques de l'organisation, prenant en compte ses stratégies métiers et ses objectifs généraux. L'appréciation des risques permet d'identifier les sources de risques et les événements, et d'évaluer les impacts potentiels et la probabilité d'occurrence des risques;

b) les exigences découlant de la réglementation et des textes d'application, des règlements et des contrats devant être respectés par une organisation, et les exigences socioculturelles. Les exemples particuliers incluent la garantie d'une fourniture d'énergie fiable, efficace et sécurisée, ainsi qu'une conformité fiable aux exigences d'un marché de l'énergie dérégulé, notamment le transfert fiable et sécurisé de données vers des parties externes;

iTeh STANDARD PREVIEW
(standards.iteh.ai)

c) les principes, objectifs et exigences métiers spécifiques auxquels est assujetti le traitement de l'information, et qui ont été développés par l'organisation pour réaliser ses fonctions métiers.

ISO/IEC 27019:2017
https://standards.iteh.ai/catalog/standards/sist/7b2fddf-c361-467c-a8c5-4c9f2bdf9cfa/iso-iec-27019-2017

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, comme par exemple:

— 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.

Les mesures de sécurité ou contrôles nécessaires sont déterminés par une évaluation méthodique des risques de sécurité. Il est nécessaire que le coût des mesures de sécurité soit équilibré par rapport aux pertes financières pouvant être engendrées par des failles de sécurité. Le résultat de l'appréciation des risques facilite:

— la définition d'actions de management adéquates et de priorités pour la gestion des risques de sécurité de l'information; et

— l'implémentation des mesures de sécurité retenues pour protéger contre ces risques.

Il convient que l'appréciation des risques soit renouvelée périodiquement pour tenir compte de tous les changements pouvant avoir une influence sur les résultats évalués.

© ISO/IEC 2017 – Tous droits réservés

Les exigences liées à l'appréciation des risques et au choix des mesures de sécurité sont données dans l'ISO/IEC 27001:2013.

0.4 Sélection des mesures de sécurité

Une fois que les exigences et les risques 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 sélectionnées et implémentées pour 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 pour les systèmes de contrôle des processus utilisés par le secteur des opérateurs de l'énergie, qui prennent en considération les exigences particulières de ces environnements. Si nécessaire, d'autres mesures peuvent être développées pour répondre à des besoins spécifiques. 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. Il convient que le choix des mesures prenne également en compte la réglementation nationale et internationale, les ordonnances légales et les règlements.

0.5 Public

Le présent document est destiné aux personnes responsables du fonctionnement 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, il détaille les mesures fondamentales conformément aux objectifs de l'ISO/IEC 27002:2013 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27019:2017
https://standards.iteh.ai/catalog/standards/sist/7b2ffdff-c361-467c-a8c5-4c9f200f9cfa/iso-iec-27019-2017

 © ISO/IEC 2017 – Tous droits réservés

Technologies de l'information — Techniques de sécurité — Mesures de sécurité de l'information pour l'industrie des opérateurs de l'énergie

1 Domaine d'application

Le présent document contient des recommandations basées sur l'ISO/IEC 27002:2013 appliquées aux systèmes de contrôle des processus utilisés par l'industrie des opérateurs de l'énergie pour contrôler et 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 et de surveillance des processus centralisées et distribuées, des automates et des systèmes d'information utilisés pour leur fonctionnement, tels que les dispositifs de programmation et de paramétrage;

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

— tous les autres systèmes d'information support utilisés dans 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 et de logs (*historian logging*), 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 télé-conduite et les technologies de contrôle à distance;

— les composants des infrastructures de comptage communicants, tels que les compteurs intelligents;

— les équipements 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 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, chez les particuliers, dans les bâtiments d'habitation ou dans les installations de clients industriels;

— les composants distribués des environnements de réseaux intelligents, par exemple dans les réseaux d'énergie, 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, des systèmes de gestion de la distribution (DMS, *Distribution Management System*) ou des systèmes de gestion des pannes (OMS, *Outage Management System*);

— 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 de processus des installations nucléaires. Ce domaine est couvert par l'IEC 62645.

Le présent document contient également une exigence relative à l'adaptation de l'appréciation des risques et des processus de traitement décrits dans l'ISO/IEC 27001:2013 aux recommandations spécifiques à l'industrie des opérateurs de l'énergie fournies dans le présent document.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27019:2017
https://standards.iteh.ai/catalog/standards/sist/7b2ffdff-c361-467c-a8c5-4c91200b0cfa/iso-iec-27019-2017

2 Références normatives

Les documents suivants cités dans le texte 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 27000, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*

ISO/IEC 27001:2013, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences*

ISO/IEC 27002:2013, *Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO/IEC 27000 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 http://www.electropedia.org/

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.1
blackout
coupure étendue du courant électrique

ISO/IEC 27019:2017
https://standards.iteh.ai/catalog/standards/sist/7b2ffdff-c361-467c-a8c5-4c9f200f9cfa/iso-iec-27019-2017

3.2
CSIRT (*Computer Security Incident Response Team*)
équipe d'experts en sécurité qui prennent en charge la gestion des incidents liés à la sécurité de l'information

3.3
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

3.4
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.

3.5
débogage
action qui consiste à analyser des dysfonctionnements de systèmes informatiques

3.6
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

© ISO/IEC 2017 – Tous droits réservés

3.7
système de management de l'énergie
SME
équipement/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 SME sert aussi couramment à désigner un ensemble d'applications utilisées par les opérateurs de réseaux de transport d'électricité pour surveiller, contrôler et optimiser les performances du système de production et/ou de transport.

3.8
fourniture d'énergie
processus de production ou stockage de l'énergie pour livraison aux clients et exploitation d'un réseau de fourniture d'énergie

3.9
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

3.10
interface homme-machine
IHM
interface utilisateur pour exploitation ou surveillance d'un système de contrôle des processus ou d'une centrale

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.11
maintenance
mesures utilisées dans le domaine de la *fourniture d'énergie* (3.8) normalement liées à l'inspection, à l'élimination de défauts et à l'amélioration

ISO/IEC 27019:2017
https://standards.iteh.ai/catalog/standards/sist/7b2ffdff-c361-467c-a8c5-4a9f200f9cfa/iso-iec-27019-2017

3.12
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.

3.13
sûreté
absence de risque intolérable

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

3.14
système de sûreté
système et composant nécessaires à assurer la sûreté

3.15
Système de supervision, de contrôle et d'acquisition de données (*Supervisory Control And Data Acquisition*)
SCADA
système de contrôle des processus (3.12) généralement utilisé pour contrôler les actifs dispersés utilisant l'acquisition de données et des commandes de supervision centralisées