Vorstellung Referat D 21

Digitalisierung der Energiewirtschaft

Michael Puchowezki, Referent D 21
14. Juli 2025

Bundesamt
für Sicherheit in der
Informationstechnik

Agenda

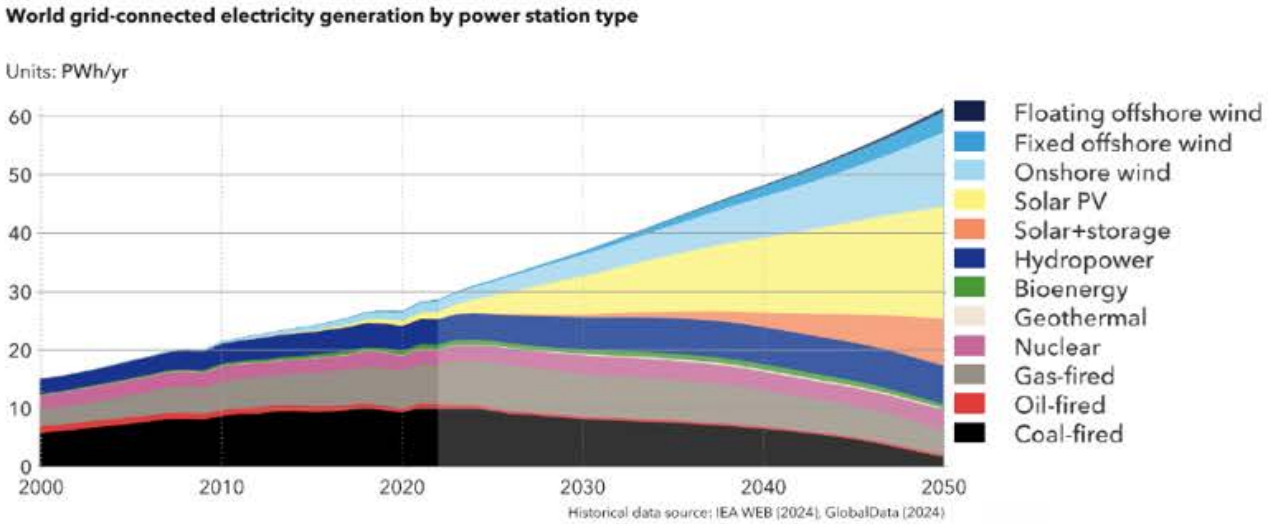
- 1. Zwischen Blackout und Energiewende
- 2. Das BSI als zentrale Instanz
- 3. Das SMGW und die Sicherheitsarchitektur
- 4. Schnittstellen und Protokolle im Bereich des SMGW
- 5. Deep-Dives in aktuelle Themen
- 6. Ausblick und Fazit
- 7. Live-Demos des Referats D21
- 8. Masterarbeit oder Karriere beim BSI

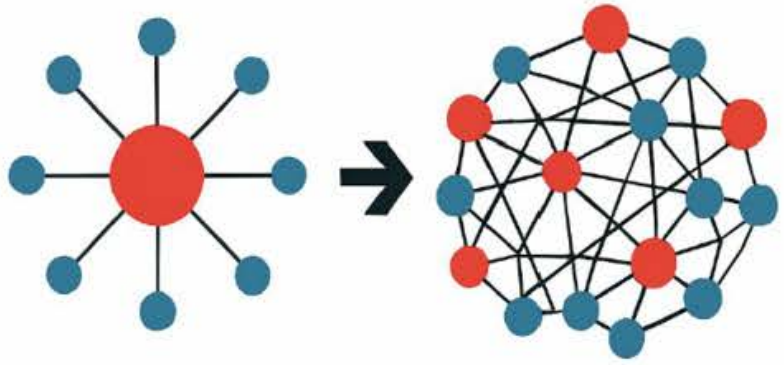
1. Zwischen Blackout und Energiewende – Cyberangriffe und Systemrisiken im Energiesektor

Bild: © AdobeStock/Azazul

Blackout – Spanien / Portugal | April 2025

Energietransformation

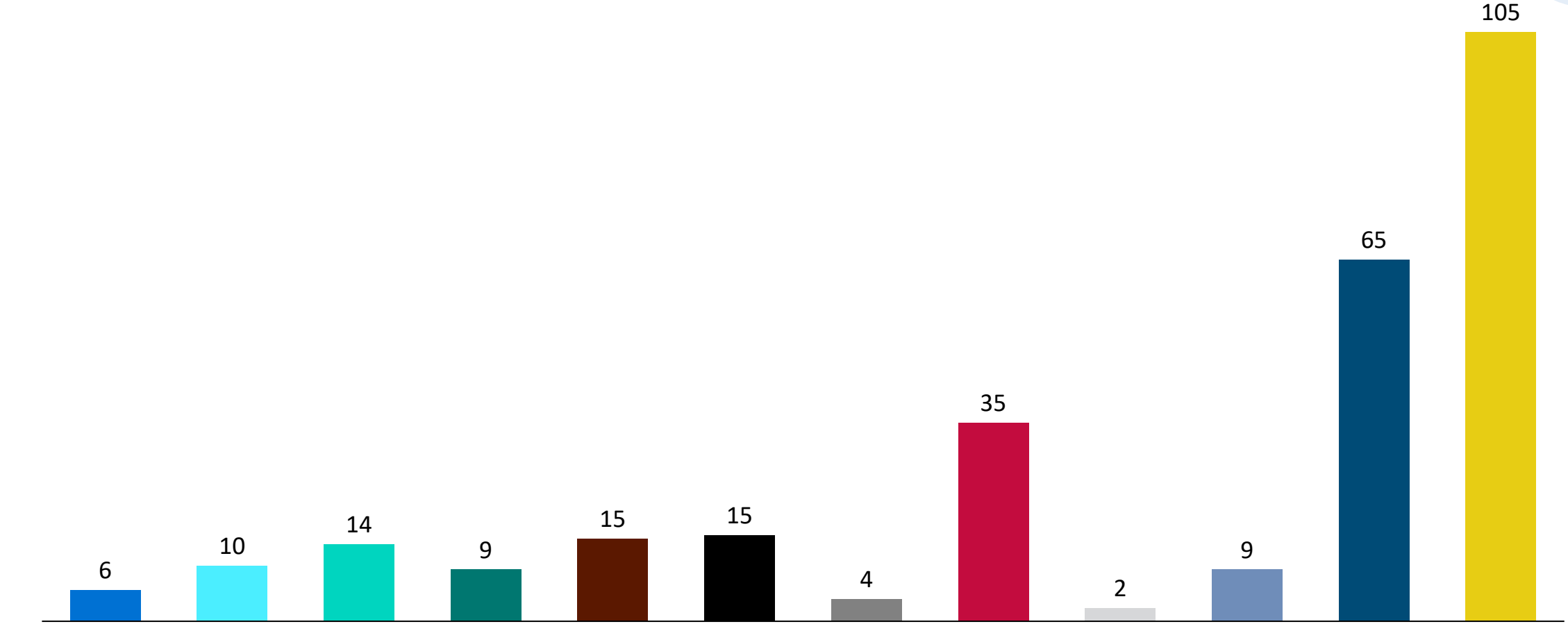




Quelle: DNV

Übersicht über die installierte Gesamtleistung der Erzeuger

Installierte Gesamtleistung [in GW], Stand 26.05.2025



Quelle: Energy-Charts.info

Cyberangriffe und kritische IT-Vorfälle weltweit

USA

Target

Cyberangriff

wirtschaftlicher Schaden

2013

Cyberangriffe und kritische IT-Vorfälle weltweit

Ukraine

Kraftwerk

Cyberangriff

Blackout

2015

Cyberangriffe und kritische IT-Vorfälle weltweit

USA

Colonial Ölpipeline

Cyberangriff

Ransomware

2021

Cyberangriffe und kritische IT-Vorfälle weltweit

Deutschland

Stadtwerke Karlsruhe

Malware

Blackout (verhindert)

2023

Cyberangriffe und kritische IT-Vorfälle weltweit

Weltweit

Crowd-Strike

fehlerhaftes Update

wirtschaftlicher Schaden

2024

Aktuelle Situation – gefühlte Lage in Deutschland

BADBOX WÄCHST, 190.000 ANDROID-GERÄTE INFIZIERT

BSI weist auf vorinstallierte Schadsoftware auf IoT-Geräten hin

Pierluigi Paganini 21. Dezember 2024

Verfassungsschutz eingeschaltet

Schwerer Cyberangriff auf die CDU

Stand: 01.06.2024 18:00 Uhr

Eine Woche vor der Europawahl ist die CDU Opfer einer Cyberattacke

Sanktionen angekündigt

USA werfen Russland Einmischung in Präsidentenwahl vor

Stand: 04.09.2024 20:41 Uhr

Cyberkriminalität

Immer mehr Lösegeldattacken

Vor allem Mittelständler sind häufig unzureichend gegen Angriffe mit Erpressungssoftware geschützt. Cyberversicherungen werden teuer.

Susanne Schier Frankfurt, Baden-Baden

Der Markt für US-Staatsanleihen ist der größte und wichtigste der Welt. Und doch gelang es Hackern am vergangenen Donnerstag, dieses riesige Geschäft durcheinanderzubringen. Der US-Ableger der chinesischen Großbank ICBC meldete eine sogenannte Ransomware-Attacke: werden die Preise tendenziell weiter steigen, da auch die Schäden aktuell wieder zunehmen", prognostizierte Hasse.

Die Juristin ist bereits seit mehr als 20 Jahren bei Munich Re tätig und seit 2019 unter anderem für das Cybergeschäft in Europa und Lateinamerika verantwortlich. Im deutschen Markt ist ein gutes Dutzend größerer Erstversicherer im Cy-

MALWARE & DROHUNGEN

Ivanti warnt vor neuen Zero-Day-Angriffen

Ivanti schließt kritische Sicherheitslücken in Connect Secure und Policy Secure

Londoner Kliniken: Cyberkriminelle veröffentlichen Daten

Infolge eines Cyberangriff auf einen Pathologiedienstleister sind Londoner Kliniken im Notbetrieb. Jetzt haben die Cyberkriminellen Daten veröffentlicht.

Updates unmöglich: Niederlande müssen Ampeln wegen Sicherheitslücke austauschen

Per Funk können Angreifer die Ampeln aus der Ferne umschalten und somit den Straßenverkehr stören. Der Austausch wird Jahre in Anspruch nehmen.

Weltweiter IT-Ausfall: Betrieb wird wieder aufgenommen

Das Update eines Programms hat weltweit Windows-Computer zum Absturz gebracht. Crowdstrike hat den Fehler mittlerweie gefunden und behoben.

Kritische Infrastruktur

Mehr Cyberangriffe auf deutsche Seehäfen

Stand: 05.09.2024 08:56 Uhr

Deutsche Seehäfen waren zuletzt immer häufiger von Cyberangriffen betroffen. Besonders seit Beginn des russischen Angriffskrieges hat die Zahl der Cyberattacken zugenommen.

NACH ÜBER 100 JAHREN

Cyberangriff drängt deutsche Firma in die Insolvenz

Der in Euskirchen ansässige Serviettenhersteller Fasana hat nach einem Cyberangriff Zahlungsprobleme. Hacker haben den Betrieb vollständig lahmgelegt.

13. Juni 2025, 12:48 Uhr

Cybercrime: KI-generierte Malware in freier Wildbahn gesichtet

Sicherheitsexperten von HP weisen auf einen beunruhigenden Trend hin: Kriminelle nutzen verstärkt generative KI zur Entwicklung von Malware.

Brennpunkt „Big picture“ Energiesektor (1. HJ 2025)

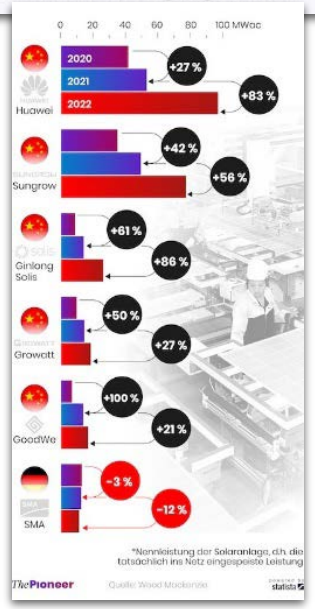
The Pioneer

Erneuerbare Energie

Chinas Macht über deutsche Solaranlagen

Zuletzt aktualisiert am 10.02.2025 16:00 Uhr

Die meisten Solarzellen auf den Dächern deutscher Eigenheime werden über die Wechselrichter von einer Handvoll chinesischer Unternehmen gesteuert, allen voran Huawei. Die Sorge vor dem Risiko für die deutsche und europäische Stromversorgung wächst.



Iberische Halbinsel

Massiver Stromausfall in Spanien und Portugal

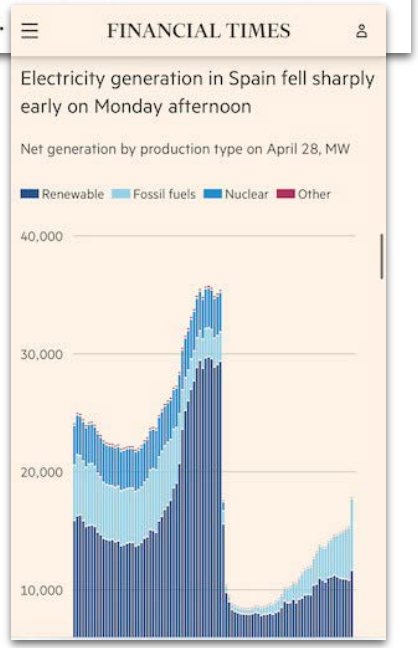
Stand: 28.04.2025 16:43 Uhr

Ein Stromausfall hat weite Teile der iberischen Halbinsel lahmgelegt. In ganz Spanien ist der Bahnverkehr ausgefallen, vielerorts gehen die Ampeln nicht mehr - auch im Nachbarland Portugal. Der Blackout könnte offenbar noch Stunden dauern.

FINANCIAL TIMES

Electricity generation in Spain fell sharply early on Monday afternoon

Net generation by production type on April 28, MW



DER SPIEGEL

Chinatechnik in Solaranlagen

S+ Forscher warnen vor Schwachstelle in Europas Stromnetz

Das Risiko eines Cyberangriffs auf Europas Stromnetz ist groß. Mehr als hundert Gigawatt an Solaranlagen nutzen chinesische Wechselrichter. Und die lassen sich fernsteuern.

30.04.2025, 12.01 Uhr

46 Schwachstellen bei Photovoltaik-Wechselrichtern gefunden. Patches für alle angreifbaren Komponenten sind vorhanden.

Fehlende Sicherheitsstandards gefährden Netzstabilität

DNV-Bericht warnt vor Cyberrisiken durch vernetzte Solaranlagen – Forderung nach EU-weiten Sicherheitsstandards für PV-Systeme

05.05.2025

Quelle: E & M powernew

DER SPIEGEL

Sabotage-Angst

US-Ermittler finden offenbar verdächtige Funkmodule aus China in Solaranlagen

Chinesische Produzenten von elektronischen Steuerungen stehen schon länger im Verdacht, ihre Produkte mit Hintertürchen für Spione oder Saboteure auszustatten. Jetzt wollen Ermittler in Solarpanels verdächtige Funkmodule aufgespürt haben.

14.05.2025, 13.42 Uhr

BSI fordert robuste Cybersicherheit für die Energieversorgung

Ort Bonn
Datum 21.05.2025

Quelle: © GettyImages zhongguo

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI

Positionspapier: Cybersicherheit im Energiesektor Deutschlands

Angespannte Lage: Bedrohungen und Schadwirkung

Bitkom-Studie:
179 Milliarden Euro Schaden durch Cyberangriffe im Jahr 2024 bei deutschen Unternehmen

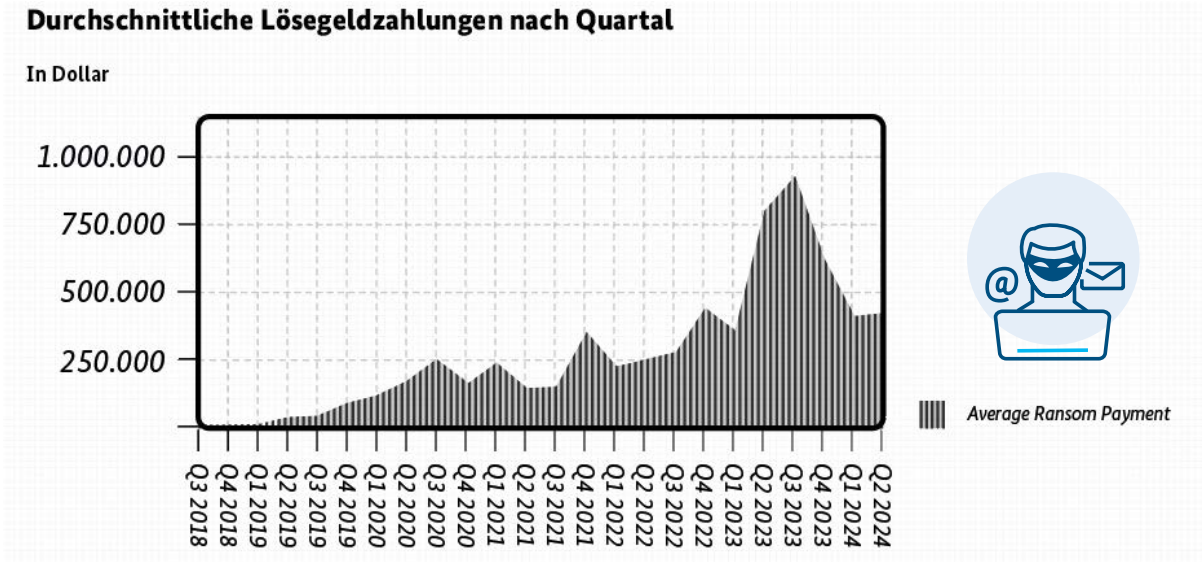
Meldungen an das BSI:
726 Meldungen aufgrund von Cybervorfällen, Anstieg um 33%

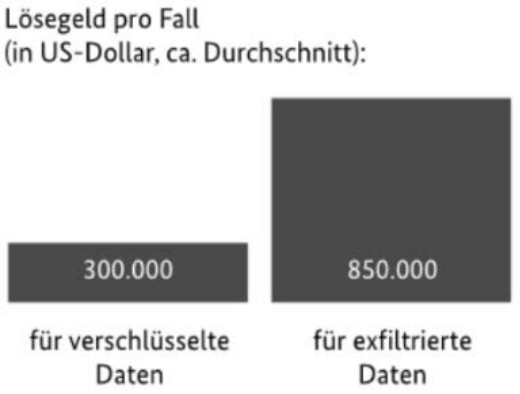
CrowdStrike-Vorfall:
5 Mrd. Dollar Schaden durch fehlerhaftes Update

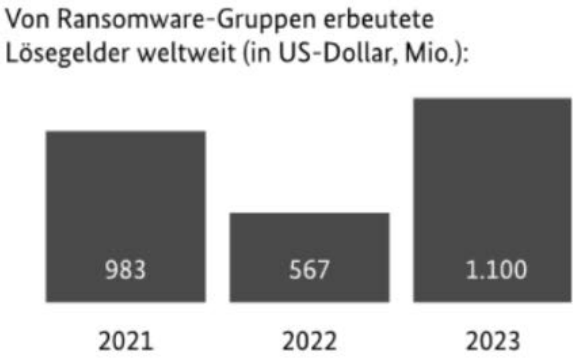
Steigende Bedrohungen im Energiesektor:
Cyberangriffe auf Energiesysteme weltweit 2024: 1 Mrd. USD

Deutschland im Fokus:
Ransomware-Gruppen bedrohen täglich KMU und Kommunen – oft mit verheerenden Folgen für lokale Infrastrukturen und Wirtschaft

Energiesektor ist Hauptziel von Ransomware und staatlichen Angreifern. Dezentralisierung erhöht Angriffsfläche: Robuste Maßnahmen unerlässlich







Zunehmende Cyber-Bedrohungen und staatliche Reaktion

Cyberangriffe auf Energiesysteme:

Gezielte Angriffe auf Netzbetreiber, Leittechnik und kritische Infrastrukturen

Herausforderungen durch Dezentralisierung der Energiesysteme:

Neue Anforderungen an die Netzstabilität durch dezentrale Energieerzeugung (PV, Speicher, Wärmepumpen, E-Mobilität, ..)

Neue Herausforderungen an Steuerung, Lastmanagement und Kommunikation

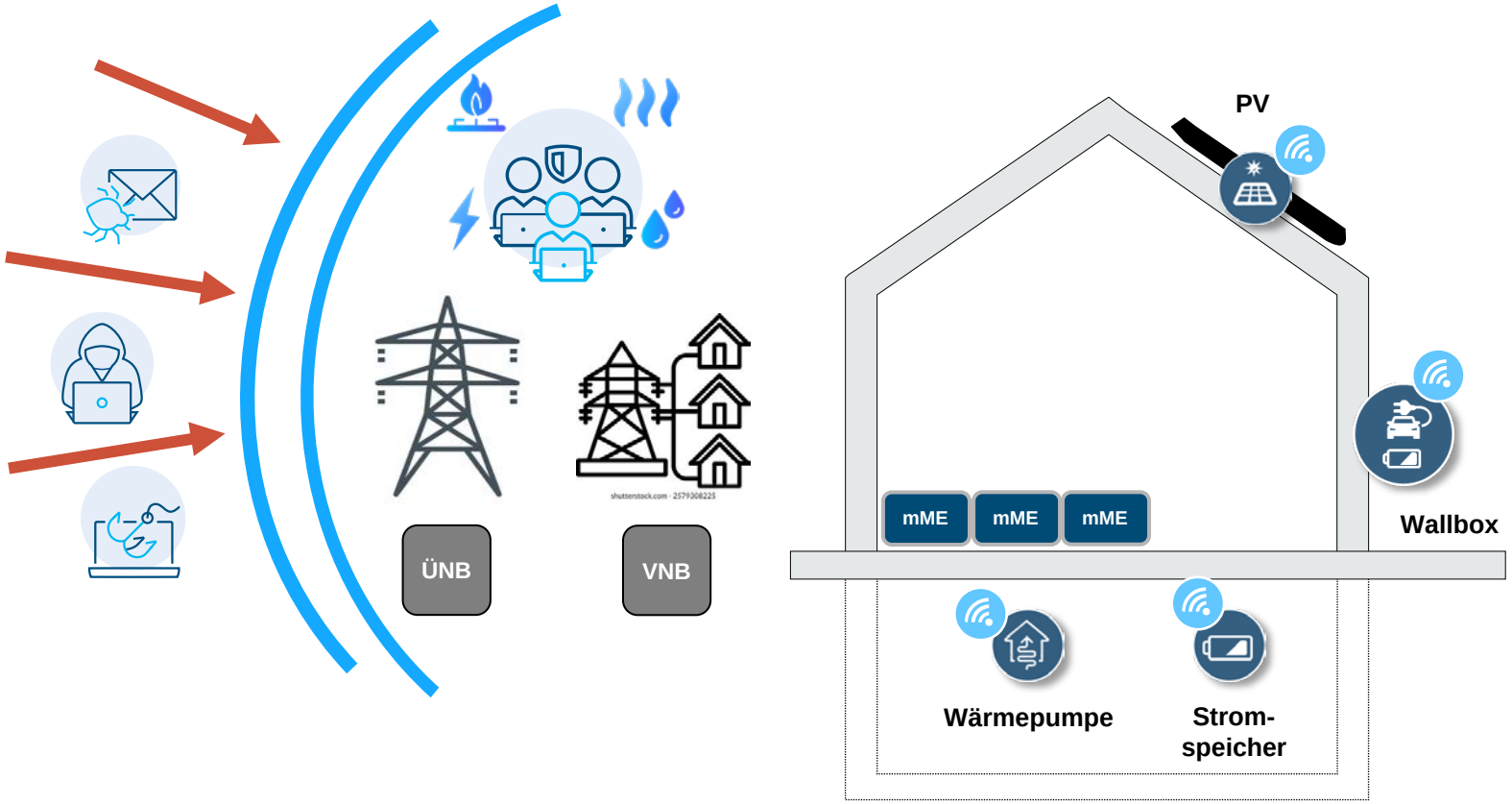
Staatliche Reaktion:

IT-Sicherheitsgesetz I & II | KRITIS-Verordnung | BSI-Gesetz

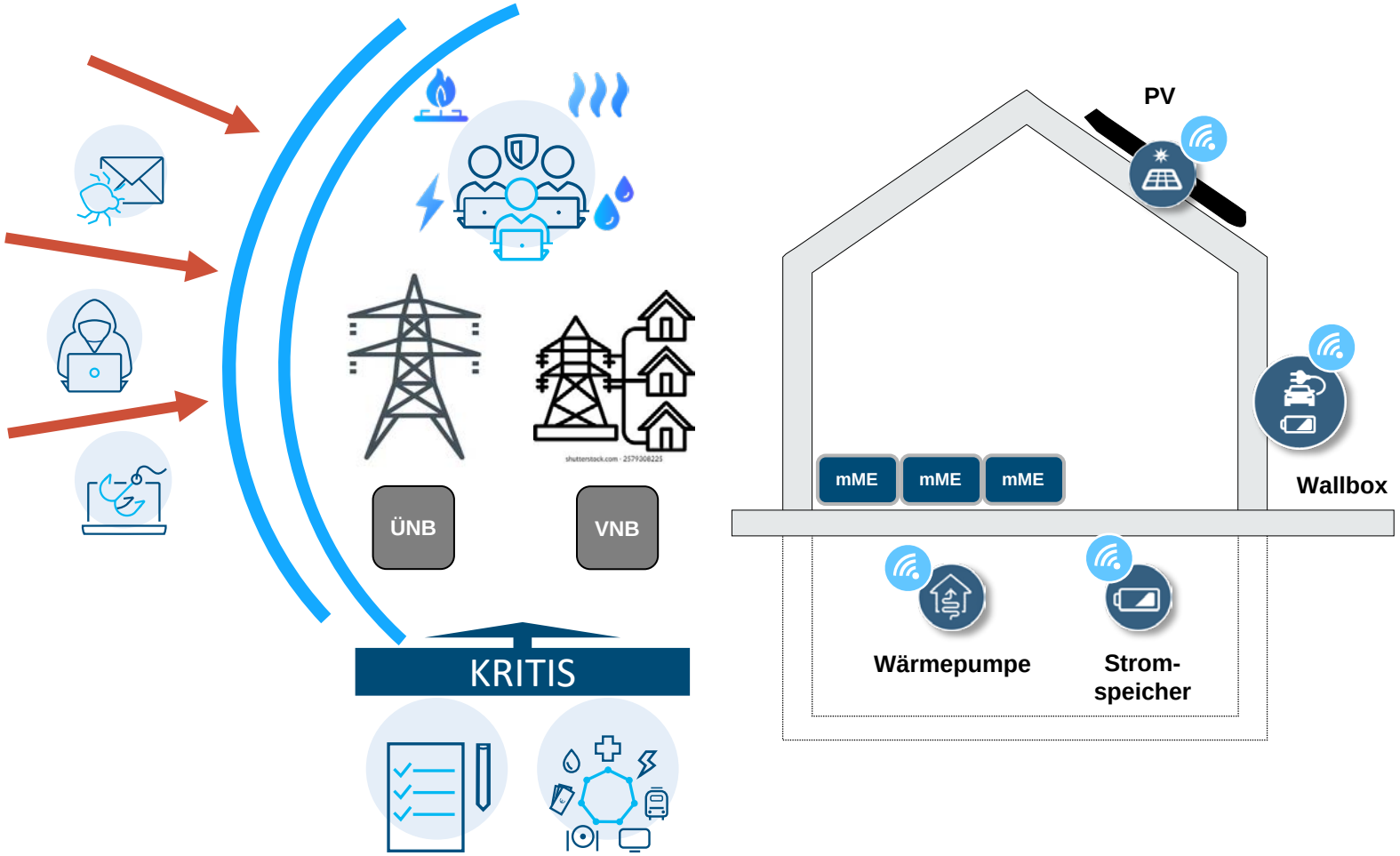
Das BSI verantwortet zentrale Sicherheitsvorgaben für die Digitalisierung der Energiesysteme

2. Das BSI als zentrale Instanz für die sichere Digitalisierung der Energiewirtschaft

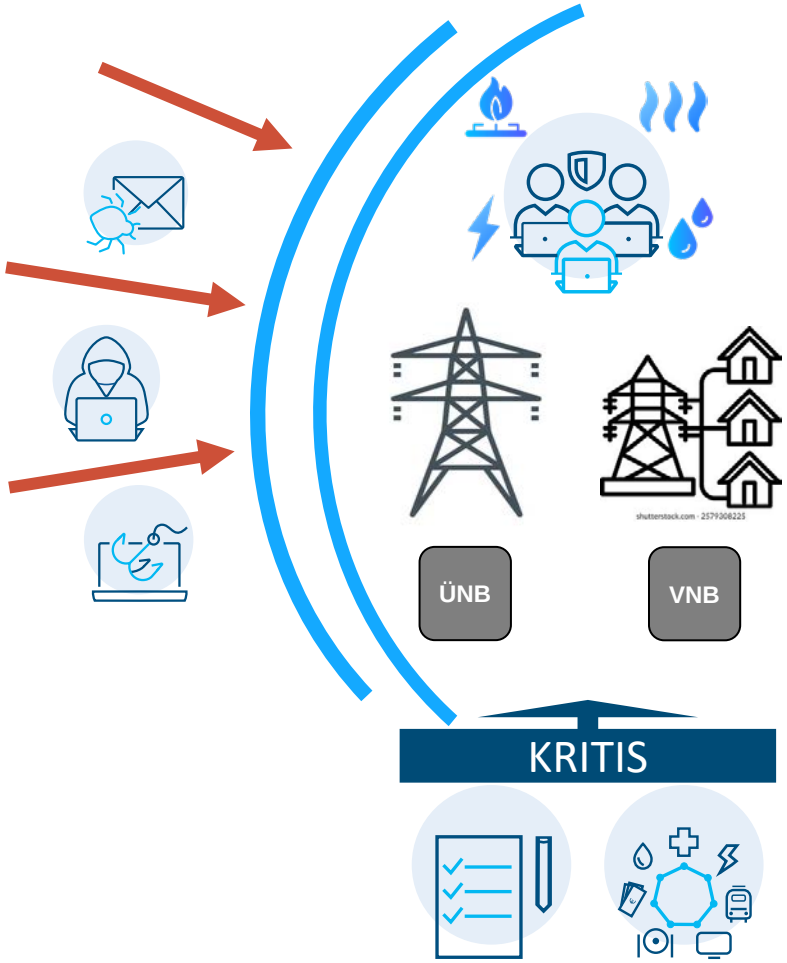
Digitalisierung der Energiewende - Cyberangriffe und dezentrale Energien

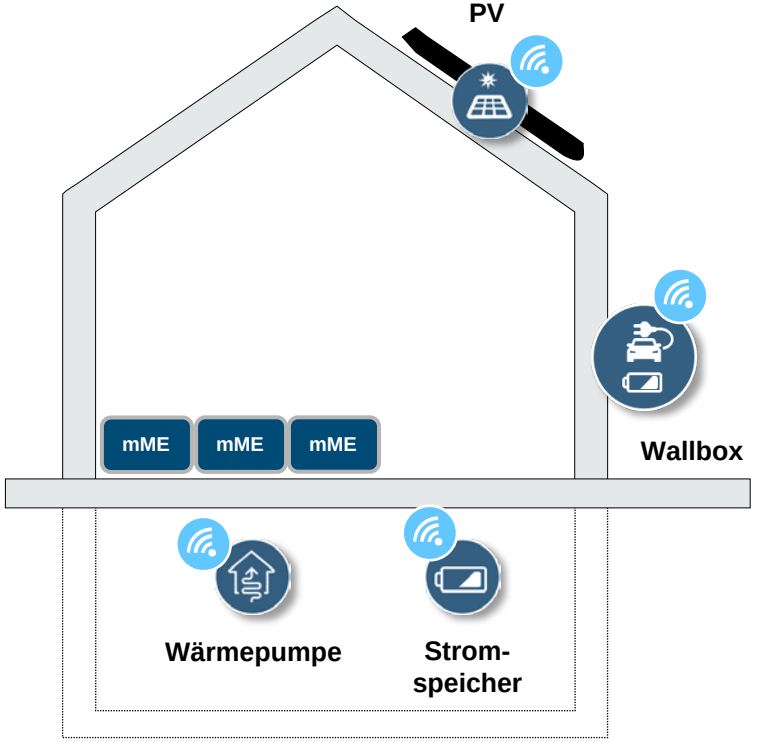


Digitalisierung der Energiewende - Cyberangriffe und dezentrale Energien



Digitalisierung der Energiewende - Cyberangriffe und dezentrale Energien





PV: ca. 3,4Mio. mit 100 GWp
- bis zu 10kWh/Tag je Haushalt
- Kapazitätsfaktor: 11-13%
- (Wetterspitzen > 50%)

WB: ca. 2,2Mio. (privat)
- 11kW je (AC) Ladepunkt
- 3-6kW zur Hauptzeit (Abends)

WP: ca. 2,5Mio. mit 12-15 TWh
- 2-6kW je Anlage
- 1,5-3kW (im Winter)

Zähler
- 46Mio. (ca. 40% analog)
- 14Mio. (ca. 60% analog)
- 40Mio. (ca. 70% analog)
- 20Mio. (ca. 60% analog)

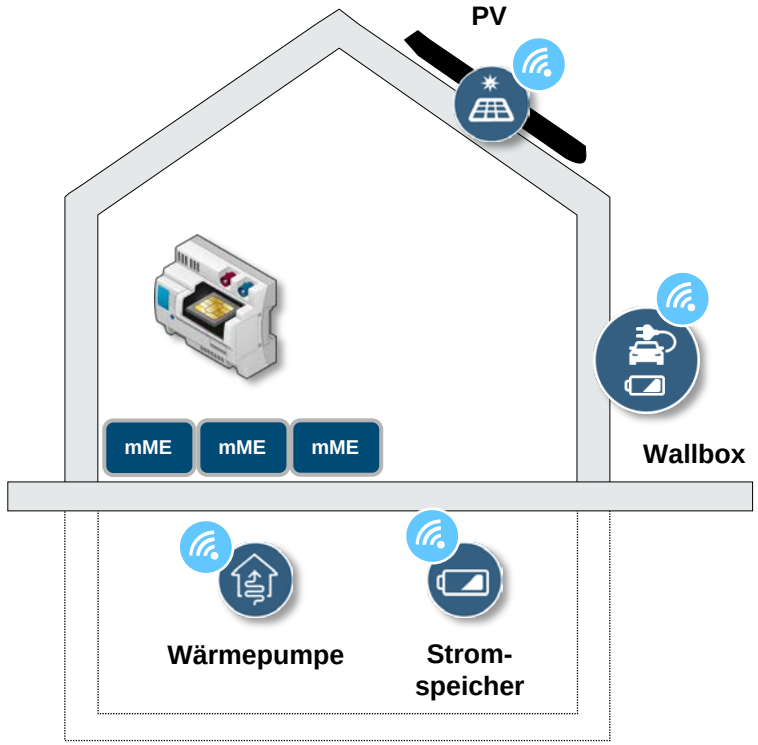
Digitalisierung der Energiewende - Cyberangriffe und dezentrale Energien

Zählerdaten (mME):

- sichere Erfassung und Verteilung von Zählerdaten

Beitrag zur Netzstabilität

- Möglichkeit zur Fernsteuerung von Verbrauchseinrichtungen
  - PV-Anlagen
  - Wallboxen
  - Wärmepumpen



Technische Anforderungen:

- sicherer WAN-Zugang für Admins und berechtigter EMT
- Transparenz für Nutzer
- Interoperabilität mit weiteren Produkten

Sicherheitsanforderungen:

- technische Durchsetzung des Datenschutz
- Sicherstellung von Vertraulichkeit, Integrität und Authentizität auf Asset-Ebene

3. Das Smart-Meter-Gateway (SMGW) und die Sicherheitsarchitektur

Smart-Meter-Gateway – Schlüsseltechnologie für die Digitalisierung der Energiewende

Datenschutz

Datenhoheit und Transparenz (beim Anschlussnutzer)
Datensparsamkeit und Zweckgebundenheit

IT-Sicherheit

10100
010
11010

Verschlüsselter und authentischer Informationsfluss
Zertifizierung nach Common Criteria mit hoher Prüftiefe

Sichere Kommunikationseinheit für Messeinrichtungen

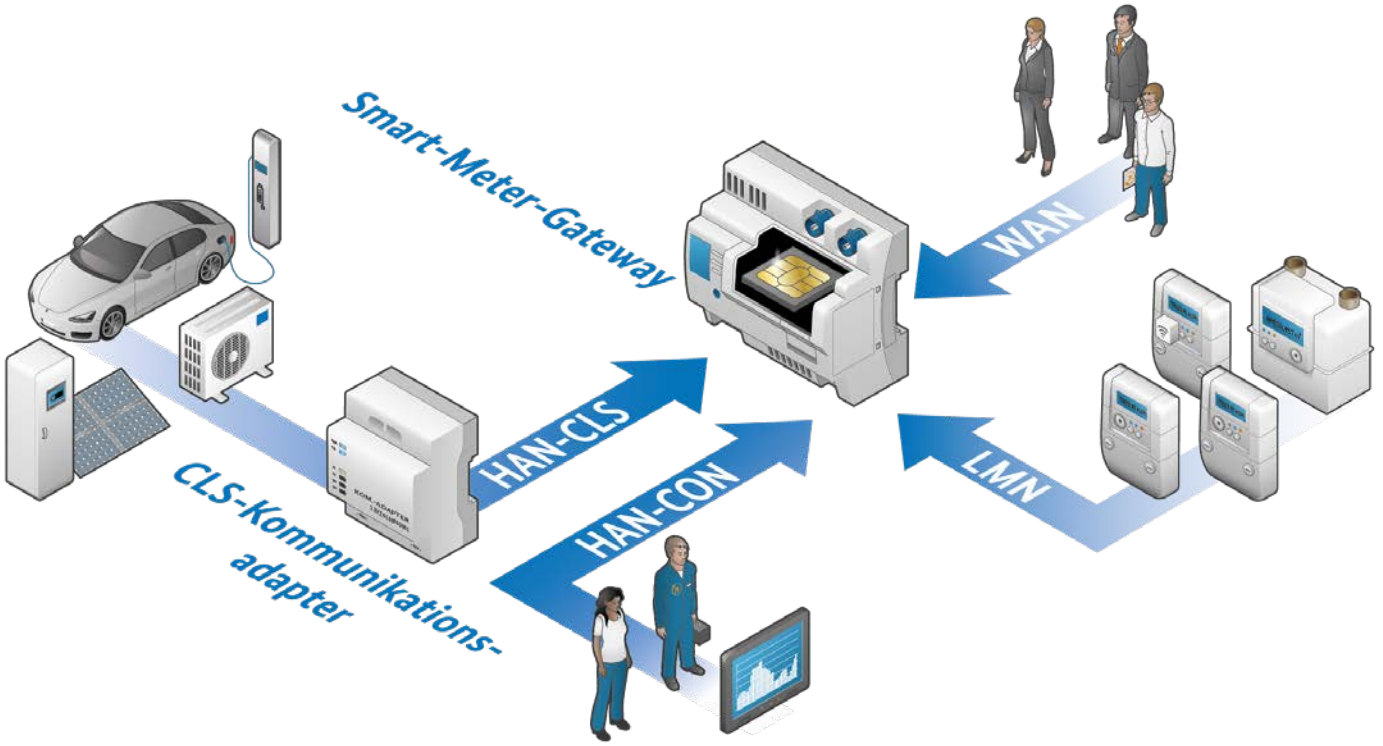
Sichere Integration von Messeinrichtungen unterschiedlicher Sparten (Strom, Gas, Wasser, Wärme) durch kommunikative Anbindung an das SMGW

Sichere Kommunikationseinheit für technische Einrichtungen im Heimnetz

Sichere Integration der Steuerungstechnik in das intelligente Netz durch kommunikative Anbindung an das SMGW

SMGW-Systemarchitektur für sichere Kommunikation

- Vertrauenswürdige Produktkomponente (**SMGW mit integriertem Sicherheitsmodul**)
- Informationssicherheit bei Administration und Betrieb (**SMGW-Administrator**)
- Vertrauenswürdige Kommunikationsinfrastruktur (**Smart-Metering-PKI**)



TR-03109-Reihe sowie PP sind Basis für interoperablen und sicheren Rollout

TR-03109-1: Smart-Meter-Gateway
5 SMGW erfolgreich zertifiziert

TR-03109-2: Sicherheitsmodul
TR-konform und CC-zertifiziert

TR-03109-3: Kryptografische Vorgaben
Alle zertifizierten Produkte erfüllen die kryptografischen Vorgaben

TR-03109-4: Smart Metering PKI
BSI ist Inhaber der Wurzelzertifikate der SM-PKI / verantwortet **Root-CA**
12 Sub-CAs, die Zertifikate für Endnutzer (EMT, -.MAK, -.API, GWH, SMGW, GWA) ausstellen

TR-03109-5: Kommunikationsadapter
10 zertifizierte CLS-Produkte
6 weitere CLS-Produkte im Zertifizierungsverfahren

TR-03109-6: Administration und Betrieb
40+ Unternehmen als GWA zertifiziert, bundesweites GWA Dienstleistungsangebot

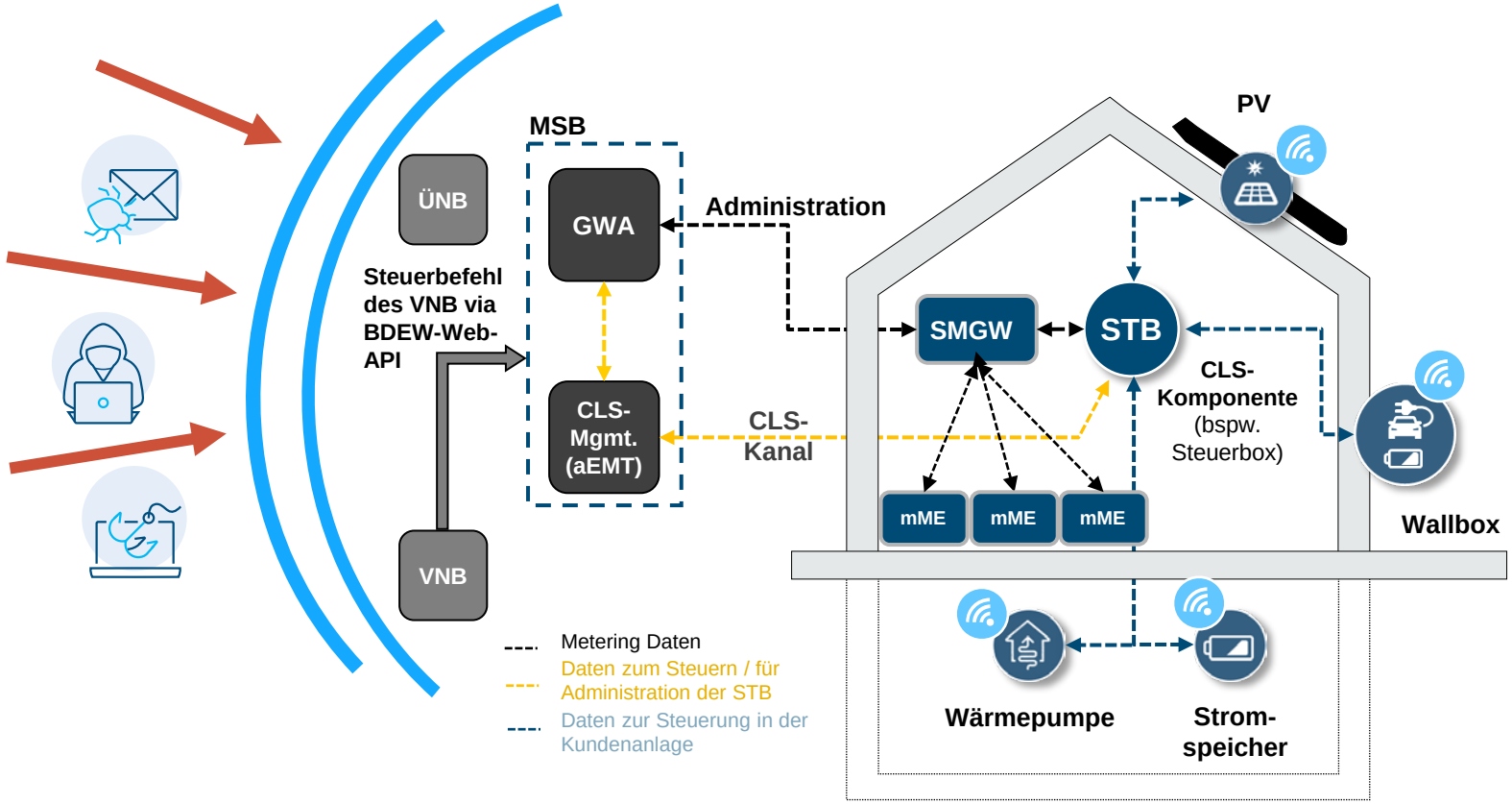
Digitalisierung der Energiewende - Cyberangriffe und dezentrale Energien

Aktuelle Entwicklungsstand:

Die TR-03109-Reihe definiert die derzeitige SMGW-Architektur als zentrale Schnittstelle zwischen Messsystemen, Erzeugern und EMT

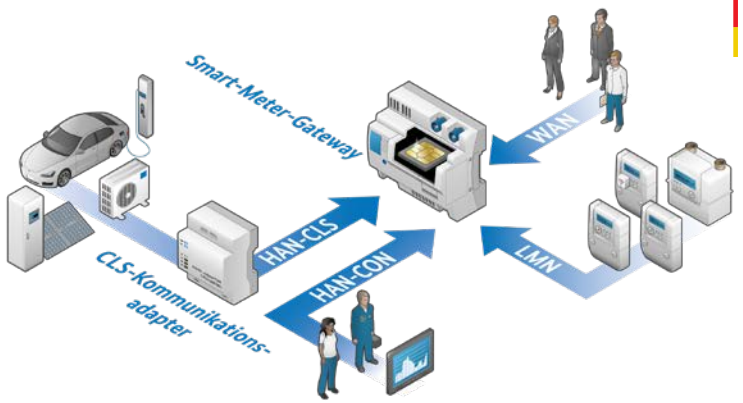
Stetiger Ausbau der Architektur:

Kontinuierliche Weiterentwicklung in enger Abstimmung mit Markt und Behörden – die SMGW-Architektur wächst stetig und integriert neue Funktionen



4. Schnittstellen und Protokolle im Bereich der Smart-Meter-Gateway (SMGW) Architektur

SMGW-Schnittstellen: LMN-Schnittstelle



Ziel und Funktion:

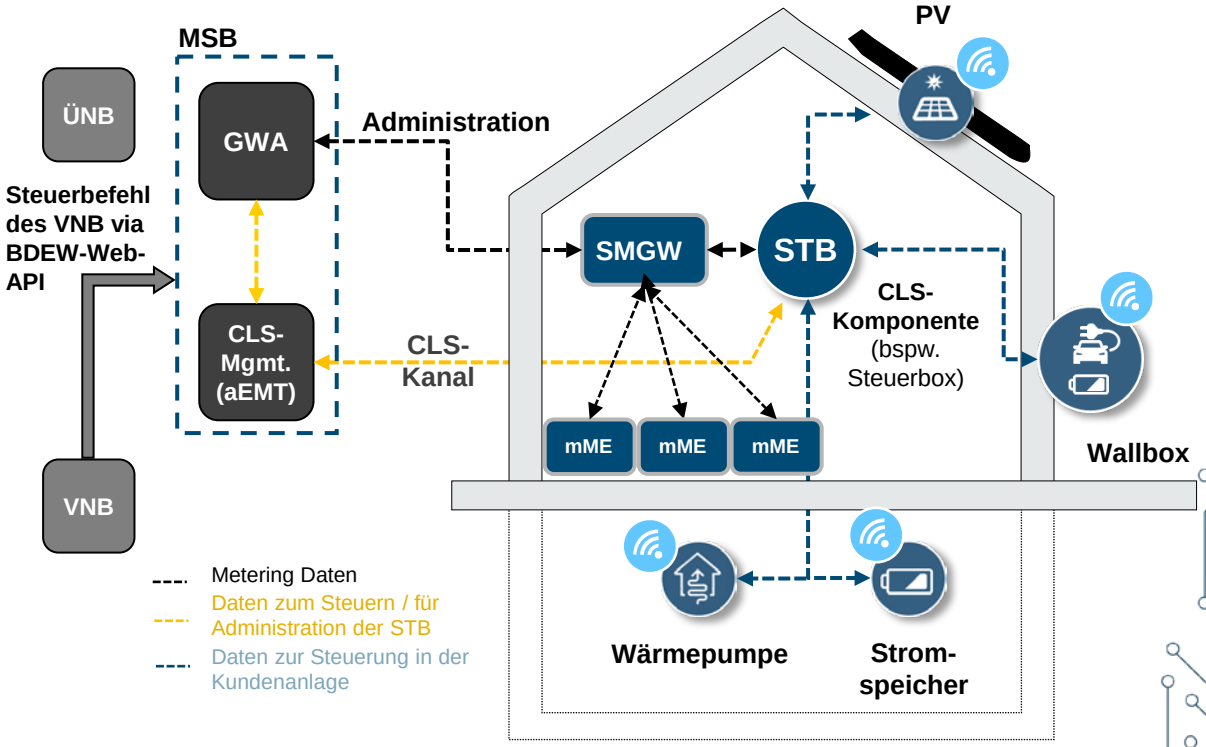
- Verbindung zu den lokalen mME (z.B. Strom, Gas, Wasser oder Wärme)

Protokolle:

- SML
- DLMS/COSEM
- M-Bus/wM-Bus
- …

SMGW-Funktionen:

- Verwaltung der Zähler
- Erfassung und Verwaltung von Messdaten anhand Auswertungsprofilen (TAF)



Protokollstapel: LMN-Kommunikation

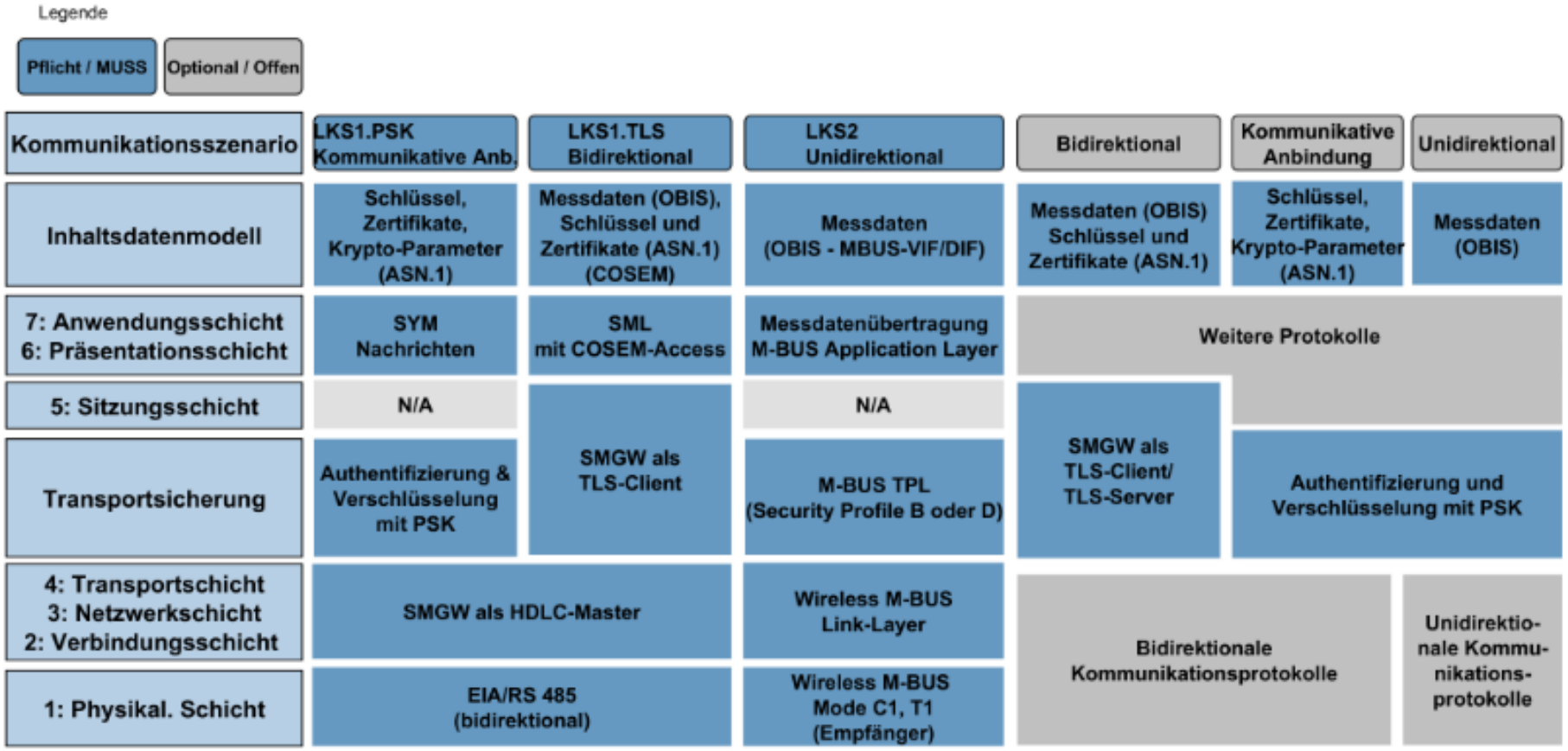
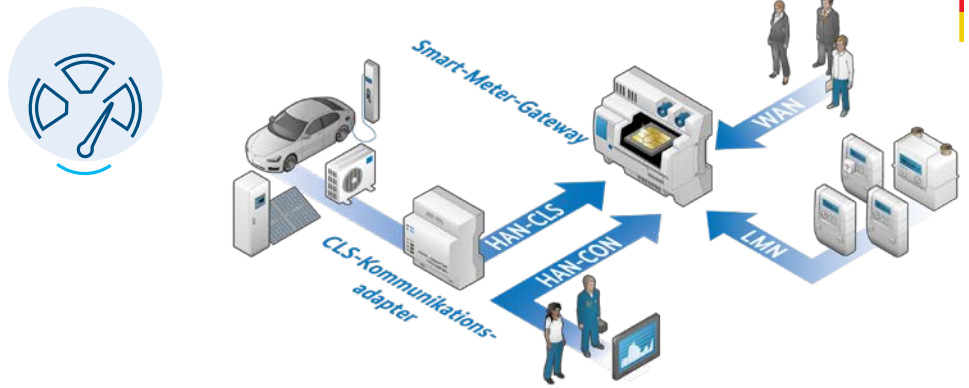


Abbildung 4.11. Protokollstapel im LMN (für drahtlose und drahtgebundene Kommunikation)

SMGW-Schnittstellen: HAN-Schnittstelle



Ziel und Funktion:

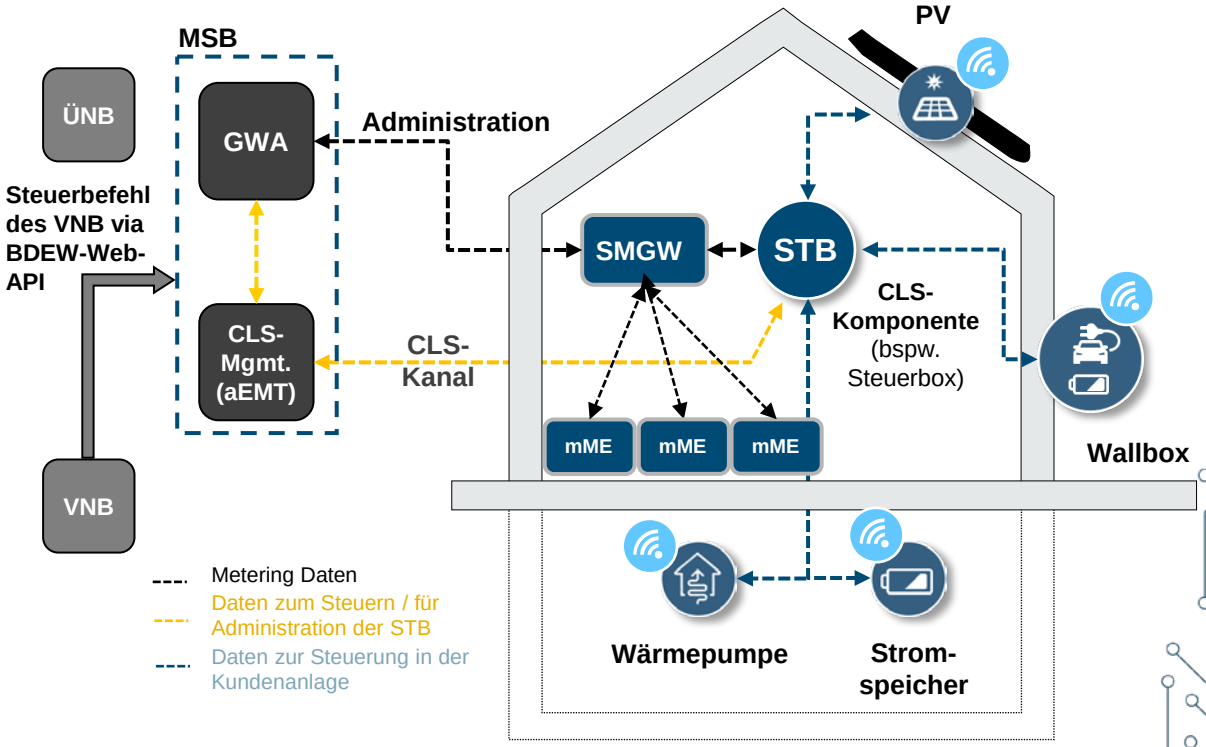
- sicherer Anbindung lokaler Geräte an das SMGW (z.B. PV, HEMS, Wallbox, Submeter, WP, Stromspeicher)
- HAN-CLS: Anbindung, Steuerung und Fernzugriff auf lokale Geräte
- HAN-CON: Anzeige von Statusdaten

Anwendungsfall-Protokolle über TLS-Proxy: (nicht von BSI vorgegeben)

- EEBus
- IEC 61850
- OCPP
- Sunspec/ModBus
- …

SMGW-Funktionen:

- Verwaltung der Geräte
- Transparenter CLS-Kanal (TLS-Proxy)



Protokollstapel: HAN-Kommunikation

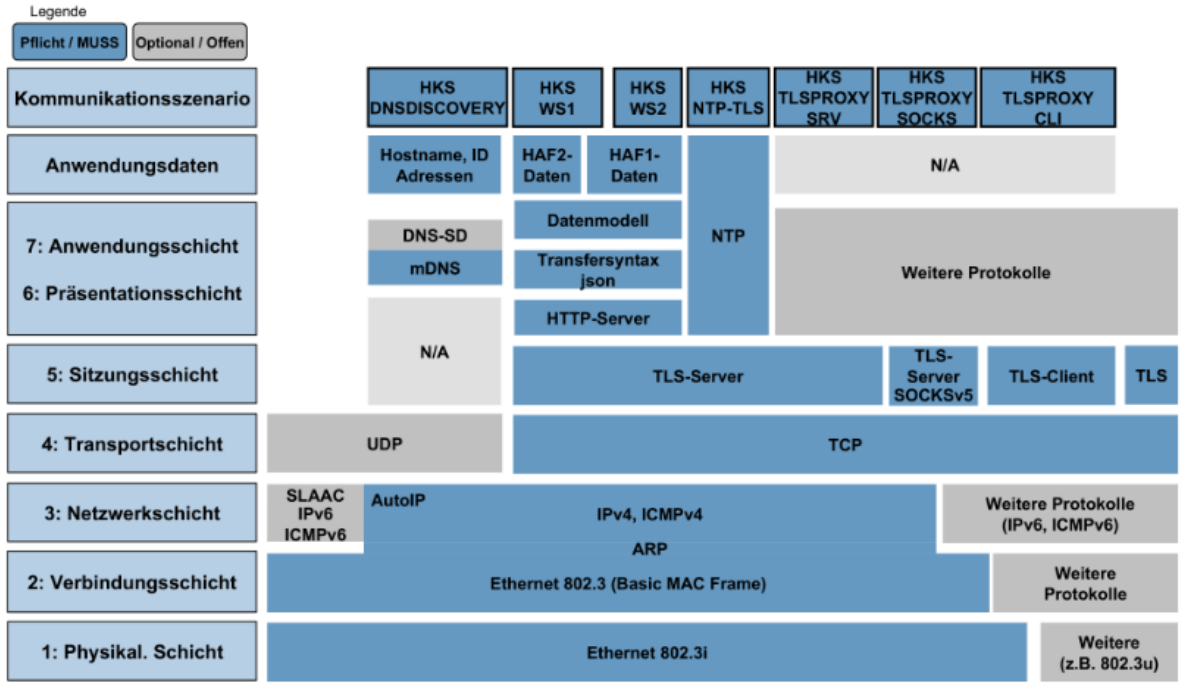


Abbildung 4.18. Protokollstapel für die HAN-Kommunikation

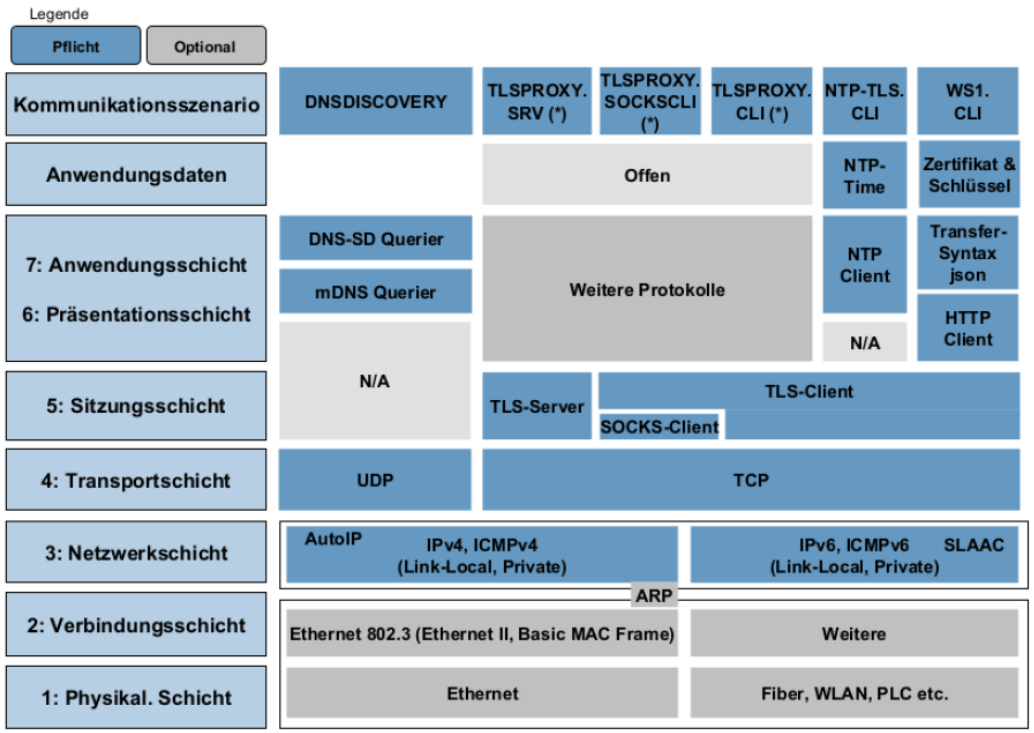
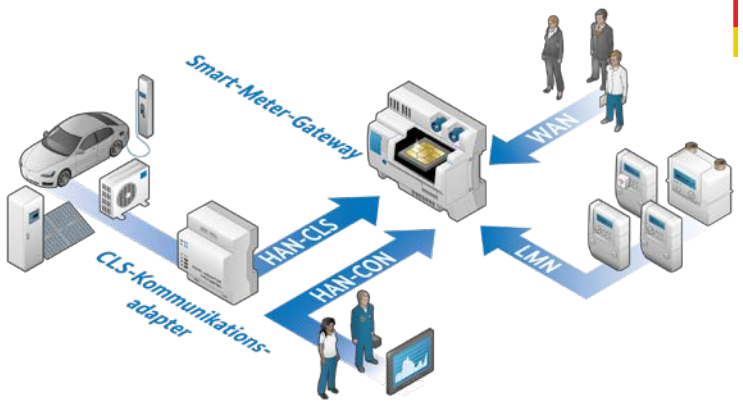


Abbildung 4.1. In dieser TR beschriebene Kommunikationsszenarien

SMGW-Schnittstellen: WAN-Schnittstelle



Ziel und Funktion:

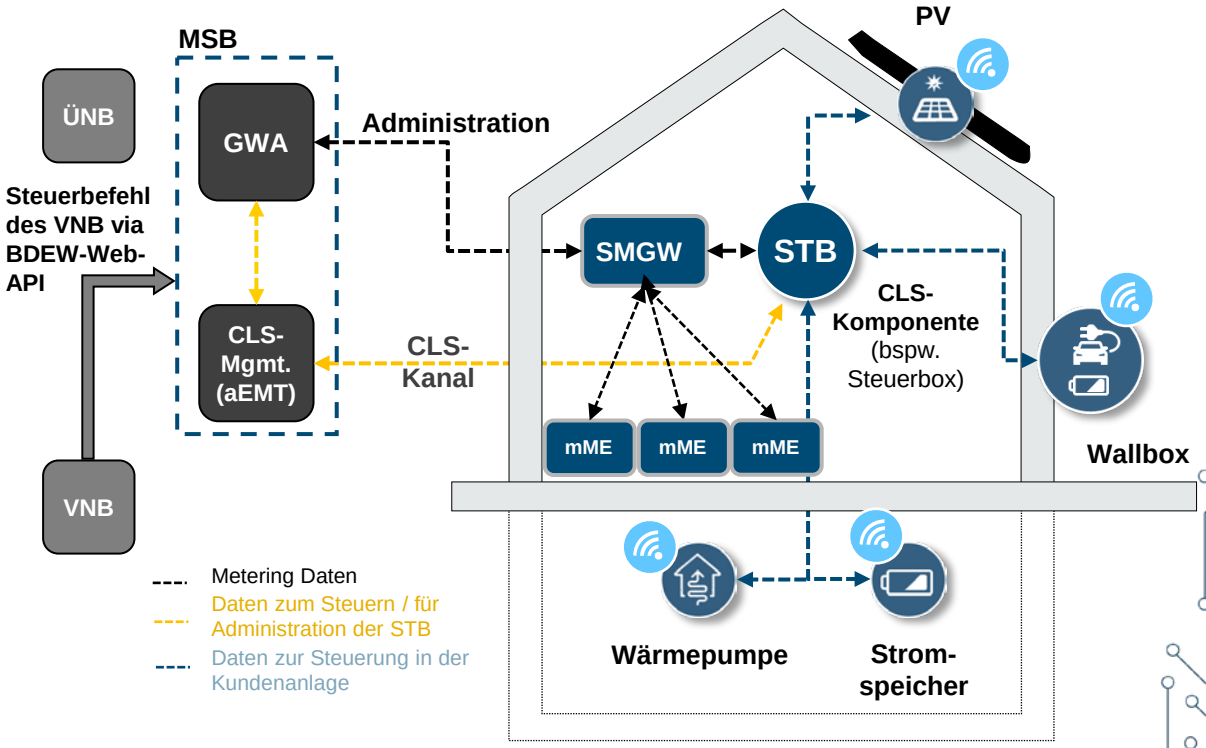
- Sichere, verschlüsselte Verbindung des SMGW zu EMT
- Ermöglicht kontrollierten Datenaustausch und Fernverwaltung durch berechtigte Rollen (z.B. GWA, MSB)

Protokolle:

- HTTP Server (RESTful) | HTTP Client
- TCP/IP
- NTP
- ...

Hauptaufgabe:

- Übertragung von Messwerten, Updates, Zeit- und Zertifikatsdaten sowie Bereitstellung von Status- und Diagnosedaten
- Fernsteuerung und Konfiguration des SMGW durch GWA



Protokollstapel: WAN-Kommunikation

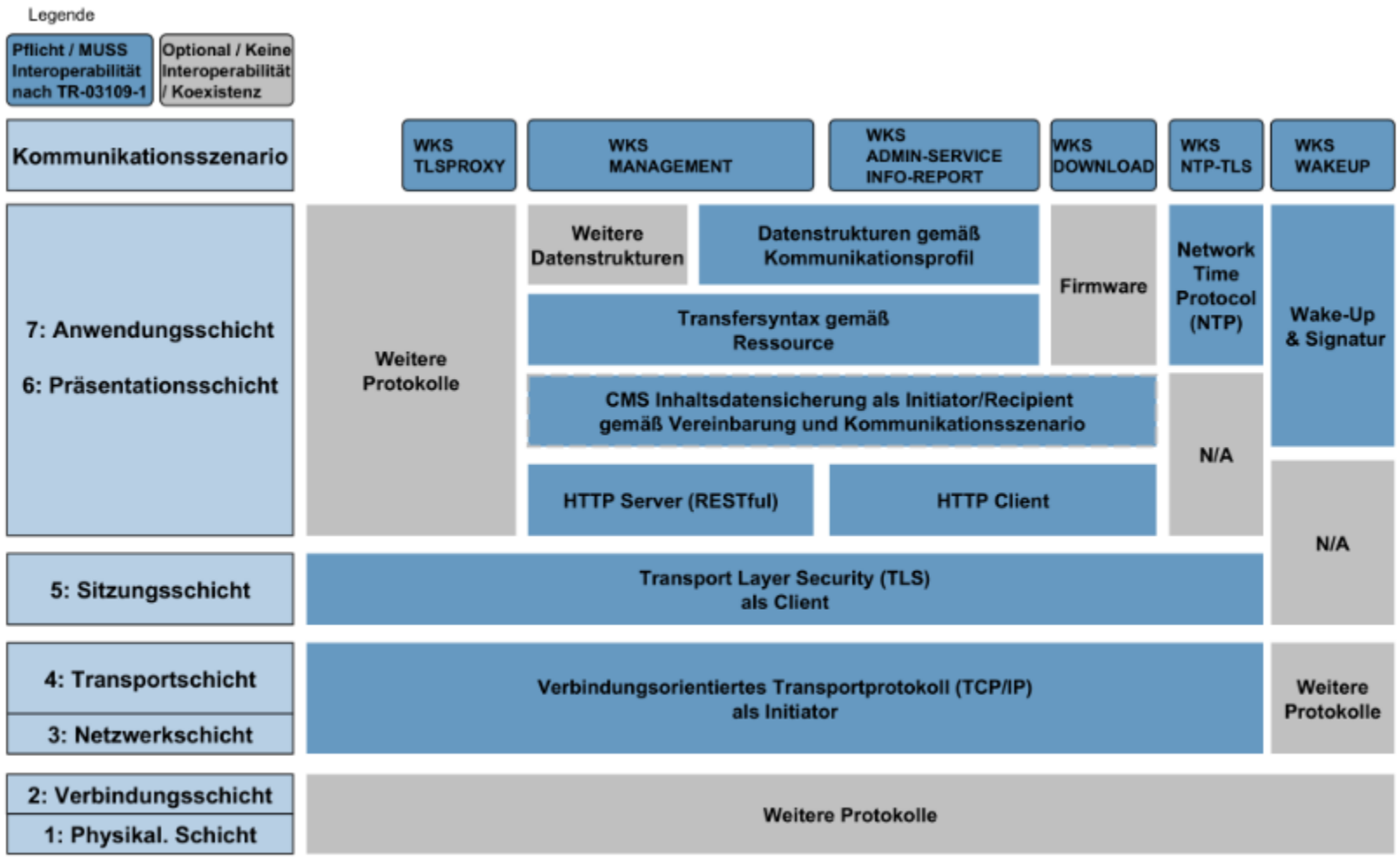


Abbildung 4.2. Protokollstapel für die WAN-Kommunikationsszenarien

5. Deep-Dives in aktuelle Themen

BSI-Standards für das SMGW (PP/TR v2.0) wurden aktualisiert

Mit der TR-03109-1 v2.0 / SMGW-PP v2.0 wurden Ende 2024 zentrale Grundlagen für einen schnelleren und wirtschaftlicheren Rollout bei gleichbleibend hoher IT-Sicherheit geschaffen.

Beschleunigung der Zertifizierungen
Größtmögliche Integration der PTB A-50.8 Anforderungen in TR-1
Herstellung automatisierter Testbarkeit

Tarifierung
Mehrspartenmetering (Gas, Wasser, Thermische Energie)
RLM-Messungen

Mehrwerte für Anschlussnutzer & Infrastruktur
Unverzügliche, interoperable Datenbereitstellung im HAN
Zeitserver + Softwareupdates für angeschlossene Komponenten

Digitaler Netzanschluss
Integrierte Steuerung (Optionales Anforderungspaket, dazu Implementierungshinweis in Vorbereitung)

Interoperabilität
WAN-API: Gemeinsame Erarbeitung mit DKE
HAN-API: Einheitliche Spezifikation (REST + JSON in openAPI)

Nachhaltigkeit
Reduzierung von Datenmengen (z.B. Verzicht auf CMS wo möglich)
Aus- und Wiedereinbau ermöglichen (Datenbereinigung)

Weiterentwicklung / Wartung
Neue TR-Struktur (Fachliche Anwendungsfälle)
Aktualisierung des PP auf neue Common Criteria-Version CC:2022

Weitere SMGW-Einsatzszenarien
Klarstellungen zum optionalen Einsatzort „am Netzknoten“
Abbildung der Einsatzumgebung im PP

Ab 2028 sollen alle neuen und installierten SMGW den erweiterten Funktionsumfang der PP & TR-1 v2.0 abdecken.

TR-03109-5 Übersicht: Zehn zertifizierte CLS-Produkte stehen zur Verfügung

Zur Einbindung der steigenden Zahl der Energiewendeanlagen ist die sichere Anbindung und Steuerung über das iMSys essenzielle Voraussetzung. Die TR-03109-5 („TR-5“) bietet die Basis für die Zertifizierung von CLS-Komponenten.

CLS-Testplattform: Unterstützung bei Entwicklung, bereits >20 Nutzer der CLS-Testplattform zur Konformitätsprüfung nach TR-5

10 zertifizierte CLS-Produkte nach TR-5:

- 5 x Steuerungseinrichtung mit Relaisschnittstelle nach TR-Verfahren: Swistec, Theben, Vivavis, Prolan, EFR
- 2 x Steuerungseinrichtung mit digitaler Schnittstelle nach TR- und BSZ-Verfahren: Theben, PPC
- 2 x Steuerungseinrichtung mit Relais- und digitaler Schnittstelle nach TR- und BSZ-Verfahren: Theben, Vivavis
- 1 x Submeter-Produktlösung (Datenkonzentrator zur Fernauslesung von Wärmemengen) nach TR- und BSZ-Verfahren: PPC

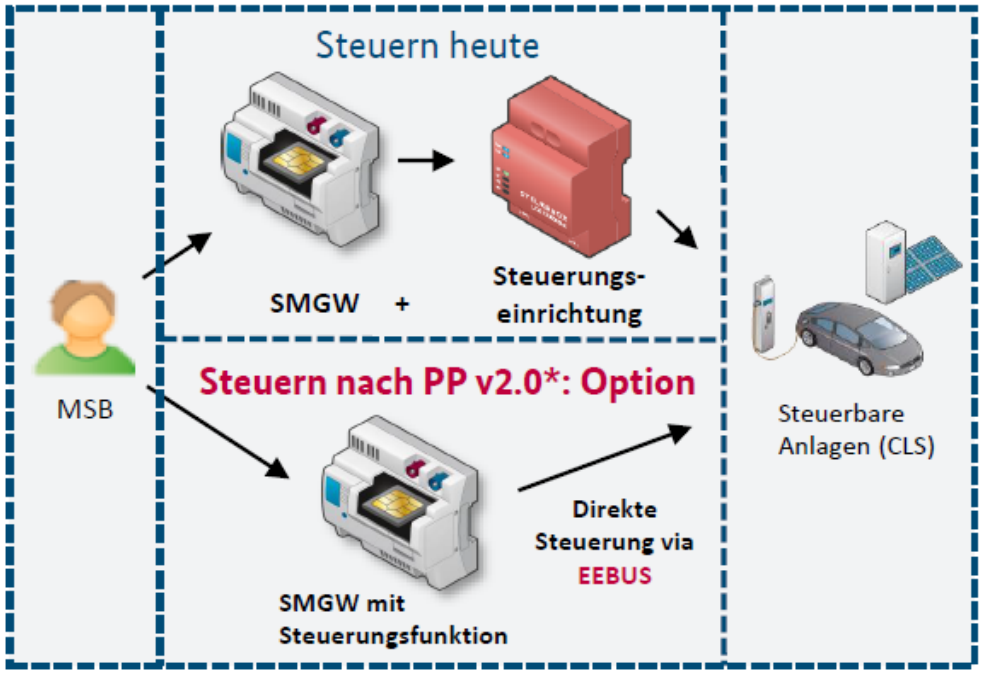
5 weitere CLS-Produkte im Zertifizierungsverfahren nach TR-5:

- 3 x Steuerungseinrichtung mit Relais- und digitaler Schnittstelle im TR- und BSZ-Verfahren
- 1 x Steuerungseinrichtung mit Relaisschnittstelle
- 1 x Submeter-Produktlösung (Datenkonzentrator zur Fernauslesung von Wärmemengen) im TR- und BSZ-Verfahren

Mit den ersten zertifizierten Produkten nach TR und BSZ ist ein wichtiger Schritt für den sicheren und interoperablen Betrieb von CLS-Produkten am SMGW geschaffen.

„Digitaler Netzanschluss“ holt die Steuerung in das SMGW

Bereitstellung von funktionalen Anforderungen, um die direkte interoperable Steuerung aus dem SMGW als zusätzliche Möglichkeit zur „Two-Box-Solution“ über BSI-Standards zu ermöglichen.



Bisher erreicht

- Technische Erprobung in Förderprojekten
- Integration in SMGW-PP 2.0 (Opt. Functional package)
- Impulspapier „Steuerung mit Nachweisführung im SMGW“
- Standardisierungspartner-schaften mit VDE FNN und EEBUS begonnen

Ausblick 2025+

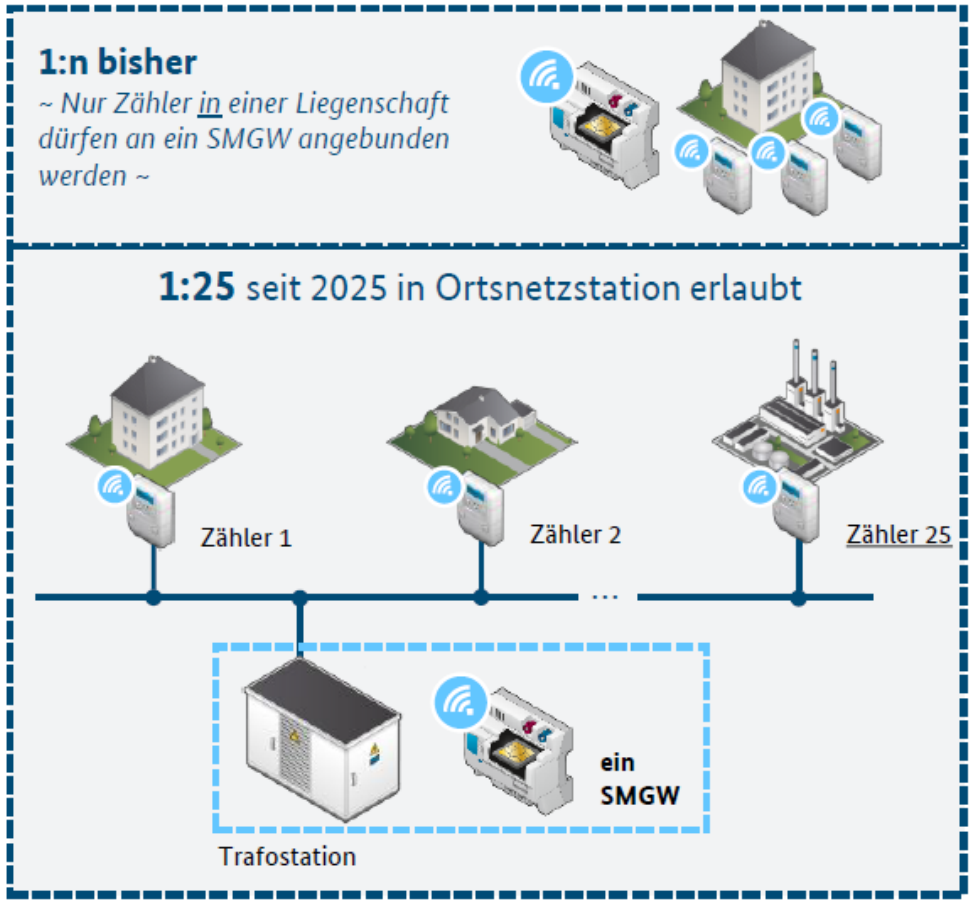
- Implementierungshinweis für direkte Steuerung via EEBUS
- Technische Erprobung des Implementierungshinweises
- Verankerung in der TR-03109-1
- Zusätzliches Angebot für den Markt etabliert

Zukünftig können steuerbare Anlagen direkt mit dem SMGW interoperabel gesteuert werden („One-Box-Solution“).
Im Rahmen von Standardisierungspartnerschaften mit VDE FNN und EEBUS wird ein Implementierungshinweis entwickelt.

** Die Architektur mit integrierter Steuerungsfunktion stellt eine Alternative zur bereits standardisierten Form der Steuerung mit dedizierter Steuerungseinrichtung dar. Diese ist beispielsweise weiterhin für Bestandsanlagen ohne digitale Schnittstelle erforderlich.*

Über „1:n“ – Ansatz skalieren iMSys massiv bei den Kosten

Seit 2025 dürfen SMGW am Netzknoten eingebaut werden → ein „Auslesegerät“ für > 25 Stromzähler*



1:n reduziert Hardwarekosten

✓ In der effektiven Nutzung des 1:n-Ansatz liegt der größte Hebel zur Reduktion der Hardwarekosten

1:n reduziert Prozesskosten

✓ Mit der drahtlosen Anbindung von Zählern an SMGW (Wireless-M-Bus) werden die Installationszeiten massiv reduziert

1:n wird in Trafostationen erlaubt

✓ Seit 2025 können Messstellenbetreiber durch den Einbau von SMGW in Trafostationen durchgängig auf 1:n-Quoten von 1:25 setzen

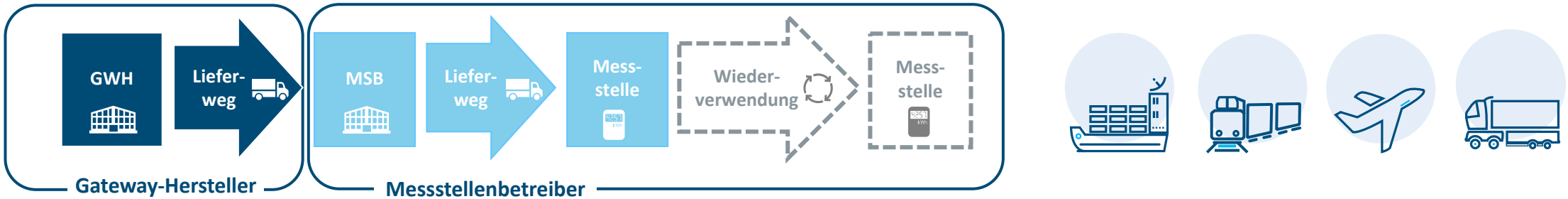
1:n in Trafostationen erschließt bisher nicht-lukrative Einbaufälle

✓ Über ein SMGW in der Trafostation können insbesondere „einfache“ Einbaufälle (Herstellung Sichtbarkeit, Visualisierung) kostengünstig erschlossen werden

** Der 1:n-Ansatz ermöglicht die Anbindung von „n“ Stromzählern an ein SMGW. Seit 2025 dürfen diese SMGW als liegenschafts-übergreifende Funklösung in Trafostationen eingebaut werden*

Anforderungskatalog zum MSB-Lieferkette in Q4/2024 veröffentlicht

Ziel: Es sollte die Sichere Lieferkette vereinfacht und die Massengeschäftstauglichkeit erhöht werden.



Neuerungen zu bestehenden zertifizierten Lieferketten:

- Der Leitfaden zur „MSB-Lieferkette“ formuliert Anforderungen für MSB, die es ermöglichen die Auslieferung sicher und an das eigene Unternehmen angepasst auszugestalten
- MSB muss seine Lieferkette in einem Sicherheitskonzept beschreiben
- MSB kann Maßnahmen massengeschäftstauglich gestalten

BSI begleitet die DigENet Projekte beratend und als Impulsgeber/-nehmer

Ziel: Durch den Förderaufruf DigENet II soll die technologische Stärkung der SMGW-Kommunikationsplattform unterstützt werden und über die Projekte wichtige Impulse zur Weiterentwicklung der BSI-Vorgaben geliefert werden.

Austausch je Quartal

MeGa	PISA	SISSY	WARAN
Messsysteme für Großerzeugungs-Anlagen	**Performance in SMGW Applications**	**SMGW als Sicherheitsanker für das Steuern im Systemverbund**	**Wärme anbinden und netzdienlich nutzen**
Konzept für Steuerung von Großerzeugungsanlagen über das SMGW sowie Feldtest	Weiterentwicklung des SMGWs, des RLM-Zählers und der Steuerbox zu einem vollwertigen iMSys (RLM)	Beschleunigte Umsetzung einer umfassenden, massentauglichen Steuerbarkeit von Flexibilität im gesamten Systemverbund mit iMSys-Infrastruktur	Kopplung des Sektors Wärme (Wärmepumpen und –netze) mit dem Sektor Strom über das iMSys

Die vier Konsortien erarbeiten Lösungsansätze für neue Anwendungen des iMSys im Rahmen ihrer Projektziele. Der Austausch mit dem BSI erfolgt über regelmäßige Termine.

6. Ausblick und Fazit

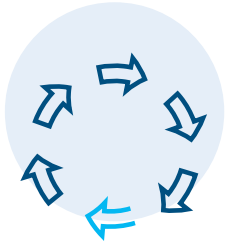
Ausblick: Smart-Meter-Rollout als Enabler für neue Flexibilitätsinstrumente zur Netzkosteneinsparungen

Durch iMSys...

- ✓ werden **mehr Netzzustandsdaten** über die aktuelle Netzauslastung erhoben werden.
- ✓ können **Einspeisung und Verbrauch** flexibel auf die **Netzbelastung** reagieren.
- ✓ können **finanzielle Anreize** gesetzt werden, sich netzdienlich zu verhalten.

... kann Netzausbau reduziert werden, da

- ✓ der Netzbetreiber die **tatsächliche Netzbelastung deutlich präziser** bestimmen und sein **Netz hierauf auslegen** kann.
- ✓ der **Netzbetreiber** in **kritischen Situationen Flexibilität** nutzen kann und das **Netz nicht mehr auf das letzte kW Leistung auslegen** muss.



Reduzierte Netzkosten durch den Pflichtrollout von iMSys mit Steuerungseinrichtungen =

- 1,8 bis 2,5 Mrd. €/a

Dem stehen ca. **27 Mio. iMSys** gegenüber, die nach heutigen POG ca. 1,8 Mrd. €/a zusätzliche Netzkosten verursachen.*

Bundesamt für Sicherheit in der Informationstechnik

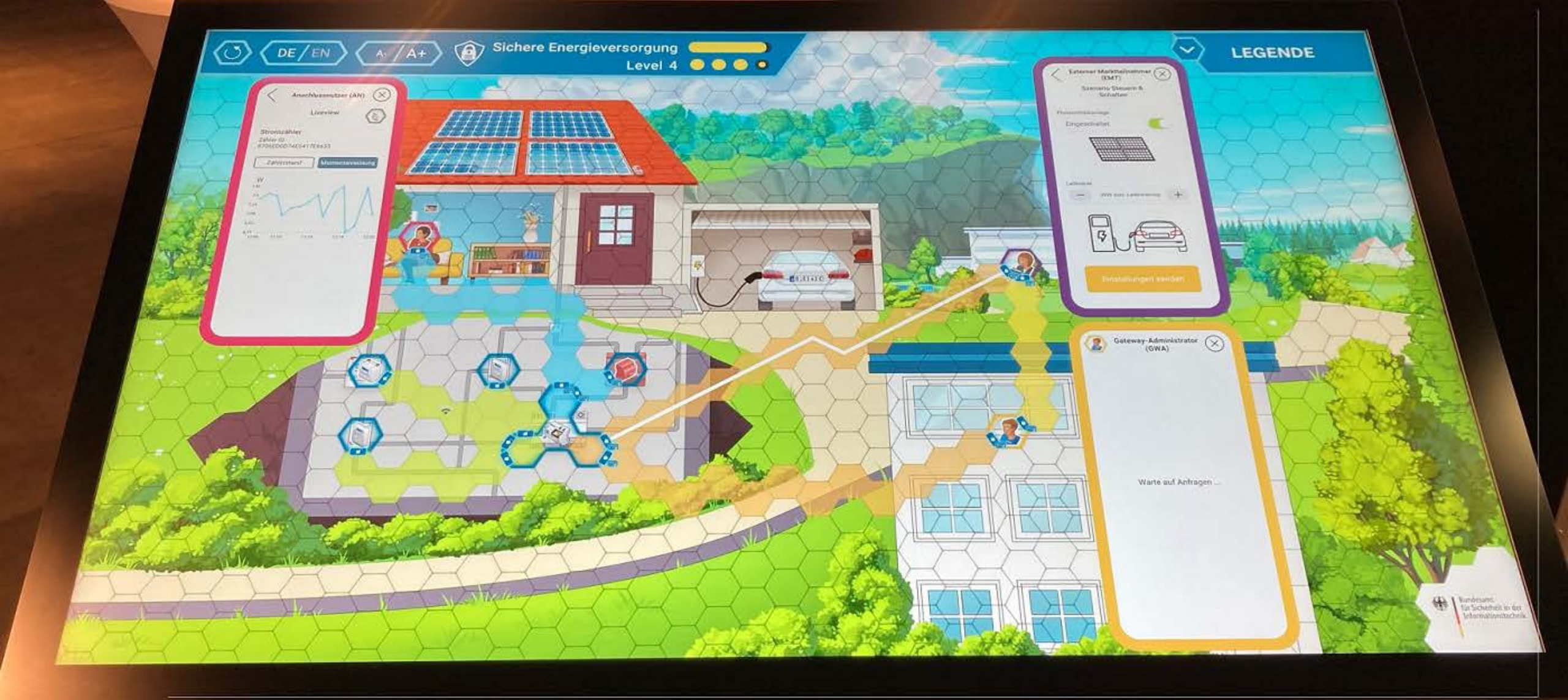
Beschleunigung des Rollouts: BSI-Standards und zertifizierte Gerätetechnik stehen bereit und werden kontinuierlich fortentwickelt

- Wichtigkeit des Themas **Cybersicherheit** steigt in Anbetracht der aktuellen Lage weiter an. Digitalisierung über das intelligente Messsystem ist damit Voraussetzung für das Gelingen der Energiewende.
- **Rollout** muss weiter **beschleunigt** werden. Wir kümmern uns um die Übersetzung der neuen rechtlichen und regulatorischen Anforderungen in Standards und die Zertifizierung benötigter Technik.
- **Zertifizierte Steuerungstechnik** zur Umsetzung von § 14a EnWG und weiteren Steuerungsfällen steht zur Verfügung.
- Intensiver **Austausch aller Stakeholder** bleibt zentral, um Schnittstellenthemen korrekt abzubilden.
- Die Weiterentwicklung der Standards wird aktiv vorangetrieben, beispielweise durch Innovationen wie den **Digitalen Netzanschluss** und Erkenntnisse aus **DigiENet II**

7. Live-Demos des Referats D21

Demonstrator - D21

„Intelligentes Messsystem“



Demo-Tisch - D21

„Intelligentes Messsystem“

D21: Sichere Ladesäuleninfrastruktur für Elektromobilität

Smart-Meter-Gateway: Schlüsseltechnologie für die Digitalisierung der Energiewende

8. Master-Arbeit oder Karriere nach dem Studium beim BSI?

Masterarbeit oder Karriere nach dem Studium beim BSI?

Gestalte die Cybersicherheit Deutschlands mit uns

- Einstiegsmöglichkeiten: Direkteinstieg, Praktikum, Werkstudium, Abschlussarbeiten.
- Viele Kollegen mit Abschluss in Informatik, Elektrotechnik oder IT-Sicherheit.
- Bewerbung: https://www.bsi.bund.de/karriere
- Arbeit mit Sinn: Schutz für Millionen Menschen und unser digitales Energiesystem.

Vielen Dank für Ihre Aufmerksamkeit!

Michael Puchowezki

Michael.Puchowezki@bsi.bund.de
Tel.: +49 (0) 228 9582 6690
Mobil: +49 177 15800770

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn

www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Follow us: