

**DIN VDE 0175-110
(VDE 0175-110)**
DIN

Diese Norm ist zugleich eine **VDE-Bestimmung** im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.

VDE

ICS 29.240.01; 35.030

Einsprüche bis 2020-03-29

Entwurf
**Richtlinien zur IT-Sicherheit und Resilienz für die Smart-Energy-
Einsatzumgebung
(IEC SyCSmartEnergy/106/DC:2019);
Text Deutsch und Englisch**

Cyber Security and Resilience Guidelines for the Smart Energy Operational Environment
(IEC SyCSmartEnergy/106/DC:2019);
Text in German and English

Lignes directrices relatives à la sécurité informatique et la résilience pour l'environnement
d'utilisation d'énergie intelligente
(IEC SyCSmartEnergy/106/DC:2019);
Texte en allemand et anglais

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2019-11-29 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 bzw. für Norm-
Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de,
sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser
Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für
Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in
DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

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 87 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist ...

Inhalt	Seite
Nationales Vorwort.....	4
Kurzdarstellung	5
1 Resilienz als übergreifende Strategie zur Sicherstellung der Geschäftskontinuität.....	9
2 „Security by Design“ als kosteneffektivster Ansatz	10
3 IT vs. OT: Unterschiede zwischen den Sicherheitsanforderungen bei informationstechnologischen (IT) Umgebungen und Technologien in der Einsatzumgebung (OT)	12
4 Risikobeurteilung, Risikoverringerung und Risikolebenszyklusprozesse	14
5 IT-Sicherheitsnormen und bewährte Verfahren	16
6 Schlussfolgerungen	18
Anhang A Wesentliche Normen und Richtlinien zur IT-Sicherheit	21
A.1 Normenreihe ISO/IEC 27000 zur IT-Sicherheit.....	21
A.1.1 Normenfamilie ISO/IEC 27001 zu ISMS	21
A.1.2 ISO/IEC 27001	24
A.1.3 ISO/IEC 27002:2013	25
A.1.4 ISO/IEC 27019:2017	25
A.2 Rahmenwerk des NIST zur IT-Sicherheit.....	26
A.3 ISO 31000 und ISO 22301	29
A.3.1 ISO 31000: Risikomanagement – Prinzipien und Richtlinien.....	29
A.3.2 ISO 22301: Sicherheit und Schutz des Gemeinwesens – Business Continuity Management System – Anforderungen.....	31
A.4 NISTIR 7628: Richtlinien für die IT-Sicherheit in Smart Grids („Was“)	32
A.4.1 NISTIR 7628: IT-Sicherheitsmaßnahmen	32
A.4.2 Logisches Referenzmodell für IT-Sicherheit nach NISTIR 7628.....	33
A.5 Normenreihe IEC 62443 zur industriellen Automatisierung	35
A.5.1 Hintergrund von IEC 62443	35
A.5.2 Aufbau der IEC 62443	35
A.5.3 IEC 62443-3-3: Anforderungen an Systemsicherheit und Sicherheitsniveaus	39
A.6 Normenreihe IEC 62351 zur IT-Sicherheit in Smart Grids	41
A.6.1 Aufbau der IEC 62351	41
A.6.2 IEC 62351: IT-Sicherheitsnormen für Kommunikationsstandards	43
A.6.3 IEC 62351: Zusätzliche IT-Sicherheitsnormen und technische Berichte	43
A.6.4 IEC 62351: Technische Spezifikationen für die Konformitätsprüfung	44
A.7 IT-Sicherheit für den Energiemarkt nach IEC 62325-503	45
A.8 IT-Sicherheitsnormen für das Internet.....	46
A.8.1 Allgemeines	46

A.8.2	IETF-Normen.....	46
A.8.3	ITU-Normen.....	47
A.8.4	W3C-Standards.....	48
A.8.5	Kombinationen von Sicherheitstechnologien	48
Anhang B	Literaturhinweise.....	50

Bilder

Bild 1	– Fünf IT-Sicherheitskonzepte	6
Bild 2	– NIST-Rahmenwerk für Resilienz (<i>Quelle: N. Hanacek/NIST</i>)	10
Bild 3	– Beispiel für „Security by Design“: Elektronische Sicherheitsbereiche.....	11
Bild 4	– Beispiel für die unterschiedlichen Prioritäten bei den obersten Sicherheitszielen von IT und OT	13
Bild 5	– Risikomanagementprozess (ISO/IEC 27005:2018)	15
Bild 6	– Wesentliche Normen und Richtlinien zur IT-Sicherheit.....	18
Bild 7	– Beziehungen innerhalb der ISMS-Normenfamilie	22
Bild 8	– Rahmenwerk des NIST zur Verbesserung der IT-Sicherheit in kritischen Infrastrukturen (2017)	27
Bild 9	– Risikomanagementprozess (ISO 31000)	30
Bild 10	– Modell zum Planen, Durchführen, Prüfen und Handeln (Plan-Do-Check-Act – PDCA) nach ISO 22301	31
Bild 11	– NIST-Anforderungsfamilien für die Sicherheit von Smart Grids.....	33
Bild 12	– Grundlegendes logisches Referenzmodell als „Spaghetti-Diagramm“ nach NISTIR 7628	35
Bild 13	– Normenreihe IEC 62443 zur Industriesicherheit – Überblick (ISA99.org).....	37
Bild 14	– Anwendung von IEC 62443 durch verschiedene Rollen (ISA99.org)	39
Bild 15	– Festgelegte Security-Levels nach IEC 62443	40
Bild 16	– Normenreihe IEC 62351 zur IT-Sicherheit	43
Bild 17	– MADES-Überblick (<i>Quelle: IEC 62325-503:2018</i>)	45

Tabellen

Tabelle 1	– ISMS-Normenfamilie	22
-----------	----------------------------	----

Nationales Vorwort

Das internationale Dokument IEC SyCSmartEnergy/106/DC „Cyber Security and Resilience Guidelines for the Smart Energy Operational Environment“ (DC, en: Draft for Comments) ist unverändert in diesen Norm-Entwurf übernommen worden. Um der deutschen Öffentlichkeit frühzeitig eine Einspruchsmöglichkeit zu geben, wird mit diesem Norm-Entwurf bereits ein DC-Dokument veröffentlicht. Dieser Norm-Entwurf enthält eine noch nicht autorisierte deutsche Übersetzung.

Da die Deutsche Fassung noch nicht endgültig mit der Englischen Fassung abgeglichen ist, ist die englische Originalfassung des IEC-Dokumentes entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom SyC Smart Energy „Smart Energy“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet.

Die Internationale Elektrotechnische Kommission (IEC) und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen.

Da der Abstimmungszeitraum für einen FDIS bzw. Schluss-Entwurf FprEN nur 6 Wochen beträgt, und dann keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine „JA/NEIN“-Entscheidung möglich ist, wobei eine „NEIN“-Entscheidung fundiert begründet werden muss, wird bereits der CD als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit frühzeitig berücksichtigen zu können.

Für dieses Dokument ist das nationale Arbeitsgremium K 901 „System Komitee Smart Energy“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (www.dke.de) zuständig.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Dokuments.

Der Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

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

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Richtlinien zur IT-Sicherheit und Resilienz für die Smart-Energy-Einsatzumgebung

Kurzdarstellung

IT-Sicherheit ist für jedes Unternehmen zu einer immer wichtigeren Anforderung geworden, insbesondere für Unternehmen, die für kritische Infrastrukturen zuständig sind, wie z. B. Betreiber von Energieversorgungsnetzen, die für das Management des sich rasch weiterentwickelnden Stromversorgungssystems verantwortlich sind. Diese Energieunternehmen müssen sich in durch zunehmenden Wandel und Risiken geprägten Geschäftsumfeldern zurechtfinden und gleichzeitig ihre Dienstleistungen für Endnutzer bereitstellen und verbessern. Zu diesen geschäftlichen Herausforderungen zählt der Umstieg auf saubere Energieressourcen und die zunehmende gesellschaftliche Abhängigkeit von elektrischer Energie. Gleichzeitig haben sich wandelnde Rechtsvorschriften, atemberaubende neue Technologien und innovative Marktchancen Auswirkungen auf die bestehenden geschäftlichen Strukturen. Hierzu zählen die Vernetzung dezentraler Energiequellen, die im Eigentum Dritter sind und von diesen betrieben werden, der schnell wachsende Verbreitung von Elektrofahrzeugen, die Neuorganisation des Elektrizitätsversorgungssystems mit Mikronetzen, die Verfügbarkeit von Cloud-Diensten und die zunehmende Nutzung von „Internet of Things“ (IoT)-Technologien.

Gleichzeitig mit diesem Paradigmenwechsel in ihrem Geschäftsumfeld hat die Energiewirtschaft die Entwicklung hin zur Digitalisierung forciert und stützt sich beim Management der Stromversorgung immer stärker auf Cyberanlagen (Systeme, Steuerungen, intelligente Geräte). Diese Cyberanlagen sind für die Sicherheit, Effizienz und Zuverlässigkeit der Stromversorgung von zentraler Bedeutung.

Allerdings bringen diese Cyberanlagen aber auch schwierige Herausforderungen mit sich: Unternehmen müssen sich überlegen, wie sie der Tatsache gezielter Cyberangriffe begegnen – als Beispiel ist der erfolgreiche Angriff auf das ukrainische SCADA-System zu nennen¹ –, und wie sie sich gegen die alltäglicheren, aber ebenso kritischen Cyber-Bedrohungen wappnen, die durch persönliche Fahrlässigkeit, die Komplexität der Systeme, die Vielzahl neuer Teilnehmer auf dem Energiemarkt, technische Ausfälle und Naturkatastrophen entstehen.

Daher müssen Energieunternehmen, die sich bisher ausschließlich mit dem Systementwicklungsprozess (Auslegung, Einsatz, Integration, Verfahren und Instandhaltung) beschäftigt haben, jetzt auch IT-Sicherheitsdienste und -technologien in diese Entwicklungsprozesse einbeziehen. Infolgedessen könnten sich die neuen Systeme in Bezug auf ihre Konfigurationen, Möglichkeiten und Einschränkungen erheblich unterscheiden.

¹ https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf



Englisch	Deutsch
Security by Design	Security by Design
Resilience	Resilienz
IT versus OT	IT versus OT
Standards & Guides	Richt- & Leitlinien
Risk Assessment	Risikobeurteilung
Five Cyber Security Concepts for Smart Energy	Fünf IT-Sicherheitskonzepte für Smart Energy

Bild 1 – Fünf IT-Sicherheitskonzepte

Dieses Dokument mit dem Titel „*Richtlinien zur IT-Sicherheit und Resilienz für die Smart-Energy-Einsatzumgebung*“ bietet Leitlinien zu Fragen der IT-Sicherheit, mit denen sich diese Unternehmen auseinandersetzen müssen, um die möglichen Auswirkungen von „erfolgreichen“ Cyberangriffen auf die Sicherheit von Menschen sowie deren physischen, funktionalen, umweltbezogenen, finanziellen, gesellschaftlichen und die Reputation des Unternehmens betreffenden Folgen zu möglichst gering zu halten. Dieses Papier legt den Schwerpunkt auf die Einsatzumgebungen der Strom- und Gasversorgung², jedoch sind fast alle diese IT-Sicherheitsfragen auch auf andere Umgebungen der Energieversorgung anwendbar.

In der Einsatzumgebung der Energieversorgung existieren fünf zentrale Konzepte für IT-Sicherheit, die Energieunternehmen bei ihren Bemühungen um die Implementierung der erforderlichen IT-Sicherheitsrichtlinien, -verfahren und -technologien beachten sollten. Diese fünf Konzepte sind in Bild 1³ dargestellt und werden im Kasten unten erläutert.

Fünf zentrale Konzepte zur IT-Sicherheit und Resilienz für Smart Energy

Konzept Nr. 1. Resilienz sollte die übergreifende Strategie zur Sicherstellung der Geschäftskontinuität darstellen: Bei der allgemeinen Schwerpunktsetzung auf Resilienz müssen Unternehmen die Sicherheit, den Schutz und die Zuverlässigkeit der Prozesse und die Bereitstellung ihrer Dienste berücksichtigen. Resilienz schließt Sicherheitsmaßnahmen ein, mit denen Auswirkungen verringert werden können, und zwar nicht nur im Vorfeld von Zwischenfällen (feststellen und verhindern), sondern auch während dieser Zwischenfälle (erkennen und reagieren) sowie nach Behebung von deren Auswirkungen (wiederherstellen). Um die

² In diesem Dokument umfasst die Einsatzumgebung der Strom- und Gasversorgung die Betriebsbereiche Übertragung und Verteilung, Wartungseinsätze vor Ort, Stromerzeugung und Interaktionen mit dem Energiemarkt und Nebenmärkten. Es wird davon ausgegangen, dass es „Graubereiche“ bezüglich der Zugehörigkeit eines Systems zu einem bestimmten Umfeld gibt, und es bestehen zahlreiche Interaktionen zwischen Betriebssystemen und Unternehmenssystemen, die Auswirkungen auf die Tätigkeiten haben könnten. Daher wird der Begriff „Umgebung“ als Oberbegriff zur Benennung der Unterschiede zwischen Entitäten verwendet, die physikalische Prozesse und Prozesse beeinflussen können, und jenen, die keinen direkten Einfluss auf physikalische Prozesse und Systeme ausüben. Dies schließt „IT“-Systeme ein, die „OT“-Systeme beeinflussen könnten.

³ Sofern nicht anderweitig vermerkt, wurden alle Diagramme von CSTF-Mitgliedern erstellt.

Resilienz ihrer Cyberanlagen zu gewährleisten, müssen Unternehmen gleichermaßen deren Sicherheit, Schutz und Zuverlässigkeit berücksichtigen. Resilienz beinhaltet somit einen fortwährenden Verbesserungsprozess zur Unterstützung der Geschäftskontinuität. Resilienz ist nicht nur ein technisches Problem, sondern muss einen übergreifenden geschäftlichen Ansatz einbeziehen, der IT-Sicherheitstechniken mit Systementwicklung und -betrieb zur Vorbereitung auf und Anpassung an sich verändernde Bedingungen kombiniert sowie die Widerstandsfähigkeit gegenüber und die schnelle Wiederherstellung nach Störungen gewährleistet. Informationsaustausch und Interoperabilität innerhalb von und zwischen Unternehmen werden ebenfalls immer mehr zu einem zentralen Bestandteil der Resilienz.

Konzept Nr. 2. „Security by Design“ ist der kosteneffektivste Sicherheitsansatz: Sicherheit ist entscheidend für alle kritischen Infrastrukturen und sollte von Anfang an in die Auslegung von Systemen und betrieblichen Tätigkeiten einbezogen und nicht erst nach der Implementierung der Systeme umgesetzt werden. Dies bedeutet, dass die Produkte, die Systeme, die Prozesse und die Organisation von Anfang mit Blick auf Sicherheit konzipiert oder eingerichtet werden sollten. Da jedoch davon ausgegangen werden muss, dass bestehende Systeme nicht ohne Weiteres durch Sicherheitsvorkehrungen ergänzt werden können – insbesondere, weil Systemkomponenten unterschiedliche Lebensdauern aufweisen können –, ist es unerlässlich, dass auch bei diesen bestehenden Systemen der Übergang zu sicherheitsbasierten Auslegungen durch die Einbeziehung von Sicherheitsmaßnahmen in alle Systemnachrüstungen und -erweiterungen bewerkstelligt wird. „Security by Design“ kombiniert geschäftliche Organisationsrichtlinien mit Sicherheitsverfahren und unterstützenden Technologien. Die Organisationsrichtlinien umfassen Sicherheitsbestimmungen, Mitarbeiterschulungen und eine klare Aufgabentrennung, während die Sicherheitsverfahren den Informationsaustausch der CERTs (Computer Emergency Response Teams – Computer-Notfallteams), Backup- und Wiederherstellungspläne sowie sichere Betriebsabläufe beinhalten. Zu den sicheren Technologien zählen physische und logische Techniken wie z. B. physische Standortzugangsschleusen, Zugangssteuerung, die Authentisierung und Autorisierung jedweder Kommunikation und Sicherheitsprotokolle.

Konzept Nr. 3. „IT“ und „OT“ sind ähnlich, aber nicht identisch: Technologien in Einsatzumgebungen (in diesem Dokument als „OT“ bezeichnet) weisen viele Sicherheitseinschränkungen und -anforderungen auf, durch die sie sich von informationstechnologischen (IT) Umgebungen unterscheiden. Die Hauptgrund dafür ist, dass es sich bei Elektrizitätsversorgungssystemen um cyber-physische Systeme handelt und Sicherheitsvorfälle zu Zwischenfällen führen können, die die physische Sicherheit und/oder die Stromversorgung betreffen, während physische Folgen in Unternehmensumgebungen normalerweise nicht als Problem auftreten. In IT-Umgebungen ist die Vertraulichkeit der sensiblen Geschäfts- und Kundendaten normalerweise der wichtigste Aspekt. Im Vergleich dazu sind in OT-Umgebungen die Verfügbarkeit, Authentisierung, Autorisierung und Datenintegrität in Elektrizitätsversorgungssystemen entscheidendere Anforderungen, da die Daten von Elektrizitätsversorgungssystemen nicht als sensibel betrachtet werden. Gleichzeitig stützen sich OT-Umgebungen zunehmend auf Cybertechnologien und übernehmen immer mehr Geräte und Plattformen aus der Welt der IT, während sich IT und OT bezüglich der Nutzung bekannter und stetig weiterentwickelter IoT-Technologien einander immer stärker annähern. Durch diese Vernetzung von IT und OT und die zunehmende Abhängigkeit von der IoT-Technologie ergeben sich zusätzliche Anfälligkeiten und damit Herausforderungen für die Gewährleistung von Sicherheit im Energieumfeld. Daher muss bei der Auswahl geeigneter Sicherheitsmaßnahmen der Schwerpunkt auf die in der Risikobeurteilung festgelegten Sicherheitsanforderungen gelegt werden.

Konzept Nr. 4. Risikobeurteilung, Risikoverringerung und die kontinuierliche Aktualisierung von Prozessen sind von grundlegender Bedeutung für die Verbesserung der Sicherheit: Auf Grundlage der geschäftlichen Anforderungen des Unternehmens muss dessen Gefährdung durch Sicherheitsrisiken (Sicherheit von Menschen sowie physische, funktionale, umweltbezogene, finanzielle, gesellschaftliche und die Reputation des Unternehmens betreffende Aspekte) für alle seine Geschäftsprozesse bestimmt werden. Bei der Risikobeurteilung wird die Anfälligkeit von Systemen und Prozessen für vorsätzliche oder durch Fahrlässigkeit verursachte Bedrohungen festgestellt, außerdem werden potenzielle Auswirkungen bestimmt und die Wahrscheinlichkeit dafür eingeschätzt, dass das Vorfalsszenario tatsächlich eintritt. Bei der Entwicklung einer Risikoverringerungsstrategie müssen betriebliche Einschränkungen berücksichtigt werden. Zudem muss nach technischen Auslegungen und betrieblichen Verfahren zur Verbesserung der Resilienz gesucht werden. Dabei müssen gleichzeitig die Kosten für die Umsetzung einer derartigen Strategie zur Verringerung potenzieller Risiken bewertet werden, und es ist zu beurteilen, inwiefern diese tatsächlich eine Minderung des Risikos bewirken. Die Risikobeurteilung erfordert zudem, dass die Risikoverringerungsprozesse bei regelmäßig stattfindenden Sicherheitsüberprüfungen einer Neubewertung unterzogen oder durch tatsächliche Sicherheitsvorfälle ausgelöst werden.

Konzept Nr. 5. IT-Sicherheitsnormen und Richtlinien zu bewährten Verfahren für OT-Umgebungen im Energiebereich sollten angewendet werden, um den Risikomanagementprozess zu unterstützen und Sicherheitsprogramme und -richtlinien einzurichten: IT-Sicherheitsmaßnahmen sollten nicht „neu erfunden“ werden. Wesentliche IT-Sicherheitsnormen und Richtlinien zu bewährten Verfahren wurden für verschiedene Sicherheitsbereiche und -zwecke bereits entwickelt. Bei der Planung der IT-Sicherheit sollten diese IT-Sicherheitsnormen und -richtlinien angewendet werden, um Resilienz, allgemeine Sicherheit und Interoperabilität in der gesamten energiebezogenen OT-Umgebung zu verbessern und dabei zum jeweiligen Zeitpunkt auf die richtigen Normen, Richtlinien und Verfahren für die entsprechenden Zwecke zurückgreifen.

1 Resilienz als übergreifende Strategie zur Sicherstellung der Geschäftskontinuität

Resilienz muss die übergreifende Strategie zur Sicherstellung der Geschäftskontinuität darstellen: Resilienz umfasst Maßnahmen, mit denen Auswirkungen von Zwischenfällen, die Schutz, Sicherheit und Zuverlässigkeit betreffen, verringert werden können, und zwar nicht nur im Vorfeld derartiger Zwischenfälle (feststellen und verhindern), sondern auch währenddessen (erkennen und reagieren) sowie nach Behebung von deren Auswirkungen (wiederherstellen). Dieses Dokument legt den Schwerpunkt auf die Aspekte der IT-Sicherheit, berücksichtigt dabei aber auch Schutz und die Zuverlässigkeit als zugrundeliegende Anforderungen, da diese häufig zur Bewältigung von Herausforderungen beitragen können. So bieten z. B. das Rahmenwerk des NIST zur IT-Sicherheit⁴ und ISO/IEC 27001/27002/27019 Beschreibungen dieser Resilienzkonzepte für die IT-Sicherheit (siehe Bild 2).

IT-Sicherheit umfasst weit mehr als die Verhinderung von bösartigen Hackerangriffen. IT-Sicherheit bedeutet für Smart Energy eine Verbesserung der Resilienz⁵ des Elektrizitätsversorgungssystems durch Verringerung der Bedrohungen durch die Sicherheit betreffende „Vorfälle“, die Auswirkungen auf die Cyberanlagen⁶ haben und zu Störungen der Betriebsabläufe führen könnten.

⁴ Rahmenwerk des NIST zur IT-Sicherheit <https://www.nist.gov/cyberframework>

⁵ Resilienz wird definiert als die „Fähigkeit der Vorbereitung auf und Anpassung an sich verändernde Bedingungen sowie die Widerstandsfähigkeit gegenüber und die schnelle Wiederherstellung nach Störungen. Resilienz beinhaltet die Fähigkeit, vorsätzlichen Angriffen, Unfällen oder auf Naturereignissen beruhenden Bedrohungen oder Vorfällen standzuhalten und in den Ausgangszustand zurückzukehren.“ [QUELLE: US Presidential Policy Directive – Critical Infrastructure Security and Resilience]. Nach einer ergänzenden Definition schließt Resilienz Folgendes ein: „die Fähigkeit, die Größenordnung und/oder Dauer von Störereignissen zu verringern. Die Effektivität einer resilienten Infrastruktur oder Unternehmung hängt von deren Fähigkeit ab, ein Störereignis zu antizipieren, zu absorbieren, sich anzupassen und/oder schnell in den Ausgangszustand zurückzukehren.“

⁶ Unter einer Cyberanlage wird jedwede Einrichtung verstanden, die über Computerrechenleistung verfügt, einschließlich der Steuerungen von Hardwareressourcen, aber nicht der Hardwareressourcen selbst (z. B. elektromechanische Trennschalter). Cyberanlagen können von physischen Handlungen (Durchschneiden eines Drahtes, Beschädigung eines Transformators) als auch von Cyberhandlungen (Einschleusung von Malware, unbeabsichtigte Eingabe fehlerhafter Daten) betroffen sein.



Englisch	Deutsch
Cybersecurity Framework Version 1.1	Rahmenwerk zur IT-Sicherheit, Version 1.1
Identify	Feststellung
Protect	Schutz
Detect	Erkennung
Respond	Reaktion
Recover	Wiederherstellung

Bild 2 – NIST-Rahmenwerk für Resilienz (Quelle: N. Hanacek/NIST)

Zur Verringerung von Bedrohungen der Resilienz werden IT-Sicherheitstechniken (wie Zugangssteuerung, Authentisierung, Erkennung von abweichendem Verhalten und Vorfallsprotokollierung) mit organisatorischen und technischen Verfahren kombiniert, die dem Unternehmen die Vorbereitung auf und Anpassung an sich verändernde Bedingungen ermöglichen sowie diesem Widerstandsfähigkeit gegenüber und die schnelle Wiederherstellung nach Störungen ermöglichen. Zu diesen technischen Verfahren gehören herkömmliche Maßnahmen zur Sicherstellung der Zuverlässigkeit des Elektrizitätsversorgungssystems wie z. B. redundante Einrichtungen, Kontingenzanalysen und Reservesysteme, aber auch Verfahren, deren Schwerpunkt auf den Schwachstellen von Cyberanlagen liegt und die sich z. B. mit Planungen bei einem Ausfall mehrerer Cyberanlagen, den Isolierungsmöglichkeiten zur Begrenzung der Ausbreitung von Cyberangriffen und sogar mit der Schulung von Mitarbeitern in der manuellen Ausübung von Tätigkeiten befassen, die normalerweise automatisch durchgeführt werden.

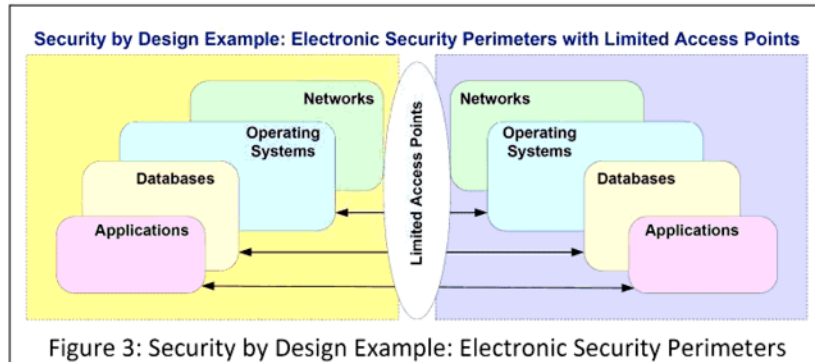
Fehler stellen den häufigsten „Cyber-Zwischenfall“ dar, daher werden Prüfungen bei der Datenerfassung und verbindliche Maßnahmen zur Unterstützung der Resilienz angewendet. Da Personen mit genauen Kenntnissen über den Betrieb des Elektrizitätsversorgungssystems auch die gefährlichsten Angreifer sein könnten, sind zusätzliche technische und die IT-Sicherheit betreffende Verfahren vorzusehen, um dieser Art von Schwachstellen entgegenzuwirken, z. B. Zwei-Faktor-Authentisierung, Trennung von Netzwerken und die ständige Überwachung auf anormalen Datenverkehr. Auch Stürme können Auswirkungen sowohl auf das Elektrizitätsversorgungssystem als auch auf dessen Cyberanlagen haben, so dass Reservegeneratoren, Kommunikationsnetze und Ersatzanlagen an sicheren Standorten untergebracht, aber gleichzeitig einfach zugänglich sein sollten, wenn sie benötigt werden.

2 „Security by Design“ als kosteneffektivster Ansatz

Die Berücksichtigung von Sicherheitsaspekten bereits von Beginn der Auslegungsphase an stellt den kosteneffektivsten Ansatz zur Gewährleistung der IT-Sicherheit dar, da auf diese Weise Risiken und finanzielle Aufwendungen möglichst gering gehalten werden. Effektive Sicherheit kann nicht einfach in den bestehenden betrieblichen Prozessen eines Elektrizitätsversorgungssystems „nachgerüstet“ werden, sondern sollte einen wesentlichen Bestandteil der Systemauslegungen und -konfigurationen, der Betriebsverfahren und der Informationstechnologien darstellen. Die nachträgliche Einführung von Sicherheitsverfahren und -technologien ist zudem kostenintensiv, da sie häufig „ad hoc“ geschieht und umfangreiche Änderungen an Systemkonfigurationen sowie erhebliche Nachschulungen des Personals erforderlich macht. Wenn Sicherheit

von Anfang an Bestandteil der Auslegung ist, wird sie zu einem normalen Bestandteil der Lebenszyklen von Cyberanlagen in Elektrizitätsversorgungssystemen und der betrieblichen Verfahren.

Der Begriff „Security by Design“ deckt zahlreiche Aspekte wie die Auslegung von Komponenten, Softwareimplementierungen, System- und Netzwerkkonfigurationen, Planungsverfahren und Datenverwaltung ab. Viele der Vorteile von „Security by Design“ können auch dann umgesetzt werden, wenn Systeme gerade aktualisiert oder nach und nach ersetzt werden, da die Existenz eines sorgfältig durchdachten Sicherheitsplans für die Einbeziehung von Sicherheitsaspekten bei jedem Schritt einer Erweiterung oder eines Austauschs entscheidend ist.



Englisch	Deutsch
Security by Design Example: Electronic Security Perimeters with Limited Access Points	Beispiel für „Security by Design“: Elektronische Sicherheitsbereiche mit Punkten eingeschränkten Zugangs
Networks	Netzwerke
Operating Systems	Betriebssysteme
Databases	Datenbanken
Applications	Anwendungen
Limited Access Points	Punkte eingeschränkten Zugangs

Bild 3 – Beispiel für „Security by Design“: Elektronische Sicherheitsbereiche

Zu den verschiedenen Aspekten der Sicherheitsauslegung gehört die Vergegenwärtigung potenzieller Bedrohungen und Schwachstellen mittels einer Risikoanalyse unter Berücksichtigung der Umgebungen, in denen die betreffende Komponente eingesetzt wird, bevor die System- und Netzwerkkonfiguration abgeschlossen wird.

Wenn sich z. B. kritische Systeme innerhalb einer klar bezeichneten elektronischen Sicherheitszone befinden, können für den Zugriff auf diese kritischen System die in diesen Bereichen bereitgestellten Zugangssteuerungen und Überwachungsmaßnahmen verwendet werden, um es Personen zu ermöglichen, sich zwischen den verschiedenen Sicherheitszonen zu bewegen (siehe Bild 3). Eine derartige Auslegung reduziert „Angriffsflächen“, die von böswilligen Akteuren ausgenutzt oder einfach nur versehentlich unzulässig verwendet werden könnten.

„Security by Design“ gestattet zudem eine größere Konsistenz über alle Systeme hinweg mit genau festgelegten Konfigurationen der Netzwerke und Informationsflüsse. Die Nutzer verfügen anstelle von ad hoc festgelegten Sicherheitsansätzen über konsistente Verfahren, denen sie folgen. Diese Konsistenz ist einfacher umzusetzen und zu unterhalten, zeichnet sich durch eine geringere Wahrscheinlichkeit von Sicherheitslücken aus und ermöglicht ein Management mit geringeren Kosten.

„Security by Design“-Konzepte können bei der Maßnahmenplanung für das unvermeidliche Szenario „erfolgreicher“ Sicherheitsvorfälle (Ausfallszenarien) Anwendung finden, die zur Entwicklung von Verfahren zur Bewältigung derartiger Sicherheitsvorfälle wie z. B. die Berücksichtigung von Degradationsmodi bei der Auslegung veranlassen sollten.

Bei „Security by Design“ kann die Zugangssteuerung bis auf die Datenebenen – nicht nur bis auf die Systemebenen – umgesetzt werden, was eine echte Ende-zu-Ende-Sicherheit zwischen den Nutzern und bei ihrem Datenzugriff ermöglicht und so sehr genau einschränkt, wer welche Daten überwachen und/oder kontrollieren kann. Dieselbe Zugangssteuerung kann auch auf die Datenflüsse zwischen Softwareanwendungen in der OT-Umgebung angewendet werden.

Die Flüsse gültiger Informationen zur richtigen Stelle innerhalb des richtigen Zeitrahmens stellen die wichtigsten Anforderungen für Einsatzumgebungen dar. Mit „Security by Design“, das üblicherweise neue oder aktualisierte Anwendungen erfordert, kann sichergestellt werden, dass diese Zusicherung durch sichere Protokolle gegeben wird, die nativ von den Systemen unterstützt werden und Bestandteil von deren Kernfunktionen sind. So kann z. B. die Validierung von Informationen dazu beitragen, die Bedrohung durch Personen zu verringern, die über entsprechende Kenntnisse zur Störung der Betriebsabläufe im Elektrizitätsversorgungssystem verfügen, indem sichergestellt wird, dass die Datenverifizierung in jedem System technisch implementiert ist. Gleichzeitig kann der Zugriff auf Daten durch Anforderungen der Sicherheitsrichtlinien eingeschränkt werden.

Durch Sicherheitsrichtlinien, die bereits bei der Auslegung der Systeme festgeschrieben wurden, können Verfahren für den Einkauf und die Aktualisierung der Systeme eingerichtet werden. Mit Hilfe derartiger Sicherheitsrichtlinien können die Konfigurationen der Kommunikationsnetze sorgfältig ausgelegt und die Sicherheit der Lieferkette besser eingeschätzt und verwaltet werden.

Allerdings können Sicherheitsmaßnahmen anerkanntermaßen nicht ohne Weiteres nachträglich in bestehende Systeme integriert werden, insbesondere da die Komponenten von Elektrizitätsversorgungssystemen deutlich voneinander abweichende Lebenszyklen aufweisen können. Daher ist es unerlässlich, dass auch bei bestehenden Systemen der Übergang zu sicherheitsbasierten Auslegungen durch die Einbeziehung von Sicherheitsmaßnahmen in alle Systemnachrüstungen und -erweiterungen bewerkstelligt werden sollte.

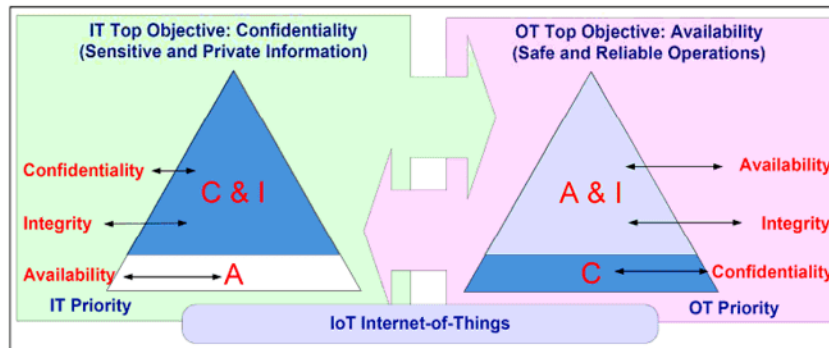
3 IT vs. OT: Unterschiede zwischen den Sicherheitsanforderungen bei informationstechnologischen (IT) Umgebungen und Technologien in der Einsatzumgebung (OT)

In herkömmlichen Geschäftsumgebungen wird die IT-Abteilung als Experte für alles betrachtet, was unter den Begriff „IT-Sicherheit“ gefasst wird. Bei den meisten Cyberanlagen des Unternehmens ist dieses IT-Fachwissen geeignet, bestehende Bedrohungen nachzuvollziehen und diesen zu begegnen sowie Verfahren zur Schwachstellenminimierung zu entwickeln und auf Angriffe zu reagieren. Im Allgemeinen geht es bei den Cyberanlagen von Unternehmen meist darum, die Vertraulichkeit der in den Computersystemen gespeicherten Informationen zu gewährleisten, so dass bei der IT-Sicherheit hauptsächlich der Schwerpunkt auf die Verhinderung des Zugriffs auf diese sensiblen Daten gelegt wird.

Jedoch können Technologien in der Einsatzumgebung (OT) Einfluss auf das Management des cyber-physischen Elektrizitätsversorgungssystems und somit auf Sicherheit und Zuverlässigkeit nehmen. Daher zeichnen sich Technologien in der OT-Umgebung durch abweichende Anforderungen und Einschränkungen bei der Anwendung von Sicherheitsmaßnahmen aus, mit denen sichergestellt wird, dass diese Systeme auch weiterhin dasselbe Sicherheits- und Zuverlässigkeitsniveau in Bezug auf das Elektrizitätsversorgungssystem gewährleisten. So müssen bei den Sicherheitsmaßnahmen beispielsweise die Latenzzeitanforderungen der Systeme in der OT-Umgebung berücksichtigt werden, da die Informationsflüsse in Unterwerken Latenzen von weniger als ein paar Millisekunden aufweisen können, während SCADA-Systeme in Netzleitstellen möglicherweise Latenzen im Sekundenbereich benötigen.

In der OT-Umgebung können vorsätzlich herbeigeführte Sicherheitsvorfälle oder auf Fahrlässigkeit zurückzuführende Fehler und Ausfälle von Cyberanlagen ebenfalls physische Rückwirkungen haben, da es sich bei Elektrizitätsversorgungssystemen um „cyber-physische Systeme“ handelt. Die Rückwirkung mit den weitreichendsten Folgen betrifft die Sicherheit: Die vorsätzliche oder fahrlässige Fehlbedienung einer Cyberanlage könnte zu Beschädigungen oder sogar Todesfällen führen. Die zweitwichtigste Rückwirkung betrifft die Zuverlässigkeit des Elektrizitätsversorgungssystems in Bezug auf die Bereitstellung von elektrischer Energie bzw. des Gasversorgungssystems in Bezug auf die Versorgung der Kunden mit Gasenergie. Obwohl diese OT-Infrastrukturen schon immer im Hinblick auf die Zuverlässigkeit ihrer physischen Anlagen (Generatoren, Trennschalter, Transformatoren, Stromleitungen, Gasleitungen) als

wichtigster Auslegungsanforderung errichtet wurden, muss heutzutage die Zuverlässigkeit der unterstützenden Cyberanlagen ebenfalls in demselben Maße gewährleistet werden.



Englisch	Deutsch
IT Top Objective: Confidentiality (Sensitive and Private Information)	Oberstes Ziel für IT: Vertraulichkeit (Sensible und vertrauliche Informationen)
Confidentiality	Vertraulichkeit
Integrity	Integrität
Availability	Verfügbarkeit
IT Priority	Priorität für IT
C&I	VT&I
A	VF
OT Top Objective: Availability (Safe and Reliable Operations)	Oberstes Ziel für OT: Verfügbarkeit (Sicherer und zuverlässiger Betrieb)
OT Priority	Priorität für OT
A&I	VF&I
C	VT
IoT Internet of Things	IoT Internet of Things (Internet der Dinge)

Bild 4 – Beispiel für die unterschiedlichen Prioritäten bei den obersten Sicherheitszielen von IT und OT

Wie in Bild 4 dargestellt, ist in IT-Umgebungen die Vertraulichkeit der sensiblen Geschäfts- und Kundendaten normalerweise der wichtigste Aspekt. Im Vergleich dazu sind in OT-Umgebungen die Verfügbarkeit, Authentisierung, Autorisierung und Datenintegrität in Elektrizitätsversorgungssystemen entscheidendere Anforderungen, da die Daten von Elektrizitätsversorgungssystemen nicht als sensibel betrachtet werden.

Aufgrund ihrer Erfahrung bei der Schwerpunktsetzung auf die Zuverlässigkeit des Energiesystems verstehen die Experten häufig am besten, welche Reaktionen auf Sicherheitsvorfälle, die die Cyberanlagen betreffen, angemessen sind, und nutzen ihr internetbezogenes IT-Wissen dazu, über die beste Anwendung von technischen Verfahren und Betriebsabläufen auf die „physischen“ Energiesysteme zu befinden, um die Auswirkungen derartiger, die Cyberanlagen betreffender Vorfälle so geringfügig wie möglich zu halten.

Einsatzumgebungen zeichnen sich durch einige sehr spezifische Sicherheits Herausforderungen aus. So sind beispielsweise aufgrund der Hochverfügbarkeit der physischen Anlagen und der Cyberanlagen technische Auslegungen erforderlich, die in Bezug auf diese Anlagen den Schwerpunkt auf Redundanz, Hochverfügbarkeit, Hochleistungsanforderungen legen. Durch die Sicherheitsanforderungen der OT-Umgebung können Änderungen bei Netzwerkkonfigurationen und Informationsflüssen notwendig werden, die z. B. die Verwendung von Sicherheitsbereichen, demilitarisierter Zonen und Firewalls vorsehen. Zusätzlich können mit sehr hoher Geschwindigkeit in Echtzeit ablaufende Prozesse, die Peer-to-peer-Interaktionen, autonome Aktionen, Zeitsensitivität und andere Eigenschaften beinhalten, andere Sicherheitslösungen

erforderlich machen als jene, die üblicherweise in der IT zum Einsatz kommen und die z. B. lediglich eine Authentisierung und keine Verschlüsselung erfordern.

Gleichzeitig sind bei diesen Auslegungen betriebliche Einschränkungen zu berücksichtigen. So können beispielsweise eingeschränkte Ausrüstungsressourcen (Zeitvorgabe, Bandbreite, Netzzugang) die IT-Sicherheitsverfahren und -technologien, die genutzt werden könnten, beeinflussen. Insbesondere starke Verschlüsselungstechniken oder die Online-Kommunikation mit Zertifizierungsstellen sind für Betriebsanlagen im Allgemeinen nicht möglich. Außerdem wird die Zeitplanung für Systemwartung und Einrichtungsaktualisierungen oder -erweiterungen durch die betrieblichen Anforderungen des Elektrizitätsversorgungssystems eingeschränkt, so dass nur kurze Zeitfenster im Frühling oder Herbst bleiben, in denen die Einrichtungen für derartige Aktualisierungen außer Betrieb genommen werden können.

Ein weiteres beschränkendes Element für die Anwendung von IT-Sicherheitsmaßnahmen besteht in der großen Zahl bestehender Einrichtungen mit langen Lebenszyklen, die nicht ohne Weiteres um IT-Sicherheitstechniken erweitert werden können. Daher müssen andere Sicherheitsmaßnahmen gefunden werden wie z. B. virtuelle private Netze (VPN) oder Verfahren zur Isolierung oder Trennung der Geräte. Zusätzlich sollte angesichts der kritischen Bedeutung des Elektrizitätsversorgungssystems darauf geachtet werden, dass durch die Sicherheitsmaßnahmen keine Betriebsabläufe, insbesondere keine Notbetriebsabläufe, unterbunden werden, sondern dass die Sicherheitsverfahren in bestimmten Szenarien außer Kraft gesetzt werden können.

Eine weitere große Änderung betrifft die Notwendigkeit der Nutzung von Netzwerken und Technologien des Internets der Dinge (Internet of Things – IoT), insbesondere für die Interaktion mit Kundenstandorten zur Überwachung und zum Management der dezentralen Energieversorgung (DER) sowie zur Kommunikation mit intelligenten Zählern. Die Nutzung des IoT impliziert, dass sich Energieversorger nicht mehr allein auf ihre eigenen Kommunikationsnetze verlassen können, aber dennoch nach wie vor IT-Sicherheitstechniken bei den Interaktionen über öffentliche Netze mittels bekannter Kommunikationstechnologien anwenden müssen.

4 Risikobeurteilung, Risikoverringung und Risikolebenszyklusprozesse

Risikobeurteilung, Risikoverringung und die kontinuierliche Aktualisierung von Prozessen sind grundlegende Methodiken zur Gewährleistung der Sicherheit. Anhand der geschäftlichen (finanziellen, die Marke betreffenden, betrieblichen, gesellschaftlichen) Anforderungen und mit Hilfe der bewährten, in internationalen Normen festgelegten Methodiken, die auf OT-Umgebungen anwendbar sind, können Unternehmen die Anfälligkeit für Sicherheitsrisiken bestimmen, geeignete Sicherheitsmaßnahmen auswählen und anwenden, diese genau befolgen und bei Bedarf im Rahmen eines kontinuierlichen Verbesserungsprozesses aktualisieren.

Die Risikobeurteilung beinhaltet sowohl objektive als auch subjektive Analysen. Es existieren zahlreiche Verfahren und Leitlinien zur Risikobeurteilung, die dazu verwendet werden können, die Risiken in der OT-Umgebung festzustellen. Die Auswahl des richtigen Risikobeurteilungsverfahrens für verschiedene Situationen und Umgebungen kann aufgrund der jeweiligen Einschränkungen, die in den einzelnen Unternehmen bestehen und die z. B. durch nationale Vorschriften, zeitliche Beschränkungen und Richtlinien der Geschäftsführung gegeben sind, eine anspruchsvolle Aufgabe darstellen.

Außerdem existiert keine einzelne oder perfekte Herangehensweise zur Risikoverringung. In der OT-Umgebung muss bei den gewählten Prinzipien zur Beschäftigung mit der Risikoverringung die vollständige Integration der betrieblichen Einschränkungen der Systeme stattfinden, um der persönlichen Sicherheit Rechnung zu tragen, für den Schutz der physischen Anlagen zu sorgen und die erforderliche Leistung dieser Systeme sicherzustellen.

Zur Gewährleistung eines bestmöglichen Risikobeurteilungsprozesses ist es entscheidend, die Experten aus jedem Energieversorgungsbereich direkt als Teil des IT-Sicherheitsteams zu integrieren und nicht nur als Mitwirkende bei den Lebenszyklusaktualisierungen im Rahmen der Risikobeurteilung zu betrachten.

Ein Risiko kann als Kombination der Folgen, die das Auftreten eines unerwünschten Ereignisses hätte, und der Wahrscheinlichkeit des Auftretens des Ereignisses beschrieben werden.

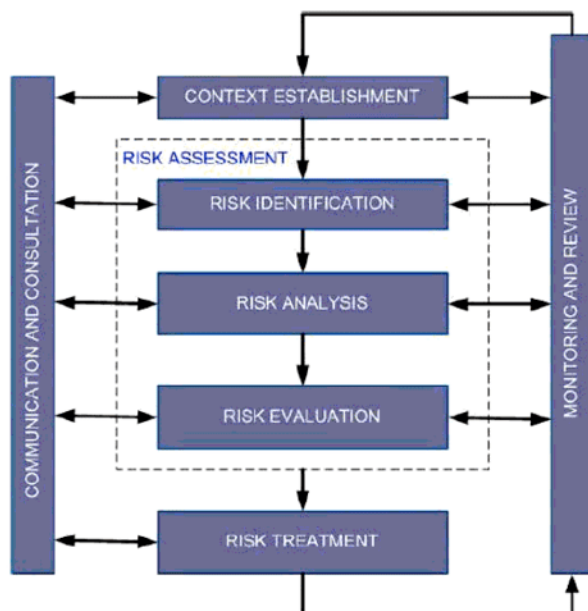
- Die Folgen können sich auf die Sicherheit beziehen oder finanzielle, umweltbezogene, gesellschaftliche und andere Aspekte eines Ereignisses betreffen (z. B. fehlerhafter Prozess, Informationsverlust, Schädigung des Personals)
- Risiken sollten festgestellt, quantifiziert oder qualitativ beschrieben sowie anhand der für das Unternehmen relevanten Risikokriterien und Ziele priorisiert werden.

Bei der Risikobeurteilung sollten Risiken festgestellt, quantifiziert und anhand von Kriterien für die Risikoakzeptanz und Zielen, die für das Unternehmen relevant sind, priorisiert werden. Die Ergebnisse sollten als Richtschnur dienen und die entsprechende Managementmaßnahme und die Prioritäten für den Umgang mit IT-Sicherheitsrisiken und die Umsetzung ausgewählter Maßnahmen zum Schutz vor diesen Risiken bestimmen. Die Risikobeurteilung sollte Folgendes umfassen:

- Den systematischen Ansatz zur Einschätzung der Größenordnung der Risiken (Risikoanalyse) und
- den Prozess zum Vergleich der eingeschätzten Risiken mit den Risikokriterien zur Bestimmung der Signifikanz der Risiken (Risikobewertung).

In Bild 5 ist der allgemeine Risikomanagementprozess dargestellt. Zu dessen wesentlichen Schritten gehören:

- Erfassung der grundlegenden geschäftlichen und regulatorischen Anforderungen, die für die OT-Umgebung gelten, und Feststellung der (sicherheitsbezogenen, wirtschaftlichen, betrieblichen) Auswirkungen, wenn diese nicht erfüllt werden.
- Auswahl des Risikobeurteilungsverfahrens auf Grundlage der unternehmensbezogenen Anforderungen und Einschränkungen.
- Auswahl des Umfangs der durchzuführenden Risikobeurteilung auf Grundlage der Grenzen der Zielsysteme, einschließlich nicht nur der innerhalb der Grenzen liegenden Systeme, sondern auch der Schnittstellen mit anderen OT-Systemen und Systemen, die nicht zur OT gehören.



Englisch	Deutsch
Communication and consultation	Kommunikation und Beratung
Context establishment	Kontextbestimmung
Risk assessment	Risikobeurteilung
Risk identification	Risikoidentifizierung
Risk analysis	Risikoanalyse
Risk evaluation	Risikobewertung
Risk treatment	Risikobehandlung
Monitoring and review	Überwachung und Prüfung

Bild 5 – Risikomanagementprozess (ISO/IEC 27005:2018)

- Bedrohungen können im Zusammenhang mit der physischen Einrichtung, Informationen, Prozessen, Interaktionen, Konfigurationen und anderen Anlagen stehen.
- Risikoverringung beinhaltet die Abwägung des Risikos gegen die Kosten, die durch die Verringerung des betreffenden Risikos auf ein akzeptables Niveau entstehen. In internen Sicherheitsrichtlinien muss festgelegt sein, was als „akzeptiertes Risiko“ zu betrachten ist. Die Risikoverringung kann eine Aktualisierung der Risikobeurteilung beinhalten um sicherzustellen, dass die Risiken tatsächlich akzeptabel sind, insbesondere dann, wenn im Rahmen der Risikoverringung viele Änderungen durchgeführt wurden.
- Anwendung von Sicherheitsmaßnahmen⁷ zur Verringerung der festgestellten Risiken:
 - Lösungen für Sicherheitsmaßnahmen können aus organisatorischen Maßnahmen, Prozessen und/oder Technologien bestehen, die in den Systemen umgesetzt werden.
 - Die Wirksamkeit von Lösungen für Sicherheitsmaßnahmen könnte beurteilt werden, um zu bestimmen, ob dadurch das Risiko tatsächlich auf ein akzeptables Niveau verringert wurde.
 - Diese Lösungen für Sicherheitsmaßnahmen können sowohl IT-Sicherheitsmaßnahmen als auch energietechnische Maßnahmen (Verfahren, Technologien und/oder Betriebsabläufe in Echtzeit) beinhalten.
- Sobald die Risikobeurteilung abgeschlossen und Lösungen zur Risikoverringung ausgewählt wurden, werden diese Lösungen in den Systemen umgesetzt.
 - Im Zeitverlauf ist sicherzustellen, dass die Maßnahmen ordnungsgemäß angewendet wurden und tatsächlich die erwarteten Verringerungen bewirken.
 - Ein Sicherungsprozess, z. B. in Form eines Audits, ist durchzuführen, eventuell durch eine andere Gruppe.
- Bestimmung der tatsächlich umzusetzenden Maßnahmen (d. h. der spezifischen Verfahren und/oder Technologien und/oder kommerziellen Produkte), die bei den verschiedenen Sicherheitsmaßnahmen anzuwenden sind.
 - Einige Lösungen für Sicherheitsmaßnahmen lassen sich in bestimmten Systemen möglicherweise nicht umsetzen; dies betrifft insbesondere bereits bestehende Systeme (z. B. Virenschutzanwendungen oder Verfahren zur Installation von Sicherheitspatches).
 - Einschränkungen bei diesen Maßnahmenlösungen sollten festgestellt werden, da eine Vielzahl von Problemen auftreten kann, was auf die vielen unterschiedlichen OT-Umgebungen zurückzuführen ist, z. B. unterschiedliche Einschränkungen in einer Unterwerkumgebung (lange Zeiträume zwischen Gelegenheiten, die Systeme zu patchen) oder einer DER-Umgebung (geringe Sicherheitskenntnisse vor Ort).
- Im Zeitverlauf sollten alle diese Maßnahmenlösungen überwacht werden um sicherzustellen, dass sie nach wie vor wirksam sind bzw. um zu überprüfen, ob mögliche Angriffe unter Umständen die Maßnahmenlösungen überwunden haben.
 - In allen Fällen sollten mögliche Sicherheitsvorfälle, die durch diese Überwachung festgestellt wurden, einem zentralen CERT-Standort gemeldet werden.
 - Das CERT sollte in der Lage sein, die eingehenden Meldungen nach Wichtigkeit zu filtern und die Bedeutung eines jeden Sicherheitsvorfalls oder einer Reihe von Sicherheitsvorfällen einzuschätzen.

5 IT-Sicherheitsnormen und bewährte Verfahren

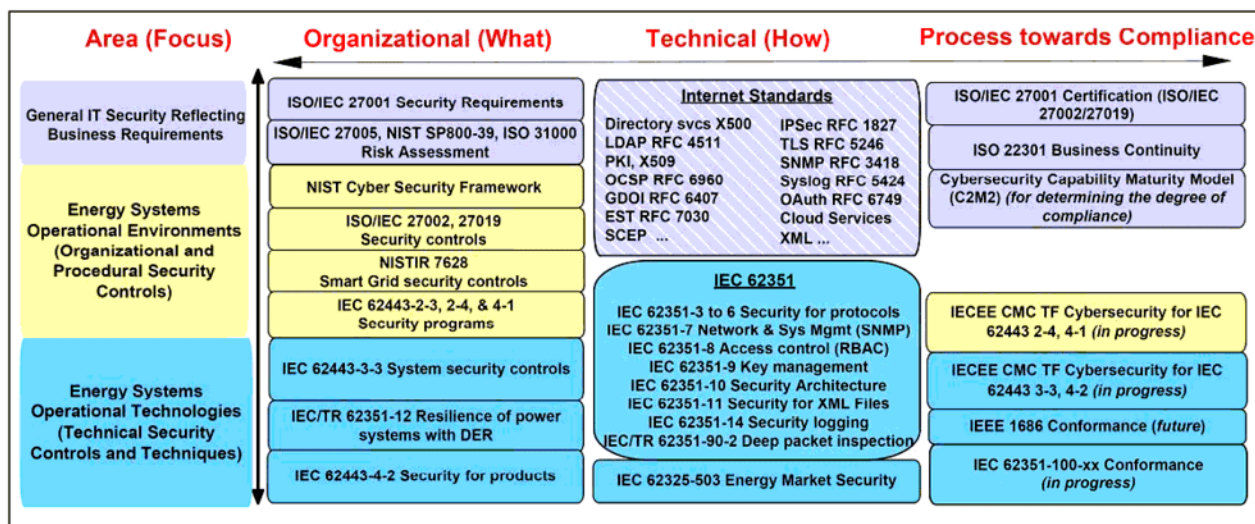
Angeichts der Komplexität der Geschäftsprozesse und der großen Vielfalt von Cyberanlagen, die in der Smart-Energy-Umgebung zum Einsatz kommen, existiert keine einzelne IT-Sicherheitsnorm, die auf alle Sicherheitsanforderungen, Sicherheitsmaßnahmen, Resilienzstrategien und Technologien eingehen kann. Einige Normen und Richtlinien richten den Schwerpunkt auf die grundlegenden organisatorischen

⁷ Maßnahme (aus ISO/IEC 27000:2018): Handlung, durch die ein Risiko modifiziert wird. Anmerkung 1 zum Begriff: Zu den Maßnahmen zählen jedwede Prozesse, Richtlinienapparate, Praktiken oder andere Handlungen, durch die ein Risiko modifiziert wird. Anmerkung 2 zum Begriff: Es ist möglich, dass Maßnahmen nicht immer die beabsichtigte oder angenommene modifizierende Wirkung entfalten

Sicherheitsanforderungen und detaillierteren empfohlenen Maßnahmen (das „Was“), während sich andere Normen auf die Technologien konzentrieren, die genutzt werden können, um diese IT-Sicherheitsmaßnahmen mittels validierter Techniken und mit einem Schwerpunkt auf Interoperabilität bereitzustellen (das „Wie“).

Während viele zusätzliche Dokumente und Vorschriften auf nationaler und lokaler Ebene Anwendung finden, sind in Bild 6 die wichtigsten IT-Sicherheitsnormen und bewährten Verfahren von IEC, ISO, IEEE, NIST und IETF wiedergegeben, geordnet nach Typ („Was“, „Wie“, Prozess zur Normerfüllung) und nach Ebene (übergreifende allgemeine Ebene, übergreifende energiespezifische Ebene, detaillierte technische Ebene).

Cyber Security Standards and Guidelines that Apply to Smart Energy Operational Environments



Englisch	Deutsch
Cyber Security Standards and Guidelines that Apply to Smart Energy Operational Environments	Normen und Richtlinien zur IT-Sicherheit, die auf Smart-Energy-Einsatzumgebungen Anwendung finden
Area (Focus)	Bereich (Schwerpunkt)
General IT Security Reflecting Business Requirements	Allgemeine IT-Sicherheit, die die Geschäftsanforderungen widerspiegelt
Energy Systems Operational Environments (Organizational and Procedural Security Controls)	Einsatzumgebungen von Energiesystemen (organisatorische und verfahrensbezogene Sicherheitsmaßnahmen)
Energy Systems Operational Technologies (Technical Security Controls and Techniques)	Betriebstechnologien von Energiesystemen (technische Sicherheitsmaßnahmen und Techniken)
Organizational (What)	Organisatorisch („Was“)
ISO/IEC 27001 Security Requirements	ISO/IEC 27001: Schutzanforderungen
ISO/IEC 27005, NIST SP800-39, ISO 31000 Risk Assessment	ISO/IEC 27005, NIST SP800-39, ISO 31000: Risikobeurteilung
NIST Cyber Security Framework	Rahmenwerk des NIST zur IT-Sicherheit
ISO/IEC 27002, 27019 Security controls	ISO/IEC 27002, 27019: Sicherheitsmaßnahmen
NISTIR 7628 Smart Grid security controls	NISTIR 7628: Sicherheitsmaßnahmen für Smart Grids
IEC 62443-2-3, 2-4, & 4-1 Security programs	IEC 62443-2-3, 2-4, & 4-1: Sicherheitsprogramme
IEC 62443-3-3 System security controls	IEC 62443-3-3: Maßnahmen zur Systemsicherheit
IEC/TR 62351-12 Resilience of power systems with DER	IEC/TR 62351-12: Resilienz von Elektrizitätsversorgungssystemen mit DER
IEC 62443-4-2 Security for products	IEC 62443-4-2: Sicherheit für Produkte

Technical (How)	Technisch („Wie“)
Internet Standards	Internet-Normen
Directory svcs X500	Verz.dienst X.500
Cloud Services	Cloud-Dienste
IEC 62351-3 to 6 Security for protocols	IEC 62351-3 bis 6: Sicherheit für Protokolle
IEC 62351-7 Network & Sys Mgmt (SNMP)	IEC 62351-7: Netzwerk- & Systemmanagement (SNMP)
IEC 62351-8 Access control (RBAC)	IEC 62351-8: Zugangssteuerung (RBAC)
IEC 62351-9 Key management	IEC 62351-9: Schlüsselmanagement
IEC 62351-10 Security Architecture	IEC 62351-10: Sicherheitsarchitektur
IEC 62351-11 Security for XML Files	IEC 62351-11: Sicherheit für XML-Dateien
IEC 62351-14 Security logging	IEC 62351-14: Sicherheit für Event Logging
IEC/TR 62351-90-2 Deep packet inspection	IEC/TR 62351-90-2: Deep Packet Inspection
IEC 62325-503 Energy Market Security	IEC 62325-503: Sicherheit im Energiemarkt
Process towards Compliance	Prozess zur Normerfüllung
ISO/IEC 27001 Certification (ISO/IEC 27002/27019)	ISO/IEC 27001 Zertifizierung (ISO/IEC 27002/27019)
ISO 22301 Business Continuity	ISO 22301: Geschäftskontinuität
Cybersecurity Capability Maturity Model (C2M2) (for determining the degree of compliance)	Cybersecurity Capability Maturity Model (C2M2) (zur Bestimmung des Erfüllungsgrades)
IECEE CMC TF Cybersecurity for IEC 62443 2-4, 4-1 (in progress)	IECEE CMC TF Cybersecurity für IEC 62443 2-4, 4-1 (in Arbeit)
IECEE CMC TF Cybersecurity for IEC 62443 3-3, 4-2 (in progress)	IECEE CMC TF Cybersecurity für IEC 62443 3-3, 4-2 (in Arbeit)
IEEE 1686 Conformance (future)	IEEE 1686: Konformität (zukünftig)
IEC 62351-100-xx Conformance (in progress)	IEC 62351-100-xx: Konformität (in Arbeit)

Bild 6 – Wesentliche Normen und Richtlinien zur IT-Sicherheit

Anhang A enthält weitere Details zu den wesentlichen Normen und bewährten Verfahren zur IT-Sicherheit.

6 Schlussfolgerungen

Da IT-Sicherheit zu einer immer wichtigeren Anforderung für jedes Unternehmen geworden ist, um in einer immer stärker automatisierten Umgebung zu überleben, müssen sich dessen Führungskräfte der wesentlichen sicherheits- und resilienzbezogenen Merkmale ihres Geschäfts bewusst sein, da die Sicherheitskultur von der Spitze der Unternehmens ausgehen muss. Sicherheitsrichtlinien, Sicherheitsverfahren und Sicherheitstechnologien können nur dann effektiv sein, wenn Sicherheit und Resilienz seitens der obersten Leitung als kritisch angesehen werden und dies hinunter auf alle Ebenen kommuniziert wird. Diese Anforderung ist besonders wichtig für Unternehmen im Bereich von als kritisch angesehenen Infrastrukturen, insbesondere Unternehmen, die in der Einsatzumgebung der Energiewirtschaft tätig sind.

Fünf Konzepte für die IT-Sicherheit sollten Führungskräfte in der Einsatzumgebung der Energiewirtschaft bei ihren Bemühungen um die Implementierung der erforderlichen IT-Sicherheitsrichtlinien, -verfahren und -technologien kennen.

- **Konzept Nr. 1. Resilienz** sollte die übergreifende Strategie zur Sicherstellung der Geschäftskontinuität darstellen: Bei der allgemeinen Schwerpunktsetzung auf Resilienz müssen Unternehmen die Sicherheit, den Schutz und die Zuverlässigkeit der Prozesse und die Bereitstellung ihrer Dienste berücksichtigen. Resilienz schließt Sicherheitsmaßnahmen ein, mit

denen Auswirkungen verringert werden können, und zwar nicht nur im Vorfeld von Zwischenfällen (feststellen und verhindern), sondern auch während dieser Zwischenfälle (erkennen und reagieren) sowie nach Behebung von deren Auswirkungen (wiederherstellen).

- **Konzept Nr. 2. Security by Design** ist der kosteneffektivste Sicherheitsansatz: Sicherheit ist entscheidend für alle kritischen Infrastrukturen und sollte von Anfang an in die Auslegung von Systemen und betrieblichen Tätigkeiten einbezogen und nicht erst nach der Implementierung der Systeme umgesetzt werden. Da jedoch davon ausgegangen werden muss, dass bestehende Systeme nicht ohne Weiteres durch Sicherheitsvorkehrungen ergänzt werden können, ist es unerlässlich, dass auch bei diesen bestehenden Systemen der Übergang zu sicherheitsbasierten Auslegungen durch die Einbeziehung von Sicherheitsmaßnahmen in alle Systemnachrüstungen und -erweiterungen bewerkstelligt wird.
- **Konzept Nr. 3. „IT“ und „OT“ sind ähnlich, aber nicht identisch:** Technologien in Einsatzumgebungen (in diesem Dokument als „OT“ bezeichnet) weisen viele Sicherheitseinschränkungen und -anforderungen auf, durch die sie sich von informationstechnologischen (IT) Umgebungen unterscheiden. Die Hauptgrund dafür ist, dass es sich bei Energiesystemen um cyber-physische Systeme handelt und Sicherheitsvorfälle zu Zwischenfällen führen können, die die physische Sicherheit und/oder wesentliche Energieverluste betreffen. Daher sind Verfügbarkeit, Authentisierung, Autorisierung und die Integrität der betrieblichen Informationen üblicherweise kritischere Anforderungen als Vertraulichkeit. Gleichwohl stützen sich sowohl IT- als auch OT-Umgebungen im zunehmenden Maße auf IoT-Technologien.
- **Konzept Nr. 4. Risikobeurteilung, Risikoverringerung und die kontinuierliche Aktualisierung von Prozessen** sind von grundlegender Bedeutung für die Verbesserung der Sicherheit: Auf Grundlage der geschäftlichen Anforderungen des Unternehmens muss dessen Gefährdung durch Sicherheitsrisiken (Sicherheit von Menschen sowie physische, funktionale, umweltbezogene, finanzielle, gesellschaftliche und die Reputation des Unternehmens betreffende Aspekte) für alle seine Geschäftsprozesse bestimmt werden. Bei der Risikobeurteilung wird die Anfälligkeit von Systemen und Prozessen für vorsätzliche oder durch Fahrlässigkeit verursachte Bedrohungen festgestellt, außerdem werden potenzielle Auswirkungen der Vorfälle bestimmt und die Wahrscheinlichkeit dafür eingeschätzt, dass das Vorfalleszenario tatsächlich eintritt.
- **Konzept Nr. 5. IT-Sicherheitsnormen und Richtlinien zu bewährten Verfahren** für OT-Umgebungen im Energiebereich sollten angewendet werden, um den Risikomanagementprozess zu unterstützen und Sicherheitsprogramme und -richtlinien zum jeweiligen Zeitpunkt einzurichten. IT-Sicherheitsmaßnahmen sollten nicht „neu *erfunden*“ werden, da wesentliche IT-Sicherheitsnormen und Richtlinien zu bewährten Verfahren für verschiedene Sicherheitsbereiche und -zwecke bereits entwickelt wurden. Bei der Planung der IT-Sicherheit sollten diese IT-Sicherheitsnormen und -richtlinien angewendet werden, um Resilienz, allgemeine Sicherheit und Interoperabilität in der gesamten energiebezogenen OT-Umgebung zu verbessern und dabei zum jeweiligen Zeitpunkt auf die richtigen Normen, Richtlinien und Verfahren für die entsprechenden Zwecke zurückgreifen.

Unter Berücksichtigung dieser 5 Konzepte lauten einige der wesentlichen Schlussfolgerungen:

- Die Leitungsebene muss im Bereich der IT-Sicherheit die führende Rolle übernehmen. Viele IT-Sicherheitsprobleme sind auf der Leitungsebene zu behandeln. Hierzu zählen Sicherheitsrichtlinien, Systemarchitekturen, Personalorganisation, Sicherheitsverfahren und die verschiedenen Arten von Sicherheitstechnologien.
 - Insbesondere müssen Schulungs- und Weiterbildungsprogramme im Bereich der Sicherheit sowie Richtlinien entwickelt werden, die zum Austausch über Sicherheitsschwachstellen, Bedrohungen und Informationen über Lösungen mit anderen Unternehmen, z. B. über die CERTs, dienen.
 - So bedeutet z. B. die Tatsache, dass die Kommunikation verschlüsselt ist, nicht automatisch, dass die Systeme sicher sind – entwendete oder erratene Passwörter können nach wie vor gefährliche Eingriffe in cyber-physische Systeme ermöglichen.
- Die bestehenden IT-Sicherheitsnormen und bewährten Verfahren in Bezug auf Sicherheitsanforderungen und -maßnahmen sind recht ausgereift und sollten den Ausgangspunkt eines jeden IT-Sicherheitsprozesses darstellen. Jedoch entfaltet die Umsetzung der Sicherheitsverfahren und -technologien zur Erfüllung der Anforderungen dieser bestehenden Normen möglicherweise nicht ihre volle Wirkung:

- IT-Normen werden regelmäßig überarbeitet und aktualisiert, um auf neu entdeckte Sicherheitsprobleme einzugehen und sind daher unter Umständen nicht verfügbar und/oder vollständig.
- Neue Technologien bringen immer auch neue Bedrohungen und/oder Anfälligkeiten mit sich, für die neue Normen oder Richtlinien entwickelt werden müssen.
- Hacker finden immer neue Möglichkeiten, Schwachstellen auszunutzen und Sicherheitsvorfälle herbeizuführen. Normen und Richtlinien können nicht immer schnell genug angepasst werden, um diesen neuen Bedrohungen zu begegnen.
- Die Einhaltung der IT-Sicherheitsnormen bietet ein hohes Maß an Sicherheit, dies bedeutet jedoch nicht unbedingt, dass die Systeme völlig sicher sind, einerseits weil es die Komplexität der Systeme und ihrer Konfigurationen unmöglich machen kann, auf alle IT-Sicherheitsprobleme einzugehen und andererseits weil immer auch „erfolgreiche“ Angriffe vorkommen werden.
- Durch IT-Sicherheitsnormen kann die Interoperabilität dieser zunehmend komplexen Kommunikationssysteme mittels Festlegung eines validierten und begrenzten Bestands von Sicherheitstechnologien und -verfahren unterstützt werden.
- Die fortwährende Überwachung und Verbesserung der Sicherheitsmaßnahmen ist von entscheidender Bedeutung, da die Technologien einem stetigen Wandel unterworfen sind, täglich neue Schwachstellen entdeckt werden und Hacker den Entwicklern von IT-Sicherheitslösungen stets einen Schritt voraus sind.

Anhang A

Wesentliche Normen und Richtlinien zur IT-Sicherheit⁸

A.1 Normenreihe ISO/IEC 27000 zur IT-Sicherheit

A.1.1 Normenfamilie ISO/IEC 27001 zu ISMS

Die Normenreihe ISO/IEC 27000 deckt einen großen Bereich von IT-Sicherheitsanforderungen und -richtlinien ab, die unter anderem die Einrichtung des in diesem Anhang behandelten ISMS (*Information Security Management System* – Informationssicherheitsmanagementsystem) betreffen. Wie in Bild 7 und Tabelle 1 dargestellt, ist diese Normenfamilie ISO/IEC 27001 im Laufe der letzten Jahre stark erweitert worden.

ISO/IEC 27001 (zusammen mit anderen Normen der Familie 27XXX) bildet außerdem den Rahmen für externe Audits und die Zertifizierung des ISMS eines Unternehmens. Unternehmen können ihr Informationssicherheitsmanagementsystem von unabhängigen Zertifizierungsstellen nach ISO/IEC 27001 zertifizieren lassen, die von einer nationalen Akkreditierungsstelle anerkannt sein müssen.

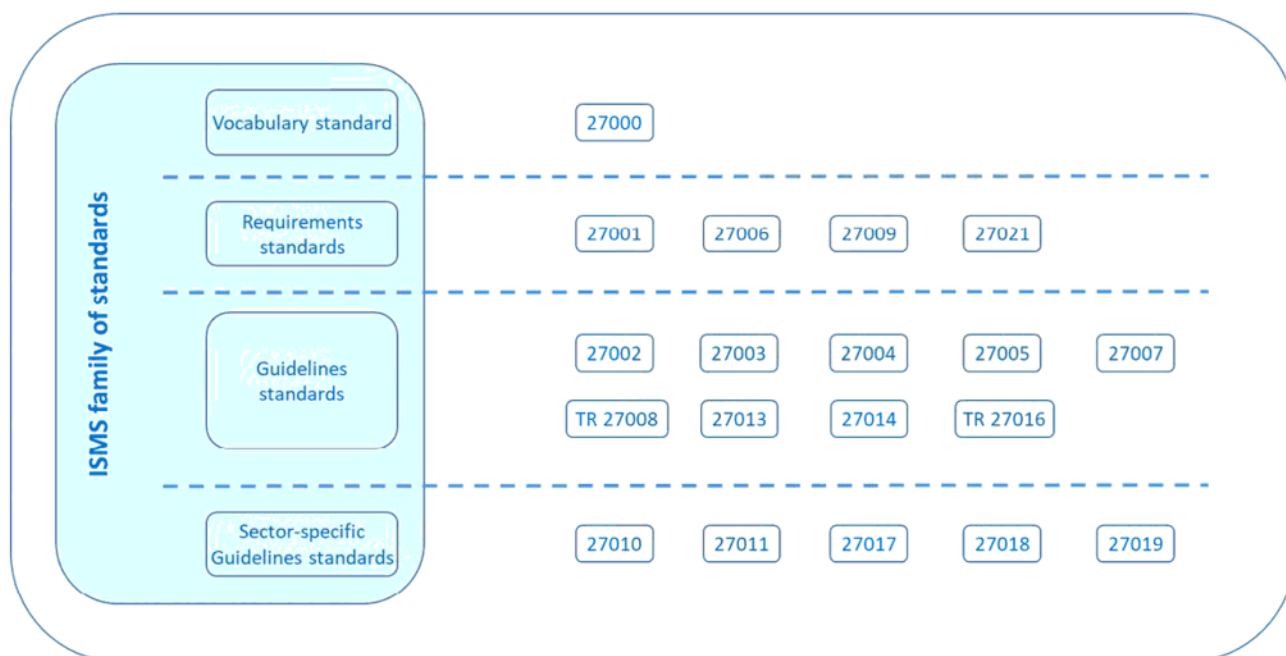
Die Normenfamilie zu ISMS besteht aus aufeinander bezogenen Normen, die bereits veröffentlicht wurden oder in Entwicklung sind, und enthält eine Reihe bedeutsamer Strukturkomponenten. Bei diesen Komponenten liegt der Schwerpunkt auf:

- Normen, in denen die Anforderung für ein ISMS beschrieben werden (ISO/IEC 27001);
- Anforderungen für Zertifizierungsstellen (ISO/IEC 27006), die die Übereinstimmung mit ISO/IEC 27001 bescheinigen und
- Zusätzlicher Anforderungsrahmen für sektorspezifische Implementierungen des ISMS (ISO/IEC 27009).

Weitere Dokumente dienen als Orientierung für verschiedene Aspekte einer ISMS-Umsetzung und beschäftigen sich mit einem allgemeinen Prozess sowie mit der sektorspezifischen Orientierung.

Die Beziehungen zwischen den ISMS-Normenfamilien sind im nachstehenden Bild veranschaulicht:

⁸ In diesem Dokument werden die einzelnen Normen nur anhand ihrer Nummer in Bezug genommen; dabei ist zu beachten, dass einige Anforderungen in einer Norm aufgrund von Überarbeitungen und Neuveröffentlichungen der Normen Änderungen erfahren können. Das Datum der aktuellen Ausgabe kann bei der veröffentlichenden Organisation erfragt werden.



Englisch	Deutsch
ISMS family of standards	ISMS-Normenfamilie
Vocabulary standard	Terminologie-Norm
Requirements standards	Anforderungsnormen
Guidelines standards	Richtliniennormen
Sector-specific Guidelines standards	Sektorspezifische Richtliniennormen

Bild 7^{N1} – Beziehungen innerhalb der ISMS-Normenfamilie

Tabelle 1^{N2} – ISMS-Normenfamilie (1 von 3)

Norm	Titel	Typ
ISO/IEC 27000:2018	Information technology – Security techniques – Information security management systems – Overview and vocabulary [Informationstechnik – Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie]	Terminologie
ISO/IEC 27001:2013	Information technology – Security techniques – Information security management systems – Requirements [Informationstechnik – Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen]	Anforderungen
ISO/IEC 27006:2015	Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems [Informationstechnik – Sicherheitsverfahren – Anforderungen an Institutionen, die Audits und Zertifizierungen von Informationssicherheits-Managementsystemen anbieten]	

^{N1} Nationale Fußnote: Fehlerhafte Benummerung entsprechend dem IEC-Original. Diese muss „Bild A.1“ lauten. Änderung ist bei IEC beantragt.

^{N2} Nationale Fußnote: Fehlerhafte Benummerung entsprechend dem IEC-Original. Diese muss „Tabelle A.1“ lauten. Änderung ist bei IEC beantragt

Tabelle 1 (2 von 3)

Norm	Titel	Typ
ISO/IEC 27009:2016	Information technology – Security techniques – Sector-specific application of ISO/IEC 27001 – Requirements [Informationstechnik – Sicherheitsverfahren – Sektorspezifische Anwendung der ISO/IEC 27001]	
ISO/IEC 27021:2017	Information technology – Security techniques – Competence requirements for information security management systems professionals [Informationstechnik – Sicherheitsverfahren – Anforderungen an die Kompetenz von Sachkundigen für Informationssicherheits-Managementsysteme]	
ISO/IEC 27002:2013	Information technology – Security techniques – Code of practice for information security controls [Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen]	Richtlinien
ISO/IEC 27003:2017	Information technology – Security techniques – Information security management systems – Guidance [Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anleitung]	
ISO/IEC 27004:2016	Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation [Informationstechnik – Sicherheitsverfahren – Informationssicherheits-Management – Überwachung, Messung, Analyse und Evaluation]	
ISO/IEC 27005:2018	Information technology – Security techniques – Information security risk management [Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Risikomanagement]	
ISO/IEC 27007:2017	Information technology – Security techniques – Guidelines for information security management systems auditing [Informationstechnik – Sicherheitsverfahren – Leitfaden für das Audit von Informationssicherheitsmanagementsystemen]	
ISO/IEC TS 27008:2019	Information technology – Security techniques – Guidelines for the assessment of information security controls	
ISO/IEC 27013:2015	Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 [Informationstechnik – Sicherheitsverfahren – Leitfaden für die gemeinsame Einführung von ISO/IEC 27001 und ISO/IEC 20000-1]	
ISO/IEC 27014:2013	Information technology – Security techniques – Governance of information security [Informationstechnik – IT-Sicherheitsverfahren – Governance von Informationssicherheit]	
ISO/IEC TR 27016:2014	Information technology – Security techniques – Information security management – Organizational economics [Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheitsmanagement – organisationelle Wirtschaftlichkeit]	
ISO/IEC 27010:2015	Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications [Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagement für sektor- und organisationsübergreifende Kommunikation]	Sektorspezifische Richtlinien

Tabelle 1 (3 von 3)

Norm	Titel	Typ
ISO/IEC 27011:2016	Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations [Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen auf Grundlage von ISO/IEC 27002 für Telekommunikationsorganisationen]	
ISO/IEC 27017:2015	Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services [Informationstechnik – Sicherheitsverfahren – Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend auf ISO/IEC 27002 für Cloud Dienste]	
ISO/IEC 27018:2019	Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors [Informationstechnik – Sicherheitsverfahren – Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung]	
ISO/IEC 27019:2017	Information technology – Security techniques – Information security controls for the energy utility industry [Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmaßnahmen für die Energieversorgung]	

Die relevantesten Normen für die Umsetzung eines ISMS in Smart Grids sind ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27019. Diese Normen werden in den folgenden Abschnitten dargestellt.

A.1.2 ISO/IEC 27001

Die ISO/IEC 27001 ist eine weltweit anerkannte Norm, die Anforderungen zur Einrichtung eines Managementsystems für Informationssicherheit (Information Security Management System – ISMS) enthält. Ein ISMS wird beschrieben als „ein systematisches Modell für die Einführung, die Umsetzung, den Betrieb, die Überwachung, die Überprüfung, die Pflege und die Verbesserung der Informationssicherheit einer Organisation, um Geschäftsziele zu erreichen. Es basiert auf einer Risikobeurteilung und dem Risikoakzeptanzniveau der Organisation und dient dazu, die Risiken wirksam zu behandeln und zu handhaben.“⁹.

Zur Einführung, Überwachung, Pflege und Verbesserung eines ISMS sind die folgenden Schritte anzuwenden und fortwährend zu wiederholen:

- Feststellung der Informationsressourcen und der jeweiligen Informationssicherheitsanforderungen unter Berücksichtigung der gesetzlichen, regulatorischen und vertraglichen Anforderungen;
- Bewertung der Informationssicherheitsrisiken und Umgang mit Informationssicherheitsrisiken einschließlich
 - einer Risikoanalyse und Risikobewertung;
 - der Anwendung geeigneter Maßnahmen und der Risikoübernahme;
- der Auswahl und Umsetzung relevanter Maßnahmen zum Umgang mit inakzeptablen Risiken.
 - Die Maßnahmen können aus ISO/IEC 27002 und allen sektorspezifischen Normen der ISO/IEC 27002 ausgewählt werden, z. B. ISO/IEC 27019 für die Energiebranche;
- Überwachung, Vorhaltung und Verbesserung der Wirksamkeit von Maßnahmen in Verbindung mit den Informationsressourcen des Unternehmens.

⁹ ISO/IEC 27000:2018 Informationstechnik – Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie

A.1.3 ISO/IEC 27002:2013

ISO/IEC 27002 ist ein Praxisleitfaden – ein Bündel allgemeiner Maßnahmen, die sich mit Maßnahmenzielen der Informationssicherheit zur Verringerung von Sicherheitsrisiken beschäftigen, die z. B. die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen betreffen.

Die Sicherheitsmaßnahmen der ISO/IEC 27002 unterteilen sich in die folgenden Hauptabschnitte:

- Organisation der Informationssicherheit
- Personalsicherheit
- Verwaltung der Werte
- Zugangssteuerung
- Kryptographie
- Physische und umgebungsbezogene Sicherheit
- Betriebssicherheit
- Kommunikationssicherheit
- Anschaffung, Entwicklung und Instandhaltung von Systemen
- Lieferantenbeziehungen
- Handhabung von Informationssicherheitsvorfällen
- Compliance

A.1.4 ISO/IEC 27019:2017

ISO/IEC 27019 enthält Leitlinien auf Grundlage von ISO/IEC 27002 für das Informationssicherheitsmanagement zur Anwendung auf Prozesssteuerungssysteme, wie sie in der Energieversorgung eingesetzt werden. Das Ziel der ISO/IEC 27019 besteht in der Erweiterung des Normenwerks der ISO/IEC 27000 auf den Bereich der Prozesssteuerungssysteme und der Automatisierungstechnologie. Dies ermöglicht der Energieversorgungsbranche die Umsetzung eines normierten Informationssicherheits-Managementsystems (ISMS) in Übereinstimmung mit ISO/IEC 27001, das sich von der geschäftlichen Ebene bis zur Prozesssteuerungsebene erstreckt.

Der Anwendungsbereich der ISO/IEC 27019 umfasst Systeme der Prozesssteuerung der Energieversorgung, die zur Steuerung, Regelung 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 gesamte IT-gestützte 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 und Dokumentation;
- die gesamte, in der Prozesstechnik eingesetzte Kommunikationstechnik, z. B. Netzwerk-, Telemetrie-, Fernwirk- und Fernsteuertechnik;
- digitale Mess- und Zählvorrichtungen, z. B. zur Messung der Energieverbrauchs-, Erzeugungs- und Emissionswerte;
- digitale Schutz- und Safety-Systeme, z. B. Schutzgeräte oder Sicherheits-Steuerungen;
- verteilte Komponenten zukünftiger Smart-Grid-Umgebungen;
- alle Arten von Software, Firmware und Anwendungen, die auf den vorgenannten Systemen eingesetzt werden.

A.2 Rahmenwerk des NIST zur IT-Sicherheit

Das Rahmenwerk des NIST zur IT-Sicherheit bietet einen Richtlinienrahmen zur Computersicherheit, mit dem Unternehmen ihre Fähigkeit zur Ermittlung ihrer Cyberanlagen, zur weitestgehenden Vermeidung von Sicherheitsvorfällen, zur Erkennung von unvermeidlichen Sicherheitsvorfällen, zur Reaktion auf Sicherheitsvorfälle und zu deren Bewältigung, auch bei dadurch bestehenden Beeinträchtigungen von Systemfunktionen, und zur schließlichen Wiederherstellung nach derartigen Sicherheitsvorfällen bewerten und verbessern können. In Bild 8 ist das Rahmenwerk als übersichtliches Diagramm dargestellt; in den folgenden Abschnitten wird auf die wesentlichen Aspekte des Rahmenwerks eingegangen.

Feststellung: „Entwicklung des organisatorischen Verständnisses für den Umgang mit IT-Sicherheitsrisiken für Systeme, Anlagen, Daten und Funktionen.“

- Verwaltung der Werte (ID.AM): Daten, Personal, Geräte, Systeme und Einrichtungen, die es dem Unternehmen ermöglichen, seinem Geschäftszweck nachzugehen, werden entsprechend ihrer relativen Bedeutung für die geschäftlichen Ziele und die Risikostrategie des Unternehmens festgestellt und verwaltet.
- Geschäftsumfeld (ID.BE): Die Mission, Ziele, Interessensvertreter und Aktivitäten eines Unternehmens sind bekannt und priorisiert; diese Informationen werden dazu verwendet, IT-Sicherheitsrollen, Verantwortlichkeiten und Entscheidungen des Risikomanagements festzulegen.
- Governance (ID.GV): Die Richtlinien, Verfahren und Prozesse zur Verwaltung und Überwachung der regulatorischen, gesetzlichen, risiko- und umweltbezogenen sowie betrieblichen Anforderungen sind bekannt und bestimmen das Management der IT-Sicherheitsrisiken.
- Risikobeurteilung (ID.RA): Das Unternehmen kennt die IT-Sicherheitsrisiken für seine Betriebsabläufe (einschließlich Mission, Funktionen, Image oder Reputation), Anlagen und Mitarbeiter.
- Risikomanagementstrategie (ID.RM): Die Prioritäten, Einschränkungen, Risikotoleranzen und Annahmen des Unternehmens werden ermittelt und zur Unterstützung von betrieblichen Entscheidungen erwartet.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
DE	Detect	PR.PT	Protective Technology
		DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
RS	Respond	DE.DP	Detection Processes
		RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
RC	Recover	RS.IM	Improvements
		RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Englisch	Deutsch
Function Unique Identifier	Eindeutiger Funktionsbezeichner
Function	Funktion
Category Unique Identifier	Eindeutiger Kategorienbezeichner
Category	Kategorie
Identify	Feststellung

Protect	Schutz
Detect	Erkennung
Respond	Reaktion
Recover	Wiederherstellung
Asset Management	Verwaltung der Werte
Business Environment	Geschäftsumfeld
Governance	Governance
Risk Assessment	Risikobeurteilung
Risk Management Strategy	Risikomanagementstrategie
Access Control	Zugangssteuerung
Awareness and Training	Bewusstsein und Schulung
Data Security	Datensicherheit
Information Protection Processes and Procedures	Prozesse und Verfahren zum Informationsschutz
Maintenance	Wartung
Protective Technology	Schutztechnologie
Anomalies and Events	Anomalien und Vorfälle
Security Continuous Monitoring	Fortwährende Sicherheitsüberwachung
Detection Processes	Erkennungsprozesse
Response Planning	Reaktionsplanung
Communications	Kommunikation
Analysis	Analyse
Mitigation	Schadensbegrenzung
Improvements	Verbesserungen
Recovery Planning	Wiederherstellungsplanung
Improvements	Verbesserungen
Communications	Kommunikation

Bild 8 – Rahmenwerk des NIST zur Verbesserung der IT-Sicherheit in kritischen Infrastrukturen (2017)

Schutz: „Entwicklung und Umsetzung der geeigneten Sicherungsmaßnahmen zur Gewährleistung der Bereitstellung kritischer Infrastrukturdienste.“

- Zugangssteuerung (PR.AC): Der Zugang zu Anlagen und zugehörigen Einrichtungen ist beschränkt auf autorisierte Benutzer, Prozesse oder Geräte sowie auf zugelassene Aktivitäten und Transaktionen.
- Bewusstsein und Schulung (PR.AT): Personal und Partner des Unternehmens erhalten eine Weiterbildung zur Entwicklung eines Bewusstseins für das Thema IT-Sicherheit und werden entsprechend geschult, um ihren Aufgaben und Verantwortlichkeiten im Bereich IT-Sicherheit entsprechend den geltenden Richtlinien, Verfahren und Vereinbarungen nachzukommen.
- Datensicherheit (PR.DS): Informationen und Aufzeichnungen (Daten) werden entsprechend der Risikostrategie des Unternehmens zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der Informationen verwaltet.