Norme belge

ISO/IEC 27019:2017

NBN ISO/IEC 27019:2018

Technologies de l'information - Techniques de sécurité - Mesures de sécurité de l'information pour l'industrie des opérateurs de l'énergie (ISO/IEC 27019:2017 - Première édition 2017-10)

Valable à partir de 27-11-2018

Remplace NBN ISO/IEC TR 27019:2014

ICS: 03.100.70, 29.035.30

Bureau de Normalisation
Rue Joseph-II 40 bte 6
1000 Bruxelles

T. +32 2 738 01 11
F. +32 2 733 42 64
info@nbn.be

BTW BE0880.857.592
IBAN BE41 0003 2556 2110
BIC Code BPOTBEB1

www.nbn.be

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

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

DOCUMENT PROTÉGÉ PAR COPYRIGHT

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

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.

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.

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.

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.

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

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;

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.

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.

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.

NORME INTERNATIONALE **ISO/IEC 27019:2017(F)**

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.

