TeleTrusT
Pioneers in IT security.

Informationstag "IT-Sicherheit im Smart Grid"

Berlin, 23.05.2012

DIN SPEC 27009
Informationssicherheit in Energienetzen

Deutsche Normungsinitiative zur IT-Sicherheit in Smart Grids

Rolf-Dieter Kasper
RWE Deutschland AG

Agenda

- Motivation und Hintergrund
- Inhalte der DIN spec 27009
- Internationale Aktivitäten

Ziel der Politik ist es, bis 2020 in der EU und in Deutschland „Smart Energy“ zu realisieren

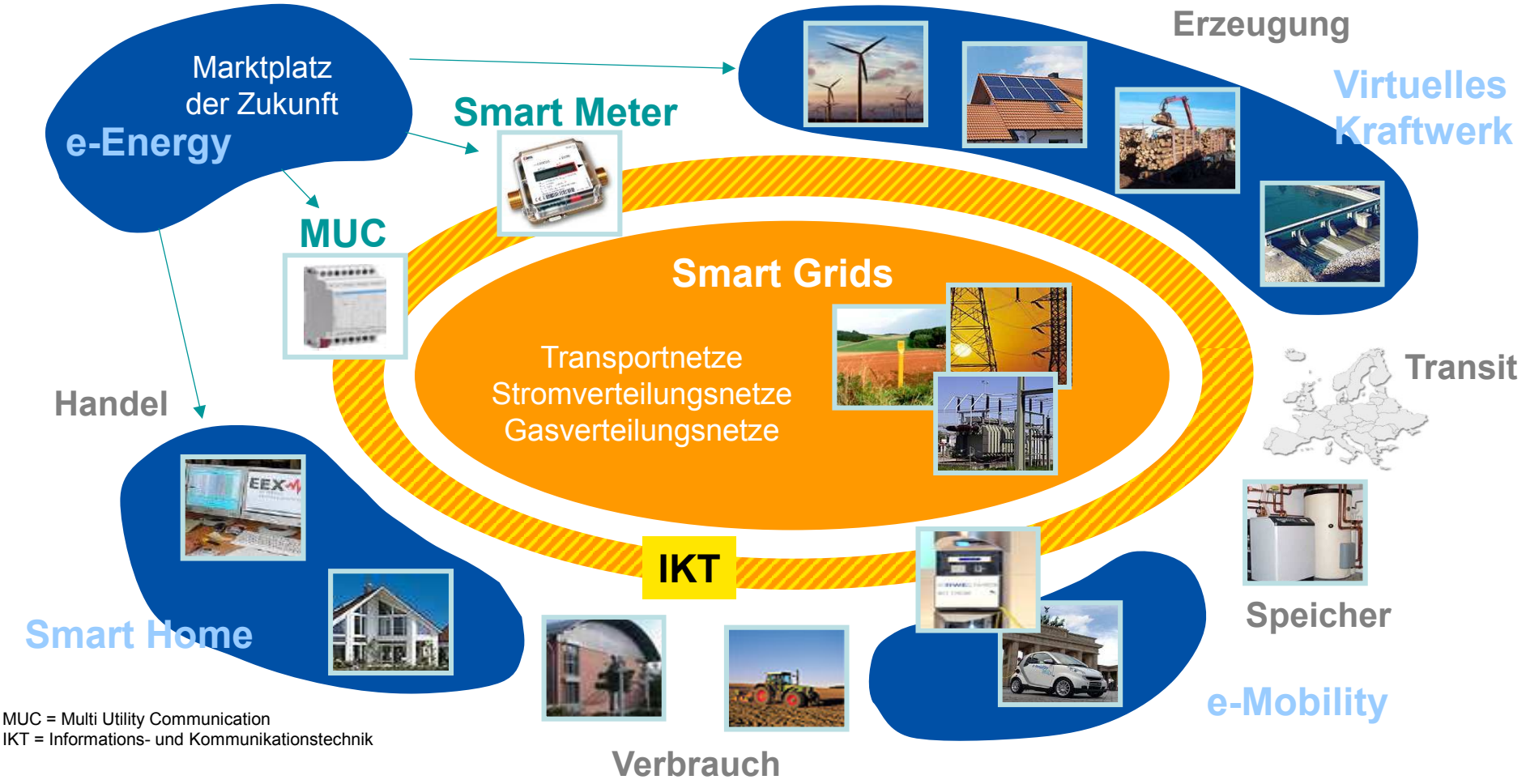
Politische Ziele im Energiekonzept der Bundesregierung:

- Reduzierung von Treibhausgasen gegenüber 1990 um
  - 40% bis 2020
  - 80% bis 2050
- Steigerung des Anteils der Stromerzeugung aus erneuerbaren Energien am Bruttostromverbrauch auf
  - 50% bis 2030
  - 65% bis 2040
  - 80% bis 2050

Wesentliche Handlungsfelder im Energiekonzept der Bundesregierung:

- Erneuerbare Energien als tragende Säule zukünftiger Energieversorgung
- Energieeffizienz
- Abkehr von der Kernenergie bis 2020
- Leistungsfähige Netzinfrastrukturen für Strom und Integration erneuerbarer Energien
  - Intelligente Netze
- Energetische Gebäudesanierung und energieeffizientes Bauen
- Herausforderung Mobilität
- Energieforschung für Innovation und neue Technologien
- Energieversorgung im europäischen und internationalen Kontext
- Transparenz und Akzeptanz

Die technologische Herausforderung liegt in der Komplexität des Systems „Netz“ begründet.



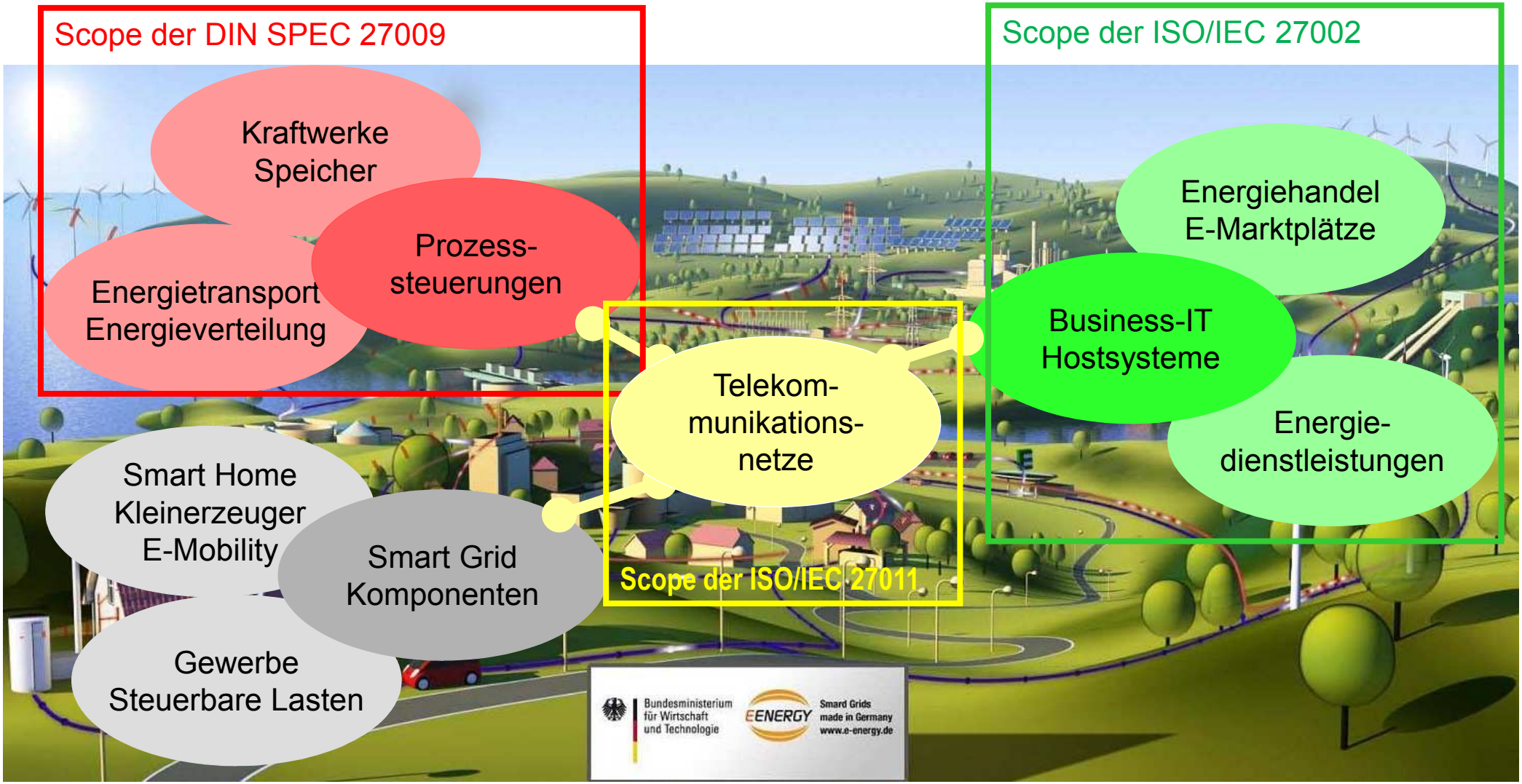
MUC = Multi Utility Communication
IKT = Informations- und Kommunikationstechnik

Motivation: Erweiterung der ISO 27000 Normenreihe um den PDV-Bereich der EVUs

- Ausgehend von den grundlegenden Sicherheits-Standards der Normenreihe ISO 27000 wurde eine Erweiterung zur Anwendung im EVU-Umfeld spezifiziert:
  - DIN/ISO 27001 definiert Anforderungen an das Informationssicherheits-Managementsystem (ISMS) und die umzusetzenden Kontrollziele.
  - DIN/ISO 27002 definiert Maßnahmen zur Umsetzung der Kontrollziele in den Bereichen Organisation, Prozesse, Betrieb und (indirekt) Technik.
  - DIN 27009 konkretisiert und ergänzt dann die ISO 27002-Anforderungen für den PDV-Bereich im EVU-Umfeld
- Vorgehen analog zur ISO 27011 für den Bereich Telekommunikation

- Berücksichtigung aller relevanten Bereiche, insbesondere auch der Organisation und des sicheren Betriebs
  - Berücksichtigung von EVU-typischen Organisationsstrukturen
  - Berücksichtigung von Anforderungen aufgrund von Regulierung
  - Konkretisierung von Anforderungen und Maßnahmen für die PDV-Technik

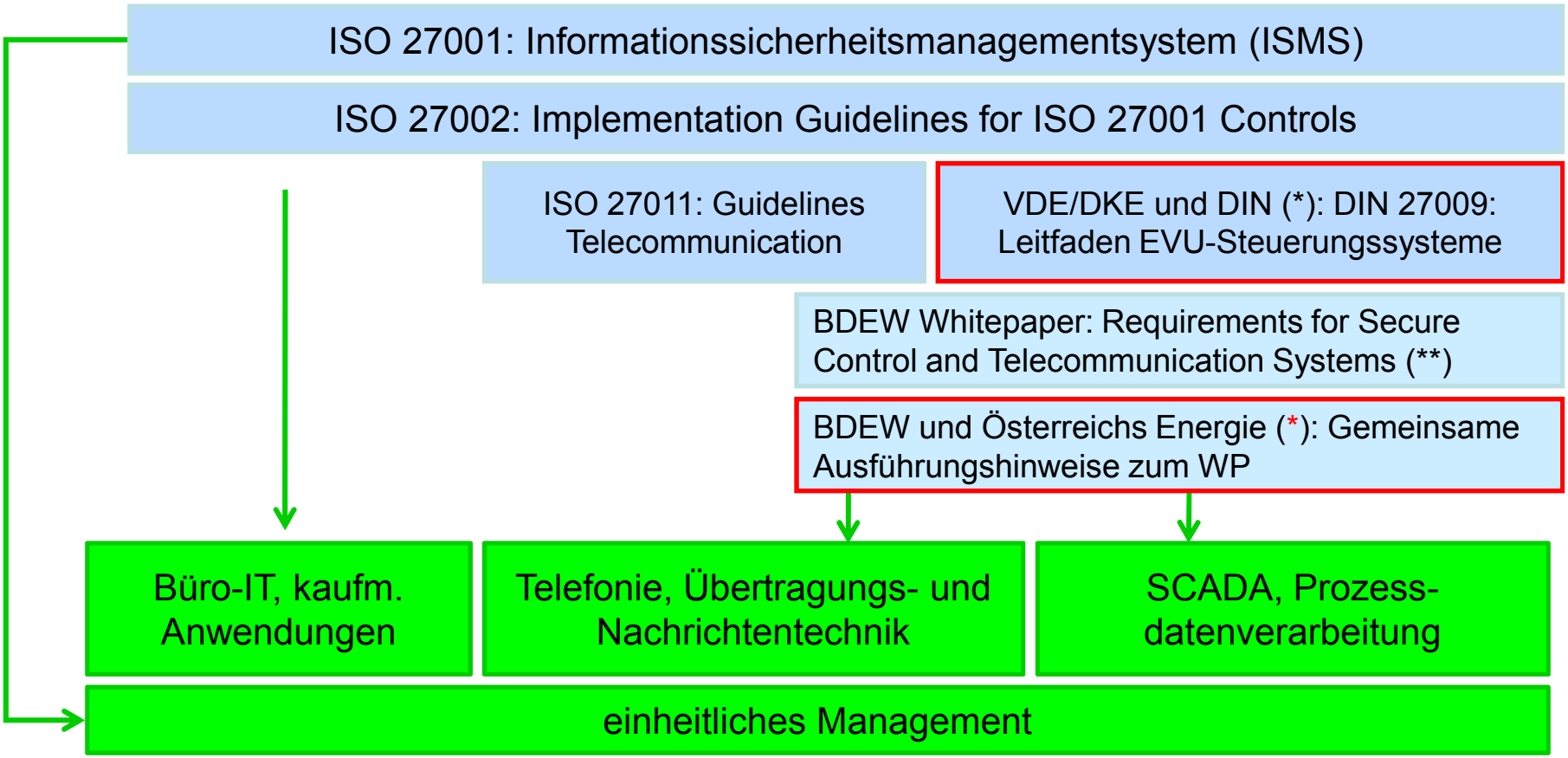
Zuordnung der Sicherheitsstandards aus der 27000er Reihe zu den Smart Grid Domänen



SCOPE der DIN SPEC 27009

- 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 Safetysysteme sowie
  - die Messtechnik inklusive der zugehörigen Kommunikations- und Fernwirktechnik.
- Diese Systeme werden im Standard unter dem vereinfachten Oberbegriff „**Prozesssteuerungs-systeme**“ zusammengefasst.

Standardisierung nach ISO/IEC 27000 in Zusammenarbeit mit weiteren Verbänden



* **Verabschiedet**

** Das bdew Whitepaper befasst sich nur mit der typischen Anwendung der Telekommunikation im Rahmen der PDV, nicht aber umfassend mit allen von der ISO 27001 erfassten Systemen.

Gliederung und Inhalte der DIN 27009

- Aufbau analog zur DIN/ISO 27002:
  - Bei unveränderten Maßnahmen/Controls Verweis auf 27002-Abschnitt
  - Bei erweiterten Maßnahmen/Controls gilt der ursprüngliche 27002-Inhalt, zusätzlich wurden spezifische Inhalte in den folgenden Kategorien ergänzt
    - Umsetzungsanleitung für die Energieversorgung
    - Weitere Informationen für die Energieversorgung
  - Ergänzte Maßnahmenziele und Controls wurden in den entsprechenden 27002-Kapiteln eingefügt

- Anhang
  - Verweis auf BDEW-Whitepaper, Mapping der Maßnahmen der DIN 27009 auf die entsprechenden Sicherheitsanforderungen des Whitepapers

Beispiel

- Erweiterung
- Verweis
- Ergänzung

9.2.3 Sicherheit der Verkabelung

Die Maßnahme 9.2.3 der DIN ISO/IEC 27002:2008 wird wie folgt erweitert:

Umsetzungsanleitung für die Energieversorgung

Speziell im Umfeld von Transport- und Verteilnetzen sind die Kommunikationsnetzwerke großräumig in der Fläche installiert, um die Kommunikation mit den Außenstandorten und Fernzugriffe zu ermöglichen. Häufig ist es dabei nicht möglich, die Außenverkabelung auf einem zur Innenverkabelung äquivalenten Schutzniveau abzusichern. Die damit verbundenen Risiken sollten entsprechend bewertet und soweit möglich durch zusätzliche, angepasste physische Schutzmaßnahmen reduziert werden. In Abhängigkeit der Sensibilität der übertragenen Daten sollten auch ergänzende, nicht-physische Schutzmaßnahmen wie eine kryptographische Sicherung in Betracht gezogen werden.

9.2.4 Instandhaltung von Gerätschaften

Die Maßnahme 9.2.4 der DIN ISO/IEC 27002:2008 ist entsprechend anzuwenden.

9.2.5 Sicherheit von außerhalb des Standorts befindlicher Ausrüstung

Die Maßnahme 9.2.5 der DIN ISO/IEC 27002:2008 ist entsprechend anzuwenden.

9.2.6 Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln

Die Maßnahme 9.2.6 der DIN ISO/IEC 27002:2008 ist entsprechend anzuwenden.

9.2.7 Entfernung von Eigentum

Die Maßnahme 9.2.7 der DIN ISO/IEC 27002:2008 ist entsprechend anzuwenden.

9.3 Sicherheit in Räumlichkeiten Dritter

Dieses Maßnahmenziel und zugehörige Maßnahmen sind in der DIN ISO/IEC 27002:2008 nicht enthalten.

Ziel: Schutz von Betriebseinrichtungen außerhalb von Räumlichkeiten des Energieversorgers vor physischen und umgebungsbezogenen Bedrohungen.

Erweiterungen und Ergänzungen der DIN SPEC 27009 gegenüber der ISO 27002

ISO 27002 Clause *	Extensions in DIN SPEC 27009
6 - Organization of information security	5
7 - Asset management	3
8 - Human resources security	3
9 - Physical and environmental security	11
10 - Communications and operations management	9
11 - Access control	6
12 - Information systems acquisition, development and maintenance	2
14 - Business continuity management	2
15 - Compliance	1

* **Keine Änderungen in Clause 5 und 13**

Ergänzten Sicherheitskategorien und Maßnahmenziele

Nummer	Titel	Maßnahmenziel
9.3	Sicherheit in Räumlichkeiten Dritter	Schutz von Betriebseinrichtungen außerhalb von Räumlichkeiten des Energieversorgers vor physischen und umgebungsbezogenen Bedrohungen.
10.11	Altsysteme	Zum Schutz vor durch Altsysteme entstehende Risiken, bei denen keine entsprechenden Sicherheitsmaßnahmen umgesetzt werden können.
10.12	Betriebssicher-heit	Zur Gewährleistung der Integrität und Verfügbarkeit von Funktionen der Betriebssicherheit (Safety-Funktionen).
14.2	Wesentliche Notfalldienste	Ziel: Sicherstellung der Verfügbarkeit wesentlicher Notfalldienste im Falle von Großstörungen, Naturkatastrophen, Unfällen oder anderen weitreichenden Notfallsituationen.

Überblick der ergänzten Maßnahmen (1/3)

Nummer	Titel	Maßnahme
9.1.7	Sichern von Leitstellen	Maßnahmen zur Gewährleistung der physischen Sicherheit von Leitstellen mit zentralen Prozesssteuerungssystemen wie Steuerungsservern, MMI-Systemen und unterstützende Systemen, sollten konzipiert, entwickelt und umgesetzt werden.
9.1.8	Sicherung von Technikräumen	Maßnahmen zur Gewährleistung der physischen Sicherheit von Technikräumen für Prozesssteuerungssysteme der Energieversorgung sollten konzipiert, entwickelt und umgesetzt werden.
9.1.9	Sicherung von Außenstandorten	Maßnahmen zur Gewährleistung der physischen Sicherheit von dezentralen Außenstandorten, an denen Prozesssteuerungssysteme der Energieversorgung betrieben werden, sollten konzipiert, entwickelt und umgesetzt werden.
9.3.1	Betriebseinrichtung in Bereichen anderer Energieversorger	Wenn Energieversorger Betriebseinrichtungen außerhalb der eigenen Gelände oder Räumlichkeiten in den Verantwortungsbereichen anderer Versorger betreiben, wie beispielsweise in Übergabestationen, sollte die Betriebseinrichtung in einem gesicherten Bereich positioniert werden…

Überblick der ergänzten Maßnahmen (2/3)

Nummer	Titel	Maßnahme
9.3.2	Betriebsein-richtung beim Kunden vor Ort	Wenn Energieversorger Betriebseinrichtungen beim Kunden vor Ort betreiben, z. B. um die Energielieferung zu steuern, zu messen und/oder um zusätzliche Dienste bereitzustellen, sollte die Betriebseinrichtung geschützt werden…
9.3.3	Gekoppelte Steuerungs- und Kommunikations-systeme	Wenn Prozesssteuerungssysteme und zugehörige Kommunikationsverbindungen mit externen Dritten gekoppelt werden, sollten die Verantwortungsgrenzen und Schnittstellen zu allen externen Beteiligten klar definiert und spezifiziert werden, so dass jedes Unternehmen in einem angemessenen Zeitraum abgetrennt und isoliert werden kann…
10.6.3	Sicherung der Prozessdaten-kommunikation	Maßnahmen zur Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit der internen und externen Prozessdatenkommunikation sollten in Abhängigkeit der Sensibilität der übertragenen Daten konzipiert, entwickelt und umgesetzt werden.
10.11.1	Behandlung von Altsystemen	Alle herkömmlichen Prozesssteuerungssystemtechnologien, Systeme und Komponenten (Legacy-Systeme) sollten mit ihren potentiellen Informationssicherheitsschwachstellen identifiziert werden…

Überblick der ergänzten Maßnahmen (3/3)

Nummer	Titel	Maßnahme
10.12.1	Integrität und Verfügbarkeit von Funktionen der Betriebssicherheit	Die Integrität und Verfügbarkeit von Informationswerten (Information Assets), Systemen, Komponenten und Funktionen, die zur Gewährleistung der Betriebssicherheit (Safety) benötigt werden, sollte im Einklang mit den branchenspezifische Normen und Gesetzen sichergestellt werden.
11.4.8	Logische Anbindung von externen Prozess-steuerungs-systemen	Vor der logischen Kopplung von Prozesssteuerungssystemen und den zugehörigen Kommunikationsverbindungen mit externen Dritten, sollte vom Energieversorger sichergestellt werden, dass ausschließlich erlaubte Kommunikation und Informationsflüsse sowie berechtigte Steuerbefehle und Meldungen über die Kommunikationsverbindung ausgetauscht werden können…
14.2.1	Notfall-Kommunikation	Im Falle von Großstörungen, Naturkatastrophen, Unfällen oder anderen möglichen Notfallsituationen sollten Energieversorger sicherstellen, dass wichtige Kommunikationsverbindungen mit dem eigenen Notfallpersonal oder dem Notfallpersonal anderer Versorger, wichtigen Prozesssteuerungssystemen und externen Notfall-Organisationen, die zum Schutz, zur Behandlung oder zur Wiederherstellung nach solchen Vorfällen notwendig sind, zur Verfügung stehen.

Internationalisierung der DIN SPEC 27009 über ISO/IEC JTC1 SC27 IT Security techniques

- Juli 2010
  Idee zur 27009 wird in einer gemeinsamen Sitzung von DKE und DIN entwickelt
- März 2012
  Die Englische Übersetzung der 27009 wurde mit einen Berichtsentwurf der Working Group Smart Grid Information Security (WG SGIS) bei CEN - CENELEC - ETSI europaweit verteilt
- April 2012
  Seit dem 1.4.2012 ist die DIN SPEC 27009 in Deutschland veröffentlicht
- Mai 2012
  Der DIN hat die englische Übersetzung der 27009 bei der SC27 Sitzung in Stockholm als nationalen Beitrag zur Smart Grid Normung vorgestellt
- Juni 2012
  Aufgrund des internationalen Feedbacks will der DIN die 27009 als FASTTRACK über JTC 1 in die internationale Normung einbringen.

Nächste Stritte hier in Deutschland

- Erstanwender der 27009 treffen hier auf 2 Problemlagen
  1. Wie organisiert man ein schlankes ISMS im Prozessbereich bzw. im Unternehmen ?
  2. Und wie setzt man die Controls des Standard nun konkret um ?
- Ad. 1) Bereitstellung von branchenspezifischen Leitfäden, Richtlinien und Verfahrensbeschreibungen
  - ISMS Rahmenpolicy und operative ISMS Policy
  - Anforderung beim Neubau:
    - BDEW Whitepaper „sichere TK- und Steuerungssysteme (2008)
    - Ausführungshinweise zum BDEW WP (2011)
  - Sicherer IT-Betrieb und Betriebskonzepte in der PDV
  - Sicherheitsrichtlinie Dienstleister
  - ISMS Reporting
  - ISMS Implementierung in kleinen Energieunternehmen
- Ad. 2) Bereitstellung von Umsetzungshinweisen
  - Zentrale und dezentrale Leittechnik
  - Kopplung zwischen Prozesswelt und Büro-IT-Welt
  - Wartungskonzepte (Wartungs-PCs und Remotezugriffe)

Fragen ?