DIN EN ISO/IEC 27019

ICS 03.100.70

Ersatz für
DIN ISO/IEC TR 27019
(DIN SPEC 27019):2015-03

Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmaßnahmen für die Energieversorgung (ISO/IEC 27019:2017, korrigierte Fassung 2019-08); Deutsche Fassung EN ISO/IEC 27019:2020

Information technology –
Security techniques –
Information security controls for the energy utility industry (ISO/IEC 27019:2017, Corrected version 2019-08);
German version EN ISO/IEC 27019:2020

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, Version corrigée 2019-08);
Version allemande EN ISO/IEC 27019:2020

Gesamtumfang 52 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27019:2020-08

Nationales Vorwort

Dieses Dokument enthält die deutsche Übersetzung der Internationalen Norm ISO/IEC 27019:2017, die vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ erarbeitet wurde, dessen Sekretariat von ANSI (USA) gehalten wird.

Das internationale Dokument (ISO/IEC 27019:2017, korrigierte Fassung 2019-08) ist unverändert übernommen worden.

Das zuständige deutsche Normungsgremium ist der Arbeitskreis NA 043-01-27-01 AK „Anforderungen, Dienste und Richtlinien für IT Sicherheitssysteme“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Für die in diesem Dokument zitierten internationalen Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO/IEC 27000	siehe	DIN EN ISO/IEC 27000
ISO/IEC 27001:2013	siehe	DIN EN ISO/IEC 27001:2017-06
ISO/IEC 27002:2013	siehe	DIN EN ISO/IEC 27002:2017-06
IEC 62351 (all parts)	siehe	DIN EN 62351 (alle Teile)

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Änderungen

Gegenüber DIN ISO/IEC TR 27019 (DIN SPEC 27019):2015-03 wurden folgende Änderungen vorgenommen:

a) der Anwendungsbereich wurde geändert und umfasst nun auch den Öl-Energie-Sektor;

b) die Veröffentlichungsform wurde von einen internationalen Technical Report in eine Internationale Norm geändert;

c) das Dokument wurde an die neue Struktur der ISO/IEC 27002 Ausgabe 2013 angepasst;

d) der Titel wurde geändert;

e) der technische Inhalt wurde an den entsprechenden Stellen angepasst, um die aktuellen Entwicklungen im Energiesektor zu berücksichtigen.

Frühere Ausgaben

DIN SPEC 27009: 2012-04
DIN ISO/IEC TR 27019 (DIN SPEC 27019): 2015-03

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27019:2020-08

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN EN ISO/IEC 27000, *Informationstechnik — Sicherheitsverfahren — Informationssicherheits-Managementsysteme — Überblick und Terminologie*

DIN EN ISO/IEC 27001:2017-06, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27001:2017*

DIN EN ISO/IEC 27002:2017-06, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27002:2017*

DIN EN 62351 (alle Teile), *Management von Systemen der Energietechnik und zugehöriger Datenaustausch — Daten- und Kommunikationssicherheit*

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27019:2020-08

— Leerseite —

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27019:2020-08

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO/IEC 27019

März 2020

ICS 03.100.70

Deutsche Fassung

Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmaßnahmen für die Energieversorgung (ISO/IEC 27019:2017, korrigierte Fassung 2019-08)

Information technology —
Security techniques —
Information security controls for the energy utility industry
(ISO/IEC 27019:2017, Corrected version 2019-08)

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, Version corrigée 2019-08)

Diese Europäische Norm wurde vom CEN am 2. März 2020 angenommen.

Die CEN- und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Management-Zentrum des CEN-CENELEC oder bei jedem CEN- und CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN- und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum des CEN-CENELEC mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

CEN-CENELEC Management-Zentrum:
Rue de la Science 23, B-1040 Brüssel

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27019:2020-08

Inhalt

Seite

Europäisches Vorwort ... 6
Vorwort ... 7
0Einleitung ... 9
0.1 Hintergrund und Kontext ... 9
0.2 Sicherheitsaspekte für Prozesssteuerungssysteme bei Energieversorgern ... 10
0.3 Anforderungen an Informationssicherheit ... 10
0.4 Auswahl der Maßnahmen ... 11
0.5 Zielgruppe ... 11
1 Anwendungsbereich ... 12
2 Normative Verweisungen ... 13
3 Begriffe ... 13
4 Aufbau dieses Dokuments ... 15
4.1 Allgemein ... 15
4.2 Anpassung der ISO/IEC 27001:2013-Anforderungen ... 15
4.3 Energieversorgungsspezifische Maßnahmen mit Bezug zu ISO/IEC 27002:2013 ... 16
5 Informationssicherheitsrichtlinien ... 16
6 Organisation der Informationssicherheit ... 16
6.1 Interne Organisation ... 16
6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten ... 16
6.1.2 Aufgabentrennung ... 16
6.1.3 Kontakt mit Behörden ... 16
6.1.4 Kontakt mit speziellen Interessensgruppen ... 17
6.1.5 Informationssicherheit im Projektmanagement ... 17
6.1.6 ENR - Identifizierung von Risiken in Zusammenhang mit Externen ... 17
6.1.7 ENR - Adressieren von Sicherheit im Umgang mit Kunden ... 18
6.2 Mobilgeräte und Telearbeit ... 18
6.2.1 Richtlinie zu Mobilgeräten ... 18
6.2.2 Telearbeit ... 19
7 Personalsicherheit ... 19
7.1 Vor der Beschäftigung ... 19
7.1.1 Sicherheitsüberprüfung ... 19
7.1.2 Beschäftigungs- und Vertragsbedingungen ... 20
7.2 Während der Beschäftigung ... 20
7.2.1 Verantwortlichkeiten der Leitung ... 20
7.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung ... 20
7.2.3 Maßregelungsprozess ... 20
7.3 Beendigung und Änderung der Beschäftigung ... 20
8 Verwaltung der Werte ... 20
8.1 Verantwortlichkeit für Werte ... 20
8.1.1 Inventarisierung der Werte ... 20
8.1.2 Zuständigkeit für Werte ... 21
8.1.3 Zulässiger Gebrauch von Werten ... 21
8.1.4 Rückgabe von Werten ... 21

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27019:2020-08

8.2 Informationsklassifizierung ... 21
8.2.1 Klassifizierung von Information ... 21
8.2.2 Kennzeichnung von Information ... 22
8.2.3 Handhabung von Werten ... 22
8.3 Handhabung von Datenträgern ... 22

9 Zugangssteuerung ... 22
9.1 Geschäftsanforderungen an die Zugangssteuerung ... 22
9.1.1 Zugangssteuerungsrichtlinie ... 22
9.1.2 Zugang zu Netzwerken und Netzwerkdiensten ... 23
9.2 Benutzerzugangsverwaltung ... 23
9.2.1 Registrierung und Deregistrierung von Benutzern ... 23
9.2.2 Zuteilung von Benutzerzugängen ... 23
9.2.3 Verwaltung privilegierter Zugangsrechte ... 23
9.2.4 Verwaltung geheimer Authentisierungsinformation von Benutzern ... 23
9.2.5 Überprüfung von Benutzerzugangsrechten ... 23
9.2.6 Entzug oder Anpassung von Zugangsrechten ... 23
9.3 Benutzerverantwortlichkeiten ... 24
9.3.1 Gebrauch geheimer Authentisierungsinformation ... 24
9.4 Zugangssteuerung für Systeme und Anwendungen ... 24
9.4.1 Informationszugangsbeschränkung ... 24
9.4.2 Sichere Anmeldeverfahren ... 24
9.4.3 System zur Verwaltung von Kennwörtern ... 24
9.4.4 Gebrauch von Hilfsprogrammen mit privilegierten Rechten ... 25
9.4.5 Zugangssteuerung für Quellcode von Programmen ... 25

10 Kryptographie ... 25
10.1 Kryptographische Maßnahmen ... 25
10.1.1 Richtlinie zum Gebrauch von kryptographischen Maßnahmen ... 25
10.1.2 Schlüsselverwaltung ... 25

11 Physische und umgebungsbezogene Sicherheit ... 25
11.1 Sicherheitsbereiche ... 25
11.1.1 Physische Sicherheitsperimeter ... 25
11.1.2 Physische Zutrittssteuerung ... 25
11.1.3 Sichern von Büros, Räumen und Einrichtungen ... 26
11.1.4 Schutz vor externen und umweltbedingten Bedrohungen ... 26
11.1.5 Arbeiten in Sicherheitsbereichen ... 26
11.1.6 Anlieferungs- und Ladebereiche ... 26
11.1.7 ENR — Sichern von Leitstellen ... 26
11.1.8 ENR — Sicherung von Technikräumen ... 27
11.1.9 ENR — Sicherung von Außenstandorten ... 28
11.2 Geräte und Betriebsmittel ... 29
11.2.1 Platzierung und Schutz von Geräten und Betriebsmitteln ... 29
11.2.2 Versorgungseinrichtungen ... 29
11.2.3 Sicherheit der Verkabelung ... 29
11.2.4 Instandhaltung von Geräten und Betriebsmitteln ... 29
11.2.5 Entfernen von Werten ... 30
11.2.6 Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten ... 30
11.2.7 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln ... 30
11.2.8 Unbeaufsichtigte Benutzergeräte ... 30
11.2.9 Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren ... 30
11.3 ENR — Sicherheit in Räumlichkeiten Dritter ... 30
11.3.1 ENR — Betriebseinrichtung in Bereichen anderer Energieversorger ... 30
11.3.2 ENR - Betriebseinrichtung beim Kunden vor Ort ... 31
11.3.3 ENR — Gekoppelte Steuerungs- und Kommunikationssysteme ... 31

12 Betriebssicherheit ... 32

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27019:2020-08

12.1 Betriebsabläufe und -verantwortlichkeiten 32
12.1.1 Dokumentierte Bedienabläufe 32
12.1.2 Änderungssteuerung 32
12.1.3 Kapazitätssteuerung 32
12.1.4 Trennung von Entwicklungs-, Test- und Betriebsumgebungen 32
12.2 Schutz vor Schadsoftware 33
12.2.1 Maßnahmen gegen Schadsoftware 33
12.3 Datensicherung 33
12.4 Protokollierung und Überwachung 33
12.4.1 Ereignisprotokollierung 33
12.4.2 Schutz der Protokollinformation 33
12.4.3 Administratoren- und Bedienerprotokolle 33
12.4.4 Uhrensynchronisation 34
12.5 Steuerung von Software im Betrieb 34
12.5.1 Installation von Software auf Systemen im Betrieb 34
12.6 Handhabung technischer Schwachstellen 34
12.6.1 Handhabung von technischen Schwachstellen 34
12.6.2 Einschränkungen von Softwareinstallation 34
12.7 Audits von Informationssystemen 35
12.8 ENR — Altsysteme 35
12.8.1 ENR — Behandlung von Altsystemen 35
12.9 ENR - Safety-Funktionen 35
12.9.1 ENR — Integrität und Verfügbarkeit von Safety-Funktionen 36

13 Kommunikationssicherheit 36
13.1 Netzwerksicherheitsmanagement 36
13.1.1 Netzwerksteuerungsmaßnahmen 36
13.1.2 Sicherheit von Netzwerkdiensten 36
13.1.3 Trennung in Netzwerken 36
13.1.4 ENR — Sicherung der Prozessdatenkommunikation 37
13.1.5 ENR — Logische Anbindung von externen Prozesssteuerungssystemen 37
13.2 Informationsübertragung 38

14 Anschaffung, Entwicklung und Instandhaltung von Systemen 38
14.1 Sicherheitsanforderungen an Informationssysteme 38
14.1.1 Analyse und Spezifikation von Informationssicherheitsanforderungen 38
14.1.2 Sicherung von Anwendungsdiensten in öffentlichen Netzwerken 38
14.1.3 Schutz der Transaktionen bei Anwendungsdiensten 38
14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen 38
14.2.1 Richtlinie für sichere Entwicklung 38
14.2.2 Verfahren zur Verwaltung von Systemänderungen 38
14.2.3 Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform 38
14.2.4 Beschränkung von Änderungen an Softwarepaketen 39
14.2.5 Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme 39
14.2.6 Sichere Entwicklungsumgebung 39
14.2.7 Ausgegliederte Entwicklung 39
14.2.8 Testen der Systemsicherheit 39
14.2.9 Systemabnahmetest 39
14.2.10 ENR — Least Functionality 39
14.3 Testdaten 39

15 Lieferantenbeziehungen 40
15.1 Informationssicherheit in Lieferantenbeziehungen 40
15.1.1 Informationssicherheitsrichtlinie für Lieferantenbeziehungen 40
15.1.2 Behandlung von Sicherheit in Lieferantenvereinbarungen 40
15.1.3 Lieferkette für Informations- und Kommunikationstechnologie 40
15.2 Steuerung der Dienstleistungserbringung von Lieferanten 40

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27019:2020-08

16 Handhabung von Informationssicherheitsvorfällen 40
16.1 Handhabung von Informationssicherheitsvorfällen und -verbesserungen 40
16.1.1 Verantwortlichkeiten und Verfahren 40
16.1.2 Meldung von Informationssicherheitsereignissen 40
16.1.3 Meldung von Schwächen in der Informationssicherheit 40
16.1.4 Beurteilung von und Entscheidung über Informationssicherheitsereignisse 41
16.1.5 Reaktion auf Informationssicherheitsvorfälle 41
16.1.6 Erkenntnisse aus Informationssicherheitsvorfällen 41
16.1.7 Sammeln von Beweismaterial 41

17 Informationssicherheitsaspekte beim Business Continuity Management 41
17.1 Aufrechterhalten der Informationssicherheit 41
17.2 Redundanzen 41
17.2.1 Verfügbarkeit von informationsverarbeitenden Einrichtungen 41
17.2.2 ENR — Notfallkommunikation 42

18 Compliance 43
18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen 43
18.1.1 Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen 43
18.1.2 Geistige Eigentumsrechte 43
18.1.3 Schutz von Aufzeichnungen 43
18.1.4 Privatsphäre und Schutz von personenbezogener Information 43
18.1.5 Regelungen bezüglich kryptographischer Maßnahmen 43
18.2 Überprüfungen der Informationssicherheit 44
18.2.1 Unabhängige Überprüfung der Informationssicherheit 44
18.2.2 Einhaltung von Sicherheitsrichtlinien und –standards 44
18.2.3 Überprüfung der Einhaltung von technischen Vorgaben 44

Anhang A (normativ) Energieversorgungs-spezifische Referenzmaßnahmenziele und Maßnahmen 45

Literaturhinweise 48

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27019:2020-08

Europäisches Vorwort

Der Text von ISO/IEC 27019:2017 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als EN ISO/IEC 27019:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis September 2020, und etwaige entgegenstehende nationale Normen müssen bis September 2020 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 27019:2017 wurde von CEN als EN ISO/IEC 27019:2020 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27019:2020-08

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames Technisches Komitee, ISO/IEC JTC 1 (JTC, en: Joint Technical Committee), eingerichtet.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/IEC JTC 1, *Information technology,* Unterkomitee SC 27, *IT Security techniques,* erarbeitet.

Diese erste Ausgabe annulliert und ersetzt die erste Ausgabe (ISO/IEC TR 27019:2013), die technisch überarbeitet wurde.

Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende:

— der Anwendungsbereich wurde geändert und umfasst nun auch den Öl-Energie-Sektor;

— die Veröffentlichungsform wurde von einen internationalen Technical Report in eine Internationale Norm geändert;

— das Vorgängerdokument wurde an die Struktur der ISO/IEC 27002:2005 angepasst. Das neue Dokument wurde an die neue Struktur der ISO/IEC 27002:2013 angepasst;

— der Titel wurde geändert;

— der technische Inhalt wurde an den entsprechenden Stellen angepasst, um die aktuellen Entwicklungen im Energiesektor zu berücksichtigen.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27019:2020-08

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html zu finden.

In dieser korrigierten Version von ISO/IEC 27019:2017 wurde „sollten“ durch „sind zu“ in Tabelle A.1, 11.1.7 ersetzt.

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27019:2020-08

0 Einleitung

0.1 Hintergrund und Kontext

Dieses Dokument definiert auf Basis der Norm ISO/IEC 27002:2013 „Code of practice for information security controls“ Umsetzungsanleitungen zur Realisierung eines Informationssicherheitsmanagements für Prozesssteuerungssysteme der Energieversorgung. Das Ziel dieses Dokuments ist die Erweiterung von ISO/IEC 27002:2013 auf den Bereich der Prozesssteuerungs- und Automatisierungstechnik, um der Energieversorgungsbranche die Implementierung eines einheitlichen, spezifischen Informationssicherheitsmanagementsystems (ISMS) auf Basis der Norm ISO/IEC 27001:2013, von der Geschäfts- bis zur Prozessebene, zu ermöglichen.

In Ergänzung zu den in ISO/IEC 27002:2013 aufgeführten Sicherheitszielen und Maßnahmen haben Prozesssteuerungssysteme der Energieversorgung zusätzliche, besondere Anforderungen. Im Vergleich mit herkömmlichen Informations- und Kommunikationstechnik-Umgebungen (z. B. Büro-IT, Energiehandelssysteme) bestehen grundsätzliche und signifikante Unterschiede bezüglich der Entwicklung, des Betriebs, der Instandhaltung und Wartung und des Einsatzumfelds von Prozesssteuerungssystemen. Des Weiteren kann die in diesem Dokument behandelte Prozesstechnik ein integraler Bestandteil von Kritischen Infrastrukturen und zwingend für deren sicheren und störungsfreien Betrieb notwendig sein. Diese Unterscheidungen und Charakteristiken sind im Managementprozess von Prozesssteuerungssystemen umfassend zu berücksichtigen und rechtfertigen eine getrennte Betrachtung innerhalb der Normenreihe ISO/IEC 27000.

Aus Design- und Funktionssicht handelt es sich bei Prozesssteuerungssystemen in der Energieversorgungsbranche um Informationsverarbeitungssysteme. Sie erfassen Prozessdaten und nutzen Sensoren für die Zustandsüberwachung physischer Prozesse. Die Systeme verarbeiten die erhobenen Daten und generieren Steuersignale, die Aktivitäten über Aktoren regulieren. Die Steuerung und Regelung verläuft automatisiert, das Bedienpersonal hat aber außerdem die Möglichkeit, manuell einzugreifen. Damit sind Informationen und Informationsverarbeitungssysteme ein wesentlicher Teil der zentralen Betriebsprozesse in Energieversorgungsunternehmen. Angemessene Sicherheitsmaßnahmen sind entsprechend wichtig und sollten, genau wie in anderen organisatorischen Einheiten, Anwendung finden.

In Prozesssteuerungsumgebungen kommen immer häufiger Software- und Hardwarekomponenten (z. B. programmierbare Logik) auf Basis von Standard-Informations- und Kommunikationstechnik zum Einsatz, worauf dieses Dokument ebenfalls näher eingeht. Weiterhin sind Prozesssteuerungssysteme in der Energieversorgung immer stärker vernetzt und bilden komplexe Systeme. Risiken, die aus dieser Entwicklung resultieren, bedürfen der Betrachtung in einer Risikobewertung.

Informationen und Informationsverarbeitungssysteme in Prozesssteuerungsumgebungen sind immer öfter Bedrohungen und Sicherheitslücken ausgesetzt. Daher ist es im Prozesssteuerungsbereich des Energieversorgungssektors von wesentlicher Bedeutung, durch die Einführung und kontinuierliche Verbesserung eines ISMS auf Basis der Vorgaben der ISO/IEC 27001:2013 eine ausreichende Informationssicherheit sicherzustellen.

Eine effektive Informationssicherheit im Prozesssteuerungsbereich lässt sich in der Energieversorgungsbranche durch die Einführung, Umsetzung, Überwachung, Überprüfung und — wo notwendig — Optimierung der in diesem Dokument aufgeführten relevanten Maßnahmen erzielen, um die speziellen Sicherheits- und Geschäftsziele der Organisation zu erreichen. Die besondere Rolle der Energieversorger für die Gesellschaft und die ökonomische Notwendigkeit einer sicheren und zuverlässigen Energieversorgung verdienen hier besondere Aufmerksamkeit. Letztendlich beruht der Gesamterfolg der Cybersicherheit im Energiesektor auf den gemeinschaftlichen Anstrengungen aller Beteiligten (Hersteller, Lieferanten, Versorger, Kunden usw.).

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27019:2020-08

0.2 Sicherheitsaspekte für Prozesssteuerungssysteme bei Energieversorgern

Der Bedarf nach einem allgemeingültigen Informationssicherheits-Rahmenwerk für den Prozesssteuerungsbereich der Energieversorgung ergibt sich aus unterschiedlichen Grundanforderungen:

a) Kunden erwarten eine sichere, zuverlässige Energieversorgung.

b) Rechtliche und regulatorische Anforderungen fordern den sicheren, verlässlichen Betrieb der Energieversorgungssysteme.

c) Energieversorger benötigen Informationssicherheit, um die eigenen Geschäftsinteressen zu wahren, Kundenbedürfnisse zu erfüllen und gesetzliche Bestimmungen einzuhalten.

0.3 Anforderungen an Informationssicherheit

Es ist wichtig, dass Energieversorger ihre Sicherheitsanforderungen identifizieren. Als Basis für diese Anforderungen dienen drei wesentliche Quellen:

a) Die Ergebnisse einer organisationsinternen Risikobewertung unter Berücksichtigung der allgemeinen Geschäftsziele und -strategien der Organisation. Im Rahmen dieser Risikobewertung werden Risikoquellen und -szenarien identifiziert sowie mögliche Konsequenzen und Eintrittswahrscheinlichkeiten dieser Risiken bewertet.

b) Durch Gesetze, Verordnungen, Regulierungen und Verträge vorgegebene Anforderungen, die eine Organisation einzuhalten hat. Hierbei sind die soziokulturellen Verpflichtungen einzubeziehen. Konkrete Beispiele umfassen die Sicherstellung einer zuverlässigen und effektiven Energieversorgung sowie die zuverlässige Erfüllung der Bedingungen eines deregulierten Energiemarktes, insbesondere der zuverlässige und sichere Datenaustausch mit externen Parteien.

c) Die spezifischen Regeln, Ziele und geschäftlichen Bedingungen für Informationsverarbeitung, die von der Organisation zur Unterstützung der eigenen Geschäftsprozesse entwickelt wurden.

ANMERKUNG Es ist wichtig, dass Energieversorgungsunternehmen sicherstellen, dass die Sicherheitsanforderungen von Prozesssteuerungssystemen analysiert und in den Richtlinien für Informationssicherheit ausreichend berücksichtigt werden. Teil der Analyse der Informationssicherheitsanforderungen und -ziele ist der Einbezug aller relevanten Kriterien für eine sichere Energieversorgung und -lieferung, z. B.:

— Beeinträchtigung der Versorgungssicherheit;

— Einschränkung des Energieflusses;

— betroffener Bevölkerungsanteil;

— Gefahr für Leib und Leben;

— Auswirkung auf andere Kritische Infrastrukturen;

— Auswirkungen auf den Datenschutz;

— finanzielle Auswirkungen.

Die notwendigen Sicherheitsmaßnahmen werden durch eine methodische Bewertung der Sicherheitsrisiken ermittelt. Es ist erforderlich, die Kosten der Maßnahmen gegen mögliche wirtschaftliche Verluste durch auftretende Sicherheitsprobleme abzuwägen. Die Ergebnisse dieser Risikoanalyse unterstützen:

— die Definition angemessener Managementaktionen und -prioritäten zur Behandlung von Informationssicherheitsrisiken; und

— die Umsetzung der ausgewählten Maßnahmen zur Abwehr dieser Risiken.

AVA Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27019:2020-08

Diese Risikobewertung sollte in regelmäßigen Abständen wiederholt werden, um sämtliche Veränderungen mit zu berücksichtigen, welche die bewerteten Ergebnisse beeinflussen können.

Anforderungen für die Risikobewertung und Auswahl geeigneter Maßnahmen sind in ISO/IEC 27001:2013 festgelegt.

0.4 Auswahl der Maßnahmen

Sobald die Sicherheitsanforderungen und -risiken identifiziert und eine entsprechende Behandlung festgelegt wurden, sollten geeignete Maßnahmen ausgewählt und umgesetzt werden, um sicherzustellen, dass die identifizierten Risiken so auf ein akzeptables Maß reduziert werden.

Zusätzlich zu den Maßnahmen, die mit einem umfassenden Informationssicherheitsmanagementsystem einhergehen, enthält dieses Dokument weitere Hilfen und branchenspezifische Maßnahmen für Prozesssteuerungssysteme der Energieversorgungsbranche, unter Berücksichtigung der besonderen Anforderungen dieser Umgebung. Falls notwendig, können weitere Maßnahmen entwickelt werden, um bestimmten Anforderungen zu genügen. Die Auswahl der Sicherheitsmaßnahmen hängt letztlich von organisationsinternen Entscheidungen ab, die auf Basis interner Risikoakzeptanzkriterien, den Möglichkeiten, diesen Risiken zu begegnen, und dem allgemeinen Risikomanagementkonzept der Organisation getroffen werden. Die Maßnahmenauswahl sollte außerdem relevante nationale und internationale Gesetze, Rechtsverordnungen und Vorschriften berücksichtigen.

0.5 Zielgruppe

Dieses Dokument richtet sich an die System- und Betriebsverantwortlichen von Prozesssteuerungssystemen der Energieversorgung und die zuständigen Informationssicherheitsverantwortlichen sowie an Hersteller, Systemintegratoren und Auditoren. Für diese Zielgruppe werden die grundlegenden Maßnahmen und Maßnahmenziele der Norm ISO/IEC 27002:2013 präzisiert und spezifische Maßnahmen für die Prozesssteuerungssysteme der Energieversorgungsbranche, unterstützende Systeme und die zugehörige Infrastruktur definiert.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27019:2020-08

1 Anwendungsbereich

Dieses Dokument gibt auf Basis von ISO/IEC 27002:2013 Hinweise für Systeme der Prozesssteuerung der Energieversorgung, die zur Steuerung, Regelung und Überwachung von Gewinnung oder Erzeugung, Übertragung, Speicherung und Verteilung von Strom, Gas, Öl und Wärme und für die Steuerung von unterstützenden Prozessen dienen. Dies umfasst insbesondere:

— zentrale und dezentrale Prozesssteuerungs-, Leit-, Automatisierungs- und Überwachungstechnik sowie die für ihren Betrieb genutzten Informationssysteme, wie z. B. Programmier- und Parametriergeräte;

— digitale Steuerungen und Automatisierungskomponenten wie Leit- und Feldgeräte oder Speicherprogrammierbare Steuerungen (SPSen), inklusive digitaler Sensor- und Aktorelemente;

— alle weiteren in der Prozesstechnik genutzten unterstützenden Informationssysteme, z. B. für die Aufgabe der ergänzenden Datenvisualisierung und zur Steuerung, Überwachung, Datenarchivierung, Langzeitprotokollierung, Berichtswesen und zur Dokumentation;

— in der Prozesstechnik eingesetzte Kommunikationstechnik, z. B. Netzwerk-, Telemetrie-, Fernwirk- und Fernsteuertechnik;

— Advanced-Metering-Infrastruktur-(AMI)-Komponenten, z. B. intelligente Zähler;

— Mess- und Zählvorrichtungen, z. B. zur Emissionswerterfassung;

— digitale Schutz- und Safety-Systeme, z. B. Schutzgeräte, Sicherheits-Steuerungen und Notfallsteuerungsmechanismen;

— Energiemanagementsysteme, z. B. für dezentrale Energieerzeugungssysteme, elektrische Ladeinfrastrukturen, in Privathaushalten, Wohngebäuden oder industriellen Kundeninstallationen;

— verteilte Komponenten von Smart-Grid-Umgebungen, z. B. in Energienetzen, Privathaushalten, Wohngebäuden oder industriellen Kundeninstallationen;

— alle Arten von Software, Firmware und Anwendungen, die auf den vorgenannten Systemen eingesetzt werden, z. B. Netzführungs-Anwendungen oder Ausfallmanagementsysteme;

— jegliche Lokalität mit den oben erwähnten Anlagen oder Systemen;

— Fernwartungssysteme für die oben aufgeführten Systeme.

Nicht im Geltungsbereich dieses Dokuments liegt der Bereich der Prozesssteuerung von Kernenergieanlagen. Dieser Bereich wird von IEC 62645 abgedeckt.

Darüber hinaus enthält dieses Dokument eine Anforderung, um die in ISO/IEC 27001:2013 beschriebenen Risikobeurteilungs- und -behandlungsprozesse an die in diesem Dokument enthaltenen energiesektorspezifischen Empfehlungen anzupassen.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27019:2020-08