

**DIN ISO/IEC 27019**

ICS 03.100.70; 35.030; 35.240.50

**Entwurf**

Einsprüche bis 2018-09-06  
Vorgesehen als Ersatz für  
DIN ISO/IEC TR 27019  
(DIN SPEC 27019):2015-03

**Informationstechnik –  
Sicherheitsverfahren –  
Informationssicherheitsmaßnahmen für die Energieversorgung  
(ISO/IEC 27019:2017);  
Text Deutsch und Englisch**

Information technology –  
Security techniques –  
Information security controls for the energy utility industry (ISO/IEC 27019:2017);  
Text in German and English

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);  
Texte en allemand et anglais

**Anwendungswarnvermerk**

Dieser Norm-Entwurf mit Erscheinungsdatum 2018-07-06 wird der Öffentlichkeit zur Prüfung und  
Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs  
besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter [www.din.de/go/entwuerfe](http://www.din.de/go/entwuerfe) bzw. für Norm-  
Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter [www.entwuerfe.normenbibliothek.de](http://www.entwuerfe.normenbibliothek.de),  
sofern dort wiedergegeben;
- oder als Datei per E-Mail an [nia@din.de](mailto:nia@din.de) möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im  
Internet unter [www.din.de/go/stellungnahmen-norm-entwuerfe](http://www.din.de/go/stellungnahmen-norm-entwuerfe) oder für Stellungnahmen zu Norm-  
Entwürfen der DKE unter [www.dke.de/stellungnahme](http://www.dke.de/stellungnahme) abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA),  
10772 Berlin, Burggrafenstr. 6, 10787 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten  
Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 89 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

## Inhalt

|                                                                                   | Seite |
|-----------------------------------------------------------------------------------|-------|
| Nationales Vorwort .....                                                          | 6     |
| Nationaler Anhang NA (informativ) Literaturhinweise .....                         | 7     |
| Vorwort .....                                                                     | 8     |
| 0 Einleitung.....                                                                 | 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 Energieversorgungs-spezifische 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 |
| 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 .....                                       | 22 |
| 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 .....                                                    | 23 |
| 9.3.1  | Gebrauch geheimer Authentisierungsinformation .....                                   | 23 |
| 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 .....                         | 24 |
| 9.4.5  | Zugangssteuerung für Quellcode von Programmen .....                                   | 24 |
| 10     | Kryptographie .....                                                                   | 24 |
| 10.1   | Kryptographische Maßnahmen .....                                                      | 24 |
| 10.1.1 | Richtlinie zum Gebrauch von kryptographischen Maßnahmen .....                         | 24 |
| 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 .....                                     | 25 |
| 11.1.4 | Schutz vor externen und umweltbedingten Bedrohungen .....                             | 25 |
| 11.1.5 | Arbeiten in Sicherheitsbereichen .....                                                | 25 |
| 11.1.6 | Anlieferungs- und Ladebereiche .....                                                  | 25 |
| 11.1.7 | ENR – Sichern von Leitstellen .....                                                   | 25 |
| 11.1.8 | ENR – Sicherung von Technikräumen .....                                               | 26 |
| 11.1.9 | ENR – Sicherung von Außenstandorten .....                                             | 28 |
| 11.2   | Geräte und Betriebsmittel .....                                                       | 28 |
| 11.2.1 | Platzierung und Schutz von Geräten und Betriebsmitteln .....                          | 28 |
| 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 .....                                                            | 29 |
| 11.2.6 | Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten ..... | 29 |
| 11.2.7 | Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln .....        | 29 |
| 11.2.8 | Unbeaufsichtigte Benutzergeräte .....                                                 | 29 |
| 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 .....                                   | 30 |
| 11.3.3 | ENR – Gekoppelte Steuerungs- und Kommunikationssysteme .....                          | 31 |

|                |                                                                                              |           |
|----------------|----------------------------------------------------------------------------------------------|-----------|
| <b>12</b>      | <b>Betriebssicherheit .....</b>                                                              | <b>31</b> |
| <b>12.1</b>    | <b>Betriebsabläufe und -verantwortlichkeiten.....</b>                                        | <b>31</b> |
| <b>12.1.1</b>  | <b>Dokumentierte Bedienabläufe .....</b>                                                     | <b>31</b> |
| <b>12.1.2</b>  | <b>Änderungssteuerung.....</b>                                                               | <b>32</b> |
| <b>12.1.3</b>  | <b>Kapazitätssteuerung .....</b>                                                             | <b>32</b> |
| <b>12.1.4</b>  | <b>Trennung von Entwicklungs-, Test- und Betriebsumgebungen.....</b>                         | <b>32</b> |
| <b>12.2</b>    | <b>Schutz vor Schadsoftware.....</b>                                                         | <b>32</b> |
| <b>12.2.1</b>  | <b>Maßnahmen gegen Schadsoftware.....</b>                                                    | <b>32</b> |
| <b>12.3</b>    | <b>Datensicherung.....</b>                                                                   | <b>33</b> |
| <b>12.4</b>    | <b>Protokollierung und Überwachung.....</b>                                                  | <b>33</b> |
| <b>12.4.1</b>  | <b>Ereignisprotokollierung .....</b>                                                         | <b>33</b> |
| <b>12.4.2</b>  | <b>Schutz der Protokollinformation .....</b>                                                 | <b>33</b> |
| <b>12.4.3</b>  | <b>Administratoren- und Bedienerprotokolle .....</b>                                         | <b>33</b> |
| <b>12.4.4</b>  | <b>Uhrensynchronisation.....</b>                                                             | <b>33</b> |
| <b>12.5</b>    | <b>Steuerung von Software im Betrieb .....</b>                                               | <b>34</b> |
| <b>12.5.1</b>  | <b>Installation von Software auf Systemen im Betrieb.....</b>                                | <b>34</b> |
| <b>12.6</b>    | <b>Handhabung technischer Schwachstellen.....</b>                                            | <b>34</b> |
| <b>12.6.1</b>  | <b>Handhabung von technischen Schwachstellen.....</b>                                        | <b>34</b> |
| <b>12.6.2</b>  | <b>Einschränkungen von Softwareinstallation .....</b>                                        | <b>34</b> |
| <b>12.7</b>    | <b>Audits von Informationssystemen.....</b>                                                  | <b>34</b> |
| <b>12.8</b>    | <b>ENR - Altsysteme.....</b>                                                                 | <b>34</b> |
| <b>12.8.1</b>  | <b>ENR – Behandlung von Altsystemen.....</b>                                                 | <b>34</b> |
| <b>12.9</b>    | <b>ENR - Safety-Funktionen .....</b>                                                         | <b>35</b> |
| <b>12.9.1</b>  | <b>ENR – Integrität und Verfügbarkeit von Safety-Funktionen .....</b>                        | <b>35</b> |
| <b>13</b>      | <b>Kommunikationssicherheit.....</b>                                                         | <b>36</b> |
| <b>13.1</b>    | <b>Netzwerksicherheitsmanagement.....</b>                                                    | <b>36</b> |
| <b>13.1.1</b>  | <b>Netzwerksteuerungsmaßnahmen .....</b>                                                     | <b>36</b> |
| <b>13.1.2</b>  | <b>Sicherheit von Netzwerkdiensten.....</b>                                                  | <b>36</b> |
| <b>13.1.3</b>  | <b>Trennung in Netzwerken.....</b>                                                           | <b>36</b> |
| <b>13.1.4</b>  | <b>ENR – Sicherung der Prozessdatenkommunikation .....</b>                                   | <b>36</b> |
| <b>13.1.5</b>  | <b>ENR – Logische Anbindung von externen Prozesssteuerungssystemen .....</b>                 | <b>37</b> |
| <b>13.2</b>    | <b>Informationsübertragung .....</b>                                                         | <b>37</b> |
| <b>14</b>      | <b>Anschaffung, Entwicklung und Instandhaltung von Systemen.....</b>                         | <b>38</b> |
| <b>14.1</b>    | <b>Sicherheitsanforderungen an Informationssysteme.....</b>                                  | <b>38</b> |
| <b>14.1.1</b>  | <b>Analyse und Spezifikation von Informationssicherheitsanforderungen.....</b>               | <b>38</b> |
| <b>14.1.2</b>  | <b>Sicherung von Anwendungsdiensten in öffentlichen Netzwerken .....</b>                     | <b>38</b> |
| <b>14.1.3</b>  | <b>Schutz der Transaktionen bei Anwendungsdiensten.....</b>                                  | <b>38</b> |
| <b>14.2</b>    | <b>Sicherheit in Entwicklungs- und Unterstützungsprozessen .....</b>                         | <b>38</b> |
| <b>14.2.1</b>  | <b>Richtlinie für sichere Entwicklung .....</b>                                              | <b>38</b> |
| <b>14.2.2</b>  | <b>Verfahren zur Verwaltung von Systemänderungen.....</b>                                    | <b>38</b> |
| <b>14.2.3</b>  | <b>Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform .....</b> | <b>38</b> |
| <b>14.2.4</b>  | <b>Beschränkung von Änderungen an Softwarepaketen.....</b>                                   | <b>38</b> |
| <b>14.2.5</b>  | <b>Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme .....</b>             | <b>38</b> |
| <b>14.2.6</b>  | <b>Sichere Entwicklungsumgebung .....</b>                                                    | <b>38</b> |
| <b>14.2.7</b>  | <b>Ausgegliederte Entwicklung.....</b>                                                       | <b>38</b> |
| <b>14.2.8</b>  | <b>Testen der Systemsicherheit.....</b>                                                      | <b>38</b> |
| <b>14.2.9</b>  | <b>Systemabnahmetest .....</b>                                                               | <b>38</b> |
| <b>14.2.10</b> | <b>ENR – Least Functionality .....</b>                                                       | <b>39</b> |
| <b>14.3</b>    | <b>Testdaten .....</b>                                                                       | <b>39</b> |
| <b>15</b>      | <b>Lieferantenbeziehungen.....</b>                                                           | <b>39</b> |
| <b>15.1</b>    | <b>Informationssicherheit in Lieferantenbeziehungen .....</b>                                | <b>39</b> |
| <b>15.1.1</b>  | <b>Informationssicherheitsrichtlinie für Lieferantenbeziehungen .....</b>                    | <b>39</b> |
| <b>15.1.2</b>  | <b>Behandlung von Sicherheit in Lieferantenvereinbarungen.....</b>                           | <b>39</b> |
| <b>15.1.3</b>  | <b>Lieferkette für Informations- und Kommunikationstechnologie.....</b>                      | <b>39</b> |

|                                |                                                                                          |           |
|--------------------------------|------------------------------------------------------------------------------------------|-----------|
| <b>15.2</b>                    | <b>Steuerung der Dienstleistungserbringung von Lieferanten.....</b>                      | <b>39</b> |
| <b>16</b>                      | <b>Handhabung von Informationssicherheitsvorfällen .....</b>                             | <b>40</b> |
| <b>16.1</b>                    | <b>Handhabung von Informationssicherheitsvorfällen und -verbesserungen.....</b>          | <b>40</b> |
| <b>16.1.1</b>                  | <b>Verantwortlichkeiten und Verfahren .....</b>                                          | <b>40</b> |
| <b>16.1.2</b>                  | <b>Meldung von Informationssicherheitsereignissen .....</b>                              | <b>40</b> |
| <b>16.1.3</b>                  | <b>Meldung von Schwächen in der Informationssicherheit.....</b>                          | <b>40</b> |
| <b>16.1.4</b>                  | <b>Beurteilung von und Entscheidung über Informationssicherheitsereignisse .....</b>     | <b>40</b> |
| <b>16.1.5</b>                  | <b>Reaktion auf Informationssicherheitsvorfälle .....</b>                                | <b>40</b> |
| <b>16.1.6</b>                  | <b>Erkenntnisse aus Informationssicherheitsvorfällen .....</b>                           | <b>40</b> |
| <b>16.1.7</b>                  | <b>Sammeln von Beweismaterial.....</b>                                                   | <b>40</b> |
| <b>17</b>                      | <b>Informationssicherheitsaspekte beim Business Continuity Management.....</b>           | <b>40</b> |
| <b>17.1</b>                    | <b>Aufrechterhalten der Informationssicherheit.....</b>                                  | <b>40</b> |
| <b>17.2</b>                    | <b>Redundanzen .....</b>                                                                 | <b>41</b> |
| <b>17.2.1</b>                  | <b>Verfügbarkeit von informationsverarbeitenden Einrichtungen .....</b>                  | <b>41</b> |
| <b>17.2.2</b>                  | <b>ENR – Notfallkommunikation.....</b>                                                   | <b>41</b> |
| <b>18</b>                      | <b>Compliance.....</b>                                                                   | <b>42</b> |
| <b>18.1</b>                    | <b>Einhaltung gesetzlicher und vertraglicher Anforderungen .....</b>                     | <b>42</b> |
| <b>18.1.1</b>                  | <b>Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen .....</b> | <b>42</b> |
| <b>18.1.2</b>                  | <b>Geistige Eigentumsrechte .....</b>                                                    | <b>42</b> |
| <b>18.1.3</b>                  | <b>Schutz von Aufzeichnungen .....</b>                                                   | <b>42</b> |
| <b>18.1.4</b>                  | <b>Privatsphäre und Schutz von personenbezogener Information.....</b>                    | <b>42</b> |
| <b>18.1.5</b>                  | <b>Regelungen bezüglich kryptographischer Maßnahmen.....</b>                             | <b>42</b> |
| <b>18.2</b>                    | <b>Überprüfungen der Informationssicherheit.....</b>                                     | <b>43</b> |
| <b>18.2.1</b>                  | <b>Unabhängige Überprüfung der Informationssicherheit.....</b>                           | <b>43</b> |
| <b>18.2.2</b>                  | <b>Einhaltung von Sicherheitsrichtlinien und -standards .....</b>                        | <b>43</b> |
| <b>18.2.3</b>                  | <b>Überprüfung der Einhaltung von technischen Vorgaben.....</b>                          | <b>43</b> |
| <b>Anhang A (normativ)</b>     | <b>Energieversorgungs-spezifische Referenzmaßnahmenziele und Maßnahmen .....</b>         | <b>44</b> |
| <b>Literaturhinweise .....</b> |                                                                                          | <b>47</b> |

## **Nationales Vorwort**

Dieses Dokument enthält die deutsche Übersetzung der Internationalen Norm ISO/IEC 27019:2018, der vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ erarbeitet wurde, dessen Sekretariat von ANSI (USA) gehalten wird.

Das internationale Dokument (ISO/IEC 27019:2018) ist unverändert in diesen Norm-Entwurf übernommen worden.

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

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

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)    |

## **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 einem 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.

## 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), *Datenmodelle, Schnittstellen und Informationsaustausch für Planung und Betrieb von Energieversorgungsunternehmen — Daten- und Kommunikationssicherheit*

## 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](http://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](http://www.iso.org/patents)).

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

Eine Erläuterung zum freiwilligen Charakter von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen, sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO) hinsichtlich technischer Handelshemmnisse (TBT) berücksichtigt, enthält der folgende Link [www.iso.org/iso/foreword.html](http://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 zweite Ausgabe 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 einem internationalen Technical Report in eine Internationale Norm geändert;
- das Dokument wurde an die neue Struktur der ISO/IEC 27002 Ausgabe 2013 angepasst;
- der Titel wurde geändert;
- der technische Inhalt wurde an den entsprechenden Stellen angepasst, um die aktuellen Entwicklungen im Energiesektor zu berücksichtigen.

## **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 der Energieversorgung, 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, Energiehandelsysteme) 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 ISO/IEC 27000 Normenreihe.

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 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, sollten in der Risikobewertung entsprechend mitberücksichtigt werden.

Informationen und Informationsverarbeitungssysteme in Prozesssteuerungsumgebungen sind immer öfter Bedrohungen und Sicherheitslücken ausgesetzt, daher ist es im Prozesssteuerungsbereich essentiell 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 (Versorger, Lieferanten und Dienstleister, Kunden usw.).

## 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) Stromversorger 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. Die Kosten der Maßnahmen sollten gegen mögliche wirtschaftliche Verluste durch auftretende Sicherheitsprobleme abgewogen werden. 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.

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 organisations-internen Entscheidungen ab, die auf Basis interner Risikoakzeptanzkriterien, 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 detailliert sie die grundlegenden Maßnahmen und Maßnahmenziele der Norm ISO/IEC 27002:2013 und definiert spezifische Maßnahmen für die Prozesssteuerungssysteme der Energieversorgungsbranche, unterstützende Systeme und die zugehörige Infrastruktur.

## 1 Anwendungsbereich

Dieses Dokument gibt auf Basis von ISO/IEC 27002:2013 Empfehlungen 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 Dokumentation;
- in der Prozesstechnik eingesetzte Kommunikationstechnik, z. B. Netzwerk-, Telemetrie-, Fernwirk- und Fernsteuertechnik;
- Advanced-Metering-Infrastruktur-(AMI)-Komponenten wie 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 energiesektor-spezifischen Empfehlungen anzupassen.

## 2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

## 3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 27000 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

— ISO Online Browsing Platform: <http://www.iso.org/obp>

— IEC Electropedia: <http://www.electropedia.org/>

### 3.1

#### **Schwarzfall**

weitreichender Ausfall der Stromversorgung

### 3.2

#### **Computer Security Incident Response Team**

##### **CSIRT**

Team von Sicherheitsexperten, das bei der Lösung von konkreten Informationssicherheitsvorfällen unterstützend wirkt

### 3.3

#### **kritischer Wert (Asset)**

Wert, der direkten Einfluss auf die Gewinnung oder Erzeugung, Übertragung, Speicherung und Verteilung von Strom, Gas, Öl und Wärme haben kann

### 3.4

#### **kritische Infrastruktur**

Organisationen und Einrichtungen, die für das Funktionieren der Gesellschaft und der Wirtschaft als Ganzes von entscheidender Bedeutung sind

Anmerkung 1 zum Begriff: Ein Ausfall oder eine Beeinträchtigung solcher Organisationen und Einrichtungen könnte nachhaltige Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit und andere weitreichende Folgen nach sich ziehen.

### 3.5

#### **Debugging**

Fehleranalyse in Computersystemen

### 3.6

#### **Verteilnetz**

Netz für die Verteilung von Elektrizität mit hoher, mittlerer oder niedriger Spannung oder für den Transport von Gas oder Wärme über örtliche oder regionale Leitungsnetze

### 3.7

#### **Energiemanagementsystem**

EMS

Anlage oder Infrastruktur zur Überwachung, Messung und Steuerung des Energieverbrauchs in Privathaushalten, Wohngebäuden oder industriellen Kundeninstallationen

Anmerkung 1 zum Begriff: Der Begriff EMS wird häufig auch zur Beschreibung von Gruppen von Anwendungen verwendet, die von Übertragungsnetzbetreibern zur Überwachung, Steuerung und Optimierung der Leistung von Energieerzeugungs- und/oder -übertragungssystemen genutzt werden.

### 3.8

#### **Energieversorgung**

Prozess der Erzeugung, Gewinnung oder Speicherung von Energie zur Belieferung von Kunden sowie der Betrieb eines Energieversorgungsnetzes

### 3.9

#### **Energieversorger**

natürliche oder juristische Person, die Energie in Form von Elektrizität, Gas, Öl oder Wärme an andere liefert, ein Energieversorgungsnetz oder eine Speicheranlage betreibt

### 3.10

#### **Mensch-Maschine-Interface**

MMI

Benutzerschnittstelle zum Bedienen und Beobachten des Prozesssteuerungssystems bzw. der Anlage

### 3.11

#### **Wartung**

Maßnahmen, die im Bereich der *Energieversorgung* (3.8) üblicherweise Inspektion, Entstörung und Verbesserung betreffen

### 3.12

#### **Prozesssteuerungssystem**

System zur Steuerung, Regelung und Überwachung von Erzeugung, Gewinnung, Übertragung, Speicherung und Verteilung von Strom, Gas, Öl und Wärme, einschließlich der Steuerung unterstützender Prozesse

Anmerkung 1 zum Begriff: Prozesssteuerungssysteme werden, etwas allgemeiner, häufig auch als industrielle Steuerungssysteme bezeichnet. In diesem Dokument beziehen sich die Begriffe Prozesssteuerungssystem und industrielles Steuerungssystem ausschließlich auf Technologien und Komponenten, die in der Energieversorgungsbranche eingesetzt werden.

### 3.13

#### **Safety**

Freiheit von untragbaren Risiken

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

### 3.14

#### **Safety-Systeme**

Systeme und Komponenten, die zur Sicherstellung der *Safety* (3.13) benötigt werden

### 3.15

#### **Supervisory Control and Data Acquisition**

SCADA

*Prozesssteuerungssystem* (3.12), das zur Überwachung, Steuerung, Regelung und Datenerfassung von dezentralen Anlagen genutzt wird

### 3.16

#### **Smart Grid**

elektrisches Versorgungssystem, das Informationsaustausch- und -steuerungstechnologien, verteiltes Rechnen und entsprechende Sensoren und Aktoren nutzt

Anmerkung 1 zum Begriff: Smart-Grid-Technologien kommen z. B. wie folgt zum Einsatz:

- um die Handlungen und Verhaltensweisen von Netznutzern und anderen Beteiligten in Einklang zu bringen;
- um eine effiziente, nachhaltige, wirtschaftliche und sichere Stromversorgung zu gewährleisten.

### 3.17

#### **Transportnetz**

Übertragungsnetz zum Transport von Elektrizität über ein Höchstspannungs- und Hochspannungsnetz oder ein Fernleitungsnetz zum Transport von Erdgas durch ein Hochdruckrohrnetz

## **4 Aufbau dieses Dokuments**

### **4.1 Allgemein**

Dies ist eine sektorspezifische Norm mit Bezug zu ISO/IEC 27002:2013. Die Energieversorgungs-spezifischen Referenzmaßnahmenziele und -maßnahmen sind in Anhang A aufgeführt.

### **4.2 Anpassung der ISO/IEC 27001:2013-Anforderungen**

Die Anforderung nach ISO/IEC 27001:2013, 6.1.3 c) wird wie folgt verfeinert:

Die in 6.1.3 b) festgelegten Maßnahmen sind mit den Maßnahmen in ISO/IEC 27001:2013, Anhang A und in Anhang A dieses Dokuments zu vergleichen und zu überprüfen, dass keine erforderlichen Maßnahmen ausgelassen wurden.

Die Anforderung nach ISO/IEC 27001:2013, 6.1.3 d) wird wie folgt verfeinert:

Es ist eine Erklärung zur Anwendbarkeit zu erstellen, die folgendes enthält:

- die erforderlichen Maßnahmen [siehe ISO/IEC 27001:2013, 6.1.3 b) und c)];
- Gründe für deren Einbeziehung;
- ob sie umgesetzt sind oder nicht; und
- Gründe für die Nichteinbeziehung von Maßnahmen aus ISO/IEC 27001:2013, Anhang A oder Anhang A dieses Dokuments.

**ANMERKUNG** Diese Anpassungen sind aufgrund der Einführung neuer, Energieversorgungs-spezifischer Maßnahmen in diesem Dokument erforderlich.

Alle weiteren Anforderungen aus den Abschnitten 4 bis 10 von ISO/IEC 27001:2013 gelten unverändert. Hier ergeben sich keine zusätzlichen Anforderungen für die Energieversorgungsbranche.

### 4.3 Energieversorgungs-spezifische Maßnahmen mit Bezug zu ISO/IEC 27002:2013

Alle Energieversorgungs-spezifischen Abschnitte, Maßnahmenziele, Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen und jene nach ISO/IEC 27002:2013, die unverändert gelten, sind in den Abschnitten 5 bis 18 aufgeführt.

ANMERKUNG Überschriften von Abschnitten, Unterabschnitten und Maßnahmen, die in ISO/IEC 27002:2013 nicht enthalten sind, sind mit dem Präfix „ENR“ gekennzeichnet.

## 5 Informationssicherheitsrichtlinien

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, Abschnitt 5.

## 6 Organisation der Informationssicherheit

### 6.1 Interne Organisation

#### 6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten

Zusätzliche Umsetzungsanleitung für ISO/IEC 27002:2013, 6.1.1:

Die relevanten Steuerungssystemtechniker, Telekommunikationstechniker und anderen Beschäftigten sollten über ihre zugewiesenen Rollen und Verantwortlichkeiten informiert werden, insbesondere hinsichtlich der Informationssicherheitsaspekte der Prozesssteuerungssysteme.

#### 6.1.2 Aufgabentrennung

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 6.1.2.

#### 6.1.3 Kontakt mit Behörden

Zusätzliche Umsetzungsanleitung für ISO/IEC 27002:2013, 6.1.3:

Die Anwendungen und die Infrastruktur der Prozesssteuerungssysteme der Energieversorgung können einen Bestandteil Kritischer Infrastrukturen darstellen und somit für das Funktionieren des Gemeinwesens und für die Funktionsfähigkeit von Wirtschaft und Gesellschaft essentiell sein. Betreiber dieser Systeme sollten daher den Kontakt zu allen relevanten Behörden pflegen. Zusätzlich zu den relevanten öffentlichen Stellen (z. B. Feuerwehr, Polizeidienststellen) können dies z. B. sein:

- nationale und internationale Behörden und Kooperationseinrichtungen zum Schutz Kritischer Infrastrukturen;
- nationale und internationale CSIRT-Organisationen;
- Katastrophenschutz- sowie Katastrophenhilfsorganisationen;
- Gefahrenabwehrorganisationen und -personal.

Für die Betreiber von Komponenten Kritischer Infrastrukturen können zusätzliche lokale oder übergreifende Regularien und Gesetze zum Kontakt mit Behörden gelten. Energieversorger sollten sicherstellen, dass die Informationen, die sie über Kontakte zu Behörden erhalten, im Kontext der eigenen Organisation von entsprechend fachlich kompetenten Experten analysiert und bewertet sowie zeitnah an Verantwortliche in der Organisation weitergereicht werden.

Zusätzliche Informationen zu ISO/IEC 27002:2013, 6.1.3:

Im Rahmen des Tagesbetriebs und der Betriebseinsatzplanungen sowie zur Vorbereitung auf außergewöhnliche Situationen können Wetterinformationen erforderlich sein. Daher sollten direkte Kontakte zu den zuständigen lokalen, regionalen und nationalen Wetterdiensten und entsprechenden Informationsdiensten (z. B. Gewitterwarnung, Blitzortung) bestehen.

**6.1.4 Kontakt mit speziellen Interessensgruppen**

Zusätzliche Umsetzungsanleitung für ISO/IEC 27002:2013, 6.1.4:

Zum Austausch von Informationen zur Sicherheitsthematik im Umfeld der Prozesssteuerungstechnik und um eine organisationsübergreifende Zusammenarbeit zu ermöglichen, sollte der Kontakt zu nationalen und internationalen Hersteller- und Betreiberorganisationen und den dort für Sicherheit zuständigen Arbeitskreisen gepflegt werden. Beim Informationsaustausch sollte die gültige Rechtslage beachtet werden.

Energieversorger sollten sicherstellen, dass die Informationen, die sie über Kontakte zu speziellen Interessensgruppen erhalten, im Kontext der eigenen Organisation von entsprechend fachlich kompetenten Experten analysiert und bewertet sowie zeitnah an Verantwortliche in der Organisation weitergereicht werden.

**6.1.5 Informationssicherheit im Projektmanagement**

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 6.1.5.

**6.1.6 ENR — Identifizierung von Risiken in Zusammenhang mit Externen**

Zusätzliche Maßnahme zu ISO/IEC 27002:2013, 6.1:

**Maßnahme**

Die Risiken für Informationen und informationsverarbeitende Einrichtungen der Organisation, die durch Geschäftsprozesse unter Beteiligung Externer verursacht werden, sollten identifiziert und angemessene Maßnahmen umgesetzt werden, bevor Externen der Zugriff gewährt wird.

**Anleitung zur Umsetzung**

Prozesssteuerungssysteme können aus komplexen und individuell angepassten Systemen und Komponenten bestehen. Systemhersteller, Integratoren und andere Externe sind daher häufig sehr stark in die Betriebs- und Wartungsprozesse eingebunden. Zur Wartung und Fehlerbehebung können von diesen Externen Remote-Zugänge, die eine Wartung von einem anderen Standort ermöglichen, benötigt werden. Mitarbeiter von Externen können Zutritt zu Sicherheitsbereichen für eine Wartung vor Ort benötigen.

Die enge Zusammenarbeit der unterschiedlichen Systembetreiber auf Gewinnungs-, Erzeugungs-, Übertragungs- und Verteilnetzebene kann eine enge Kopplung zwischen Steuerungs- und Kommunikationsnetzwerken verschiedener Organisationen notwendig machen. Außerdem kann der Zugriff auf Informationen, die mit kritischen Werten (Assets) zusammenhängen, durch Externe wie Hersteller, Systemintegratoren oder Geschäftspartner erforderlich sein.

Die aus den Zugriffen auf kritische Werte (Assets) und damit zusammenhängenden Informationen durch Externe resultierenden Gefährdungen sollte insbesondere im Hinblick auf das Risiko für den zu steuernden bzw. zu überwachenden physischen Primärprozess bewertet und berücksichtigt werden. Wenn Externe auf kritische Werte (Assets) oder vertrauliche Informationen zugreifen können, sollte – z. B. durch entsprechende vertragliche Vereinbarungen – sichergestellt werden, dass sie vergleichbare Sicherheitsstandards einhalten, wie sie für die interne Organisation des Energieversorgers festgelegt sind.

### 6.1.7 ENR - Adressieren von Sicherheit im Umgang mit Kunden

Zusätzliche Maßnahme zu ISO/IEC 27002:2013, 6.1:

#### **Maßnahme**

Alle identifizierten Sicherheitsanforderungen sollten berücksichtigt sein, bevor Kunden Zugang zu Informationen oder Werten der Organisation gegeben wird.

#### **Anleitung zur Umsetzung**

Die komplexen und vielseitigen Beziehungen zwischen den Werteeigentümern, Systembetreibern, Dienstleistern sowie internen und externen Kunden im Energieversorgungssektor können in getrennten Verantwortlichkeiten für die Wartung, den Betrieb und das Eigentum von Organisationswerten resultieren. Beispiele hierfür sind:

- ein interner Dienstleister, der für den Betrieb und die Wartung der Infrastruktur des Transport- oder Verteilnetzes verantwortlich und einer separaten internen Organisationseinheit zugeordnet ist;
- ein Dienstleister, der für den Betrieb und die Wartung von Kraftwerken oder dezentralen Erzeugungseinheiten verantwortlich ist;
- ein interner oder externer Dienstleister, der für den Betrieb von Infrastrukturen der Prozesssteuerung verantwortlich ist;
- ein interner oder externer Kunde mit Verbindung zur Energieversorgungsinfrastruktur und den zugehörigen Prozesssteuerungssystemen und Kommunikationsinfrastrukturen.

Die verschiedenen, und/oder komplexen Geschäftsbeziehungen sollten bei der Identifizierung und Adressierung von Sicherheitsanforderungen bei Gewährung von Kundenzugriffen auf Informationen oder Werte berücksichtigt werden. Wenn Betriebseinrichtungen bei anderen Energieversorgern oder Kunden betrieben werden, oder bei der Kopplung von Prozesssteuerungssystemen, sollten die in 11.3.1, 11.3.2, 11.3.3 und 13.1.5 beschriebenen Maßnahmen berücksichtigt werden.

## 6.2 Mobilgeräte und Telearbeit

### 6.2.1 Richtlinie zu Mobilgeräten

Zusätzliche Umsetzungsanleitung für ISO/IEC 27002:2013, 6.2.1:

Wo in Prozesssteuerungsnetzwerken Mobilgeräte zum Einsatz kommen, sollten Energieversorger die folgenden Aspekte in ihren Sicherheitsrichtlinien für Mobilgeräte berücksichtigen:

- a) Definition und Zuordnung von Rollen, die bestimmte Tätigkeiten ausführen dürfen, welche Zugriff auf Prozesssteuerungssysteme durch mobile Geräte erfordern;
- b) Identifizierung von Aktionen, die diese Geräte ausführen dürfen sowie des Zeitraums, innerhalb dessen diese Aktionen erlaubt sind und expliziter Festlegung von notfallbedingten Ausnahmen;
- c) Festlegung der Änderungen, die am Gerät vorgenommen werden dürfen, wer diese Änderungen durchführen darf und wie solche Änderungen vorgenommen werden dürfen;
- d) Vorgabe der Standorte und Kommunikationsnetzwerke, die diese Geräte für den Zugriff nutzen dürfen, z. B. zu Hause, Büro, Außenstelle oder Einsatzfahrzeuge;

- e) Definition jeglicher Prozesse, die zur Verwaltung von Sicherheitsmechanismen wie Schlüsselmanagement, Zugangssteuerung, Konfigurationsverwaltung und Identitätsmanagement notwendig sind;
- f) Festlegung, wie jedes Gerät sich mit dem Prozesssteuerungsnetzwerk verbinden darf, z. B. über ein Gateway, Demilitarisierte Zonen, VPN-Tunnel;
- g) Trennung der Nutzung in Prozesssteuerungs- und andere Netzwerken (z. B. Büronetzwerke);
- h) Bestimmung von Datentypen, die übermittelt werden dürfen und explizite Unterbindung der Übermittlung aller anderen Datentypen.

### **6.2.2 Telearbeit**

#### Zusätzliche Umsetzungsanleitung für ISO/IEC 27002:2013, 6.2.2:

Fernzugriff auf Prozesssteuerungssysteme durch Mitarbeiter des Energieversorgungsunternehmens, Lieferanten oder andere externe Parteien sollte mehrfachen Sicherheitsmaßnahmen unterliegen, einschließlich:

- a) Multi-Faktor-Authentifizierung;
- b) Einsatz von Techniken, die ausschließlich indirekte Verbindungen zum Zielsystem oder -netzwerk zulassen;
- c) Minimierung der Funktionen, die über den Fernzugriff ausgeführt werden können, wie z. B. Fernsteuerung, Fernkonfigurierung und Programmierung von Prozesssteuerungssystemen;
- d) Überprüfung des Sicherheitsstatus des Fernzugriffsystems (z. B. aktueller Patch-Stand und Schadsoftwareschutz; Nichtvorhandensein von unerlaubten Programmen) und Schutz vor der Übertragung von Schadsoftware vom Fernzugriffssystem (siehe 12.2.1);
- e) Erzwingung zulässiger Zugriffsstandorte und/oder -systeme;
- f) Gewährleistung, dass der Fernzugriff überwacht und kontrolliert wird und dass Veränderungen und Modifizierungen kritischer Werte (Assets) nachvollziehbar sind;
- g) Sicherstellung, dass für Fernzugriff und Fernwartung ausschließlich bekannte und genehmigte Werkzeuge verwendet werden sollten.

## **7 Personalsicherheit**

### **7.1 Vor der Beschäftigung**

#### **7.1.1 Sicherheitsüberprüfung**

##### Zusätzliche Umsetzungsanleitung für ISO/IEC 27002:2013, 7.1.1:

Für Schlüsselpersonal, das Zugriff auf kritische Werte (Assets) hat oder für Betriebs- und Wartungsprozesse von kritischen Werten (Assets) verantwortlich ist, sollte ein genauer Überprüfungsprozess in Betracht gezogen und bei Bedarf eingeführt werden. Dies gilt im Besonderen, wenn diese Werte Teil einer Kritischen Infrastruktur oder für deren Betrieb notwendig sind.

Bevor neues Personal auf Komponenten zugreifen darf, die Teil einer Kritischen Infrastruktur sind, ist in Abhängigkeit von den jeweiligen gesetzlichen Bestimmungen ggf. eine Sicherheitsüberprüfung durch die zuständigen Behörden notwendig.

## **7.1.2 Beschäftigungs- und Vertragsbedingungen**

### Zusätzliche Umsetzungsanleitung für ISO/IEC 27002:2013, 7.1.2:

Der Energieversorger sollte durch entsprechende Arbeitsvertragsklauseln sicherstellen, dass Schlüsselpersonal und -kompetenzen für den Betrieb Kritischer Infrastrukturen stets verfügbar sind. Die Erlaubnis zur Überschreitung der maximal zulässigen Arbeitszeit in Notfallsituationen sollte unter Berücksichtigung der gesetzlichen Rahmenbedingungen für Schlüsselpersonal mit Verantwortlichkeiten im Betrieb Kritischer Infrastrukturen und kritischer Systeme in Betracht gezogen werden. Vereinbarungen zur Überwachung und Protokollierung von besonderen Tätigkeiten wie Schalthandlungen oder Programmier- und Parametrierzugriffen sollten ebenfalls im Arbeitsvertrag Berücksichtigung finden.

## **7.2 Während der Beschäftigung**

### **7.2.1 Verantwortlichkeiten der Leitung**

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 7.2.1.

### **7.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung**

#### Zusätzliche Umsetzungsanleitung für ISO/IEC 27002:2013, 7.2.2:

Mitarbeiter, die in der Energieversorgungsbranche für Prozesssteuerungstechnik verantwortlich sind, sollten das notwendige Fachwissen und die notwendigen Kompetenzen vorweisen, um die Installation, Wartung und den sicheren Betrieb von Prozesssteuerungssystemen zu leiten und zu überwachen. Hierzu sollte auch hinreichendes Fachwissen in Bezug auf moderne Informationssystemtechnologien und Informationssicherheit gehören.

### **7.2.3 Maßregelungsprozess**

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 7.2.3.

## **7.3 Beendigung und Änderung der Beschäftigung**

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 7.3.

## **8 Verwaltung der Werte**

### **8.1 Verantwortlichkeit für Werte**

#### **8.1.1 Inventarisierung der Werte**

##### Zusätzliche Umsetzungsanleitung für ISO/IEC 27002:2013, 8.1.1:

Die Inventarliste der organisationseigenen Werte (Assets) sollte alle für die Energieversorgung relevanten Geschäftsprozesse, Prozesssteuerungssysteme sowie Informationen, Anwendungen und deren unterstützenden Werte (Assets) umfassen.

##### Zusätzliche Informationen zu ISO/IEC 27002:2013, 8.1.1:

Werte (Assets) im Bereich der Energieversorgung beinhalten viele sektorspezifische Wertetypen, wie z. B.:

- a) **Informationen:** Netzpläne, Fahrplan- und Dispatching-Daten, geographische und georeferenzierte Informationen, Krisen- und Notfallpläne, Netzwiederaufbaupläne, Schaltantragsdaten, Messwerte- und Messdaten, Zählwerte und Zählerdaten, Meldungen, Betriebsprotokolle, Anwendungsprogrammier- und Parametrierdaten, Messwert- und Meldungsarchive, Langzeit- und Trenddaten usw.;

ANMERKUNG Anwendungsprogrammier- und Parametrierdaten digitaler Steuerungs- und Automatisierungskomponenten sind hierin eingeschlossen.

- b) **Software:** Leittechnische Software, Visualisierungssysteme, Energiemanagement- und Optimierungs-Software, Simulationssoftware, Parametriersoftware, Management- und Überwachungssysteme, Betriebs- und Einsatzmanagementsysteme, Programmierungsumgebungen, Firmware, Archivierungs-, Berichts- und Langezeitprotokollierungs-Software usw.;
- c) **physische Werte:** Leittechnik- und Automatisierungskomponenten, Fernwirkkomponenten, nachrichtentechnische Komponenten, digitale Schutz- und Safety-Komponenten, digitale Mess- und Zählvorrichtungen, Smart Meter, digitale Sensoren und Aktoren, Parametrier- und Programmiergeräte, Visualisierungs- und Bedienkomponenten, digitale Überwachungs-, Schreiber- und Aufzeichnungssysteme usw.;
- d) **Dienstleistungen:** Telekommunikationsdienstleistungen, Notfallkommunikationsdienste, Informationsdienste, Wetterdienste, Medien- und Nachrichtendienste, Zeitdienste usw.

### 8.1.2 Zuständigkeit für Werte

#### Zusätzliche Umsetzungsanleitung für ISO/IEC 27002:2013, 8.1.2:

Aufgrund der potenziell komplexen Strukturen der Organisationen, die Prozesssteuerungssysteme einsetzen, können sehr unterschiedliche Verantwortlichkeiten bezüglich der kaufmännischen und betrieblichen Eigentümerschaft vorhanden sein. Daher sollte die Eigentümerschaft und die Verantwortlichkeiten in Bezug auf die Werte (Assets), sowie die Rollen der Werteeigentümer und -betreiber, hinsichtlich der Informationssicherheit definiert und dokumentiert werden.

### 8.1.3 Zulässiger Gebrauch von Werten

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 8.1.3.

### 8.1.4 Rückgabe von Werten

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 8.1.4.

## 8.2 Informationsklassifizierung

### 8.2.1 Klassifizierung von Information

#### Zusätzliche Umsetzungsanleitung für ISO/IEC 27002:2013, 8.2.1:

Spezifische Einstufungskriterien für die Energieversorgung sollten wo notwendig die folgenden Punkte umfassen:

- Werte (Assets), Systeme und Informationen zur Betriebsunterstützung von Kritischen Infrastrukturen und kritischen Werten (Assets);
- Werte (Assets), Systeme und Informationen, die zum Wiederaufbau der Energieversorgung nach einer Großstörung (Netzwiederaufbau) benötigt werden, z. B. schwarzstartfähige Systeme und Komponenten;
- Werte (Assets), Systeme und Informationen, die zur Sicherstellung der Arbeits- und der Anlagensicherheit benötigt werden;
- Werte (Assets), Systeme und Informationen, die zu Erfüllung regulatorischer Anforderungen wie z. B. Entflechtungsanforderungen oder anderer spezieller Anforderungen benötigt werden;
- Informationen, die von externen Parteien wie z. B. Kunden oder Regulierungsbehörden als vertraulich oder persönlich eingestuft werden.

### 8.2.2 Kennzeichnung von Information

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 8.2.2.

### 8.2.3 Handhabung von Werten

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 8.2.3.

## 8.3 Handhabung von Datenträgern

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 8.3.

## 9 Zugangssteuerung

### 9.1 Geschäftsanforderungen an die Zugangssteuerung

#### 9.1.1 Zugangssteuerungsrichtlinie

Zusätzliche Umsetzungsanleitung für ISO/IEC 27002:2013, 9.1.1:

Zusätzlich sollte die Richtlinie Folgendes berücksichtigen:

- a) Bedingungen und Bestimmungen für die Verwendung von Gruppenkonten, wo der Einsatz persönlicher Nutzerkonten nicht möglich ist. Festgelegt werden sollten insbesondere konkrete Ausnahmeregelungen und ergänzende Maßnahmen, um eine hinreichende Zugangssicherheit und Nachvollziehbarkeit sicherzustellen.
- b) Bedingungen und Bestimmungen für Systeme, die keine starke Passwortrichtlinie unterstützen bzw. wo dies aus betrieblichen Gründen nicht möglich ist. Festgelegt werden sollten insbesondere ergänzende Maßnahmen, um eine hinreichende Zugangssicherheit sicherzustellen.
- c) Die Notwendigkeit, dass Mitarbeiter und externe Einsatzorganisationen in erklärten Notfallsituationen die Möglichkeit haben, Zugangssicherheitsmaßnahmen außer Kraft zu setzen.
- d) Zugang zu Diensten oder Anwendungen durch nicht ausreichend authentifizierte Systeme (z. B. bei Maschine-zu-Maschine-Kommunikation). Um hier ein ausreichendes Maß an Zugangssicherheit sicherzustellen, sollten Netzwerkzugangssteuerungen oder ähnliche Maßnahmen in Betracht gezogen werden.

Zusätzliche Informationen zu ISO/IEC 27002:2013, 9.1.1:

IEC/TS 62351-8 enthält zusätzliche Empfehlungen zur Implementierung der Zugangssteuerung auf Datenobjekte in Energieversorgungssystemen durch Nutzer und automatisierte Agenten durch eine rollenbasierte Zugangssteuerung.

#### 9.1.2 Zugang zu Netzwerken und Netzwerkdiensten

Zusätzliche Umsetzungsanleitung für ISO/IEC 27002:2013, 9.1.2:

Zum Schutz von Netzwerkgeräten, die Zugriff auf kritische Netzwerke ermöglichen, sollte Folgendes berücksichtigt werden:

- a) Gewährleistung eines physischen Zugangsschutzes für Netzwerkgeräte, besonders an abgelegenen Standorten;
- b) Entfernung oder Sperrung sämtlicher Dienste und Schnittstellen der Netzwerkgeräte, die für den Normalbetrieb (z. B. ungenutzte Switch-Ports), Notbetrieb oder Wartungsoperationen nicht benötigt werden. Dies umfasst sowohl Kommunikationsschnittstellen als auch physische Ein-/Ausgabe-Schnittstellen. Diese Entfernung oder Sperrung kann durch Softwaremaßnahmen oder physische Trennung erfolgen.

## 9.2 Benutzerzugangsverwaltung

### 9.2.1 Registrierung und Deregistrierung von Benutzern

#### Zusätzliche Umsetzungsanleitung für ISO/IEC 27002:2013, 9.2.1:

Der Einsatz von eindeutigen Kennungen ist im Umfeld der Prozesssteuerungssysteme der Energieversorgung nicht immer möglich. Z. B. trifft das für den Zugriff auf das Betriebssystem oder die Firmware von Embedded-Systemen wie Automatisierungskomponenten oder für Wartungsprozesse von verteilten Systemen zu. Die daraus resultierenden Risiken sollten beachtet und risikomindernde Gegenmaßnahmen sollten umgesetzt werden.

Die Nutzung von personenbezogenen und Gruppennutzerkonten sollte den entsprechenden Protokollierungsrichtlinien entsprechen (siehe 12.4.1).

### 9.2.2 Zuteilung von Benutzerzugängen

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 9.2.2.

### 9.2.3 Verwaltung privilegierter Zugangsrechte

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 9.2.3.

### 9.2.4 Verwaltung geheimer Authentisierungsinformation von Benutzern

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 9.2.4.

### 9.2.5 Überprüfung von Benutzerzugangsrechten

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 9.2.5.

### 9.2.6 Entzug oder Anpassung von Zugangsrechten

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 9.2.6.

## 9.3 Benutzerverantwortlichkeiten

### 9.3.1 Gebrauch geheimer Authentisierungsinformation

#### Zusätzliche Umsetzungsanleitung für ISO/IEC 27002:2013, 9.3.1:

Im Prozesssteuerungsumfeld ist es nicht immer möglich, die Nutzung sicherer, geheimer Authentisierungsinformationen sicherzustellen, u. a. aus den folgenden Gründen:

- Altsysteme erlauben oftmals keine individuellen Passwörter oder Passwörter mit einer ausreichenden Stärke;
- Systeme, die in dezentralen Anlagen, wie z. B. Stationen, oder in der dezentralen Erzeugung betrieben werden, können häufig nicht an zentrale Verzeichnisdienste angebunden werden, so dass es notwendig ist, lokale Konten zu verwenden. Hierdurch sind regelmäßige Änderungen der geheimen Authentisierungsinformationen in der Regel nicht praktikabel.

Daher sollte für die Anwender klar herausgestellt werden, wann die allgemeine Richtlinie für geheime Authentisierungsinformationen angewandt wird und wo Ausnahmen erlaubt sind, z. B. wo abweichende Passwörter zu verwenden sind bzw. keine Passwörter verwendet werden können (Altsysteme).

Gerade wenn in einem System mehrere Nutzer dieselben geheimen Authentisierungsinformationen gemeinsam für den Systemzugriff verwenden, sollte Folgendes berücksichtigt werden:

- die gemeinsam genutzten geheimen Authentisierungsinformationen sollten so sicher wie möglich gewählt werden;
- sie sollten häufiger gewechselt werden als personenbezogene geheime Authentisierungsinformationen;
- sie sollten im Fall von Personalwechseln geändert werden.

Speziell die Standardpasswörter der Hersteller sollten als unsicher betrachtet und deshalb geändert werden. Der Zugriff auf geheime Authentifizierungsinformationen sollte nur Personen möglich sein, die in den Betrieb des Systems involviert sind.

## **9.4 Zugangssteuerung für Systeme und Anwendungen**

### **9.4.1 Informationszugangsbeschränkung**

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 9.4.1.

### **9.4.2 Sichere Anmeldeverfahren**

Zusätzliche Umsetzungsanleitung für ISO/IEC 27002:2013, 9.4.2:

Die Aktivierung von Session Time-outs sowie Bildschirmschonern ist für bestimmte Prozesssteuerungsanwendungen nicht anwendbar. Darunter fallen z. B. MMIs und Visualisierungsanwendungen, die zur kontinuierlichen Prozessüberwachung durch Bedienpersonal genutzt werden, z. B. in Leitwarten. Für solche Anwendungen sollten die aus unbeaufsichtigten Sitzungen entstehenden Risiken berücksichtigt und entsprechende ergänzende Gegenmaßnahmen umgesetzt werden.

### **9.4.3 System zur Verwaltung von Kennwörtern**

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 9.4.3.

### **9.4.4 Gebrauch von Hilfsprogrammen mit privilegierten Rechten**

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 9.4.4.

### **9.4.5 Zugangssteuerung für Quellcode von Programmen**

Zusätzliche Umsetzungsanleitung für ISO/IEC 27002:2013, 9.4.5:

Im Energieversorgungssektor schließt Quellcode Anwendungsprogrammier- und Parametrierdaten von digitalen Steuerungen und Automatisierungskomponenten ein.

## **10 Kryptographie**

### **10.1 Kryptographische Maßnahmen**

#### **10.1.1 Richtlinie zum Gebrauch von kryptographischen Maßnahmen**

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 10.1.1.

### **10.1.2 Schlüsselverwaltung**

Zusätzliche Informationen zu ISO/IEC 27002:2013, 10.1.2:

IEC 62351-9 legt fest, wie digitale Zertifikate und kryptographische Schlüssel in der Kommunikation von elektrischen Energieversorgungssystemen generiert, verteilt, zurückgezogen und gehandhabt werden. Dieses Dokument kann auch in anderen Energieversorgungsbereichen angewandt werden.

## **11 Physische und umgebungsbezogene Sicherheit**

### **11.1 Sicherheitsbereiche**

#### **11.1.1 Physische Sicherheitsperimeter**

Zusätzliche Umsetzungsanleitung für ISO/IEC 27002:2013, 11.1.1:

Besonders in Energietransport- und Energieverteilnetzen sowie im Bereich der dezentralen Gewinnung und Erzeugung sind die Komponenten auf dezentrale Standorte verteilt. Die Betriebsmittel werden dabei in Steuerungs- und Technikräumen in den organisationseigenen Gebäuden und in eventuell unbesetzten Außenstandorten untergebracht. Teilweise befinden sich die Betriebsmittel auch in Gebäuden oder auf dem Gelände Dritter bzw. in öffentlichen Bereichen. Da ein umfassender physischer Schutz der Außenstandorte nicht immer erreicht werden kann, sollte das Restrisiko bewertet und ggf. durch ergänzende und kompensierende Maßnahmen reduziert werden.

#### **11.1.2 Physische Zutrittssteuerung**

Zusätzliche Umsetzungsanleitung für ISO/IEC 27002:2013, 11.1.2:

Der Einsatz von Systemen zur physischen Zutrittssteuerung sollte ebenfalls für dezentrale Außenstandorte, an denen kritische Werte (Assets) vorhanden sind, in Betracht gezogen werden. Siehe 11.1.9.

#### **11.1.3 Sichern von Büros, Räumen und Einrichtungen**

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 11.1.3.

#### **11.1.4 Schutz vor externen und umweltbedingten Bedrohungen**

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 11.1.4.

#### **11.1.5 Arbeiten in Sicherheitsbereichen**

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 11.1.5.

#### **11.1.6 Anlieferungs- und Ladebereiche**

Keine zusätzlichen spezifischen Informationen für den Energieversorgungssektor für ISO/IEC 27002:2013, 11.1.6.

#### **11.1.7 ENR – Sichern von Leitstellen**

Zusätzliche Maßnahme zu ISO/IEC 27002:2013, 11.1:

#### **Maßnahme**

Maßnahmen zur Sicherstellung der physischen Sicherheit von Leitstellen, in denen z. B. Steuerungssystem-Server, MMI-Systeme und unterstützende Systeme untergebracht sind, sollten konzipiert, entwickelt und umgesetzt werden.

### **Anleitung zur Umsetzung**

Um Einrichtungen für zentrale Prozesssteuerungssysteme wie z.B. Netzleitstellen oder Leitwarten von zentralisierten oder dezentralen Kraftwerken, Produzenten oder Erzeugern (im Folgenden Leitstellen genannt) zu sichern, sollten die folgenden Punkte berücksichtigt werden:

- a) Für die Leitstelle sollte ein Standort mit stabilem Untergrund gewählt werden; ist kein solcher Standort verfügbar, sind entsprechende Maßnahmen zur Sicherstellung einer ausreichenden Tragfähigkeit des Baugrundes vorzusehen.
- b) Für die Leitstelle sollte ein Standort gewählt werden, der nicht anfällig für Gefährdungen durch Umwelteinflüsse wie Wind und Wasser ist. Für einen bereits existierenden Standort, der anfällig für derartige Umwelteinflüsse ist, sollten entsprechende Maßnahmen ergriffen werden, um Schäden zu vermeiden.
- c) Für die Leitstelle sollte ein Standort gewählt werden, der nicht anfällig für Störungen durch starke elektromagnetische Felder ist; für einen bereits existierenden Standort, der starken elektromagnetischen Feldern ausgesetzt ist, sollten entsprechende Maßnahmen ergriffen werden, um die Betriebsräume der Leitstelle durch elektromagnetische Abschirmungen zu schützen.
- d) Leitstellen sollten nicht in unmittelbarer Nähe von Einrichtungen platziert sein, die Gefahrgüter mit Explosions- und Brandgefahr lagern.
- e) In Gebieten, die durch Naturkatastrophen wie Erdbeben, Tsunamis, Vulkanausbrüche oder Tornados gefährdet sind, sollten Leitstellen in einem gegen derartige Katastrophen gesicherten Gebäude untergebracht sein.
- f) Leitstellen sollten in einem brandsicheren oder brandbeständigen Gebäude untergebracht sein.
- g) Leitstellen sollten in einem Gebäude untergebracht sein, dessen Statik für die notwendigen Deckenlasten ausgelegt ist; bei bereits existierenden Standorten sollten entsprechende Maßnahmen ergriffen werden, um eine strukturelle Stabilität sicherzustellen, die den oben genannten Statikansprüchen gerecht wird.
- h) Leitstellen sollten mit einer automatischen Brandmeldeanlage ausgestattet sein, einschließlich angemessener Frühwarn- und Löschsysteme.

### **Weitere Informationen für die Energieversorgung**

Komponenten von Prozesssteuerungssystemen werden ggf. in von Dritten betriebenen Rechenzentren zusammen mit weiterer Informations- und Kommunikationstechnik untergebracht. Eine physische Trennung zwischen Prozesssteuerungssystemen und anderen Informations- und Kommunikationstechnik-Systemen sowie eine strikte Aufgabentrennung sind wesentlich, wenn Prozesssteuerungssysteme oder die Informations- und Kommunikationstechnik durch Dritte betrieben werden. Häufig wird ein Betrieb durch Externe in Standorten realisiert, die sich nicht unter der Kontrolle des Energieversorgers befinden.

#### **11.1.8 ENR – Sicherung von Technikräumen**

Zusätzliche Maßnahme zu ISO/IEC 27002:2013, 11.1:

#### **Maßnahme**

Maßnahmen zur Sicherstellung der physischen Sicherheit von Technikräumen für Prozesssteuerungssysteme der Energieversorgung sollten konzipiert, entwickelt und umgesetzt werden.

## **Anleitung zur Umsetzung**

Um Technikräume für Prozesssteuerungssysteme der Energieversorgung (nachfolgend als Technikräume bezeichnet) zu sichern, sollten folgende Maßnahmen berücksichtigt werden:

- a) Der Technikraum sollte so positioniert werden, dass er möglichst geschützt gegen externe Schadeinwirkungen ist, z. B. extreme Umwelteinflüsse oder Naturkatastrophen. Bei bereits existierenden Technikräumen sollten Maßnahmen ergriffen werden, um sie vor derartigen Gefahren von außen zu schützen.
- b) Der Technikraum sollte so positioniert werden, dass er möglichst geschützt gegen den Zutritt durch Unbefugte ist; bei bereits existierenden Technikräumen sollten Maßnahmen ergriffen werden, um einen möglichen unbefugten Zutritt zu verhindern oder zu erkennen.
- c) Wenn möglich sollte der Technikraum unauffällig sein. Hinweise auf die Nutzung als Technikraum für Prozesssteuerungssysteme, sollten auf das Notwendigste beschränkt werden.
- d) Der Technikraum sollte so positioniert werden, dass er gegen Überflutung und das Eindringen von Wasser geschützt ist. Erfüllt der Raum diese Anforderung nicht, sollten die notwendigen Maßnahmen, wie das Anheben der Stockwerkhöhe, wasserundurchlässige Gebäudeausführung oder die Installation spezieller Entwässerungseinrichtungen usw. ergriffen werden.
- e) Der Technikraum sollte so gelegen sein, dass er möglichst gut gegen Störeinflüsse von starken elektromagnetischen Feldern geschützt ist. Erfüllt der Raum diese Anforderungen nicht, sollte er durch elektromagnetische Abschirmungen oder andere Maßnahmen geschützt werden. Dies gilt insbesondere in der Nähe von Hochspannungsanlagen, Starkstromeinrichtungen, Transformatoren usw. Für Schutz vor Störung durch elektromagnetische Felder sollte ebenfalls gesorgt werden, wenn der Technikraum für Datenspeicher- und/oder Backup-Zwecke genutzt wird.
- f) Komponenten mit erhöhtem Sicherheitsbedarf sollten in dedizierten Technikräumen mit entsprechendem physischem Schutz untergebracht werden.
- g) In erdbebengefährdeten Gebieten sollten Maßnahmen ergriffen werden, um das Zusammenbrechen und Herabfallen von Gegenständen oder Boden-, Wand- und Deckenmaterialien zu verhindern.
- h) In Technik- und Datenspeicherräumen sollten Brandschutzmaßnahmen ergriffen werden.
- i) Es sollten Maßnahmen gegen Störungen durch statische Aufladungen ergriffen werden.
- j) Kabelkanäle, die mit dem Technikraum verbunden sind, sollten brandschutztechnisch gesichert sein, so dass sie die Ausbreitung von Bränden verhindern oder hemmen.
- k) Technikräume, sowie Räume mit Klimatechnik, sollten mit automatischen Brandmeldesystemen ausgestattet sein.
- l) Technikräume, sowie Räume mit Klimatechnik, sollten mit Feuerlöschern ausgestattet sein.
- m) Technikräume sollten, wo notwendig, über eine Klimaanlage verfügen. Die Klimatisierung sollte gegen Störungen wie Stromausfälle abgesichert sein.

**ANMERKUNG** Bei Technikräume an Außenstandorten sind nicht alle der genannten Umsetzungsanleitungen vollumfänglich anwendbar (siehe 11.1.9).