TeleTrusT
Pioneers in IT security.

Informationstag "IT-Sicherheit im Smart Grid"

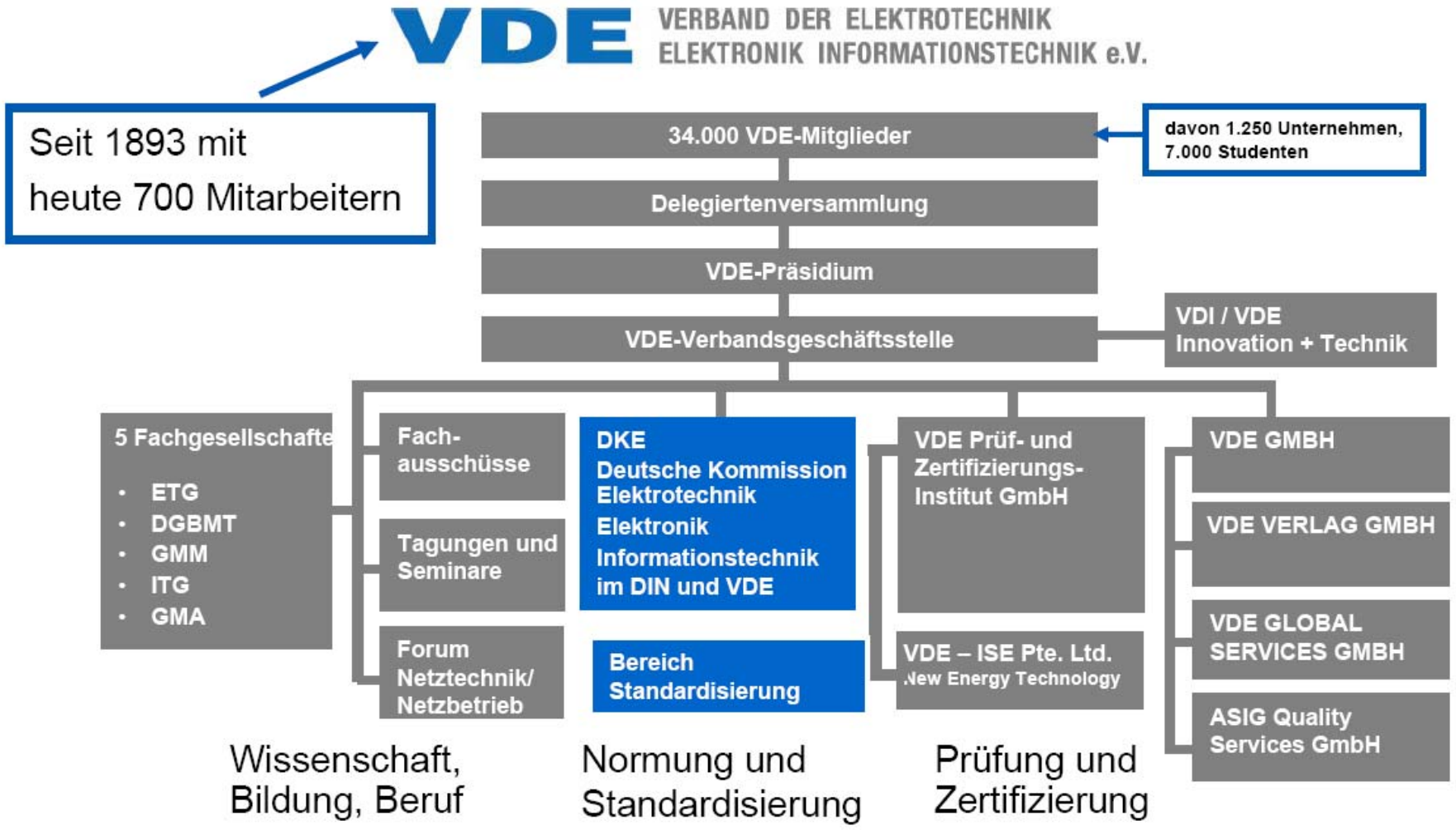
Berlin, 13.06.2013

Informationssicherheit in der Normung für das zukünftige intelligente Energienetz

Dipl.-Ing. Andreas Harner

DKE Deutsche Kommission
Elektrotechnik Elektronik Informationstechnik im DIN und VDE

VDE und DKE


VDE
VERBAND DER ELEKTROTECHNIK
ELEKTRONIK INFORMATIONSTECHNIK e.V.
Seit 1893 mit
heute 700 Mitarbeitern
34.000 VDE-Mitglieder
davon 1.250 Unternehmen,
7.000 Studenten
Delegiertenversammlung
VDE-Präsidium
VDE-Verbandsgeschäftsstelle
VDI / VDE
Innovation + Technik
5 Fachgesellschafte
ETG
DGBMT
GMM
ITG
GMA
Fach-
ausschüsse
Tagungen und
Seminare
Forum
Netztechnik/
Netzbetrieb
DKE
Deutsche Kommission
Elektrotechnik
Elektronik
Informationstechnik
im DIN und VDE
Bereich
Standardisierung
VDE Prüf- und
Zertifizierungs-
Institut GmbH
VDE – ISE Pte. Ltd.
New Energy Technology
VDE GMBH
VDE VERLAG GMBH
VDE GLOBAL
SERVICES GMBH
ASIG Quality
Services GmbH
Wissenschaft,
Bildung, Beruf
Normung und
Standardisierung
Prüfung und
Zertifizierung

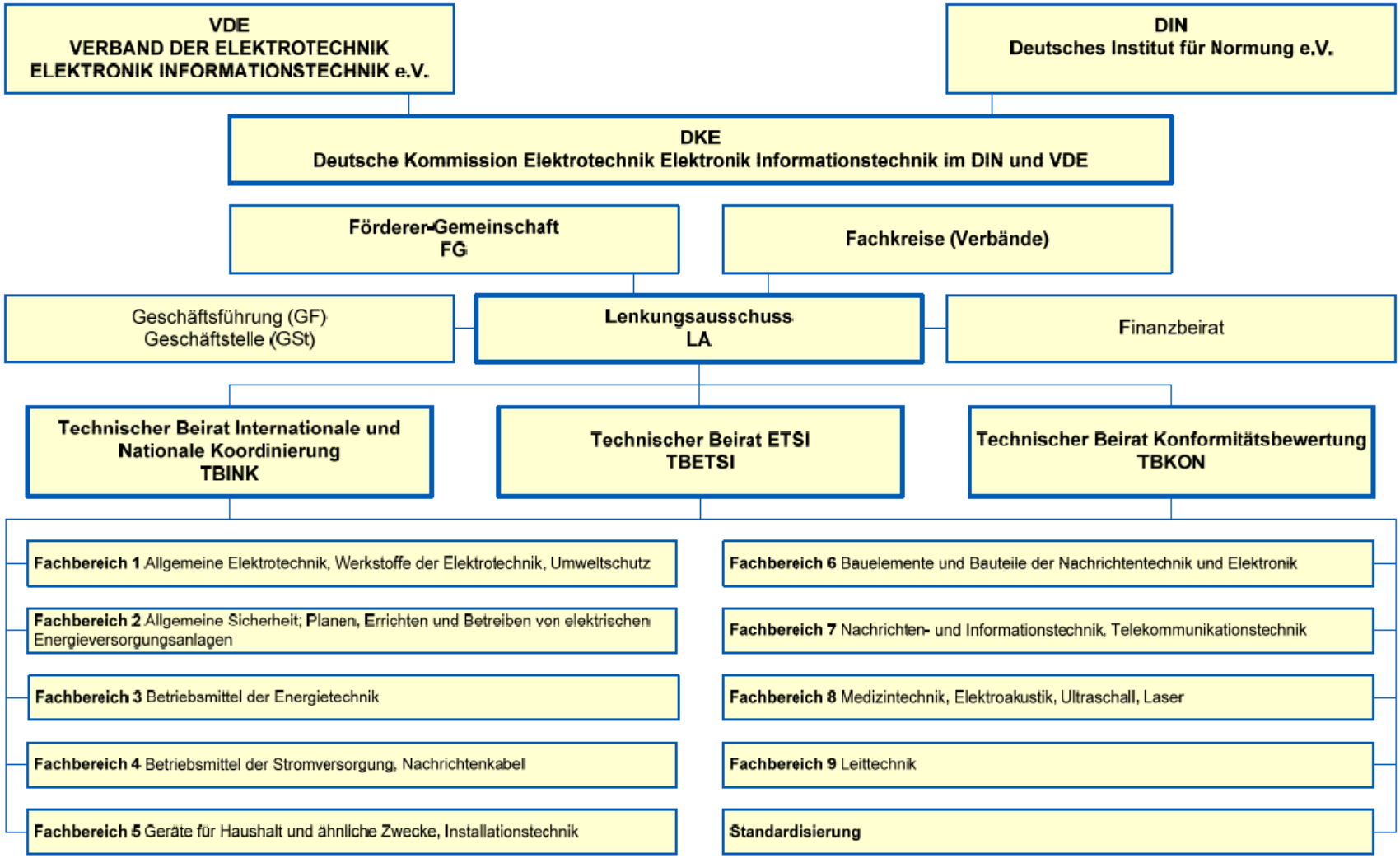
DKE
Normenvertrag

Im Jahre 1975 schlossen die Regierung der Bundesrepublik Deutschland und das DIN einen **Vertrag** folgenden Inhalts:

- **Anerkennung DIN/DKE als die zuständige Normungsorganisation** für Deutschland sowie als die Nationale Normungsorganisation in nichtstaatlichen Internationalen Normungsorganisationen
- DIN/DKE verpflichten sich, bei ihren Normungsarbeiten **das öffentliche Interesse** zu berücksichtigen
- Der Bundesregierung werden **Sitze in den Lenkungsgremien** der DIN-Normenausschüsse und der DKE eingeräumt und behördliche Stellen bei der Durchführung der Normungsarbeit beteiligt
- DIN/DKE gewährleisten die **Einhaltung der Verfahrensrichtlinien** (DIN 820) in ihren Normenausschüssen
- DIN/DKE verpflichten sich, **Anträge der Bundesregierung** auf Durchführung von Normungsarbeiten **bevorzugt zu bearbeiten**. Fristen hierzu sind abzustimmen.
- ...

DKE

Struktur der DKE



DKE
Überblick

Allgemein:

- Gemeinsames Organ von VDE und DIN (Deutsches Institut für Normung e.V.)
- Gründung 1970 als Zusammenschluss des VDE-V und des FNE
- Deutsches Mitglied in der IEC und im CENELEC
- Freier Zugang zu den DKE-Gremien sowie eine kostenfreie Teilnahme

Aufgaben:

- Erarbeiten anerkannter Regeln der Technik (Normen mit Sicherheitsfestlegungen erhalten eine VDE-Klassifikation)
- Mitarbeit bei der Veröffentlichung europäischer und internationaler Normen und Spezifikationen

Kennzahlen:

- 3.500 Technische Experten
- 290 Komitees und Unterkomitees, über 450 Arbeitskreise
- 750 Sitzungstage pro Jahr
- 40.000 Seiten (ohne ETSI)



DKE
Ziele der DKE

- **Sicherheit**
  Umfassende Sicherheit elektrotechnischer Produkte und Anlagen sowie der damit verbundenen Dienstleistungen und im Arbeitsschutz

- **Kompatibilität**
  Systemkompatibilität von Produkten und Anlagen in vernetzten Systemen und Anwendungen

- **Marktorientierung**
  Beschleunigte Marktdurchdringung neuer Technologien durch Unterstützung der Informationsprozesse mittels Normen und Spezifikationen

DKE

Ziele der DKE

- **Konsensbildung**
  Zusammenführen des Wissens und der Interessen aller betroffenen Fachkreise sowie Konsensbildung auch in kontrovers diskutierten Sachfragen

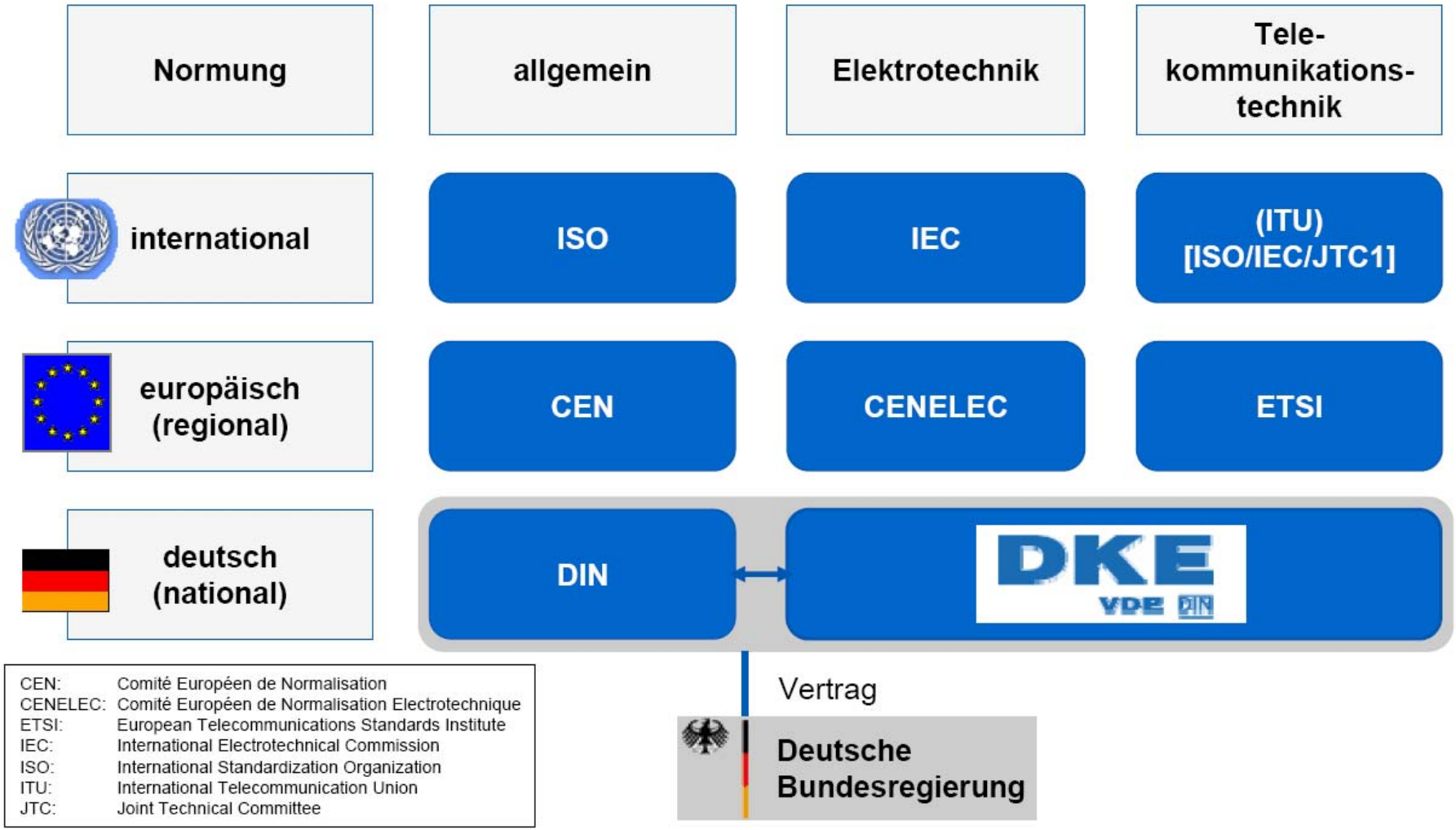
- **Interessenvertretung**
  Vertretung der deutschen Interessen bei der Weiterentwicklung der Internationalen und Europäischen Normen zum Abbau von Handelshemmnissen und zur weltweiten Öffnung der Märkte

- **Qualität**
  Qualitativ hochwertige und aktuelle technische Regeln in einem konsistenten und breit akzeptierten Normenwerk mit markt- und bedarfsorientierter Ausrichtung

- **Konformitätsbewertung**
  Weltweite Anerkennung von Konformitätsbewertungsergebnissen

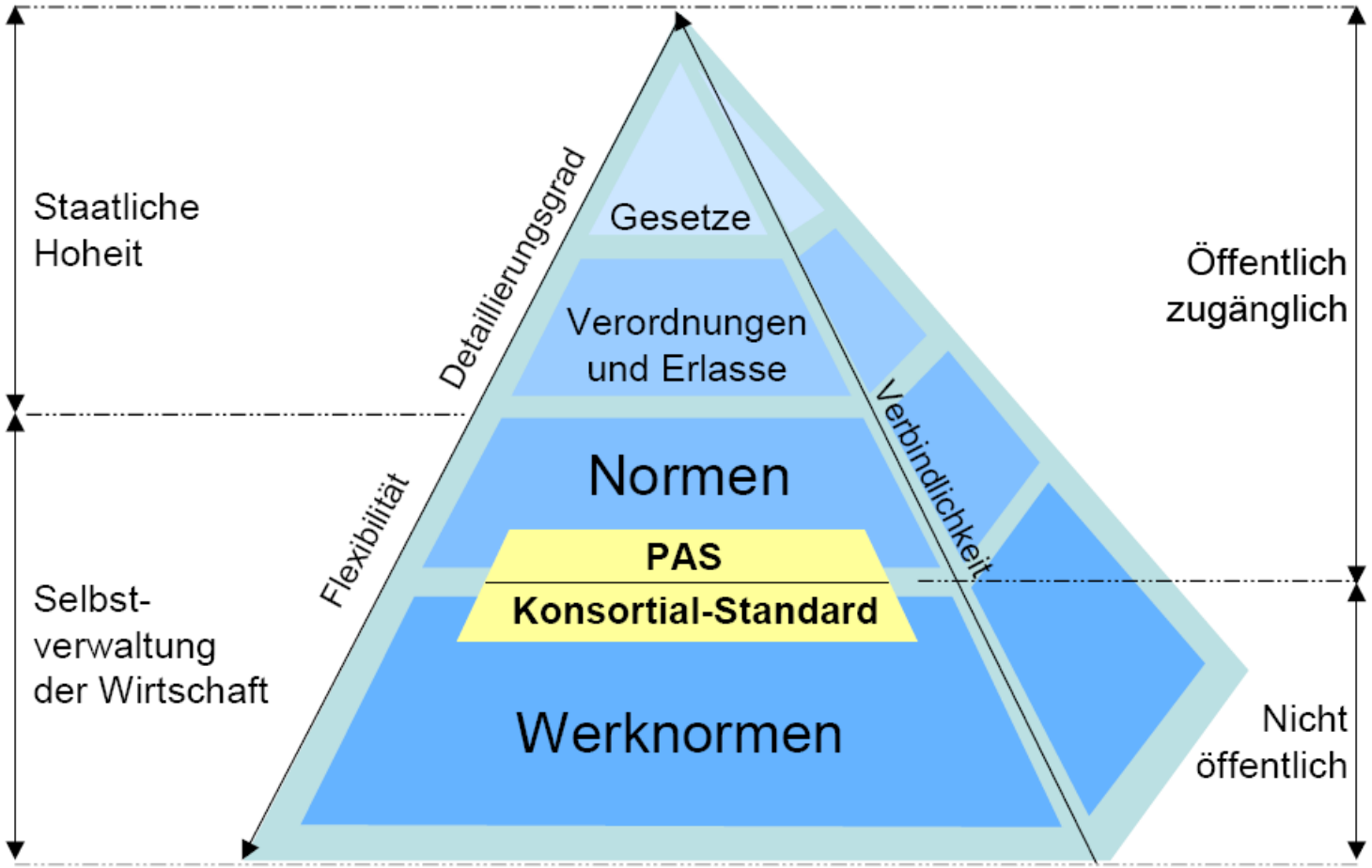
Normung und Standardisierung

Internationale Einbettung



Normung und Standardisierung

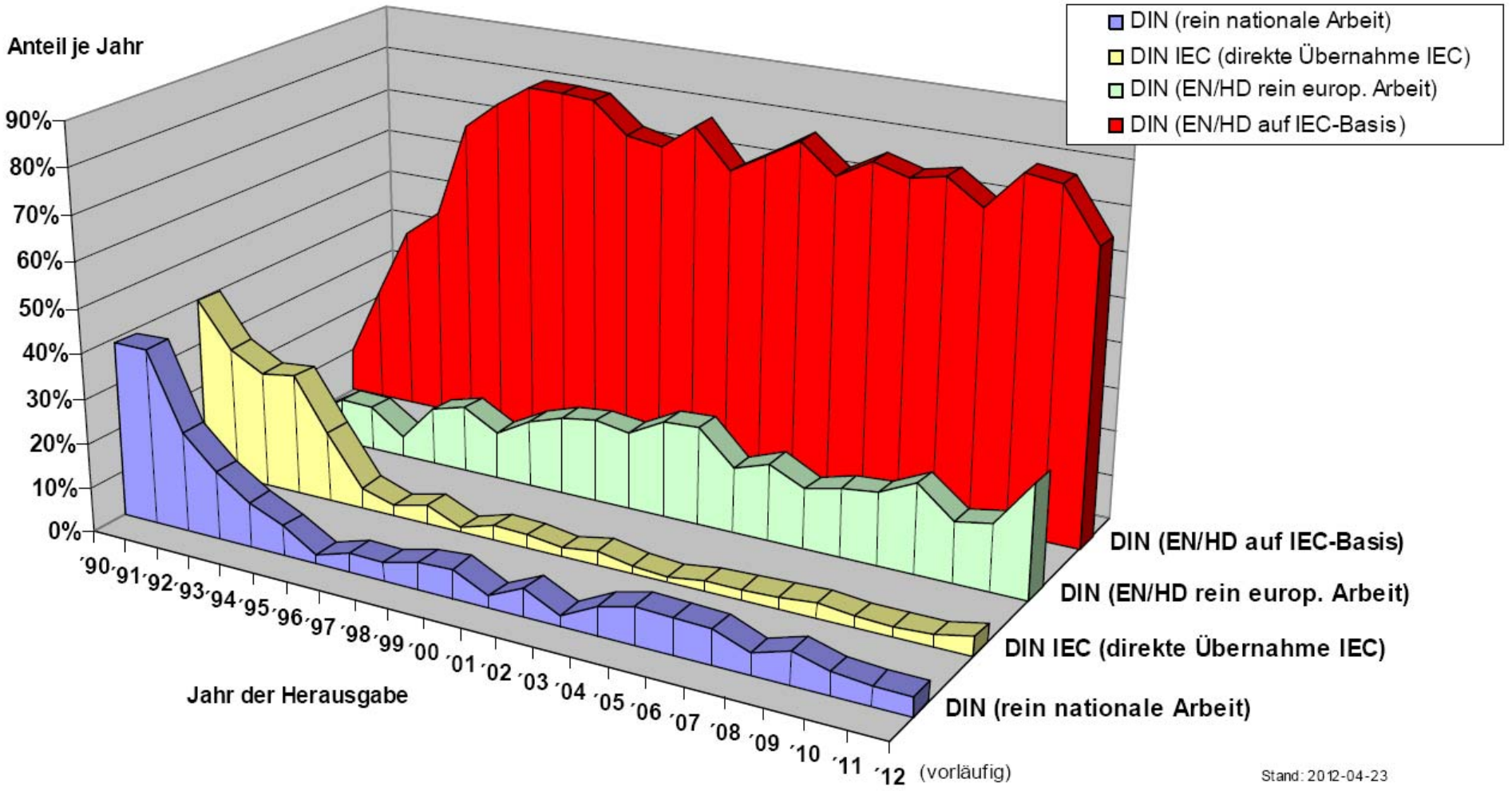
Technische Normen und Recht



PAS: Publicly Available Specification

Normung und Standardisierung

Entwicklung der elektrotechnischen Normung in Deutschland



Normung und Standardisierung

Nutzen der Normung

- Abbau von Handelshemmnissen, weltweite Marktöffnung für Produkte, Innovationen und Dienstleistungen
- Systemkompatibilität, Vereinbarkeit und Austauschbarkeit von Produkten und Anlagen
- Grundlage für Produktprüfungen: Qualität und Sicherheit
- Umfassende Sicherheit elektrotechnischer Produkte und Anlagen zum Schutz von Menschen, Tieren und Sachen
- Beschleunigung bei der Verbreitung von technischen Innovationen
- Branchen-Plattform zwischen Unternehmen, Wissenschaft, Gesellschaft und Staat

Nutzen-Effekt der Normung: 16 Mrd. Euro pro Jahr

Quelle: DIN

Smart Grid Security in der Normung

EU-Mandat M/490 - “Standards on Smart Grid“

- Weltweit sind viele Organisationen im Bereich ***„Smart Grid Security“*** aktiv:
  IEEE, ISO/IEC, CEN/CENELC, ETSI, ITU-T, CIGRE,
  IETF, ISA, NERC-CIP, NIST, DOE, DHS…..

- Vielzahl von Normen, Standards und Richtlinien
  (teilweise überlappend, fehlende Normungslandschaft)

→ Erteilung des Mandates M/490 durch die EU (DG-Energy)

Smart Grid Security in der Normung

EU-Mandat M/490 - “Standards on Smart Grid“ (2010-2012)

European Commission – DG ENERGY – M/490 Mandate

EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR ENERGY
Directorate B - Security of supply, Energy markets & Networks
B.2 - Electricity & Gas

Brussels 1st March 2011
M/490 EN

Smart Grid Mandate

Standardization Mandate
to European Standardisation Organisations (ESOs) to support
European Smart Grid deployment

Mandate Scope and Objectives

- *“ The objective of this mandate is to **develop or update a set of consistent standards** within a common European framework […] that will achieve interoperability and will enable or facilitate the implementation in Europe of […] Smart Grid services and functionalities […]. ”*
- *“ It will answer the technical and organizational needs for **sustainable “state of the art” Smart Grid Information Security (SGIS)**, Data protection and privacy (DPP), […]. “*
- *“ This will enable smart grid services through a Smart Grid information and communication system that is **inherently secure by design** within the critical infrastructure of transmission and distribution networks, as well as within the connected properties (buildings, charging station – to the final nodes).*

Smart Grid Security in der Normung

EU-Mandat M/490 - Fokus (2010-2012)

- **Technische Referenzarchitektur**
  - Integration bestehender System- und Subsystemarchitekturen
  - Darstellung der funktionalen Informationsdatenflüsse zwischen den Hauptbereichen

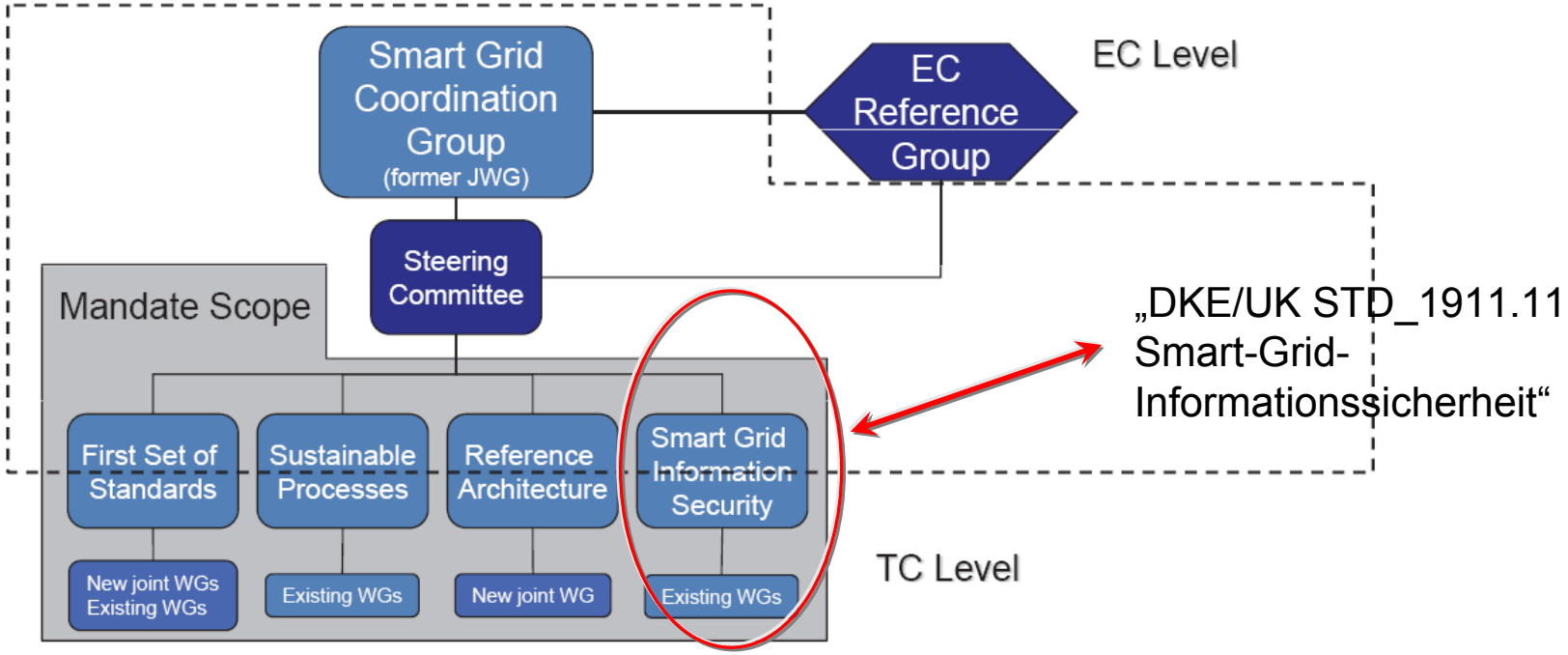
- **Kohärente Normen**
  - Förderung des Informationsaustausches (interoperable Kommunikationsprotokolle und Datenmodelle)
  - Integration aller Nutzer in den Betrieb des Stromsystems

- **Dauerhafte Normungsprozesse**
  - Anpassungen auf der Basis einer Lückenanalyse
  - Berücksichtigung grundlegender Systemauflagen:
    - → Interoperabilität
    - → Sicherheit
    - → Wahrung der Privatsphäre (Datenschutz)

Smart Grid Security in der Normung

EU-Mandat M/490 - “Standards on Smart Grid“ (2010-2012)

- Organisation:

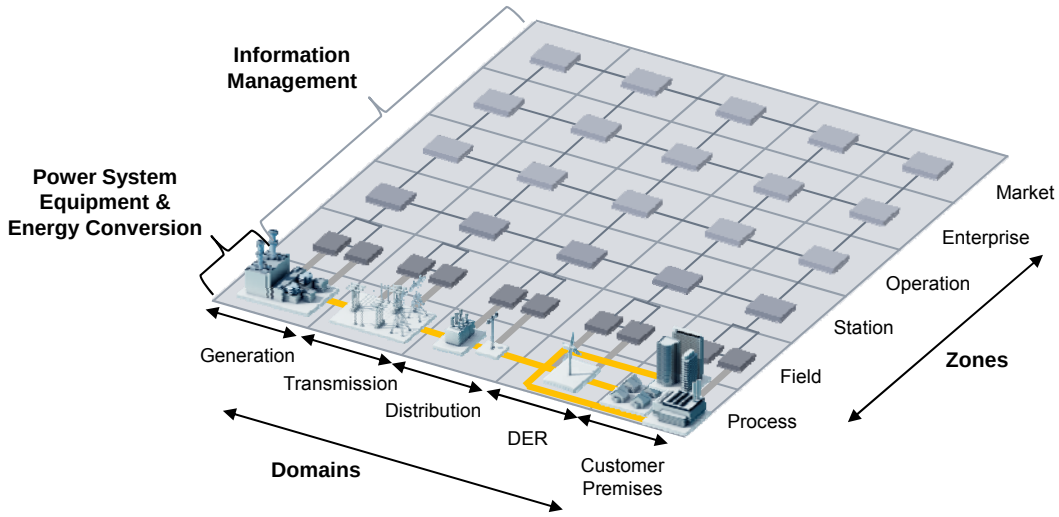


- Link der Ergebnisberichte der 4 Gruppen:
  http://www.cencenelec.eu/standards/HotTopics/SmartGrids/Pages/default.aspx
- Deutsche Normungsroadmap „E-Energy/Smart Grids 2.0“:
  http://www.dke.de/de/infocenter/seiten/artikeldetails.aspx?eslshopitemid=3ed62ad3-e1a5-4a52-bdf8-431a2b09f1f2

Smart Grid Security in der Normung

EU-Mandat M/490 - Ergebnisse - SGAM (2010-2012)

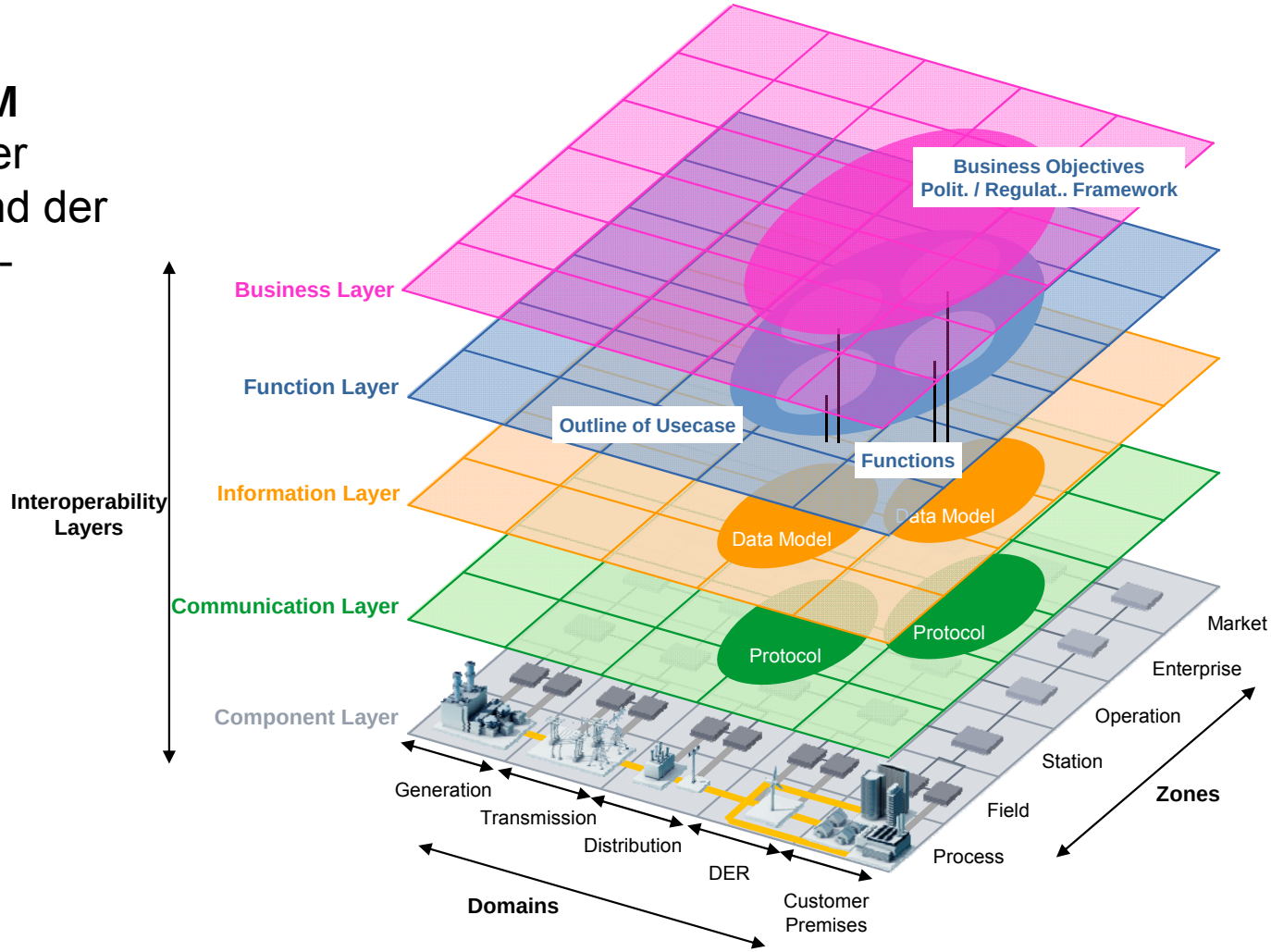
- Einführung des „Smart Grid Architecture Model (SGAM)“:
  - → abstrakte Darstellung der Smart Grid spezifischen Strukturen (Domänen und Zonen)
  - → Aspekte der Interoperabilität im Fokus
  - → Abbildung der informations- und kommunikationstechnischen Zusammenhänge
  - → Beschreibung des Ist-Zustandes (heute installierte Basis) und zukünftiger Szenarien und Migrationsschritte
  - → Erkennung von Lücken in Standards



Smart Grid Security in der Normung

EU-Mandat M/490 - Ergebnisse - SGAM (2010-2012)

Vollständiges SGAM
→ Verbindung aus der Smart-Grid-Ebene und der fünf Interoperabilitäts-schichten……..



Smart Grid Security in der Normung

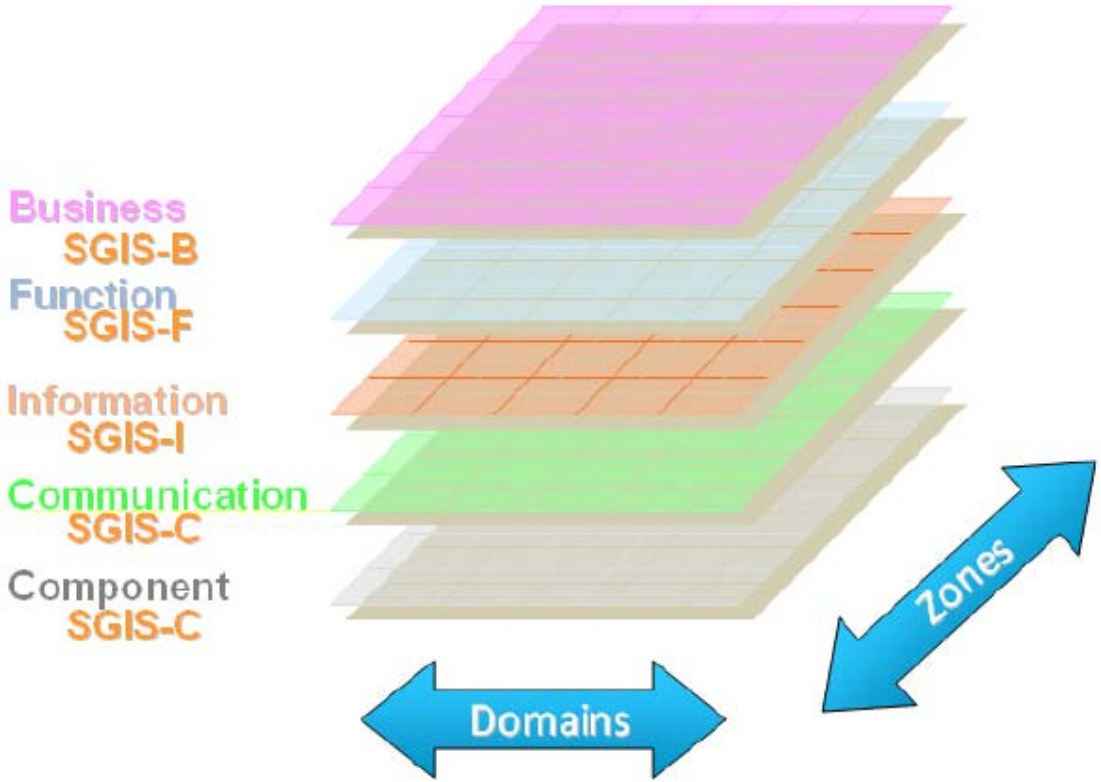
EU-Mandat M/490 – Ergebnisse - SGIS (2010-2012)

„Security view per Layer“:

Betrachtung technischer und organisatorischer Anforderungen im gesamten Smart Grid

→ Informationssicherheit ist integraler Bestandteil des SGAM!

→ Informationssicherheit hat Auswirkungen auf alle Schichten, Domänen und Zonen des Modells! („Schattenlayer“)



Smart Grid Security in der Normung

EU-Mandat M/490 - “SGIS-Anforderungen“

- Keine Priorisierung der Schutzziele: Vertraulichkeit, Integrität und Verfügbarkeit
- Schutzziele sind im Hinblick auf Wirtschaftlichkeit und Zweckmäßigkeit anzuwenden
- Abgeleitete Maßnahmen sind für jeden Use Case spezifisch zu bewerten und zu gewichten
  (Hilfestellung durch die „SGIS-Toolbox“)

Smart Grid Security in der Normung

EU-Mandat M/490 – SGIS Security levels (SGIS-SL) (2010-2012)

- *„SGIS - Security Levels (SGIS-SL) have been defined with the objective to create a bridge between electrical grid operations and information security“*
- Zur Quantifizierung des Schutzbedarfes
- Die Zuordnung eines Use Cases zu einem SL ist abhängig vom potentiellen Schaden und der Wahrscheinlichkeit

Security Level	Security Level Name	Europeans Grid Stability Scenario Security Level Examples
5	Highly Critical	Assets whose disruption could lead to a power loss above 10 GW Pan European Incident
4	Critical	Assets whose disruption could lead to a power loss from above 1 GW to 10 GW European / Country Incident
3	High	Assets whose disruption could lead to a power loss from above 100 MW to 1 GW Country / Regional Incident
2	Medium	Assets whose disruption could lead to a power loss from 1 MW to 100 MW Regional / Town Incident
1	Low	Assets whose disruption could lead to a power loss under 1 MW Town / Neighborhood Incident

Smart Grid Security in der Normung

EU-Mandat M/490 – Data Protection Class (SGIS-DPC) (2010-2012)

- Zwei Datenklassen:
  → mit Personenbezug (DPC1)
  → ohne Personenbezug (DPC2)

SG-DPC 1 Personal Information
Sensitive Personal Information
Personal Information
De-personalized Pseudonym zed Personal information
No Personal information

SG-DPC 2 System Information
System Data (i.e. Firmware), Configuration Data, Customer Credentials, Private & Public Keys, Roles /Actor IDs
Governance & Reporting Information, Logging and Audit Information
Audit & Log required information
Information to administrate remotely
Information to operate remotely (Control signals)
Business Information
Measurement data

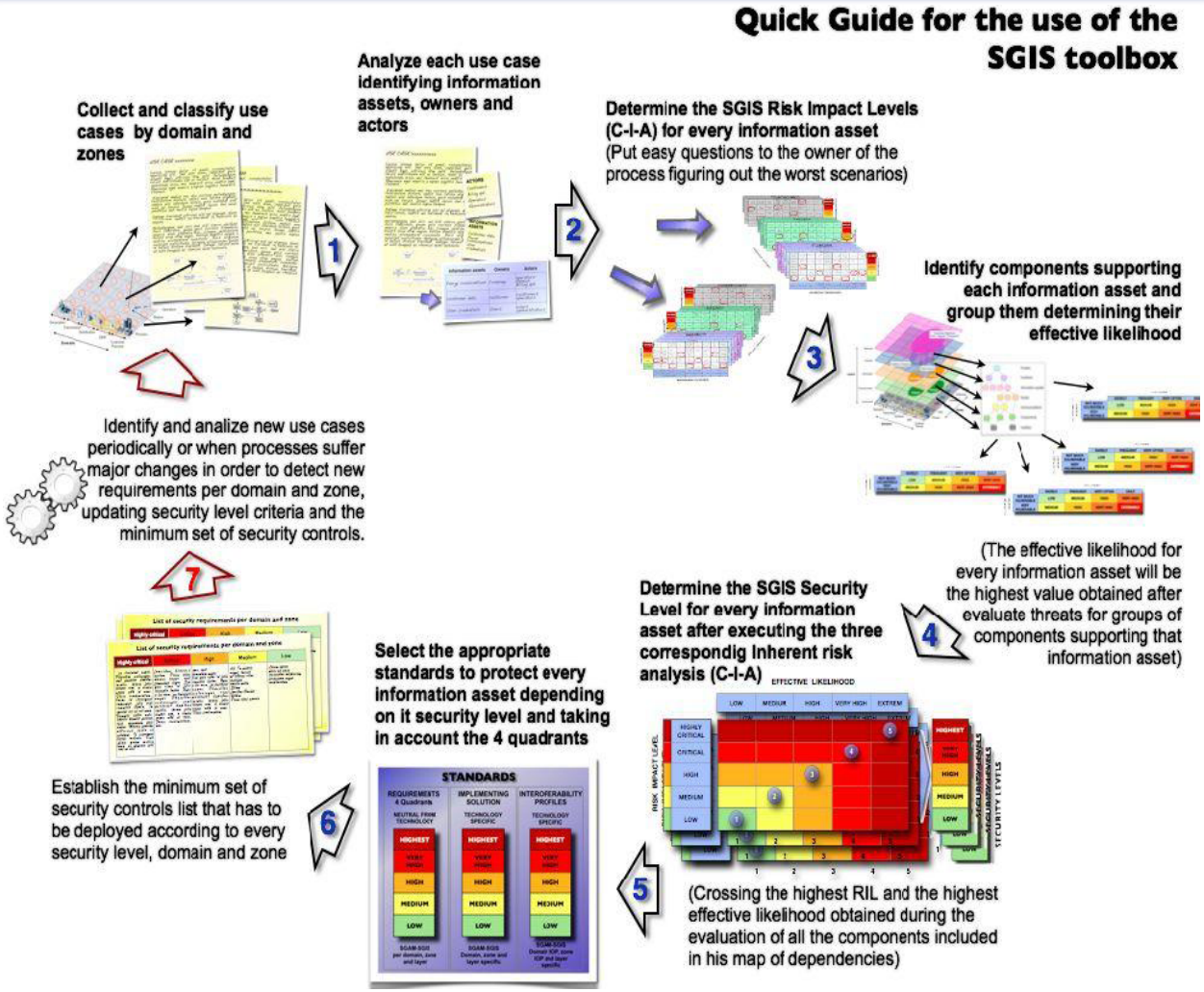
Smart Grid Security in der Normung

EU-Mandat M/490 - “SGIS-Toolbox“

Die SGIS-Toolbox soll die Frage…

How to integrate security in the „General Smart Grid Use Case Analysis Framework“ ?

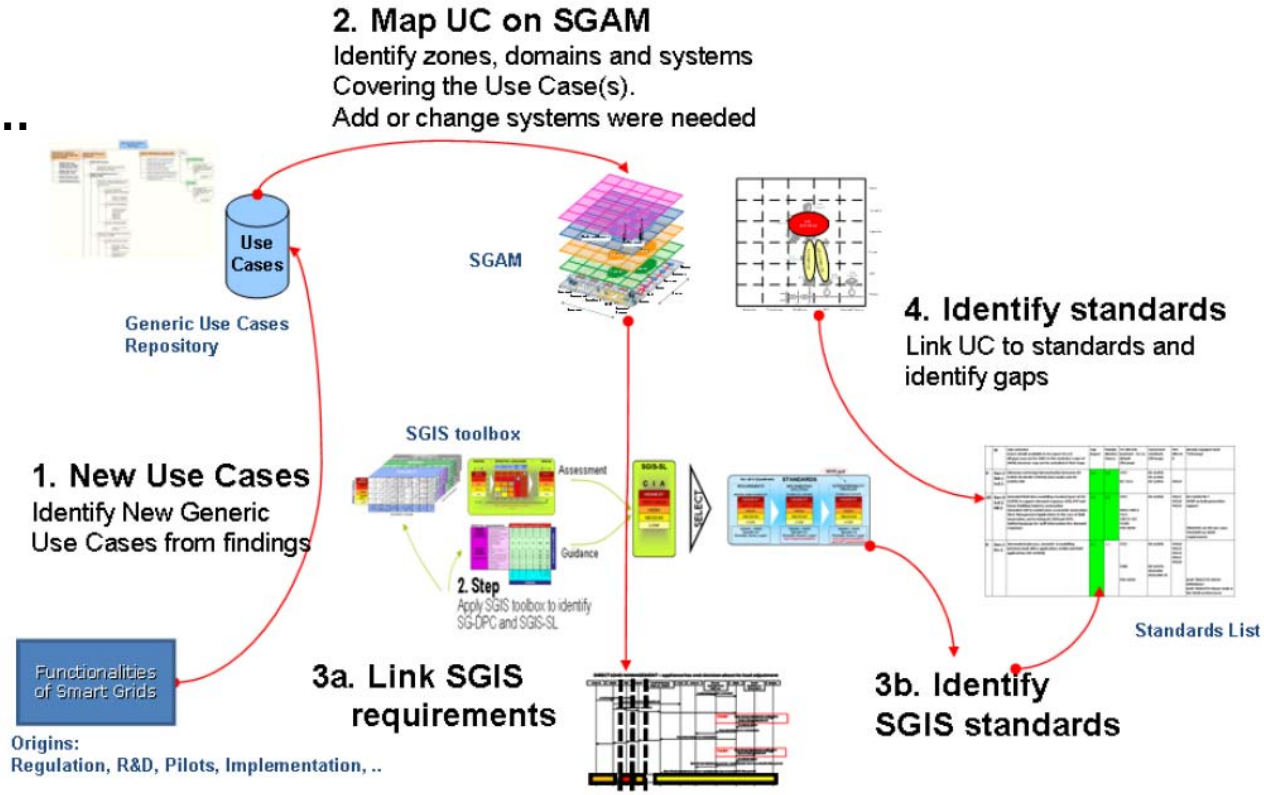
beantworten…



Smart Grid Security in der Normung

EU-Mandat M/490 – „Smart Grid Use Case General Framework"

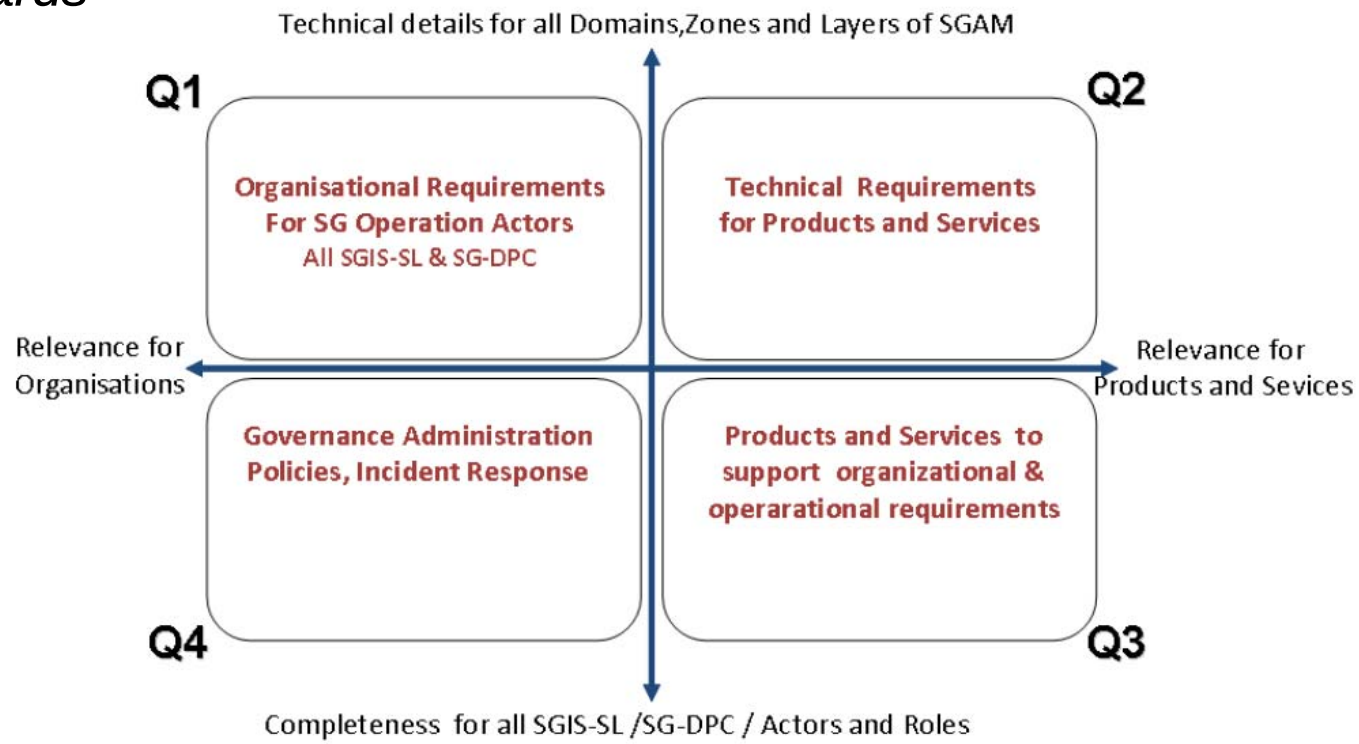
Von Use Cases
zu Lücken in Security
Standards und Normen…



Smart Grid Security in der Normung

EU-Mandat M/490 – SGIS-Normungslandschaft (2010-2012)

- *Analyse der Standards in 4 Quadranten*

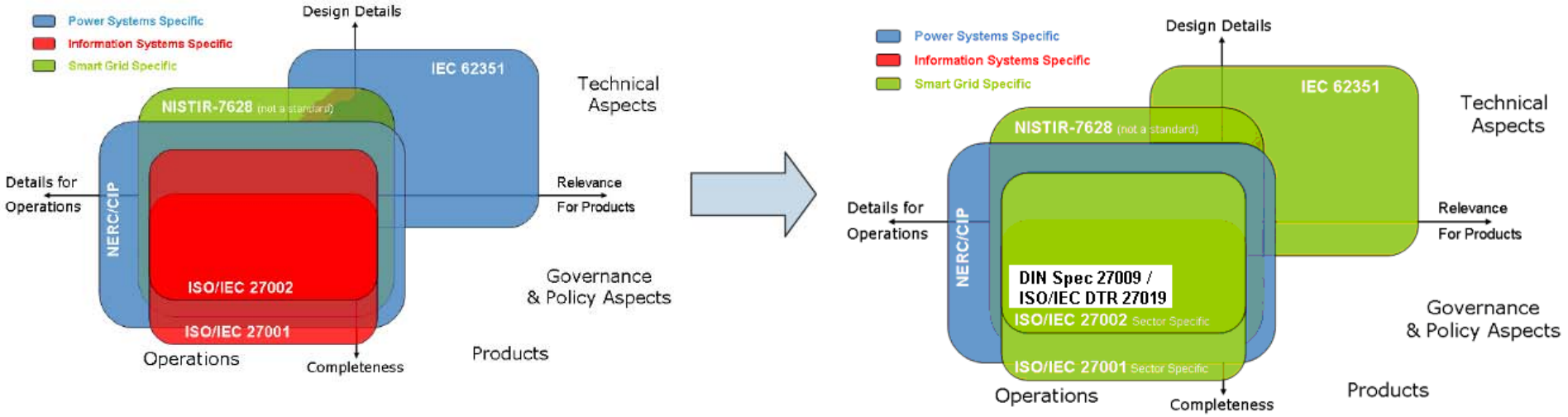


- *„Organisations“ = Smart Grid Operators*

Smart Grid Security in der Normung

EU-Mandat M/490 – SGIS-Normungslandschaft (2010-2012)

- Relevante Normen, die untersucht wurden:
  - ISO/IEC 27001
  - ISO/IEC 27002
  - IEC 62351
  - NERC CIP (US Standard)
  - NISTIR-7628 (US Guidelines)



Smart Grid Security in der Normung

EU-Mandat M/490 – Resumee (2010-2012)

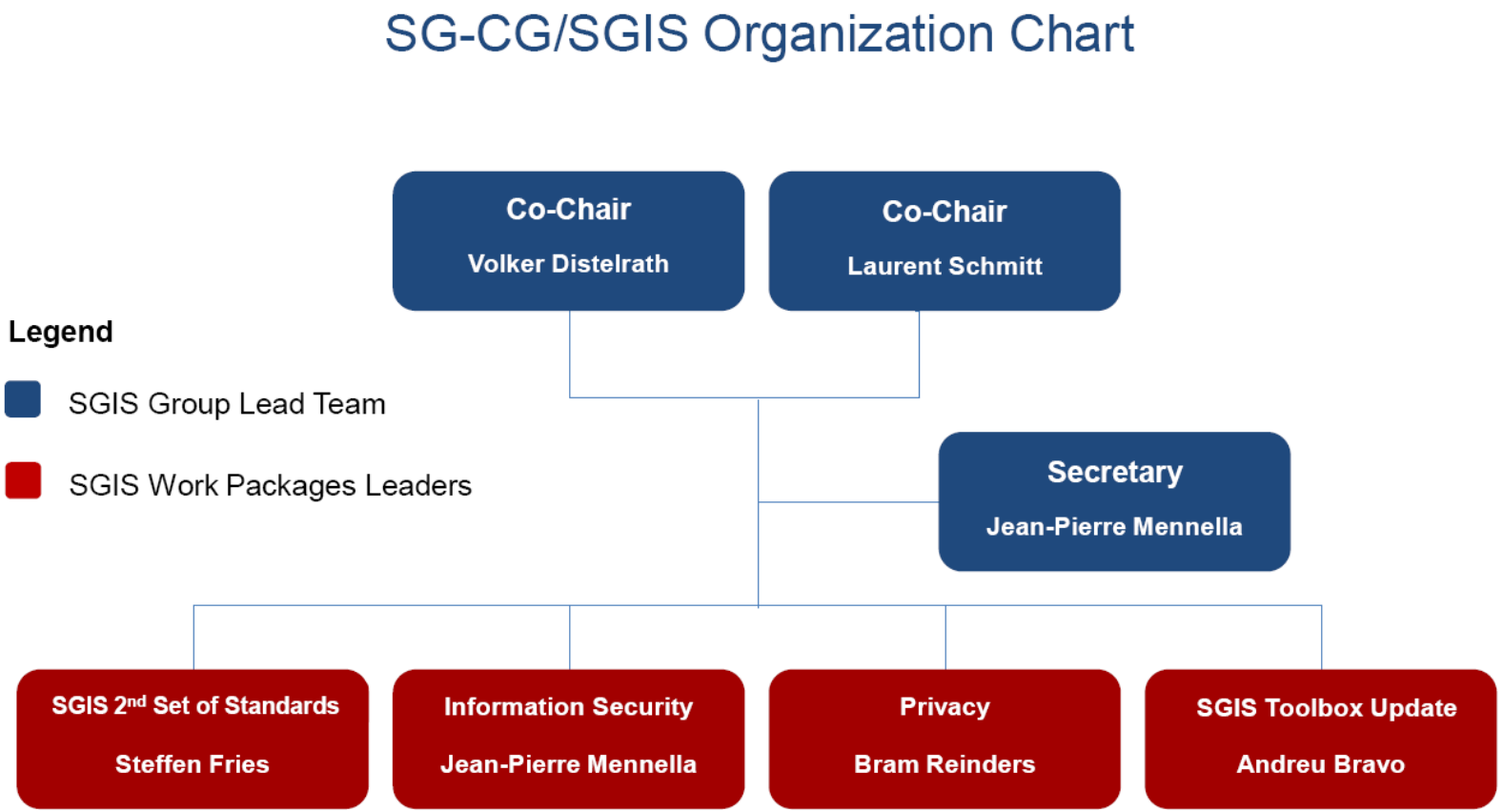
Die SGIS stellt in ihrem Bericht Ende 2012 fest:

- → relevanten Normen, um eine grundlegende Informationssicherheit im Smart Grid zu etablieren, sind verfügbar
- → Die Notwendigkeit der Erweiterung der bestehenden Normen und die Entwicklung neuer Normen besteht trotzdem, um Smart-Grid-spezifische Anforderungen an die Informationssicherheit zu integrieren
- → Besonderer Augenmerk soll dabei auf die Implementierbarkeit der Normen sowohl in Organisationen als auch in Systemkomponenten gelegt werden
- → „Security-by-Design“ und „Security-by-Default“ müssen in allen Phasen des Produktlebenszyklus berücksichtigt werden
- → Garantierte Interoperabilität soll im Fokus der zukünftigen SGIS-Aktivitäten stehen

Smart Grid Security in der Normung

EU-Mandat M/490 – Teil 2 (2013 – 2014)

- SGIS in 4 Untergruppen aufgeteilt:



Smart Grid Security in der Normung

EU-Mandat M/490 – Teil 2 (2013 – 2014)

- **WP1:** Gap Analysis Fortsetzung für
  - IEC 62351
  - ISO 270xx
  - ISO/IEC 19790 Security Requirements for crypt. Modules
  - ISO/IEC 15408 Common Criteria
  - IEC 62443 Security for industrial automation and control

- **WP2:** Best practices and Use Cases

- **WP3:** Privacy (u.a. PIA für Use Cases bestimmter Länder)

- **WP4:** Weiterentwicklung der SGIS Toolbox

- Spiegelung in Deutschland:
  „DKE/UK STD_1911.11 Smart Grid Informationssicherheit“

Smart Grid Security in der Normung

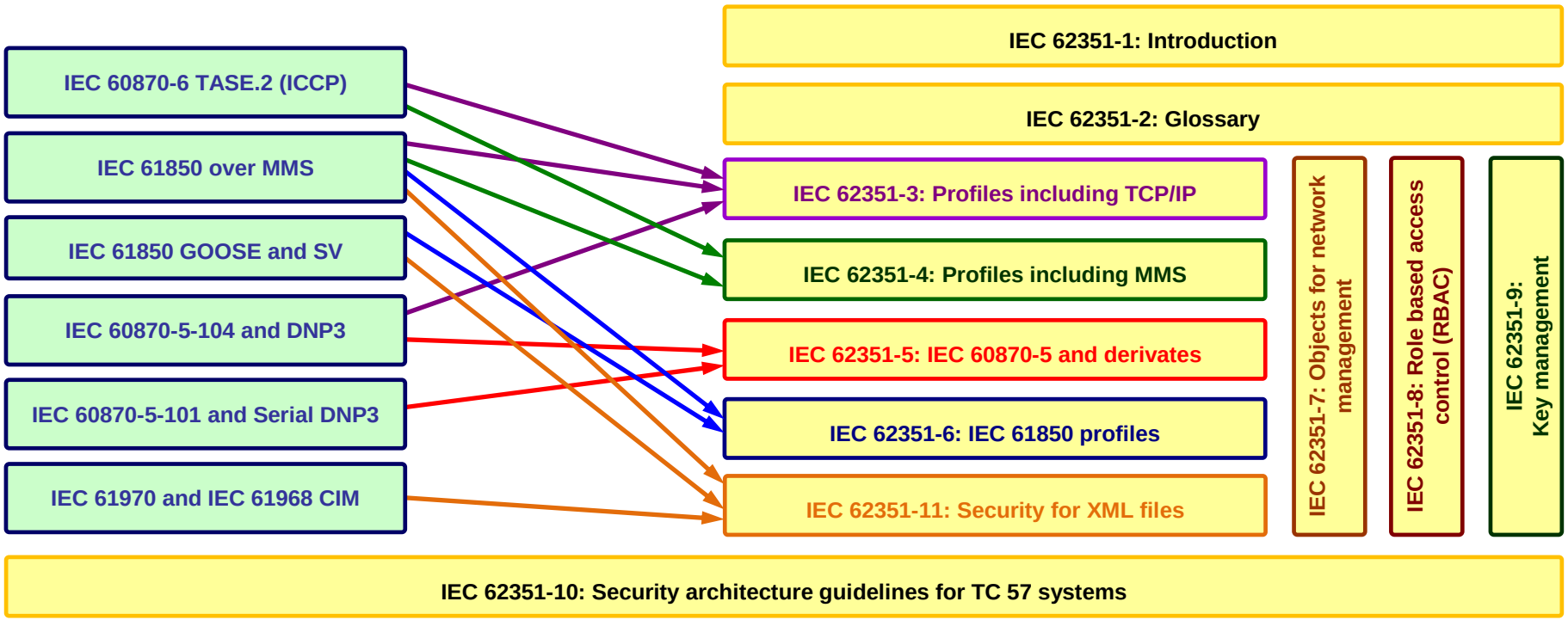
IEC TC 57 WG 15 – IEC 62351

- 11-teilige Normenreihe
- In Deutschland:
  DKE/AK 952.0.15
  "DKE-ETG-ITG Informationssicherheit in der Netz- und Stationsleittechnik"
- In internationalen Studien als zentraler, technischer Standard für Smart Grids adressiert
- Die Informationssicherheit wird als „Ende-zu-Ende-Anforderung“ gesehen, um die Schutzziele in der kritischen Infrastruktur der Netzführungssysteme zu erreichen

Smart Grid Security in der Normung

IEC TC 57 WG 15 – IEC 62351

- Kommunikationsstandards und ihre Relation zu den Teilen der IEC 62351:



Smart Grid Security in der Normung

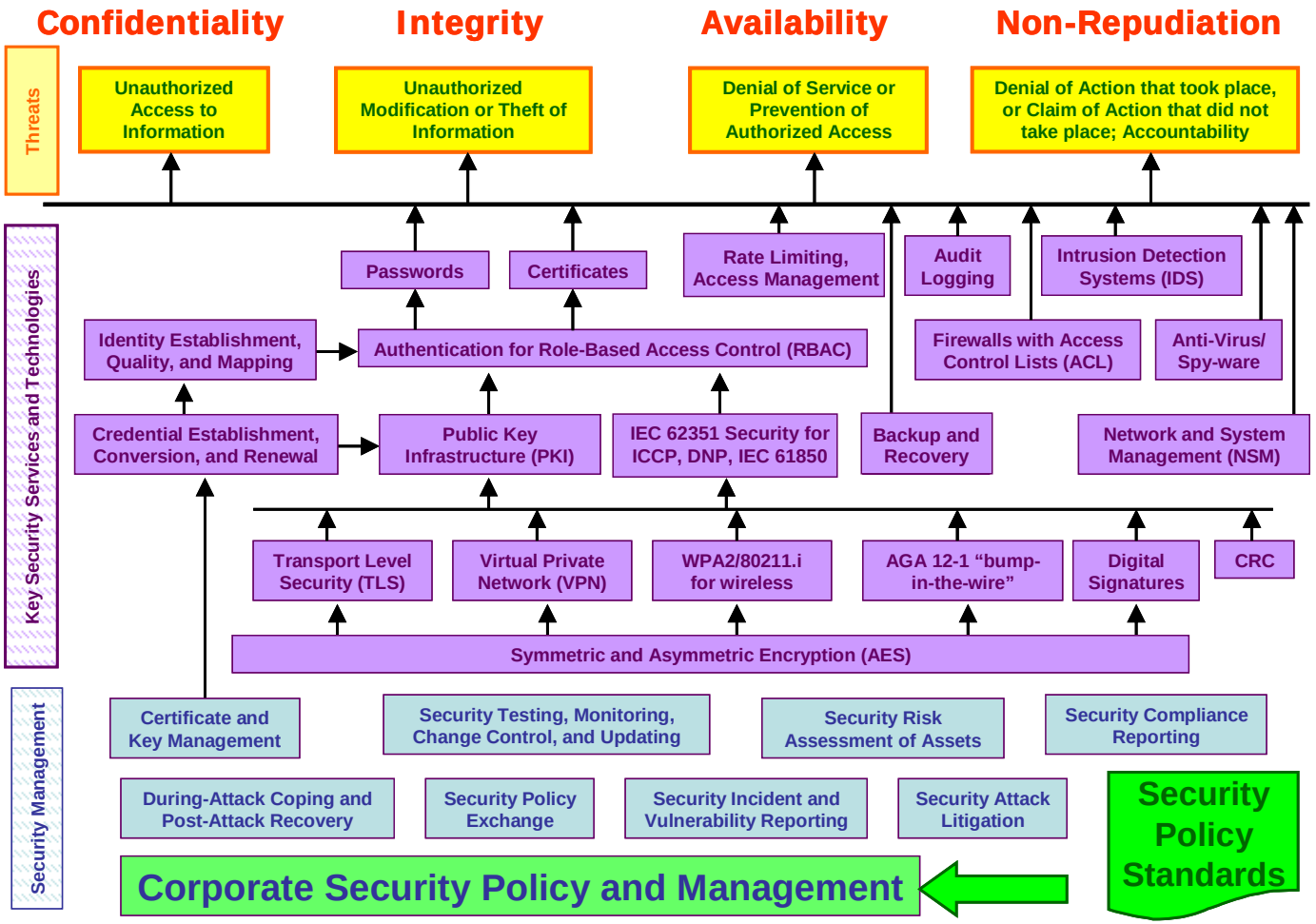
IEC TC 57 WG 15 – IEC 62351

- **IEC 62351-1: Einführung**

  Dieser Teil der Norm liefert einen Überblick und Hintergrundinformationen zum Thema Informationssicherheit in der Energiedomäne und den dort geltenden Besonderheiten. Zudem werden die relevanten Schutzziele (Confidentiality – Integrity – Availability – Non-Repudiation) und entsprechende Maßnahmen grob vorgestellt, um sich gegen bestimmte Bedrohungen zu schützen (s. Folgefolie)

Smart Grid Security in der Normung

IEC TC 57 WG 15 – IEC 62351-Schutzziele-Bedrohungen-Maßnahmen



IEC 614/07

Smart Grid Security in der Normung

IEC TC 57 WG 15 – IEC 62351

- **IEC 62351-2: Glossar**

  Begriffe und Abkürzungen

- **IEC 62351-3: Informationssicherheit – Profile basierend auf TCP/IP**

  Teil 3 der Norm beschäftigt sich mit TCP/IP-basierenden Protokollen der Netzleittechnik. Dafür wird zur Erreichung von Authentisierung, Vertraulichkeit und Integrität der Einsatz von Transport Layer Security (TLS) spezifiziert: Zum Beispiel werden optionale TLS-Bestandteile verbindlich vorgeschrieben und spezielle Anforderungen der Netzleittechnik an die zu nutzenden Zertifikate spezifiziert. Dieser Teil befindet sich derzeit in der Überarbeitung zu einer Edition 2. Dabei werden zum einen weitere TLS-Mechanismen profiliert als auch die verwendeten Cipher Suites aktualisiert.

Smart Grid Security in der Normung

IEC TC 57 WG 15 – IEC 62351

- **IEC 62351-4: Informationssicherheit – Profile basierend auf MMS**

  Im vierten Teil werden die Sicherheitserweiterungen für Protokolle definiert, die MMS (Manufacturing Message Specification, ISO 9506)) einsetzen. MMS wird für Messaging-Systeme mit Echtzeitanforderungen in der Netzleittechnik eingesetzt. Teil 4 definiert dazu TLS-basierte Prozeduren auf der Transport- und Applikationsschicht basierend auf dem Profil aus Teil 3. Derzeit werden Korrekturen, die sich aufgrund von Interoperabilitätstests ergeben haben, als Ergänzung definiert. Weiterhin ist geplant, eine Edition 2 zu erarbeiten

Smart Grid Security in der Normung

IEC TC 57 WG 15 – IEC 62351

- **IEC 62351-5: Informationssicherheit – Sicherheit für IEC 60870-5 und Derivate**

  Teil 5 der Normenreihe berücksichtigt die Besonderheiten serieller Kommunikation. Dazu werden Sicherheitsmaßnahmen definiert, um die Integrität von seriellen Verbindungen zu gewährleisten, die einen Keyed-Hash Message Authentication Code (HMAC) verwenden. Weiterhin soll im Teil 5 ein separates Schlüsselmanagement spezifiziert werden, dessen exakte Mechanismen noch in der Diskussion sind.

Smart Grid Security in der Normung

IEC TC 57 WG 15 – IEC 62351

- **IEC 62351-6: Informationssicherheit für IEC 61850 Peer-to-Peer-Profile**

Die IEC 61850 Norm spezifiziert drei Peer-to-Peer-Multicast-Protokolle, die im LAN einer Trafostation nicht zu routen sind. Prominentester Vertreter ist das GOOSE (Generic Object Orientated Substation Events) Protokoll, das für gesicherte Nachrichtenübermittlung innerhalb von 4 ms zwischen intelligenten Controllern konzipiert wurde. Unter solch harten Echtzeitbedingungen lassen sich nur begrenzte Sicherheitsmaßnahmen umsetzen, da diese einen signifikanten Effekt auf die Verarbeitung haben. Im Teil 6 sind derzeit digitale Signaturen für den Schutz der Multicast-Nachrichten definiert, die sich jedoch mit der feldgerätetypischen Hardware schlecht bis gar nicht umsetzen lassen. Eine alternative Lösung, die anstelle einer gerätespezifischen digitalen Signatur auf die Anwendung eines Gruppenschlüssels zum Errechnen eines Integritätswertes setzt, wurde im technischen Report IEC 61850-90-5 erarbeitet. Dieser Ansatz fließt nun sukzessive in die weitere Bearbeitung der verschiedenen IEC 62351 Teile mit ein.

Smart Grid Security in der Normung

IEC TC 57 WG 15 – IEC 62351

- **IEC 62351-7: Sicherheit für Netzwerk- und Systemmanagement (NSM) Datenobjektmodelle**

  Der Fokus im Teil 7 liegt auf dem Netzwerk- und Systemmanagement (NSM) der Informationsinfrastruktur der Energiesysteme. Hierzu hat die WG 15 abstrakte NSM-Datenobjekte für die Kontrolle und Überwachung des Netzwerks sowie angeschlossener Geräte definiert, um zu reflektieren, welche Informationen in einer Leitstelle notwenig sind, um die Informationsinfrastruktur ebenso zuverlässig zu managen wie die Systeme der Energieinfrastruktur. Auf diesen Informationen können typische Managementprotokolle wie SNMP aufsetzen. Durch die Überwachung des Netzwerks sollen Angriffe erkannt und frühzeitige Reaktionen hierauf ermöglicht werden.

Smart Grid Security in der Normung

IEC TC 57 WG 15 – IEC 62351

- **IEC 62351-8: Rollenbasierte Zugriffskontrolle für Leitsysteme**

  Zentrales Thema im Teil 8 der IEC 62351 ist der rollenbasierte Zugangskontrollmechanismus (Role Bases Access Control, RBAC) und dessen Integration in der gesamten Domäne der Energieversorgung. Dies ist unumgänglich, da in Schutzsystemen und Leitwarten Autorisierung und Nachverfolgbarkeit gefordert sind, z. B. um bestimmte Schalthandlungen im Energienetz eindeutig nachvollziehen zu können. Teil 8 definiert dabei drei verschiedene Möglichkeiten, die Rolleninformation zu transportieren, und setzt dabei auf die bisher verwendeten Formate wie z. B. X.509 Zertifikate.

Smart Grid Security in der Normung

IEC TC 57 WG 15 – IEC 62351

- **IEC 62351-9: Schlüsselmanagement**

  Dieser Teil befindet sich noch in der Entwicklung und legt fest, wie insbesondere digitale Zertifikate und Schlüsselmaterial generiert, verteilt, widerrufen und behandelt werden sollen, um digitale Informationen und Kommunikation sicher zu schützen. Weiterhin ist im Scope des Standards der sichere Umgang mit symmetrischen Schlüsseln (pre-shared- und Session-Schlüssel) genannt. Dabei beschreibt Teil 9 neben typischerweise einzusetzenden Protokollen und Technologien für das Key Management auch eine Reihe von Anwendungsfällen, die diese Technologien benutzen.

Smart Grid Security in der Normung

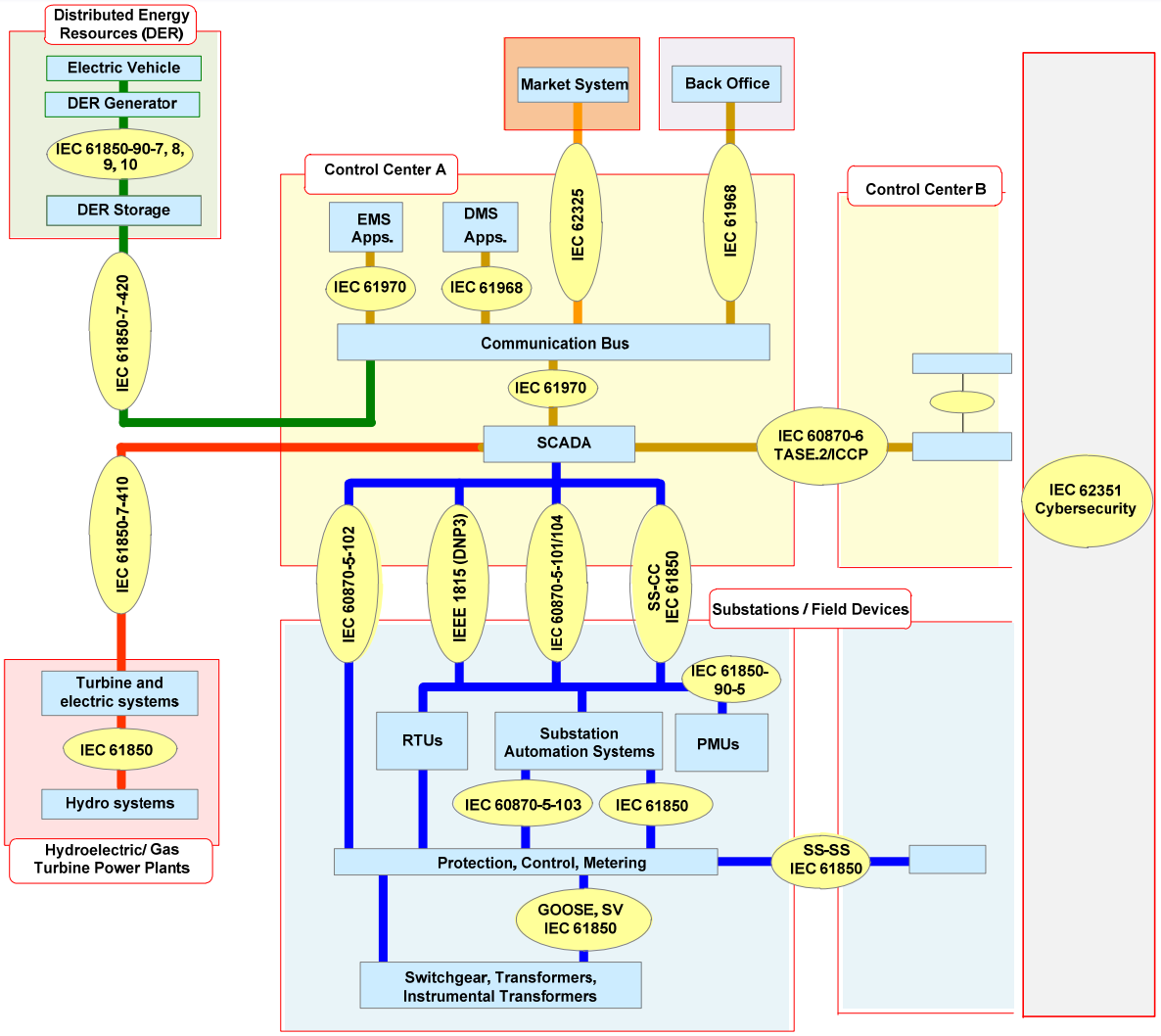
IEC TC 57 WG 15 – IEC 62351

- **IEC 62351-10: Sicherheitsarchitektur**

Teil 10 beschreibt im Rahmen eines technischen Reports Security-Architektur-Empfehlungen für Systeme der Netzleittechnik, basierend auf grundlegenden Security-Maßnahmen (Komponenten, Funktionen und ihre Interaktion). Dieser Teil der Norm soll unter anderem System-Integratoren dabei unterstützen, Systeme der Energieerzeugung, -übertragung und -verteilung sicher einzusetzen und die verfügbaren Normen anzuwenden.
Die zugrunde liegende Architektur von IEC TC 57, auf deren Basis Security-Maßnahmen aus dem Umfeld der IEC 62351 anzuwenden sind, befindet sich auf der Folgefolie…

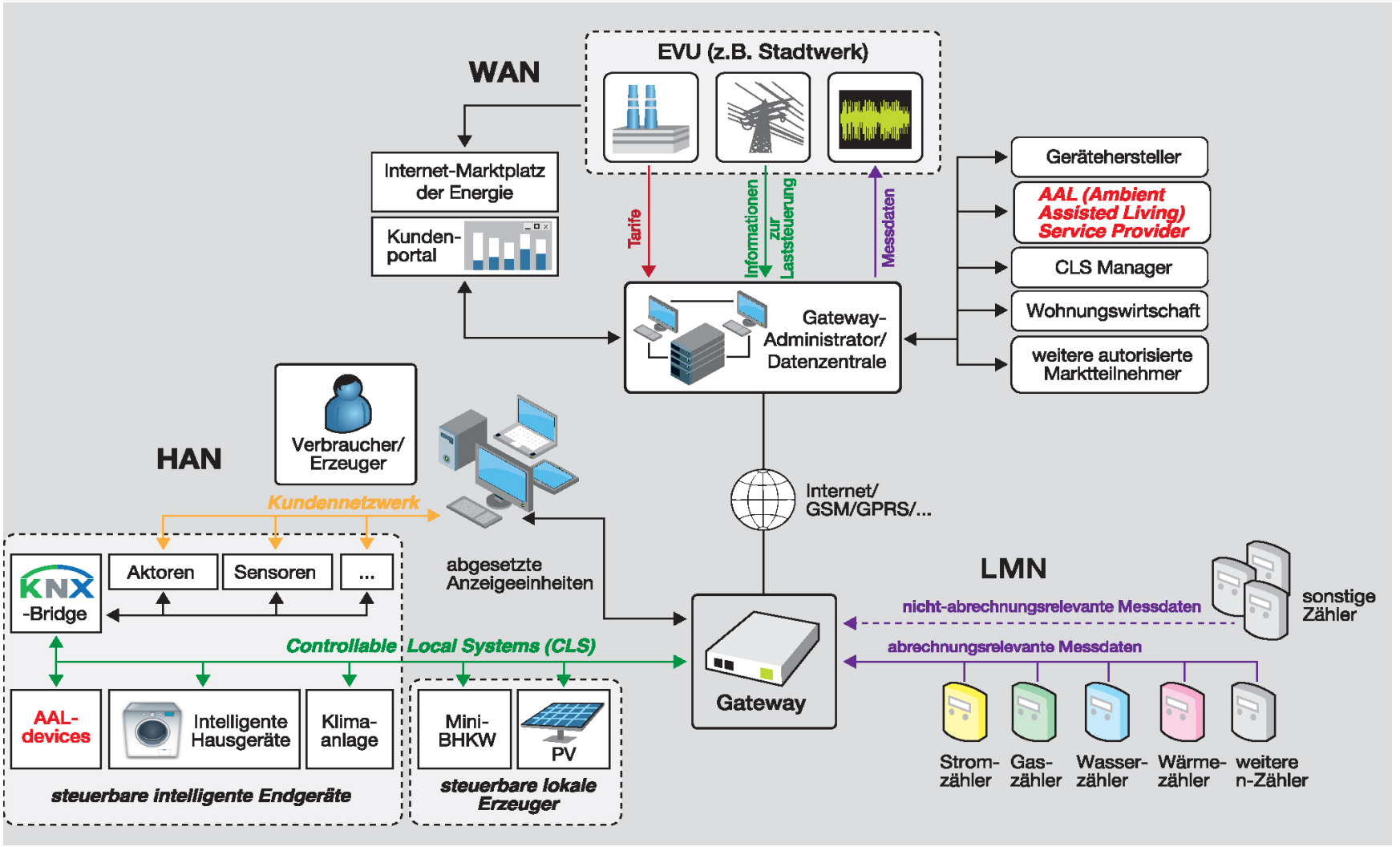
Smart Grid Security in der Normung

IEC TC 57 WG 15 – IEC 62351 IEC 62351-10: Sicherheitsarchitektur



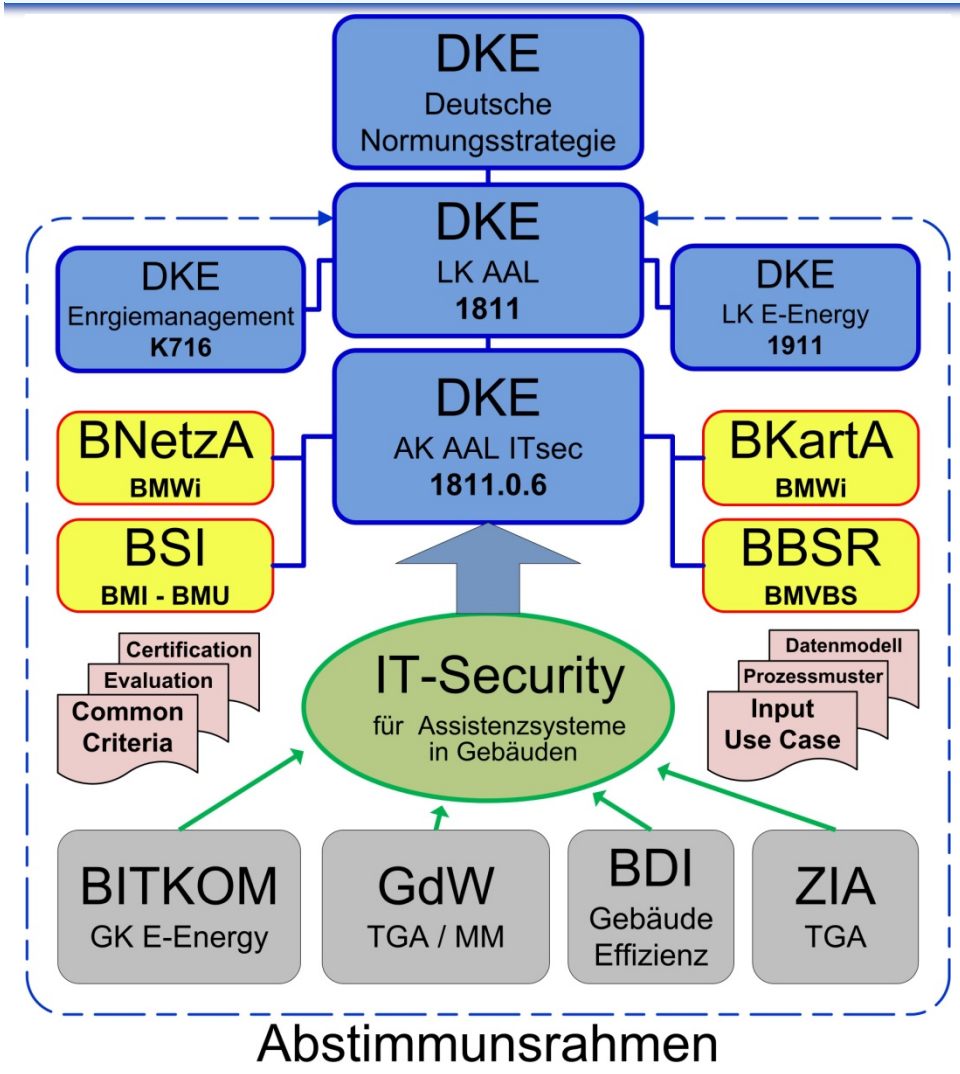
Mehrwertdienste beim Smart Meter Gateway

Ambient Assisted Living - AAL



Mehrwertdienste beim Smart Meter Gateway

Ambient Assisted Living - AAL



- Abstimmung zur EU und international
- Abstimmung zu anderen Domänen
- Abstimmung zum Rechts- und Ordnungs-rahmen
- Aufbau der Kriterien und System-strategie
- Abstimmung zu Verbands- und Einzelinteressen

Mehrwertdienste beim Smart Meter Gateway

Ambient Assisted Living - AAL

Abstimmung und Kooperation für Rahmenbedingungen

DKE/VDE/BSI/BfD/BBSR:
Abstimmung Normungsroadmap 2.x

BMVBS/BMWi/BMBF/BMU/BMI:
Abstimmung Ordnungsrahmen

5 Einrichtungen kooperieren

5 Ministerien kooperieren

Bedingungen mit einheitlicher, abgestimmter Rechtsgrundlage

Dipl. Ing. (TU) Andreas Harner
Projektmanager
Abteilung Standardisierung

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Tel.: +49 69 6308-392
E-Mail: andreas.harner@vde.com

Stresemannallee 15
60596 Frankfurt/Main

Bereich
Standardisierung