

ICS 25.040.40; 29.240.01; 35.040

Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002

Guidance for information security management of power supply control systems based on ISO/IEC 27002

Directives du système de management de la sécurité de l'information pour le système de commande du fourniture d'énergie au base de ISO/IEC 27002

Zur Erstellung einer DIN SPEC können verschiedene Verfahrensweisen herangezogen werden:
Das vorliegende Dokument wurde nach den Verfahrensregeln einer Vornorm erstellt.

Gesamtumfang 48 Seiten

Inhalt

	Seite
Vorwort	4
Einleitung.....	4
1 Anwendungsbereich	7
2 Normative Verweisungen.....	7
3 Begriffe	7
4 Übersicht	9
4.1 Aufbau dieser Norm	9
4.2 Informationssicherheits-Managementsysteme im Bereich der Energieversorgung.....	10
5 Sicherheitsleitlinie	11
6 Organisation der Informationssicherheit	11
6.1 Interne Organisation.....	11
6.2 Externe.....	13
7 Management von organisationseigenen Werten.....	14
7.1 Verantwortung für organisationseigene Werte (Assets)	14
7.2 Klassifizierung von Informationen.....	15
8 Personalsicherheit.....	15
8.1 Vor der Anstellung.....	15
8.2 Während der Anstellung	16
8.3 Beendigung oder Änderung der Anstellung	16
9 Physische und umgebungsbezogene Sicherheit.....	16
9.1 Sicherheitsbereiche.....	16
9.2 Sicherheit von Betriebsmitteln.....	19
9.3 Sicherheit in Räumlichkeiten Dritter.....	21
10 Betriebs- und Kommunikationsmanagement	22
10.1 Verfahren und Verantwortlichkeiten	22
10.2 Management der Dienstleistungserbringung von Dritten	23
10.3 Systemplanung und Abnahme	23
10.4 Schutz vor Schadsoftware und mobilem Programmcode.....	23
10.5 Backup	24
10.6 Management der Netzsicherheit.....	24
10.7 Handhabung von Speicher- und Aufzeichnungsmedien.....	25
10.8 Austausch von Informationen	25
10.9 E-Commerce-Anwendungen.....	25
10.10 Überwachung	25
10.11 Altsysteme	26
10.12 Betriebssicherheit.....	26
11 Zugangskontrolle.....	27
11.1 Geschäftsanforderungen für Zugangskontrolle.....	27
11.2 Benutzerverwaltung	27
11.3 Benutzerverantwortung	27
11.4 Zugangskontrolle für Netze	28
11.5 Zugriffskontrolle auf Betriebssysteme.....	29
11.6 Zugangskontrolle zu Anwendungen und Information	30
11.7 Mobile Computing und Telearbeit.....	30
12 Beschaffung, Entwicklung und Wartung von Informationssystemen	30
12.1 Sicherheitsanforderungen von Informationssystemen	30

	Seite
12.2 Korrekte Verarbeitung in Anwendungen	30
12.3 Kryptographische Maßnahmen.....	30
12.4 Sicherheit von Systemdateien	31
12.5 Sicherheit bei Entwicklungs- und Unterstützungsprozessen	31
12.6 Umgang mit Schwachstellen.....	31
13 Umgang mit Informationssicherheitsvorfällen.....	31
13.1 Melden von Informationssicherheitsereignissen und Schwachstellen.....	31
13.2 Umgang mit Informationssicherheitsvorfällen und Verbesserungen.....	31
14 Sicherstellung des Geschäftsbetriebs (Business Continuity Management)	31
14.1 Informationssicherheitsaspekte bei der Sicherstellung des Geschäftsbetriebs (Business Continuity Management)	31
14.2 Wesentliche Notfalldienste.....	32
15 Einhaltung von Vorgaben (Compliance).....	33
15.1 Einhaltung gesetzlicher Vorgaben	33
15.2 Einhaltung von Sicherheitsleitlinien und -standards, und technischer Vorgaben.....	34
15.3 Überlegungen zu Revisionsprüfungen von Informationssystemen	34
Anhang A (informativ) Erweiterter Maßnahmenkatalog für die Energieversorgung.....	35
Anhang B (informativ) Zusätzliche Umsetzungsempfehlungen.....	38
Literaturhinweise	48

Vorwort

Eine DIN SPEC nach dem Vornorm-Verfahren ist das Ergebnis einer Normungsarbeit, das wegen bestimmter Vorbehalte zum Inhalt oder wegen des gegenüber einer Norm abweichenden Aufstellungsverfahrens vom DIN noch nicht als Norm herausgegeben wird

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

Für diese DIN SPEC (Vornorm) gelten die für die Normungsarbeit niedergelegten Grundsätze und Regeln, insbesondere die Forderungen nach Einheitlichkeit und Widerspruchsfreiheit zum deutschen Normenwerk. Eine DIN SPEC (Vornorm) ist, wie eine Norm, nach den Regeln der DIN 820 zu erstellen. Der wesentliche Unterschied zu einer Norm ist jedoch, dass eine Vornorm nicht auf dem Konsens aller interessierten Kreise basieren muss. Daher bieten DIN SPEC (Vornorm) der Öffentlichkeit die Chance, Ergebnisse aus Normungsvorhaben zu nutzen, die aufgrund fehlenden Konsenses oder wegen bestimmter Vorbehalte zum Inhalt nicht als DIN-Norm veröffentlicht werden können. Die Erstellung einer DIN SPEC (Vornorm) wird von den betreffenden Normenausschüssen begleitet.

Diese DIN SPEC wurde erarbeitet vom NA 043-01-27-01 AK „Anforderungen, Dienste und Richtlinien für IT Sicherheitssysteme“ im Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN.

Einleitung

Diese Spezifikation definiert auf Basis des Standards DIN ISO/IEC 27002:2008-09 „Leitfaden für das Informationssicherheits-Management“ Umsetzungsanleitungen zur Realisierung von Informationssicherheits-Maßnahmen im Rahmen eines Informationssicherheits-Managements für Prozesssteuerungssysteme der Energieversorgung. Das Ziel dieser Arbeit ist die Erweiterung der ISO/IEC 27000-Standards auf den Bereich der Prozessleit- und Automatisierungstechnik der Energieversorgung, um die Implementierung eines einheitlichen Informationssicherheits-Managementsystems (ISMS) auf Basis des Standards DIN ISO/IEC 27001 für das gesamte Unternehmen, von der Geschäfts- bis hin zu Prozessebene, zu ermöglichen.

Im Fokus der Anwendung dieses Standards sind Systeme und Netzwerke zur Steuerung und Überwachung von Erzeugung, Übertragung und Verteilung von Strom, Gas und Wärme in Kombination mit der Steuerung von unterstützenden Prozessen. Dies umfasst die Leit- und Automatisierungssysteme, die Schutz- und Sicherheitssysteme sowie die Messtechnik inklusive der zugehörigen Kommunikations- und Fernwirktechnik. Diese Systeme werden im Folgenden unter dem vereinfachten Oberbegriff „Prozesssteuerungssysteme“ zusammengefasst.

In Ergänzung zu den im Standard DIN ISO/IEC 27002:2008-09 konkret formulierten Sicherheitszielen und Maßnahmen haben Prozesssteuerungssysteme der Energieversorgung zusätzliche, besondere Anforderungen. Im Vergleich mit herkömmlichen IT-Umgebungen (z. B. Büro-IT) bestehen grundsätzliche und signifikante Unterschiede bezüglich der Entwicklung, des Betriebs, der Instandhaltung und Wartung und des Einsatzumfelds von Prozesssteuerungssystemen. Des Weiteren kann die in dieser Norm 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 Standardreihe.

Im Detail bestehen die folgenden grundlegenden Unterschiede zu herkömmlichen IT-Systemen:

Sicherheitsmerkmale

Prozesssteuerungssysteme weisen gegenüber herkömmlichen IT-Umgebungen in der Regel erhöhte Anforderungen bezüglich Verfügbarkeit und Integrität auf. In verschiedenen Einsatzumgebungen darf es zu keinem Ausfall der prozessüberwachenden- und steuernden Einrichtungen kommen. Auch die Integrität der Daten ist häufig von herausragender Bedeutung. Fehlerhafte Daten können Fehlsteuerungen auslösen, zum Versagen von Schutz- und Safetyssystemen führen oder auf Grund falscher Prozessabbilder bzw. einer verfälschten Prozessdarstellung zu gefährlichen Fehlentscheidungen des Bedienpersonals führen. Diese Anforderungen müssen bereits im Systemdesign, aber auch im Systembetrieb berücksichtigt werden.

Systemarchitektur

Neben den zentralen IT-Installationen von Leitstellen für den Netzbetrieb oder in konventionellen Kraftwerken, gibt es verschiedene Systeme, die typischerweise über große Gebiete verteilt sind, z. B.:

- Prozesssteuerungs- und -überwachungssysteme in Unterstationen und Gasdruckregel- und Messanlagen,
- Prozesssteuerungs- und -überwachungssysteme für dezentrale Erzeugung wie Wind- oder Photovoltaik-Kraftwerke,
- Digitale Mess- und Zählvorrichtungen.

Häufig können diese verteilten Systeme nicht mit einem gleichwertigen physischen Schutz wie die zentralen Einrichtungen versehen werden. Dieser Umstand muss von der Systemarchitektur berücksichtigt werden, ggf. müssen zusätzliche Schutzvorkehrungen an den Schnittstellen zwischen den verteilten und den zentralen Systemen vorgesehen werden.

Ebenso können sich die Betriebs- und Managementprozesse für die verteilten Systeme von zentralisierten IT-Umgebungen unterscheiden. So ist es beispielsweise in der Regel nicht üblich, Veränderungen an betriebswichtigen Systemen in kritischen Schaltstationen oder anderen wichtigen Anlagen über Fernzugriffe vorzunehmen, es sei denn, entsprechendes Außendienstpersonal ist vor Ort.

Des Weiteren sollte die Architektur der Prozesssteuerung einen autonomen (lokalen) Betrieb ohne Netzwerkverbindung zur zentralen Installation für jeden verteilten Standort ermöglichen. Im Falle von Stromausfällen muss ein Wiederanlauf ausgewählter Anlagen auch ohne externe Energiezufuhr möglich sein, z. B. zum Netzwiederaufbau (Schwarzstartfähigkeit).

Wartung

Prozesssteuerungssysteme werden häufig für eine Laufzeit von bis zu 20 Jahren oder mehr entworfen. Sofern Standardbetriebssysteme oder -software eingesetzt werden, sind spezielle Maßnahmen im Umgang mit veralteter und von den Herstellern nicht länger unterstützter Software zu treffen.

Häufige Außerbetriebnahmen von Steuerungskomponenten, z. B. zur Installation von Patches oder Updates, sind in der Regel nicht realisierbar. Neustarts nach der Softwareinstallation könnten aufgrund von Verfügbarkeitsanforderungen nicht akzeptabel sein. Wartungsfenster müssen geplant und mit entsprechender Vorlaufzeit angesetzt werden. Besonders umfassende und sorgfältige Installations- und Funktionstests sind notwendig, um die Integrität des Prozesssteuerungssystems zu gewährleisten.

Geräteressourcen

Prozessnahe Komponenten von Prozesssteuerungssystemen sind in der Regel nur zur Verarbeitung der Prozessdaten entwickelt worden und verfügen daher häufig nicht über ausreichend Systemressourcen für die Unterstützung zusätzlicher Sicherheitsmaßnahmen wie Verschlüsselung oder Authentisierung.

Zielgruppe

Diese Spezifikation richtet sich an die System- und Betriebsverantwortlichen von Prozesssteuerungssystemen der Energieversorgung und die zuständigen Informationssicherheitsverantwortlichen sowie an Hersteller, Systemintegratoren und Auditoren. Sie detailliert für diese Zielgruppe die grundlegenden Maßnahmen und Maßnahmenziele des Standards DIN ISO/IEC 27002:2008-09 und definiert spezifische Maßnahmen für diese Prozesssteuerungssysteme, unterstützende Systeme und die zugehörige Infrastruktur.

1 Anwendungsbereich

Der Anwendungsbereich dieser Spezifikation umfasst die Systeme der Prozesssteuerung der Energieversorgung die zur Steuerung und Überwachung von Erzeugung, Übertragung, Speicherung und Verteilung von Strom, Gas und Wärme in Kombination mit der Steuerung von unterstützenden Prozessen dienen. Dies umfasst insbesondere die folgenden Systeme, Anwendungen und Komponenten:

- die gesamte IT-gestützte zentrale und dezentrale Prozess-, Leit-, Automatisierungs- und Überwachungstechnik sowie die für ihren Betrieb genutzten IT-Systeme, wie z. B. Programmier- und Parametriergeräte;
- Digitale Steuerungs- und Automatisierungskomponenten wie Leit- und Feldgeräte, Controller oder SPSen inklusive digitaler Sensor- und Aktorelemente;
- alle weiteren in der Prozesstechnik genutzten unterstützenden IT-Systeme, sei es für ergänzende Aufgaben der Visualisierung und Steuerung, zur Überwachung oder zur Archivierung und Dokumentation;
- die gesamte in der Prozesstechnik zur IT-Kommunikation eingesetzte Netzwerk-, Telemetrie-, Fernwirk- und Fernsteuertechnik;
- Digitale Mess- und Zählvorrichtungen, z. B. zur Verbrauchs- und Emissionswerterfassung;
- Digitale Schutz- und Safetyssysteme, z. B. Schutzgeräte oder Maschinenschutzkomponenten;
- verteilte Komponenten zukünftiger Smart-Grid-Umgebungen;
- alle Programme und Anwendungen, die auf den vorgenannten Systemen eingesetzt werden;

Nicht im Geltungsbereich dieser Spezifikation ist die konventionelle bzw. klassische Prozesstechnik d.h. nicht-digitale, rein elektromechanische oder elektronische Überwachungs- und Prozesssteuerungssysteme.

Telekommunikationssysteme und die Nachrichtentechnik, die im Umfeld der Prozesssteuerung eingesetzt werden, sind ebenfalls nicht im direkten Anwendungsbereich dieser Spezifikation. Sie werden durch den Standard ISO/IEC 27011 *Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002:2005* abgedeckt. Anwenden dieser Spezifikation wird empfohlen, die dort definierten Maßnahmenempfehlungen für die im Umfeld der Prozesssteuerung eingesetzten Telekommunikations- und Nachrichtentechnikssysteme umzusetzen.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. 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).

DIN ISO/IEC 27001:2008-09, *Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheits-Managementsysteme — Anforderungen (ISO/IEC 27001:2005)*

DIN ISO/IEC 27002:2008-09, *Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheits-Managementsysteme — Management (ISO/IEC 27002:2005)*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach DIN ISO/IEC 27001:2008-09, DIN ISO/IEC 27002:2008-09 und die folgenden Begriffe.

3.1

Computer Emergency Response Team CERT

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

3.2

Debugging

Fehleranalyse in Computersystemen

3.3

Energieanlage

Anlage zur Erzeugung, Umwandlung, Speicherung, Fortleitung oder Abgabe von Energie

3.4

Energieversorger

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

3.5

Kritische Infrastruktur

Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere weitreichende Folgen eintreten würden

ANMERKUNG Hierzu gehört insbesondere die Steuerung und Regelung der Energieerzeugung, -übertragung und Energieverteilung.

3.6

Mensch-Maschine-Interface

MMI

Benutzerschnittstelle zum Bedienen und Beobachten des Prozesssteuerungssystems bzw. der Anlage

3.7

Transportnetz

Übertragungs- oder Fernleitungsnetz zum Transport von Elektrizität über ein Höchstspannungs- und Hochspannungsverbundnetz bzw. Transport von Erdgas durch ein Hochdruckfernleitungsnetz

3.8

Safety

Betriebssicherheit

3.9

Safety-Systeme

Systeme und Komponenten, die zur Gewährleistung der Betriebssicherheit (Safety) benötigt werden

3.10

Schwarzfall

weitreichender Ausfall der Stromversorgung

3.11

Smart Grid

intelligentes Stromnetz, gekennzeichnet durch kommunikative Vernetzung und Steuerung der Komponenten und Verbraucher in elektrischen Energienetzen

3.12

Statement of Applicability

SOA

Erklärung zur Anwendbarkeit: Dokument, das die Maßnahmenziele und Maßnahmen beschreibt, die für das ISMS einer Organisation relevant und anwendbar sind

3.13**SPS**

Speicherprogrammierbare Steuerung

3.14**Prozesssteuerungssystem**

System, das zur Steuerung, Überwachung und Messung von Erzeugung, Übertragung, Speicherung und Verteilung von Strom, Gas und Wärme in Kombination mit der Steuerung von unterstützenden Prozessen dient

3.15**Versorgung**

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

3.16**Verteilung**

Transport von Elektrizität mit hoher, mittlerer oder niedriger Spannung über Elektrizitätsverteilernetze oder der Transport von Gas oder Wärme über örtliche oder regionale Leitungsnetze

3.17**Wartung**

alle Maßnahmen die im Bereich der Energieversorgung üblicherweise unter dem Obergriff Instandhaltung zusammengefasst werden

BEISPIEL Wartungsmaßnahmen sind bspw. Inspektion, Wartung, Entstörung und Verbesserung.

4 Übersicht**4.1 Aufbau dieser Norm**

Diese Spezifikation ist entsprechend der DIN ISO/IEC 27002:2008-09 strukturiert. Es wird direkt auf die Ziel- und Maßnahmenspezifikationen der DIN ISO/IEC 27002:2008-09 verwiesen, wenn keine zusätzlichen Detailinformationen notwendig sind. In den Fällen, in denen die Maßnahmen der DIN ISO/IEC 27002:2008-09 eine für die Energieversorgung spezifische oder erweiterte Umsetzung erfordern, wird das in Form einer Umsetzungsanleitung für die Energieversorgung und ggf. weiteren Informationen beschrieben. Eine Liste der neuen Maßnahmenziele bzw. Maßnahmen für den Energieversorgungssektor ist zusätzlich in Anhang A (Standard) aufgeführt. Ergänzende Anmerkungen und Hinweise werden in Anhang B beschrieben.

Umsetzungsempfehlungen und Informationen für die Energieversorgung wurden in den folgenden Abschnitten ergänzt:

- Organisation der Informationssicherheit (Abschnitt 6),
- Management von organisationseigenen Werten (Abschnitt 7),
- Personalsicherheit (Abschnitt 8),
- Physische und umgebungsbezogene Sicherheit (Abschnitt 9),
- Betriebs- und Kommunikationsmanagement (Abschnitt 10),
- Zugangskontrolle (Abschnitt 11),
- Beschaffung, Entwicklung und Wartung von Informationssystemen (Abschnitt 12),
- Sicherstellung des Geschäftsbetriebs (Abschnitt 14),
- Einhaltung von Vorgaben (Abschnitt 15).

4.2 Informationssicherheits-Managementsysteme im Bereich der Energieversorgung

4.2.1 Zielsetzung

Die Prozesssteuerungssysteme der Energieversorgung sind von ihrem Aufbau und ihrer Funktion nach informationsverarbeitende Systeme: Sie erfassen und überwachen über Sensoren den Zustand des gesteuerten physikalischen Prozesses, verarbeiten diese Informationen und greifen über Aktoren steuernd und regelnd ein. Die Steuerung und Regelung erfolgt hier sowohl automatisch als auch durch steuernde Eingriffe des Bedienpersonals. Informationen und informationsverarbeitende Systeme sind daher auch im Umfeld der Prozesssteuerung ein essentieller Bestandteil der Betriebsprozesse der Energieversorgung. Sie müssen deswegen ebenso wie in anderen Organisationsbereichen angemessen geschützt werden.

In zunehmendem Maße werden im Umfeld der Prozesssteuerung der Energieversorgung auch auf Standard-IT-Technologien basierende Software- und Hardwarekomponenten genutzt.

Auch deshalb sind Informationen und die informationsverarbeitende Systeme der Prozesssteuerung heutzutage einer anwachsenden Zahl von Bedrohungen und Schwachstellen ausgesetzt. Es ist deshalb essentiell, dass im Bereich der Prozesssteuerung der Energieversorgung eine hinreichende Informationssicherheit durch den Betrieb eines ISMS in Übereinstimmung mit der DIN ISO/IEC 27001 gewährleistet und einem kontinuierlichen Verbesserungsprozess unterworfen wird.

Eine effektive Informationssicherheit kann in der Prozesssteuerung der Energieversorgung erreicht werden, indem die anwendbaren Maßnahmen dieser Spezifikation eingeführt, umgesetzt, überwacht, überprüft und, falls notwendig, verbessert werden, um sicherzustellen, dass die spezifischen Sicherheits- und Geschäftsziele der Organisation erfüllt werden. Dies sollte insbesondere auch unter Berücksichtigung der herausragenden gesellschaftlichen Rolle und der wirtschaftlichen Notwendigkeit einer sicheren und zuverlässigen Energieversorgung geschehen.

4.2.2 Sicherheitsbetrachtungen für Prozesssteuerungssysteme der Energieversorgung

Der Bedarf nach einem allgemeinen und umfassenden Informationssicherheits-Regelwerk für den Bereich der Prozesssteuerung der Energieversorgung beruht auf verschiedenen Grundanforderungen:

- a) Die Kunden erwarten eine sichere und verlässliche Energieversorgung.
- b) Gesetzliche und regulatorische Anforderungen erfordern einen sicheren und zuverlässigen Betrieb der Systeme der Energieversorgung.
- c) Die Energieversorger selbst benötigen Informationssicherheit, um auch in eigenem Interesse die Anforderungen der Kunden und gesetzliche Vorschriften zu erfüllen sowie um ihre Geschäftsinteressen zu wahren.

4.2.3 Schützenswerte Informationswerte

Um ein Informationssicherheits-Management zu etablieren ist es notwendig, dass die Organisation alle organisationseigenen Werte (Assets) identifiziert. Die Identifizierung der organisationseigenen Werte und die Klärung ihrer Wichtigkeit erlaubt es, angemessene Maßnahmen umzusetzen.

Weitere Hinweise zu den organisationseigenen Werten (Assets), die eine Energieversorger-Organisation schützen sollte, finden sich in 7.1.1.

4.2.4 Aufbau eines Informationssicherheits-Managements

4.2.4.1 Festlegung der Sicherheitsanforderungen

Es ist essentiell, dass eine Energieversorger-Organisation ihre Sicherheitsanforderungen identifiziert. Hierbei gibt es drei wesentliche Quellen für Sicherheitsanforderungen:

- a) Die Ergebnisse der Risikoeinschätzung der Organisation, wobei die allgemeinen Geschäftsstrategien und Ziele der Organisation berücksichtigt werden sollten. Durch eine Risikoeinschätzung werden Bedrohungen für vorhandene organisationseigene Werte (Assets) identifiziert, Schwachstellen und Eintrittswahrscheinlichkeiten bewertet und die möglichen Auswirkungen abgeschätzt.
- b) Die Anforderungen, die sich aus Gesetzen und Verordnungen, Regelungen und Verträgen ergeben und die von einer Organisation erfüllt werden müssen, sowie sozio-kulturelle und gesellschaftliche Anforderungen. Hierzu gehören insbesondere die Gewährleistung einer zuverlässigen, effektiven und sicheren Energieversorgung und die zuverlässige Unterstützung der Prozesse im liberalisierten Energiemarkt, insbesondere ein zuverlässiger und sicherer Datenaustausch mit dritten Parteien.
- c) Die spezifischen Prinzipien, Ziele und geschäftlichen Anforderungen an die Informationsverarbeitung, die die Organisation entwickelt hat, um ihren Geschäftsbetrieb zu unterstützen.

4.2.4.2 Einschätzung der Sicherheitsrisiken

Die notwendigen Sicherheitsmaßnahmen werden durch eine methodische Betrachtung von Sicherheitsrisiken ermittelt. Der Aufwand für Maßnahmen muss gegenüber dem wirtschaftlichen Schaden, der sich aus Sicherheitsproblemen ergeben kann, abgewogen werden. Die Ergebnisse der Risikoeinschätzung unterstützen die Festlegung der geeigneten Management-Aktionen und Prioritäten für das Management von Informationssicherheitsrisiken und für die Umsetzung der Maßnahmen, die zum Schutz gegen diese Risiken ausgewählt wurden. Die Risikoeinschätzung sollte regelmäßig wiederholt werden, um alle Veränderungen zu berücksichtigen, die die Ergebnisse der Risikoeinschätzung beeinflussen können.

4.2.4.3 Auswahl von Maßnahmen

Nachdem die Sicherheitsanforderungen und Risiken identifiziert und die Entscheidungen für die Risikobehandlung getroffen wurden, sollten angemessene Maßnahmen ausgewählt und umgesetzt werden, um sicherzustellen, dass die Risiken auf ein akzeptables Niveau reduziert werden.

Diese Spezifikation bietet zusätzlich zu den Maßnahmen eines umfassenden Informationssicherheits-Managements ergänzende Hilfestellung und bereichsspezifische Maßnahmen für die Prozesssteuerungssysteme der Energieversorgung, die die dort herrschenden besonderen Anforderungen berücksichtigen. Deshalb wird den Energieversorger-Organisationen empfohlen, die Maßnahmen dieser Spezifikation umzusetzen. Bei Bedarf können auch weitere Maßnahmen entwickelt werden, um spezifische Anforderungen zu erfüllen. Die Auswahl von Sicherheitsmaßnahmen ist abhängig von den Entscheidungen, die die Organisation basierend auf den Kriterien für die Risikoakzeptanz, den Möglichkeiten der Risikobehandlung und dem allgemeinen Risikomanagement-Ansatz der Organisation getroffen hat. Diese Auswahl sollte auch alle relevanten nationalen und internationalen Gesetze, Verordnungen und Vorschriften berücksichtigen.

4.2.4.4 Entscheidende Erfolgsfaktoren

Die Inhalte der DIN ISO/IEC 27002:2008-09, 0.7, sind entsprechend anzuwenden.

5 Sicherheitsleitlinie

Die Maßnahmenziele sowie die Inhalte der DIN ISO/IEC 27002:2008-09 Abschnitt 5 sind entsprechend anzuwenden.

6 Organisation der Informationssicherheit

6.1 Interne Organisation.

6.1.1 Engagement des Managements für Informationssicherheit

Die Maßnahme 6.1.1 der DIN ISO/IEC 27002:2008-09 ist entsprechend anzuwenden.

6.1.2 Koordination der Informationssicherheit

Die Maßnahme 6.1.2 der DIN ISO/IEC 27002:2008-09 ist entsprechend anzuwenden.

6.1.3 Zuweisung der Verantwortlichkeiten für Informationssicherheit

Die Maßnahme 6.1.3 der DIN ISO/IEC 27002:2008-09 ist entsprechend anzuwenden.

6.1.4 Genehmigungsverfahren für informationsverarbeitende Einrichtungen

Die Maßnahme 6.1.4 der DIN ISO/IEC 27002:2008-09 ist entsprechend anzuwenden.

6.1.5 Vertraulichkeitsvereinbarungen

Die Maßnahme 6.1.5 der DIN ISO/IEC 27002:2008-09 ist entsprechend anzuwenden.

6.1.6 Kontakt zu Behörden

Die Maßnahme 6.1.6 der DIN ISO/IEC 27002:2008-09 wird wie folgt erweitert:

Umsetzungsanleitung für die Energieversorgung

Anwendungen und die Infrastruktur der Prozesssteuerungssysteme der Energieversorgung können einen Bestandteil der Kritischen Infrastrukturen darstellen und somit für das Gemeinwesen und für die Funktionsfähigkeit von Wirtschaft und Gesellschaft essentiell sein. Betreiber dieser Systeme sollten daher den Kontakt zu allen relevanten Behörden aufrechterhalten. Zusätzlich zu den bereits genannten Stellen können dies zum Beispiel sein:

- Nationale und internationale Behörden und Kooperationseinrichtungen zum Schutz Kritischer Infrastrukturen;
- Nationale und internationale CERT-Organisationen;
- Katastrophenschutz- sowie Katastrophenhilfsorganisationen.

Für die Betreiber von Kritischen Infrastrukturen können zusätzliche Regularien und Gesetze gelten, die entsprechend eingehalten werden müssen.

Weitere Informationen für die Energieversorgung

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

6.1.7 Kontakt zu speziellen Interessensgruppen

Die Maßnahme 6.1.7 der DIN ISO/IEC 27002:2008-09 wird wie folgt erweitert:

Umsetzungsanleitung für die Energieversorgung

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 Informationssicherheit zuständigen Arbeitskreisen aufrecht erhalten werden.

6.1.8 Unabhängige Überprüfung der Informationssicherheit

Die Maßnahme 6.1.8 der DIN ISO/IEC 27002:2008-09 ist entsprechend anzuwenden.

6.2 Externe

6.2.1 Identifizierung von Risiken in Zusammenhang mit externen Mitarbeitern

Die Maßnahme 6.2.1 der DIN ISO/IEC 27002:2008-09 wird wie folgt erweitert:

Umsetzungsanleitung für die Energieversorgung

Prozesssteuerungssysteme können aus komplexen und individuell angepassten Systemen und Komponenten bestehen. Systemhersteller und Integratoren sind daher häufig sehr stark in die Betriebs- und Wartungsprozesse eingebunden. Zur Wartung und Fehlerbehebung werden von diesen externen Unternehmen Remote-Zugänge, die eine Wartung von einem entfernten Standort ermöglichen genutzt oder Angestellte dieser externen Unternehmen benötigen Zutritt zu Sicherheitsbereichen für eine Wartung vor Ort.

Durch die enge Zusammenarbeit der unterschiedlichen Systembetreiber auf Erzeugungs-, Übertragungs- und Verteilnetzebene entsteht eine enge Kopplung zwischen Steuerungs- und Kommunikationsnetzwerken verschiedener Organisationen. Ebenso kann der Zugriff auf sensitive Informationen durch externe Hersteller, Systemintegratoren oder Geschäftspartner erforderlich sein.

Die aus den Zugriffen auf sensitive Systeme, Netzwerke und Informationen durch externe Unternehmen resultierenden Gefährdungen sollte insbesondere im Hinblick auf das Risiko für den zu steuernden bzw. zu überwachenden physikalischen Primärprozess bewertet und berücksichtigt werden.

6.2.2 Adressieren von Sicherheit im Umgang mit Kunden

Die Maßnahme 6.2.2 der DIN ISO/IEC 27002:2008-09 wird wie folgt erweitert:

Umsetzungsanleitung für die Energieversorgung

Die komplexen und vielseitigen Beziehungen zwischen den Systemeigentümern, Systembetreibern, Dienstleistungsunternehmen 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 ist 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.

Die verschiedenen, ggf. komplexen Geschäftsbeziehungen müssen bei der Identifizierung und Adressierung von Sicherheitsanforderungen bei Kundenzugriffen auf Informationswerte berücksichtigt werden. Bei der Kopplung von Prozesssteuerungssystemen sollten insbesondere die in 11.4.8 beschriebenen Maßnahmen berücksichtigt werden.

6.2.3 Adressieren von Sicherheit in Vereinbarungen mit Dritten

Die Maßnahme 6.2.2 der DIN ISO/IEC 27002:2008-09 wird wie folgt erweitert:

Umsetzungsanleitung für die Energieversorgung

Im Rahmen der Vereinbarung sollte sichergestellt werden, dass der Schutzbedarf sensibler Informationen hinreichend berücksichtigt wird.

Dort wo im Bereich der Energieversorgung Telekommunikationsdienstleistungen durch externe Dritte erbracht werden, sind spezielle Anforderungen in Bezug auf Krisen- und Notfallkommunikation insbesondere im Fall von Großstörungen, Naturkatastrophen, Unfällen oder anderen möglichen Notfallsituationen zu definieren, vertraglich festzulegen und zu überwachen. Dies gilt insbesondere im Hinblick auf ggf. notwendige Bevorrechtigungsschaltungen im Fall von Dienstüberlastungen und eine hinreichend lange Unabhängigkeit des Telekommunikationsdienstes von externer Energieversorgung (Schwarzfallfestigkeit).

7 Management von organisationseigenen Werten

7.1 Verantwortung für organisationseigene Werte (Assets)

7.1.1 Inventar der organisationseigenen Werte (Assets)

Die Maßnahme 7.1.1 der DIN ISO/IEC 27002:2008-09 wird wie folgt erweitert:

Umsetzungsanleitung für die Energieversorgung

Die verschiedenen Verantwortlichkeiten bei der Erstellung und Pflege eines Inventars aller wichtiger organisationseigenen Werte sollten spezifiziert und dokumentiert sein.

Die Liste der organisationseigenen Werte sollte dabei alle relevanten Prozesssteuerungssysteme einschließlich der Informationswerte und Anwendungen umfassen.

Weitere Informationen für die Energieversorgung

Organisationseigene Werte (Assets) im Bereich der Energieversorgung beinhalten neben den oben genannten Assets viele weitere bereichsspezifische Wertetypen, wie beispielsweise:

- a) Informationen: Netzpläne, Fahrplan- und Dispatching-Daten, geographische und georeferenzierte Informationen, Krisenpläne, Netzwiederaufbaupläne, Schaltantragsdaten, Messwerte- und Messdaten, Zählwerte, Meldungen, Betriebsprotokolle, Parametrierdaten, Messwert- und Meldungsarchive usw.
- b) Software: Leittechnische Software, Visualisierungssysteme, Energiemanagement- und Optimierungssoftware, Simulationssoftware, Parametriersoftware, Management- und Überwachungssysteme, Betriebs- und Einsatzmanagementsysteme, Programmierumgebungen, Firmware, Archivierungssoftware usw.
- c) physische Werte: Leittechnik und Automatisierungskomponenten, Fernwirkkomponenten, Nachrichtentechnische Komponenten, digitale Schutz- und Safety-Komponenten, digitale Mess- und Zählvorrichtungen, digitale Sensoren und Aktoren, Parametrier- und Programmiergeräte, Visualisierungs- und Bedienkomponenten, digitale Schreibersysteme usw.
- d) Dienstleistungen: Telekommunikationsdienstleistungen, Notfallkommunikationsdienste, Informationsdienste

7.1.2 Eigentum von organisationseigenen Werten (Assets)

Die Maßnahme 7.1.2 der DIN ISO/IEC 27002:2008-09 wird wie folgt erweitert:

Weitere Informationen für die Energieversorgung

Durch mögliche komplexe Strukturen der für den Betrieb von Prozesssteuerungssystemen verantwortlichen Unternehmen können verschiedene Verantwortlichkeiten bezüglich der kaufmännischen und betrieblichen Eigentümerschaft vorhanden sein. Daher sollte die Eigentümerschaft und die Verantwortlichkeiten in Bezug

zu den organisationseigenen Werten, sowie die Rollen der Werteeigentümer und -betreiber hinsichtlich der Informationssicherheit genau definiert und dokumentiert werden.

7.1.3 Zulässiger Gebrauch von organisationseigenen Werten (Assets)

Die Maßnahme 7.1.3 der DIN ISO/IEC 27002:2008-09 ist entsprechend anzuwenden.

7.2 Klassifizierung von Informationen

7.2.1 Regelung für die Klassifizierung

Die Maßnahme 7.2.1 der DIN ISO/IEC 27002:2008-09 wird wie folgt erweitert:

Umsetzungsanleitung für die Energieversorgung

Spezifische Einstufungskriterien für die Energieversorgung könnten die folgenden Punkte umfassen:

- unternehmerische Werte, Systeme und Informationen zur Betriebsunterstützung von Kritischen Infrastrukturen und sensiblen Systemen
- unternehmerische Werte, Systeme und Informationen, die zum Wiederaufbau der Energieversorgung nach einer Großstörung (Netzwiederaufbau) benötigt werden, z. B. schwarzstartfähige Systeme und Komponenten
- unternehmerische Werte, Systeme und Informationen, die zur Gewährleistung der funktionalen Sicherheit / Anlagensicherheit benötigt werden
- unternehmerische Werte, Systeme und Informationen, die zu Erfüllung regulatorischer Anforderungen wie beispielsweise Entflechtungsanforderungen benötigt werden bzw. für die spezifische Anforderungen umgesetzt werden müssen

7.2.2 Kennzeichnung von und Umgang mit Informationen

Die Maßnahme 7.2.2 der DIN ISO/IEC 27002:2008-09 ist entsprechend anzuwenden.

8 Personalsicherheit

8.1 Vor der Anstellung¹⁾

8.1.1 Aufgaben und Verantwortlichkeiten

Die Maßnahme 8.1.1 der DIN ISO/IEC 27002:2008-09 wird wie folgt erweitert:

Umsetzungsanleitung für die Energieversorgung

Die in der Energieversorgung für die Systemtechnik verantwortlichen Mitarbeiter sollten die entsprechenden Kenntnisse und Fähigkeiten aufweisen, um die Verantwortung zur Leitung und Aufsicht von Installation, Wartung und dem sicheren Betrieb der Prozesssteuerungssysteme zu übernehmen. Hierzu gehört auch hinreichendes Fachwissen in Bezug auf moderne Informationssystemtechnologien und Informationssicherheit.

Die relevanten Techniker und Mitarbeiter sollten über ihre zugewiesenen Rollen und Verantwortlichkeiten informiert werden. Dies gilt speziell vor dem Hintergrund der Informationssicherheit dieser Systeme.

1) Erklärung: Der Begriff „Anstellung“ wird hier benutzt, um die folgenden verschiedenen Situationen zu behandeln: Anstellung von Personen (kurzzeitig oder länger andauernd), Zuweisung von Arbeitsaufgaben, Ändern von Arbeitsaufgaben, Zuordnung von Verträgen und die Beendigung dieser Arrangements.