DKE Whitepaper

Sektorkopplung auf Basis sicherer Gateways und Router

Gefördert durch:

Bundesministerium
für Forschung, Technologie
und Raumfahrt

DKE

Whitepaper
Sektorkopplung auf Basis sicherer Gateways und Router
Offenbach

Autoren und Autorinnen:
Mana Azamat, OFFIS
Sebastian Brose, VdS
Mirko Dohse, FSO
Dieter Fischer, TAS
Stephan Holzem, TAS
Daniel Kaumanns, TAS
Stipe Mandic, DKE
Pascal Precht, GSG Oldenburg
Markus Reinke, OFFIS
Christine Rosinger, OFFIS
Athina Savvidis, DKE

Disclaimer:
Dieses Whitepaper wurde in dem durch das vom Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) über den Projektträger Jülich (PtJ) geförderten Projekt WärmewendeNordwest (WWNW) erstellt. Die in diesem Whitepaper vorgestellten Arbeiten stellen eine professionelle Einschätzung von den Projektpartnern des Forschungsprojektes auf der Grundlage von Informationen dar, die zum Zeitpunkt der Erstellung dieses Berichts zur Verfügung standen.
Die Sichtweisen und Meinungen von Autor*innen, die in diesem Dokument zum Ausdruck gebracht werden, entsprechen nicht zwangsläufig den Sichtweisen und Meinungen der gesamten DKE, deren Gremien sowie des BMFTR.

Herausgeber:
VDE Verband der Elektrotechnik Elektronik Informationstechnik e. V.
DKE Deutsche Kommission
Elektrotechnik Elektronik Informationstechnik
Merianstraße 28
63069 Offenbach
Tel. +49 69 6308-0
dke@vde.com
www.dke.de

Design:
Marc Prinz, Maren Maiwald | prinzdesign Berlin

Bildnachweise:
p. 1: natali_mis / stock.adobe.com, p. 8: JJ1990 / stock.adobe.com, p. 11: Have a nice day / stock.adobe.com, p. 15: Nicky / stock.adobe.com, p. 16: Day Of Victory Stu. / stock.adobe.com,

Juni 2025

Inhaltsverzeichnis

Abkürzungsverzeichnis

BMA	Brandmeldeanlagen
BMFTR	Bundesministerium für Forschung, Technologie und Raumfahrt
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-TR	Dachdokument BSI-TR-03109 einschließlich aller dort benannten Verweise
BSI-PP	Sicherheitsanforderungen gemäß BSI-CC-PP-0073 (Bewertung und Schutzprofile)
CLC	CENELEC
CLS	Controllable-Local System
DIN	Deutsches Institut für Normung e. V.
DKE	DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik
EMA	Einbruchmeldeanlagen
EMT	Externer Marktteilnehmer
EN	Europäische Norm
EVU	Energieversorgungsunternehmen
FF2	Forschungsfeld 2 des Projektes WWNW
FSO	FSO Fernwirk-Sicherheitssysteme Oldenburg GmbH
GMA	Gefahrenmeldeanlagen
GWA	Gateway-Administrator
GNDEW	Gesetz zum Neustart der Digitalisierung der Energiewende
GSG	GSG OLDENBURG Bau- und Wohngesellschaft mbH
IEC	International Electrotechnical Commission
LAN	Local-Metrological-Network
OFFIS	OFFIS e. V. Institut für Informatik
TAS	Telefonbau Arthur Schwabe GmbH & Co. KG
TC	Technical Committee
TR	Technische Richtlinie
ÜMA	Überfallmeldeanlage
VDE	VDE Verband der Elektrotechnik Elektronik Informationstechnik e. V.
VDE FNN	Forum Netztechnik/Netzbetrieb
VdS	VdS Schadenverhütung GmbH
WAN	Wide-Area-Network
WWNW	BMFTR-Förderprojekt WärmewendeNordwest
ZuKo	Zutrittskontrollsystem

Executive Summary

Dieses Whitepaper ist im Rahmen des BMFTR-Förderprojekts „WärmewendeNordwest“ im Forschungsfeld 2 (FF2) mit dem Titel „Sichere Gateways und Router als Grundlage für Mehrwertdienste“ erarbeitet worden. An FF2 sind Akteure der Forschung, Normung und Zertifizierung sowie Akteure der Sicherheitstechnikbranche beteiligt (DKE, VdS, TAS, FSO, OFFIS). Zusammen wird in FF2 eine sektorübergreifende Kommunikationsinfrastruktur unter Einbindung aller im Projektkontext betrachteten Anforderungen der Energiewirtschaft und der Sicherheitstechnikbranche und im Speziellen unter Einbeziehung des Smart Meter Gateways (SMGW) entwickelt.

Bei sicherheitsrelevanter Datenübertragung hat die Sicherheit gegen unbefugten Zugriff auf die Daten und die Gerätefunktionen oberste Priorität. Angriffe auf Gateways und Router im Netzwerk sind keine theoretische Möglichkeit, sondern eine reale Gefahr im Cyber Security Kontext. Sowohl die vom BSI zertifizierten SMGW als auch VdS-anerkannte Alarmübertragungsgeräte nach DIN EN-Normen wurden gegen alle diese Bedrohungen gehärtet. Es unterscheiden sich die Methoden, Sicherheit zu erreichen und nachzuweisen (PP-CC vs. DIN EN-Normen).

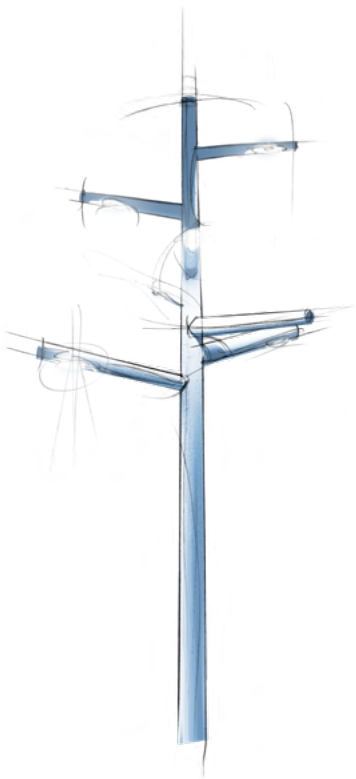
Obwohl für den eigentlichen Übertragungsweg über öffentliche Netzbetreiber hinweg bisher in den BSI-TR keinerlei Vorgaben enthalten sind (WAN-Schnittstelle[1]), ergibt es Sinn, hochverfügbare und schwarzfall-resiliente Übertragungswege zu nutzen, wie sie in der Absicherung gegen Einbruch, Überfall und Feuer schon lange Stand der Technik sind. Alle Daten, in einem Gebäude, die bisher nicht in einem SMGW erfasst werden und über das WAN transportiert werden müssen, sollten über den Sicherheitsrouter abgesichert übertragen werden.

Eine Nutzung der sicheren Übertragungsplattform nach EN 50710 und CLC/TS 50136-10 auch für SMGW hat also keinerlei Nachteile und erfüllt die gesetzlichen Anforderungen an die Messstellenanbindung. Das vorliegende Whitepaper erläutert die Hintergründe und Begründungen für diese Einschätzung und stellt sie in Relation zu anderen, derzeit verfolgten Ansätzen.

Im Rahmen dieser Gegenüberstellung wurden Handlungsempfehlungen erarbeitet, die relevanten Normungskreisen zur Verfügung gestellt werden sollen, um entsprechende Maßnahmen hieraus abzuleiten:

- Erweiterung des Scopes der DIN EN 50136: Übertragung von SMGW- Datenpaketen sowie Smart-Home Anwendungen und anderen Gebäudedaten mit Sicherheitsanforderungen
- Erweiterung des Scopes der VdS-Richtlinien: Übertragung von SMGW-Datenpaketen sowie Smart-Home Anwendungen und anderen Gebäudedaten mit Sicherheitsanforderungen
- Erweiterung des Scopes der DIN EN 50136: Übertragung der Datenmodelle des IEC TC 57 zwischen Smart-Grid und Gebäudemanagement-Systemen. Hierzu eignen sich die bereits in der DIN EN 50136 definierten Strukturen.
- Ergänzung der BSI-TR-03109 bezüglich der Möglichkeit, eine schwarzfall-resiliente Übertragungsstrecke für das SMGW gemäß DIN EN 50136 zu nutzen.

Abschließend wird als Ausblick auf die hieraus resultierenden Vorteile der Kosten-, Ressourcen- und Energieeffizienz hingewiesen und die Möglichkeit zur Beschleunigung der Energiewende in Aussicht gestellt.



1 Die WAN-Schnittstelle wird in diesem Dokument als physikalischer Übergabepunkt an das öffentliche Übertragungsnetz definiert.

1 Sichere Gateways und Router auf Grundlage für Mehrwertdienste

Das Forschungsfeld 2 (FF2) aus dem BMFTR-geförderten Forschungsprojekt WärmewendeNordwest (WWNW) mit dem Titel „Sichere Gateways und Router auf Grundlage für Mehrwertdienste“ fokussiert eine Schlüsselrolle bei der Realisierung des „Internets der Funktionen, Dinge, Energie und Dienste“.
Die Ansätze des Forschungsvorhabens versprechen eine deutliche Steigerung von Effizienz und Produktivität diverser digitaler Anwendungen und Kommunikationsverbindungen. Hierfür sollen bestehende Sektoren miteinander gekoppelt und bestehende Infrastrukturen der Alarmbearbeitung mit den zukünftig auf Gewerke zukommenden Anforderungen der Energiewirtschaft in Einklang gebracht werden. Hierbei liegt der Schwerpunkt auf Bestandsgebäuden, die ebenjene Gebäudeüberwachung bereits nutzen und die- se Infrastruktur nun mit den Anforderungen der Elektrizitäts- und Wärmeversorgung kombinieren. Durch die Nutzung derselben Infrastruktur können, über bestehende Kanäle, sowohl das Liegenschaftsmanagement um weitere Gebäudedaten, als auch die Zahl der steuerbaren Technologien, wie Wärmemengenzähler, Speicher, Aufzüge und Geräte aus dem Smart Home Bereich, erweitert werden.

Die Kopplung der Übertragungsinfrastruktur mit sektorübergreifender Digitalisierung wird im „Gesetz zur Digitalisierung der Energiewende (GDEW)“ ausdrücklich gefordert. Es ist somit eine Rahmenbedingung für die Modernisierung des „Smart Grid“. Neben der Neuorganisation und Nutzung, sowie Bereitstellung der sicheren Übertragungstechnik auf denselben Übertragungswegen wie Gebäudedaten oder Notrufsysteme, ist die Bereitstellung einer transparenten Plattform sinnvoll und wünschenswert.
Eine solche Plattform ermöglicht neue Geschäftsmodelle für bestehende Unternehmen und bietet die Chance, Mehrwertdienste für Nutzer jeglicher Art zu realisieren.

Viele Bestandsgebäude sind bereits mit umfassender Gebäudetechnik ausgestattet. Hierbei agieren diverse heterogene IT-Systeme zur Überwachung, Steuerung und Verwaltung der ihnen zugewiesenen Komponenten. Diese IT-Systeme agieren nicht nur weitestgehend unabhängig und eigenständig, sondern werden bisher nicht in der Gesamtheit der Gewerke betrachtet. So fokussiert der Ansatz der Technischen Richtlinien 03109 des BSI derzeit die Anforderungen der elektrischen Energiewirtschaft und der Messung des Gasverbrauchs, z.B. Fernwärme und Wasser sind derzeit nicht im Fokus des BSI.

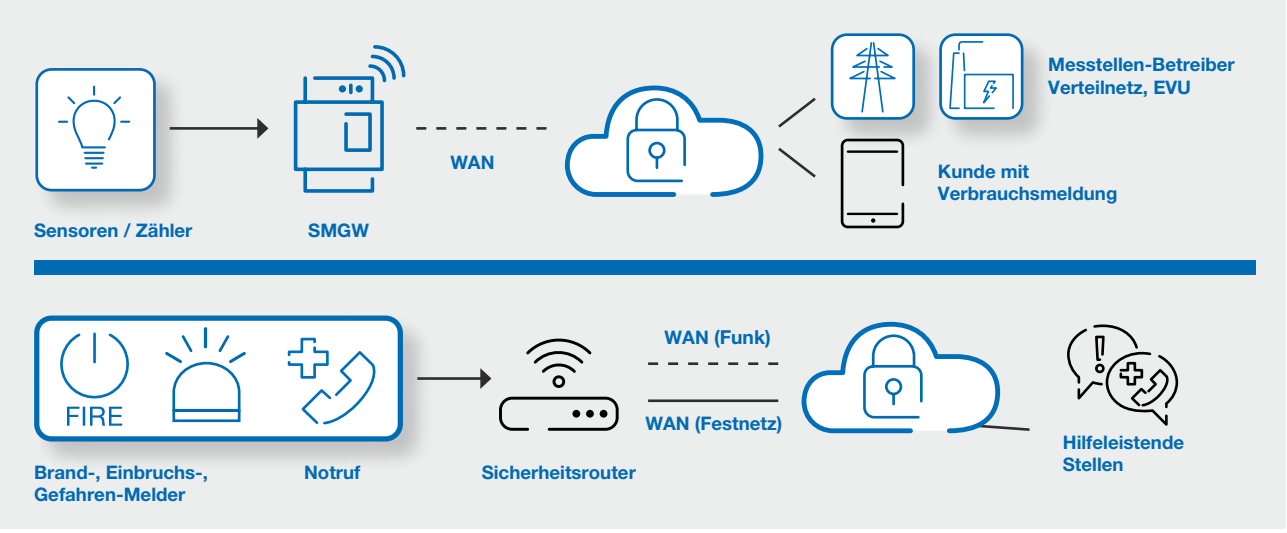


Abb. 1: Aktueller Status: Getrennte Übertragungsplattformen für Energiezähler und alle anderen Gewerke (vereinfache Darstellung)

Für eine erfolgreiche Sektorkopplung müssen alle im Gebäude vorhandenen Gewerke mit einbezogen werden können. Hierbei müssen alle anfallenden Daten, Meldungen sowie Aktoren mit ihren technischen und sicherheitsrelevanten Anforderungen in die Betrachtung einbezogen werden.
Mithilfe geschlossener Datenmodelle und offener Schnittstellen über die gesamte Prozesskette wird erst ein Zusammenschluss verschiedener Sektoren möglich. Eine weitgreifende Vernetzung könnte helfen, übergreifende Anforderungen, wie z.B. das Optimieren von Energieverbräuchen, zu ermöglichen.
Die Eindeutigkeit und Sicherheit der Daten müssen hierfür jedoch zu jeder Zeit gewährleistet sein. Übertragene Daten dürfen auf der kompletten Übertragungsstrecke keinen Interpretationsspielraum lassen und müssen eindeutig sein. Unter Einhaltung der herausgestellten Strukturen und Schnittstellen ist es möglich, dass verschiedene Unternehmen ein Teil des Prozesses werden können.

Weiter schützenswert sind Daten über Netzzustand, Erzeugung und Verbrauch in Energienetzen sowie von Alarmzuständen im Gebäude. Um Angriffe auf das System und resultierende Datenlecks zu vermeiden, wird im kompletten Erhebungsprozess „Privacy & Security by Design“ gelebt. Praktische Vorgaben für die sichere Umsetzung bieten hierbei die Technischen Richtlinien des BSI (BSI-TR-03109) und die Richtlinien des VdS für die Alarmübertragung. Die europäische Normen der Alarmübertragungstechnik und die Richtlinien des VdS sollten die weiteren Gewerke im Gebäude mit berücksichtigen.

1.1 Forschungsfeld 2 im Kontext zum Gesamtvorhaben WWNW

Im Zuge des Gesamtvorhabens spielt das Forschungsfeld 2 eine wichtige Rolle in der Strukturschaffung sicherer Datenübertragung verschiedenster Liegenschaften. Der Fokus liegt auf der sicheren Übertragung sicherheitskritischer Alarmmeldungen an hilfeleistende Stellen und Interventionsdienste. Hinzu kommen standardisierte Übertragungswege von Energiemessungen, die parallel zu den Alarmübertragungswegen an die hierfür vorgesehenen Stellen angebunden sind. Wichtig für die Behandlung energierelevanter Messungen sind unter anderem die technischen Richtlinien des BSI mit Vorgaben für intelligente Messsysteme und deren sicheren Betrieb (BSI-TR-03109). Ziel des Forschungsvorhabens im Zuge von WWNW ist es, Lösungen für die Sektorkopplung zu erarbeiten und dabei Anpassungsvorschläge für die Synchronisation der BSI-TR-03109 mit den etablierten Verfahren der Alarm- und Notrufübertragungstechnik zu geben. In WWNW wird hierbei im Feld ein sicherer Router eingesetzt, der verschiedenen Akteuren mittels einer sicheren Plattform die Möglichkeit bietet, Teil dieser Infrastruktur zu sein (siehe Kapitel 3). Aufgrund einer Microservice Architektur[2] haben alle Anbieter der Plattform die komplette Datenhoheit, da alle Anwendungen getrennt von den übrigen Systemen funktionieren. Die sichere Übertragungstechnik kann bei energetischen Optimierungen des Gebäudes installiert werden und somit eine sichere Infrastruktur schaffen, die die notwendigen Gewerke vereint. Dies bietet einen gemeinsamen Mehrwert für Wohnungswirtschaft, Sicherheitstechnik und Bewohner.[3]

2 Microservice Architekturen bestehen aus Gesamtlösungen, welche sich aus mehreren kleinen Anwendungen zusammensetzen. Die Anwendungen sind auf einer Plattform lose miteinander gekoppelt durch standardisierte Schnittstellen und können hierdurch getrennt voneinander agieren. Die verschiedenen Microservice Dienste können temporär aussetzen, ohne das Gesamtsystem zum Ausfall zu bringen. vgl. https://www.ibm. com/de-de/cloud/learn/microservices Abruf 14.02.2024

3 Vgl. https://www.waermewende-nordwest.de/projekt/forschungsfelder-und-querschnittsaktivitaeten/f/forschungsfeld-2/ Abruf 14.02.2024

1.2 Beschreibung des Forschungsfeldes 2 (Status Quo)

Das WWNW-Forschungsfeld 2 beschäftigt sich mit aktuellen Richtlinien für sichere Alarm- und Notrufübertragungstechnik. Hierbei stehen sich unterschiedliche Gewerke gegenüber. Die verschiedenen Interessensvertreter haben abweichende Ansichten und Richtlinien, die es zu erfüllen gilt. Neben den aus der Übertragungstechnik bekannten Richtlinien des VdS gibt es weitere Gewerke, die es in gesicherten Ökosystemen zu beachten gibt. Die Aufgabe des FF2-Konsortiums ist es, diese verschiedenen Player mit unterschiedlichen Gewerken zu verbinden. Denn die Anforderungen an sichere Übertragungen steigen stetig. Neben den bekannten Richtlinien kommen nun unter anderem Gremien im Austausch mit dem BSI hinzu.

Das BSI hat im Zuge des Smart Meter Gateway Rollout technische Richtlinien und ein Schutzprofil verabschiedet, die es einzuhalten gilt, um die Sektorkopplung zu ermöglichen. Die existierende Hardwarelösung des Sicherheitsrouters wird bereits mit Erfolg in der Sicherheitstechnik angewandt. Diese soll bestmöglich mit den Smart Meter Gateways abgestimmt werden. Unter Berücksichtigung dieser Vorgaben des BSI, wären nach Erkenntnissen des Projektes Änderungen notwendig, um die Infrastrukturen möglichst performant zu kombinieren. Änderungen gilt es unter Berücksichtigung der gesetzlichen Vorgaben in Fachgremien zu kommunizieren.

Hierzu sind Teilziele ein wichtiger Faktor. Zunächst werden die Anwendungsfälle aus den zu vereinenden Bereichen beschrieben. Im weiteren Verlauf werden Möglichkeiten dargeboten, die bestehenden Infrastrukturen über ein gemeinsames Gateway den unterschiedlichen Dienstanbietern zur Verfügung zu stellen.[4]

4 Vgl. https://www.waermewende-nordwest.de/projekt/forschungsfelder-und-querschnittsaktivitaeten/f/forschungsfeld-2/ Abruf 14.02.2024

1.3 Die Akteure aus WWNW-FF2

Das FF2 zeichnet sich durch Partner verschiedenster Branchen aus, die gemeinsam die Aufgaben-stellungen bewältigen und die optimalen Lösungen für die Sektoren finden. Vertreten sind Partner aus Normungsgremien, wie die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik (DKE), sowie Prüf- und Zertifizierstellen, wie die VdS Schadenverhütung GmbH.

Die **DKE** ist die in Deutschland zuständige Organisation für die Erarbeitung von Normen, Standards und Sicherheitsbestimmungen im Bereich der Elektrotechnik, Elektronik und Informationstechnik. Sie vertritt deutsche Interessen im Europäischen Komitee für Elektrotechnische Normung (CENELEC) und in der Internationalen Elektrotechnischen Kommission (IEC).

VdS gehört zu den weltweit renommiertesten Institutionen für die Unternehmenssicherheit mit den Schwerpunkten Brandschutz, Security, Naturgefahrenprävention und Cyber Security. Die Dienstleistungen umfassen Risikobeurteilungen, Prüfungen von Anlagen, Zertifizierungen von Produkten, Firmen und Fachkräften sowie ein breites Bildungsangebot. DKE und VdS sind die Schnittstelle zur Kommunikation in Fachgremien. Hinzu kommen Partner aus der Praxis, die die Technologien zur Verfügung stellen, verwalten oder nutzen.

Die sichere Infrastruktur wird von **Telefonbau Arthur Schwabe GmbH & Co. KG (TAS)** entwickelt und betrieben. TAS ist spezialisiert auf die technische Absicherung von Liegenschaften und ist führender Hersteller und Anbieter von Netzwerk-gestützten Alarmübertragungssystemen.

Die Überwachung der im Projektkontext verbauten Technik übernimmt die **Fernwirk-Sicherheitssysteme Oldenburg GmbH (FSO)**. Als Partner-Leitstelle für Errichter, Konzessionäre, NSL-Betreiber, Hersteller und Energieversorger steht FSO so für eine zukunftsorientierte und vertrauensvolle Zusammenarbeit. Mit der nach DIN EN 50518 zertifizierten Alarmempfangsstelle und dem dazugehörigen Rechenzentrum für Sicherheitstechnik steht die FSO für den höchsten europäischen Sicherheitsstandard, um den Bedürfnissen der Kunden zu entsprechen.

Für die wissenschaftliche Begleitung ist **OFFIS** zuständig. Das 1991 gegründete Institut für Informatik, OFFIS, erforscht und entwickelt anwendungsorientierte Konzepte, Lösungen und Prototypen für Informations- und Kommunikations-Systeme. OFFIS verfügt über breites Wissen im Entwurf standardisierter Systeme für IT-Strukturen, Schnittstellenbewertungen und technologische Innovationszyklen. Zudem verfügt OFFIS über Expertise von föderierten Daten- und Service-Plattformen.

Die Gebäude für den Einbau der im Zuge des Projektes entwickelten Prototypen bietet die **GSG Oldenburg Bau- und Wohnungsgesellschaft mbH (GSG)**. Als einer der größten Anbieter von Wohnraum in Oldenburg verwaltet die GSG OLDENBURG rund 10.000 Wohneinheiten. Sie kümmert sich um die Mietbetreuung und um sämtliche Facetten der kaufmännischen Verwaltung, wie etwa die Abrechnung der Betriebskosten bis hin zum Bauträgergeschäft und der Bewertung von Immobilien und Marktlage. Die GSG verwaltet auf dem Gelände des Fliegerhorst in Oldenburg ein Reallabor und hilft somit in Feldtests diese Vorhaben einzubringen.

Der Zusammenschluss dieses Konsortiums verfügt über die Expertise aus bekannten Normungsgremien, Industriepartnern mit langjähriger Erfahrung in den Bereichen der Übertragungstechnik sowie Wohnungsgesellschaften, die die Technik direkt in mehreren Gebäuden nutzen und testen können. Zudem komplettieren Partner aus der Wissenschaft das Konsortium, die die gewonnenen Erkenntnisse weiterentwickeln und fundiert untersuchen können. Das Aufbauen auf den erlangten Erkenntnissen können somit zu einem sich stetig entwickelnden Multiplikator für Normung und Unter-nehmen werden.[5]

5 Vgl. https://www.waermewende-nordwest.de/, Abruf: 14.02.2024

2 Standardisierungsrahmen

Alle Beteiligten in einem Gebäude mit Daten und Steuerungsbedarf benötigen eine effiziente und sichere Übertragung, die nur durch eine gemeinsame Infrastruktur umgesetzt werden kann.
Um die definierten Ziele des Projekts zu erreichen, ist die Einbindung von Normung und Standardisierung essenziell. In diesem Kapitel werden die relevanten Normungsgremien und Institutionen, die für die in dem Whitepaper betrachtete Sektorkopplung relevant sind, näher dargestellt.

2.1 Relevante Normungsgremien

Folgende nationale, europäische und internationale Normungsgremien sind für die in diesem Whitepaper betrachtete Sektorkopplung relevant:

Gefahrenmelde- und Überwachungsanlagen		
National	DKE/K 713	Gefahrenmelde- und Überwachungsanlagen
Europäisch	CLC/TC 79	Alarm and electronic security systems
International	IEC/TC 79	Alarm and electronic security systems

Brandmelde- und Feueralarmanlagen		
National	DIN/ NA 031-02 FBR	Fachbereichsausschuss Brandmelde- und Feueralarmanlagen
Europäisch	CEN/TC 72	Fire detection and fire alarm systems
International	ISO/TC 21/SC 3	Fire detection and alarm systems

Elektrische Systemtechnik für Heim und Gebäude (ESHG)		
National	DKE/K 716	Elektrische Systemtechnik für Heim und Gebäude (ESHG)
Europäisch	CLC/TC 205	Home and Building Electronic Systems (HBES)
International	IEC/TC 23	Electrical accessories

Active Assisted Living (AAL)		
National	DKE/K 801	System Komitee AAL
Europäisch	CEN/CLC/JTC 12	Design for All
International	IEC/SyC AAL	Active Assisted Living

Messeinrichtungen und -systeme für Elektrizität		
National	DKE/K 461	Messeinrichtungen und -systeme für Elektrizität
Europäisch	CLC/TC 13	Electrical energy measurement and control
International	IEC/TC 13	Electrical energy measurement and control
Smart Energy		
National	DKE/K 901	System Komitee Smart Energy
Europäisch	CEN/CLC/ETSI	CEN-CENELEC-ETSI Coordination Group on Smart Energy Grids
International	IEC/SyC Smart Energy	System Komitee Smart Energy
Netzleittechnik		
National	DKE/K 952	Netzleittechnik
Europäisch	CLC/TC 57	Power systems management and associated information exchange
International	IEC/TC 57	Power systems management and associated information exchange
Koordinierung im Umfeld intelligenter Messsysteme		
National	TBINK/AK_BMWK_BSI	„Koordinierung im Umfeld der intelligenten Messsystemen“ Informationsaustausch zum Thema „Metering und Umfeld im Kontext der intelligenten Messysteme“
Europäisch	--	--
International	--	--

Tabelle 1: Relevante Gremien auf nationaler, europäischer und internationaler Ebene für die Sektorkopplung

Ausführliche Beschreibungen der in Tabelle 1 benannten Gremien sind im **Anhang A** zu finden.

2.2 Nationale Institutionen

Folgende nationale Institutionen sind für die in diesem Whitepaper betrachtete Sektorkopplung relevant:

- VDE Verband der Elektrotechnik Elektronik Informationstechnik (VDE)
- DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik (DKE)
- VDE FNN Forum Netztechnik/Netzbetrieb im VDE (VDE FNN)
- DIN Deutsches Institut für Normung
- VdS Schadenverhütung GmbH
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA)

Ausführliche Beschreibungen der nationalen Institutionen sind im **Anhang B** zu finden.

3 Digitale Architektur

In diesem Kapitel wird der Fokus auf die Lösungsansätze im Projekt SiGRun gelegt. Um den geeigneten Lösungsansatz herauszufinden, werden zwei lokale Lösungsansätze gegenübergestellt.

3.1 Gegenüberstellung zwei lokaler Lösungsansätze

3.1.1 Lösungsansatz „Grundidee BSI – CLS – Schnittstelle für Smart-Home“

Das ursprüngliche Ziel des Smart-Meter-Gateways (SMGW) im Sinne der Sektorkopplung war es, neben der Erfassung und Weiterleitung von Verbrauchsdaten auch für Smart-Home- und Smart-Grid-Anwendungen eine Übertragungsplattform zu bieten. Zu diesem Zweck ist die CLS-Schnittstelle definiert worden, die einen transparenten Übertragungsweg über eine verschlüsselte Verbindung zu einem externen Marktteilnehmer (EMT) bereitstellt. In der folgenden Abbildung 2 ist dargestellt, wie die Sicherheitstechnik in die Übertragungsstrecke des SMGWs integriert werden sollte.

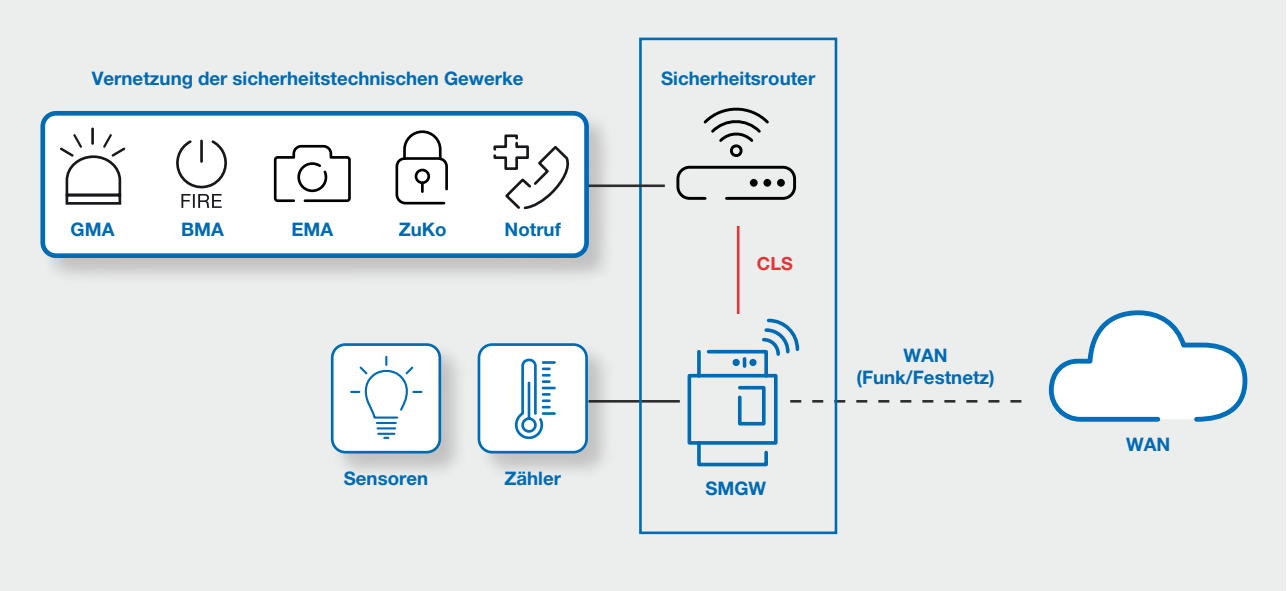


Abb. 2: Anbindung Sicherheitstechnik gem. BSI/ BMWi-Roadmap zur Energiewende

Sicherheitstechnische Meldungen der Gefahrenabwehr oder der Unterstützung hilfebedürftiger Personen sind ein wesentlicher Teil von Smart-Home-Anwendungen. Für diese Meldungen existieren europäische und internationale Normen und Richtlinien (u.a. DIN EN 50136, VdS 2471), die die CLS-Schnittstelle gegenwärtig alleine nicht erfüllen kann, da der beschriebene Lösungsansatz (siehe Abbildung 2) in Verbindung mit Sicherheitsanwendungen folgende Nachteile hat:

- Mindestens ein zusätzlicher, unabhängiger Übertragungsweg ist weiterhin erforderlich
- Keine klare Verantwortungsabgrenzung für die Verfügbarkeitsüberwachung der WAN-Übertragungsstrecke
- Keine einheitliche Remote Access Infrastruktur
- Der Sicherheitsrouter kann die Verfügbarkeit der CLS-Übertragungsstrecke nicht erkennen

3.1.2 Lösungsansatz „SMGW nutzt sichere Übertragungswege gem. DIN EN-Norm“

Um das ursprüngliche Ziel der Sektorkopplung aller Anwendungen im Gebäude oder der Liegenschaft zu erreichen, muss die Erfassung und Zwischenspeicherung von Verbrauchsdaten in einer Ebene wie Alarmanlagen, Notrufübertragungstechnik und sonstigen Smart-Home-Einrichtungen gesehen werden, die über einen Sicherheitsrouter gemeinsam die redundant aufgebaute, sicherheitstechnische Plattform über verschlüsselte Übertragungswege nutzen (wie in Abbildung 3 dargestellt). Die sichere Verbindung von SMGW zum SMGW-Admin und zum EMT der Energiewirtschaft bleibt dabei unverändert zum bestehenden SMGW-Roll-Out.

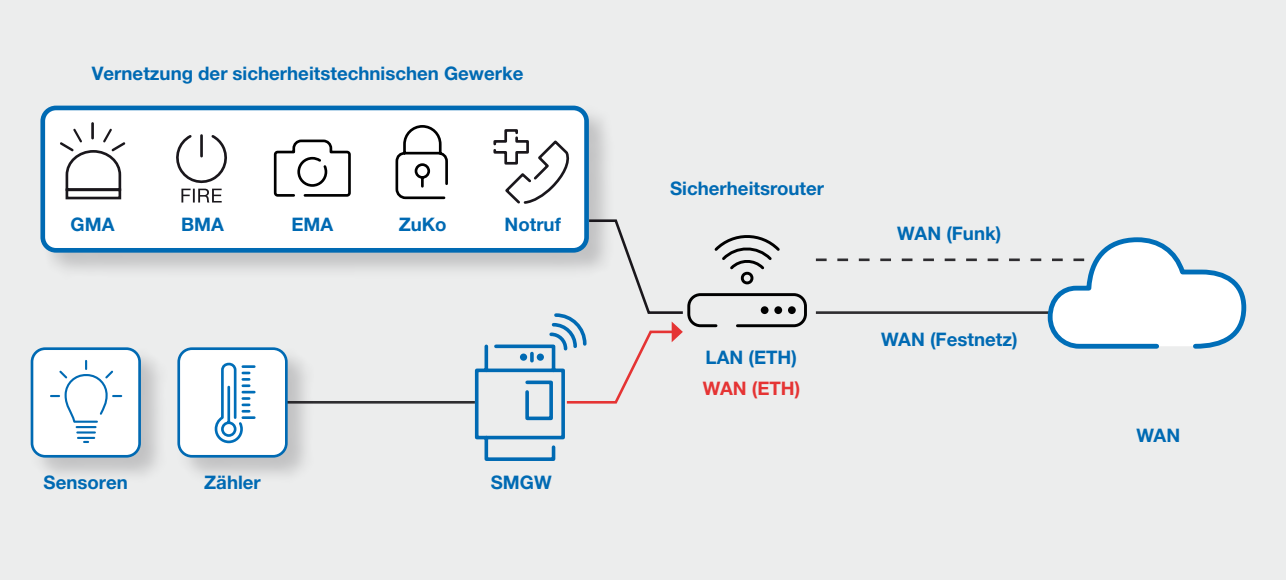


Abb. 3: Vorschlag zur gemeinsamen, kosteneffizienten Nutzung der Kommunikationsschnittstelle der sicheren und redundanten Übertragungstechnik für alle Gewerke.

Der in diesem Abschnitt beschriebene Lösungsansatz hat also mehrere Vorteile gegenüber dem Lösungsansatz nach 3.1.1:

- Nutzung redundanter Netzzugänge über DSL, Funk, LWL für zeit- und verfügbarkeitsrelevante Steuerungen
- Sichere Verbindung auch bei schlechtem Mobilfunk-Empfang am SMGW-Einbauort
- Schwarzfall-Resilienz durch Notstromversorgung des Sicherheitsrouters inkl. der Übertragungswege
- Permanente Überwachung der Übertragungswege und der Stromversorgung von Schalthandlungen
- Nutzung der etablierten, standardisierten Sicherungskette des VdS im Sinne der Sektorkopplung
- Verbesserte Nutzungsmöglichkeit auch für zeitkritische Übertragung Schalthandlungen

3.2 Anforderungen an die Plattform

Mit den Normen und Richtlinien EN 50710 sowie CLC/TS 50136-10 ist die Remote Access Infrastruktur und die damit verbundenen Dienstleistungen beschrieben und reglementiert. Die Abbildung 4 zeigt den dort beschriebenen Infrastrukturaufbau und die Verantwortung. Aufgrund der Notwendigkeit von Fernzu- griffen für proaktive Wartungen oder Ansteuerung von Aktoren muss auch die im Kontext der Sektorkopplung eingesetzte Plattform diesen Normen und Richtlinien entsprechen. Nur unter Einhaltung dieser Standards können die gewerkeübergreifenden Vernetzungen sicher gestaltet und Verantwortlichkeiten klar definiert werden.

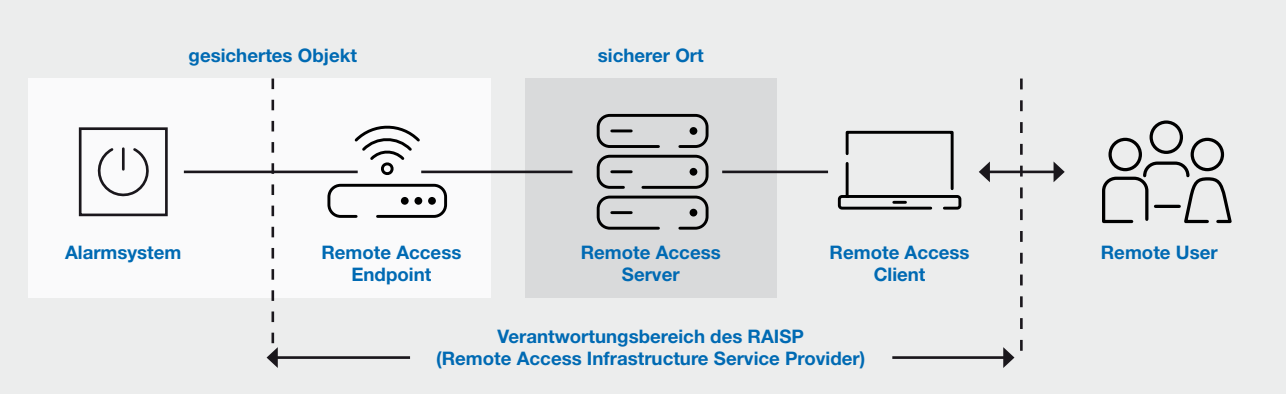


Abb. 4: Plattform für die Remote Access Infrastruktur innerhalb der WAN-Übertragung ergänzen

3.3 Wieso Lösungssatz nach 3.1.2?

Bei sicherheitsrelevanter Datenübertragung hat die Sicherheit gegen unbefugten Zugriff auf die Daten und die Gerätefunktionen oberste Priorität. Angriffe auf Gateways und Router im Netzwerk sind keine theoretische Möglichkeit, sondern eine reale Gefahr im Cyber Security Kontext. Sowohl die vom BSI zertifizierten SMGW als auch VdS anerkannte Alarmübertragungsgeräte nach DIN EN-Normen wurden gegen diese Bedrohungen gehärtet. Es unterscheiden sich lediglich die Methoden, Sicherheit zu erreichen und nachzuweisen (z. B. BSI-PP vs. DIN EN-Normen).
Obwohl für den eigentlichen Übertragungsweg über öffentliche Netzbetreiber hinweg bisher in den BSI-TR keinerlei Vorgaben enthalten sind, ergibt es Sinn, sichere, hochverfügbare und schwarzfallresiliente Übertragungswege zu nutzen, wie sie in der physischen Absicherung schon lange der Stand der Technik sind. Darüber hinaus kann das SMGW die vielen Vorteile der Übertragungstechnik der Sicherheitskette für sich nutzen:

Nr.	Vorteile Übertragungstechnik der Sicherheitskette
VS1	Notstromversorgung (bis zu 72h) (EN 54)
VS2	Kontinuierliche Verfügbarkeitsüberwachung (Anforderung von bis zu 99,9% Verfügbarkeit) (DIN EN 50136)
VS3	Zwei unabhängige Übertragungswege (EN 54/ EN 50131/ DIN VDE 0833)
VS4	Definierte Reaktionsgeschwindigkeiten bei Verbindungsstörungen / festgelegte Übertragungsdauern (DIN EN 50136)
VS5	Klare Festlegung der Verantwortungsbereiche („Ende zu Ende“) mit 24/7 Reaktionsanforderungen
VS6	Funktionsüberwachung der angebundenen Endgeräte (wie EMA, BMA, Sprechstellen, Personennotruf, IoT-Gateways)
VS7	Direkter Netzzugang gem. Telekommunikationsgesetz (TKG) §73 Abs. 1 (passiver Netzabschluss)
VS8	Weltweite/ Europaweite Normierung

Tabelle 3: Vorteile der Übertragungstechnik der Sicherheitskette

4 Handlungsempfehlungen

Das Smart Meter Gateway erfüllt gemäß MsbG die Anforderungen aus der Energiewirtschaft mit der Umsetzung von BSI-TR-03109 und BSI-CC-PP0073. Anforderungen bzgl. Gebäude- und Personensicherheit sind in diesen beiden Dokumenten nicht spezifiziert.

Die standardisierten Übertragungswege der Sicherheitstechnik können mit ihrer besonderen Zuverlässigkeit und Verfügbarkeit einen Beitrag dazu leisten, die Qualität der kommunikativen Anbindung von intelligenten Messsystemen in eine IT-Infrastruktur zu verbessern, insbesondere bei Funktionen und Schalthandlungen, die niedrige Latenzzeiten erfordern. Daher wird empfohlen, die bereits etablierten Lösungsansätze der Sicherheitstechnik im Bereich der Übertragungstechnologie in die Ausgestaltung der IT-Infrastruktur bei der Digitalisierung der Energiewende mit einzubeziehen.

Dafür sind folgende Anpassungen erforderlich:

Nr.	Handlungsempfehlungen
H1	Erweiterung des Scopes der DIN/EN 50136: Übertragung von SMGW- Datenpaketen sowie Smart-Home Anwendungen und anderen Gebäudedaten mit Sicherheitsanforderungen
H2	Erweiterung des Scopes der VdS-Richtlinien: Übertragung von SMGW-Datenpaketen sowie Smart-Home Anwendungen und anderen Gebäudedaten mit Sicherheitsanforderungen
H3	Erweiterung des Scopes der DIN/EN 50136: Übertragung der Datenmodelle des IEC TC57 zwischen Smart-Grid und Gebäudemanagement-Systemen. Hierzu eignen sich die bereits in der DIN/EN 50136 definierten Strukturen.
H4	Ergänzung der BSI-TR-03109 bezüglich der Möglichkeit, eine schwarzfall-resiliente Übertragungsstrecke für das SMGW gemäß DIN EN 50136 zu nutzen.

Tabelle 4: Handlungsempfehlungen des Projektes

5 Ausblick

Auch unter Berücksichtigung aller geforderten Sicherheitsanforderungen muss die technische Lösung zu akzeptablen Kosten bereitgestellt werden. Durch die gemeinsame Nutzung von vielen Gewerken im Gebäude (Sektorkopplung) kann dieses Ziel erreicht werden. Aufgrund der bereits installierten Sicherheitstechnik, die in einer Vielzahl an Gebäuden gemäß Bauordnung vorgeschriebenen sind, müssen hier zudem keine neuen Übertragungsgeräte installiert, sondern vorhandene Dateninfrastrukturen genutzt werden. Dieses Vorgehen leistet einen zusätzlichen Beitrag zu CO_2-Reduktion.
Weiterhin resultieren hieraus erhebliche Kosten-, Ressourcen- und Energieeffizienz-Vorteile und im Ergebnis die beschleunigte Umsetzung einer nachhaltigen Energiewende.

Ebenfalls erfordert die sichere Übertragungstechnik in Verbindung mit sicheren Plattformen keine grundlegenden Neuentwicklungen. Es können vielmehr Lösungen herangezogen werden, die bereits seit vielen Jahren vom BSI für die Absicherung kritischer Infrastrukturen (KRITIS) und sicherheitskritischer Einrichtungen geprüft und freigegeben sind.. Eine Prüfung und Zertifizierung neuer Komponenten ist nicht notwendig, denn die existierenden Lösungen basieren bereits auf internationalen Normen und Standards und sind zudem von deutschen Herstellern in ausreichender Stückzahl zu beschaffen, was wiederum einen Vorteil in Bezug auf sichere Lieferketten und Verfügbarkeit mit sich bringt. Es muss noch weiter geprüft werden, wie das 450 MHz-Netz als zusätzlicher Übertragungsweg für die weitere Nutzung genutzt werden kann.

Durch Hinzuziehen ergänzender Netze der Alarmübertragungstechnik und gemeinsamen Installationspersonal durch gegenseitige Anerkennung der Qualifikation, ließe sich der verzögerte SMGW-Roll-Out beschleunigen. Die Vorteile der in Kapitel 4 vorgestellten Handlungsempfehlungen sind unter Tabelle 5 aufgelistet:

Nr.	Vorteil Handlungsempfehlungen
VH1	Nutzung der gesicherten Übertragungswege gemäß DIN EN 50136 bei problematischer Funkanbindung
VH2	Bestehende SMGW-Installationen an einem Sicherheitsrouter sind unabhängig von Technologiewechseln der Übertragungstechnik: Gleitender Übergang z. B. bei DSL → LWL, 4G → 5G → 6G
VH3	Verfügbarkeit von Übertragungswegen auch bei lokalem Stromausfall (Schwarzfall-Resilienz)
VH4	Sicherheitsrelevante schnellstmögliche Wiedererlangung der Übertragungsverfügbarkeit nach Verbindungsstörungen
VH5	Kurzfristige Erweiterbarkeit um Anwendungen für KRITIS-Infrastrukturüberwachung sowie Smart-Home und AAL mit Sicherheitsbedarf
VH6	Bereits etablierte Plattform für Servicedienstleistungen

Tabelle 5: Vorteile Handlungsempfehlungen des Projektes

Anhang A:
Relevante Normungsgremien

DKE/K 713 Gefahrenmelde- und Überwachungsanlagen

Arbeitsgebiet Erarbeitung und Bearbeitung von Normen für Einbruch- und Überfallmeldeanlagen, Videoüberwachungsanlagen, Zutrittskontrollanlagen, Brandmeldeanlagen, Alarmempfangsstellen, Sprachalarmierungsanlagen, Personennotsignalanlagen, Personenhilferufanlagen, Werksgelände- und Freifeldüberwachungsanlagen, Gefahrenwarnsystemen und Gefahrenreaktionssystemen, sowie einfachen und preiswerten Versionen davon für Anwendungen, für die professionelle Anlagen nicht verlangt und aus Kostengründen auch nicht genommen werden.[6]

Spiegelgremien

CLC/TC 79 Alarm and electronics security systems
IEC/TC 79 Alarm and electronics security systems

DIN/ NA 031-02 FBR Fachbereichsausschuss Brandmelde- und Feueralarmanlagen

Der Fachbereichsausschuss koordiniert und steuert die Normungsarbeit im Bereich der Brandmelde- und Feueralarmanlagen.

Der Schwerpunkt der Normungsarbeit liegt für die Arbeitsausschüsse in diesem Fachbereich einerseits in der Erarbeitung der Normen der Reihe EN 54, welche fast ausschließlich harmonisierte Normen beinhaltet. Mit dieser Normungsarbeit wird dazu beigetragen, bei Brandmeldeanlagen Qualitäts- und Sicherheitsaspekte zu sichern. Andererseits werden innovative Themen wie die dynamische und adaptive Fluchtweglenkung oder die Anforderungen an digitale BOS-Objektfunkanlagen erarbeitet.

Der Fachbereichsausschuss und seine Arbeitsausschüsse spiegeln die Arbeiten des europäischen Technischen Komites CEN/TC 72 „Brandmelde- und Feueralarmanlagen".
Die Mehrzahl der Europäischen Normen im CEN/TC 72 werden im Rahmen der EU-Bauproduktenverordnung Nr. 305/2011 (EU) als harmonisierte Normen erarbeitet.
Darüber hinaus werden von den Arbeitsausschüssen des NA 031-02 FBR die Projekte des ISO/TC 21/SC 3 „Branddetektions- und Alarmierungsanlagen" betreut.

Spiegelgremien

CEN/TC 72 Fire detection and fire alarm systems
ISO/TC 21/SC 3 Fire detection and alarm system

DKE/K 716 Elektrische Systemtechnik für Heim und Gebäude (ESHG)

Das DKE/K 716 arbeitet auf dem Gebiet der Normung der „Elektrischen Systemtechnik für Heim und Gebäude (ESHG)". Hierbei handelt es sich um Kommunikationssysteme für die Fernsteuerung und das Zusammenwirken elektrischer Geräte im Haus- und Gebäudebereich, die Datenübertragung erfolgt dabei über verschiedene Übertragungsmedien. Es besteht eine enge Zusammenarbeit mit dem DKE/GUK 715.1, das internationale Vorhaben aus ISO/IEC JTC1 SC25 auf dem Gebiet der elektrischen Systemtechnik für Heim und Gebäude (ESHG) bearbeitet, während das DKE/K 716 den Schwerpunkt auf europäische Normungsvorhaben legt (CLC/TC 205). Die Signalübertragung auf elektrischen Niederspannungsnetzen und „Power Line Communication (PLC)" wird im Unterkomitee DKE/UK 716.1 „Systeme für die Kommunikation auf elektrischen Niederspannungsnetzen" behandelt. Als Spiegelgremium zu CENELEC/SC 205A leistet DKE/UK 716.1 Unterstützung in den europäischen Arbeitsgruppen und Projekten.[7]

Spiegelgremien

CLC/TC 205 Home and Building Electronic Systems (HBES)
IEC/TC 23 Electrical accessories

---

6 https://standards.cencenelec.eu/dyn/www/f?p=CEN:6, Abruf: 14.02.2024
7 (DKE, o.A.)

DKE/K 801 System Komitee AAL

Nach Gründung des System Committees auf IEC-Ebene wurde auf nationaler Ebene das System Komitee AAL (DKE/K 801) gegründet.

AAL-Technologien sind technische Hilfsmittel, die Menschen im Alltag und im Beruf unterstützen, ihre Gesundheit bewahren und fördern sowie Folgen von Krankheit und Verletzung mildern, kompensieren oder beheben. Sie zeichnen sich durch eine Vielfalt von Technologien und Komponenten aus, weshalb ein systematischer Ansatz in der Normung und Standardisierung benötigt wird. Themenübergreifende Schnittstellen zu verwandten Domänen (z. B. Smart Home) und funktionale Anforderungen in Zusammenarbeit mit relevanten Gremien, Konsortien und Foren sollen identifiziert werden, um beispielsweise die Interoperabilität sicherzustellen. Dieses Ziel des System Komitees AAL wurde bei der ersten Sitzung des Gremiums im August 2014 bestätigt.

Das Gremium beschäftigt sich u. a. mit folgenden Themen:

- Verknüpfung von AAL bezogenen Normungsaktivitäten in unterschiedlichen Technologiefeldern und Berücksichtigung des ausgeprägten Systemcharakters von AAL-Technologien
- Barrierefreiheit von AAL-Produkten und –Systemen
- Zugänglichkeit zu AAL-Systemen
- User Interfaces, Usability
- herstellerübergreifende Interoperabilität von AAL- Systemen, - Produkten und – Komponenten,
- Schnittstellen zu Smart Home, E-Health und E-Mobility
- Use Cases und Use Case Architecture, Integrationsprofile
- Datenschutz und Sicherheit im Umfeld von AAL
- Nutzeranforderungen
- Qualitätskriterien und
- Wearable Smart Devices.

Außerdem wird das Thema „Dienstleistungskette für Gefahrenmeldungen im sozialen Betreuungswesen“ behandelt.[8]

Die Koordinierung und Absprache der Normungsaktivitäten unterschiedlicher Normungsorganisationen (z. B. DIN) und aktiver Gruppen sollen im DKE/K 801 erfolgen.

Das DKE/K 801 bestätigte die Einrichtung von sieben initialen Arbeitskreisen, die für spezielle Aufgaben im AAL-Umfeld zukünftig verantwortlich sind. Das Komitee übernimmt die strategische und übergeordnete Führung dieser Arbeitskreise.

Spiegelgremien

CEN/CLC/JTC 12 Design for All
IEC/SyC AAL Active Assisted Living

DKE/K 461 Messeinrichtungen und -systeme für Elektrizität

Normung im Bereich der Messung und Steuerung von elektrischer Wechsel- und Gleichstromenergie für intelligente Messeinrichtungen (Smart Meters) und Systeme, die Teile intelligenter Netze (Smart Grids) bilden, für die Anwendung in Kraftwerken, in Netzen und bei Endverbrauchern und -erzeugern sowie die Erarbeitung internationaler Normen für Zählerprüfeinrichtungen und -verfahren.

Ausgenommen ist die Normung von Schnittstellen von Messeinrichtungen für die Verknüpfung von Netzen und für industrielle Energieverbraucher und -erzeuger die von IEC/TC 57 abgedeckt sind.

Spiegelgremien

CLC/TC 13 Electrical energy measurement
IEC/TC 13 Electrical energy measurement

---

8 (DKE, o.A.)

DKE/K 901 System Komitee Smart Energy

Das System Komitee „Smart Energy“ beschäftigt sich mit intelligenten Energie- und Regelsystemen, die sich aus Erzeugern, Speichereinrichtungen, Verbrauchern und Transporteinrichtungen unter Einsatz von Informations-, Kommunikations- und Automatisierungstechnologien zusammensetzen. Derartige intelligente Energiesysteme ermöglichen neue Markt- und Netzfunktionen und umfassen die Verknüpfung aller Energieträger in allen Sektoren, wie z. B. Strom, Power2Gas und Wärme. Das DKE/K 901 entwickelt die Themen Smart Metering/Smart Home, Smart Energy, IT-Security und Netzintegration Erneuerbarer Energien weiter. Dabei spiegelt es die Aktivitäten des gleichnamigen IEC System Committee. Das Ziel des IEC-Experten-Teams ist die Erstellung eines Entwicklungsplans und einer Roadmap. Die Koordinierung des Themas Energienetze schließt dabei nicht nur IEC-Normung, sondern auch externe und an der Normung beteiligte Gruppen wie Behörden und Konsortien mit ein. Darüber hinaus setzt sich das Komitee mit dem Thema Digitalisierung auseinander: Insbesondere Blockchains im Energiesektor werden durch eine Task Force bearbeitet.[9]

Spiegelgremien

CEN/CLC/ETSI CEN-CENELEC-ETSI Coordination Group on Smart Energy Grids
IEC/SyC Smart Energy System Komitee Smart Energy

DKE/K 952 Netzleittechnik

Ausarbeitung von Normen für Einrichtungen und Systeme der Netzleittechnik, einschließlich Netzführungssysteme (EMS), Überwachen, Steuern und Datenerfassen (SCADA), Verteilnetzautomatisierung, Schutzsignalübertragung und zugehörigen Informationsaustauschs in Echtzeit oder davon unabhängig für Planung, Betrieb und Instandhaltung von Elektrizitätsversorgungssystemen. Zur Netzführung von Energieversorgungssystemen gehört die Steuerung und Überwachung in Netzleitstellen und Stationen des Energienetzes und in einzelnen Bereichen der Primäreinrichtungen sowie Fernwirken und Schnittstellen zu Einrichtungen, Systemen und Datenbanken außerhalb des Arbeitsbereichs des IEC/TC 57 „Power systems management and associated information exchange“ und damit des DKE/K 952.[10]

Spiegelgremien

IEC/TC 57 Power systems management and associated information exchange
CLC/TC 57 Power systems management and associated information exchange

---

DKE/TBINK/AK_BMWK_BSI Koordinierung im Umfeld intelligenter Messsysteme

Informationsaustausch zum Thema „Metering und zugehörige Technologien im Umfeld intelligenter Messsysteme“.
Koordination bei Kommentierungen zu „Metering und zugehörige Technologien im Umfeld intelligenter Messsysteme“, (BSI, BMWK, BNetzA etc.).[11]

9 (DKE, o.A.)
10 (DKE, o.A.)
11 (DKE, o.A.)

Anhang B:
Nationale Institutionen

VDE Verband der Elektrotechnik Elektronik und Informationstechnik e.V.

Der VDE, eine der größten Technologie-Organisationen Europas, steht seit mehr als 130 Jahren für Innovation und technologischen Fortschritt. Als einzige Organisation weltweit vereint der VDE dabei Wissenschaft, Standardisierung, Prüfung, Zertifizierung und Anwendungsberatung unter einem Dach. Das VDE Zeichen gilt seit mehr als 100 Jahren als Synonym für höchste Sicherheitsstandards und Verbraucherschutz.

Wir setzen uns ein für die Forschungs- und Nachwuchsförderung und für das lebenslange Lernen mit Weiterbildungsangeboten „on the job“. Im VDE Netzwerk engagieren sich über 2.000 Mitarbeiter*innen an über 60 Standorten weltweit, mehr als 100.000 ehrenamtliche Expert*innen und rund 1.500 Unternehmen gestalten im Netzwerk VDE eine lebenswerte Zukunft: vernetzt, digital, elektrisch. Wir gestalten die e-diale Zukunft.

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik

Die vom VDE getragene DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik (DKE) ist die Plattform für rund 9.000 Expert*innen aus Wirtschaft, Wissenschaft und Verwaltung zur Erarbeitung von Normen, Standards und Sicherheitsbestimmungen für die Elektrotechnik, Elektronik und Informationstechnik. Normen unterstützen den weltweiten Handel und dienen u. a. der Sicherheit, Interoperabilität und Funktionalität von Produkten und Anlagen. Als Kompetenzzentrum für elektrotechnische Normung vertritt die DKE die Interessen der deutschen Wirtschaft in europäischen (CENELEC, ETSI) und internationalen Normenorganisationen (IEC). Darüber hinaus erbringt die DKE umfangreiche Dienstleistungen rund um die Normung und das VDE Vorschriftenwerk.

VDE FNN

Als technischer Regelsetzer für die Spezifikation der Komponenten des iMSys verantwortlich.
Das Forum Netztechnik/Netzbetrieb im VDE (VDE FNN) entwickelt die Stromnetze vorausschauen weiter. Ziel ist der jederzeit sichere Systembetrieb mit 100 Prozent erneuerbaren Energien.
VDE FNN macht innovative Technologien praxistauglich und gibt Antworten auf netztechnische Herausforderungen von morgen. Hier arbeiten verschiedene Fachkreise mit unterschiedlichen Interessen gemeinsam an Lösungen. Mitglieder sind über 500 Hersteller, Netzbetreiber, Versorger, Anlagenbetreiber, Behörden und wissenschaftliche Einrichtungen.

DIN

DIN Deutsches Institut für Normung e. V. (DIN) ist die unabhängige Plattform für Normung und Standardisierung in Deutschland und weltweit. Gemeinsam mit Wirtschaft, Wissenschaft, öffentlicher Hand und Zivilgesellschaft trägt DIN wesentlich dazu bei, Zukunftsfelder zu erschließen. Als Mitgestalter des digitalen und grünen Wandels leistet DIN einen wichtigen Beitrag bei der Lösung der aktuellen Herausforderungen und ermöglicht, dass sich neue Technologien, Produkte und Verfahren am Markt und in der Gesellschaft etablieren.
Rund 37.500 Expertinnen und Experten aus Wirtschaft und Forschung, von Verbraucherseite und der öffentlichen Hand bringen ihr Fachwissen in den Normungsprozess ein, den DIN als privatwirtschaftlich organisierter Projektmanager steuert. Die Ergebnisse sind marktgerechte Normen und Standards, die den weltweiten Handel fördern und der Rationalisierung, der Qualitätssicherung, dem Schutz der Gesellschaft und Umwelt sowie der Sicherheit und Verständigung dienen.

VdS Schadenverhütung GmbH

VdS gehört zu den weltweit renommiertesten Institutionen für die Unternehmenssicherheit mit den Schwerpunkten Brandschutz, Security, Naturgefahrenprävention und Cyber-Security.

Die Dienstleistungen umfassen Risikobeurteilungen, Prüfungen von Anlagen, Zertifizierungen von Produkten, Firmen und Fachkräften sowie ein breites Bildungsangebot. Zu den Kunden zählen Industrie- und Gewerbebetriebe aller Branchen, international führende Hersteller und Systemhäuser, kompetente Fachfirmen sowie risikobewusste Banken und Versicherer. VdS bietet leistungsstarke Services, die nicht nur national und europaweit, sondern mehr und mehr auch auf globalen Märkten für Sicherheit und Vertrauen stehen.

Die VdS Schadenverhütung GmbH ist eine 100 %-ige Tochtergesellschaft des Gesamtverbandes der Versicherungswirtschaft (GDV). VdS verfolgt eine Systematik des integrierten Sicherheitsansatzes, die sich im Brandschutz und Einbruchdiebstahlschutz seit Jahrzehnten bewährt hat:

- Formulierung von angemessenen Anforderungen an das gewünschte Schutzniveau durch VdS-Richtlinien. Die VdS-Richtlinien werden von der Industrie und der Versicherungswirtschaft akzeptiert und angewendet.
- Formulierung von Anforderungen sowie die Prüfung und Zertifizierung von Produkten
- Zertifizierung von Prozessen in Unternehmen
- Zertifizierung von Firmen und Fachkräften
- Erstabnahme und Revisionen von Schutzanlagen

BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cybersicherheitsbehörde des Bundes und Gestalter einer sicheren Digitalisierung in Deutschland.

Der Arbeitsauftrag des BSI umfasste von Beginn an den Schutz der Regierungsnetze und die Sicherung zentraler Netzübergänge. Mit der Novellierung des BSI-Gesetzes 2009 konnte das BSI für die Bundesbehörden verbindliche Sicherheitsstandards für die Beschaffung und den Einsatz von IT entwickeln. Das BSI wurde zudem zur zentralen Meldestelle für IT-Sicherheit innerhalb der Bundesverwaltung, um bei IT-Krisen nationaler Bedeutung durch Informationen und Analysen die Handlungsfähigkeit der Bundesregierung sicherzustellen. Für Wirtschaft, Wissenschaft, Gesellschaft sowie für die Bürgerinnen und Bürger fungierte das BSI als kompetenter Ansprechpartner und Berater für alle Fragen der Informationssicherheit.[12]

BNetzA

Regulierung zu § 14a EnWG, trifft Vorgaben zu Kommunikation und Prozessen zu Steuerung über SMGW und FNN Steuerbox.

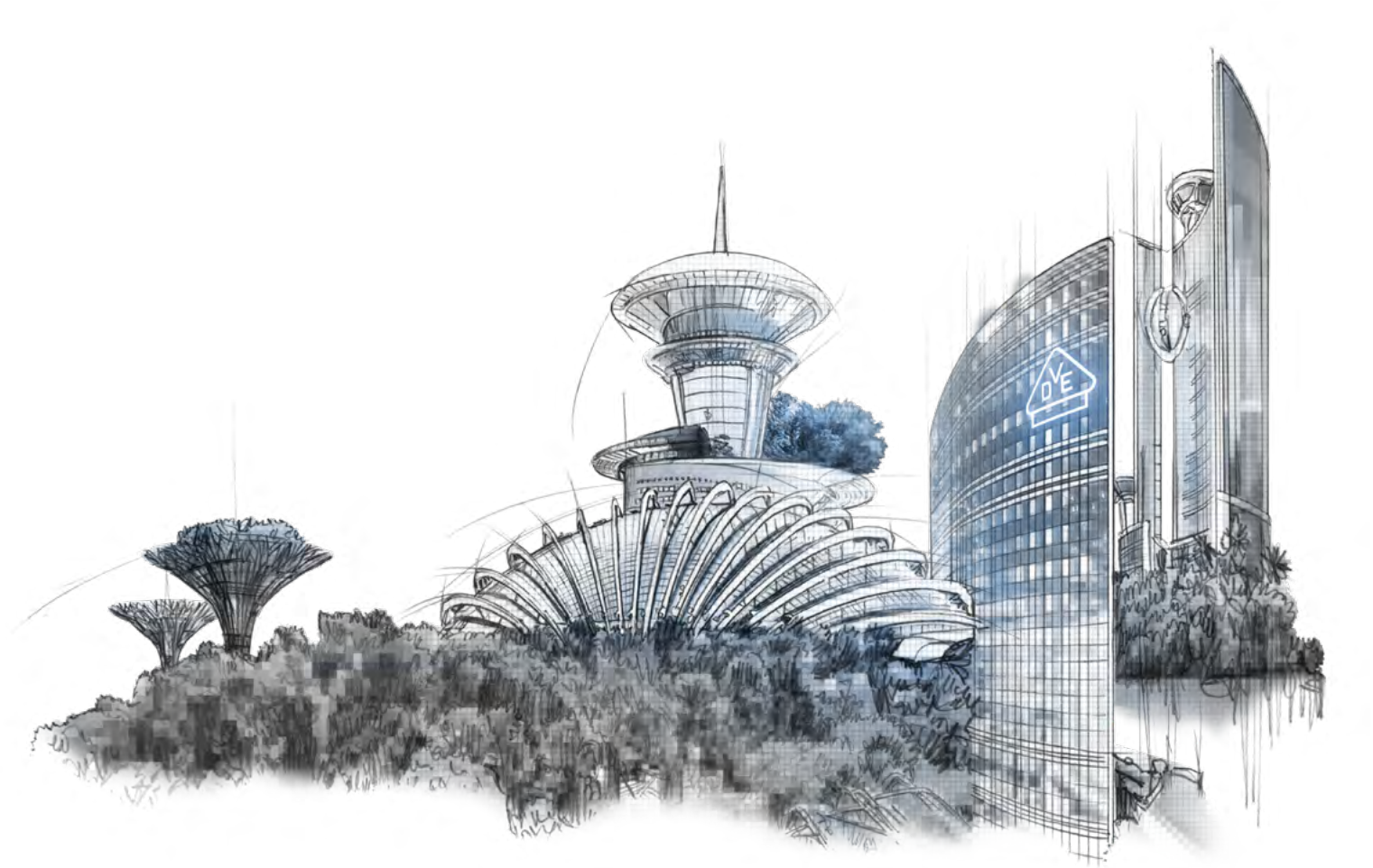
Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen mit Sitz in Bonn, kurz Bundesnetzagentur (BNetzA), ist eine Bundesoberbehörde im Geschäftsbereich des Bundeswirtschaftsministeriums. Als oberste deutsche Regulierungsbehörde bestehen ihre Aufgaben in der Aufrechterhaltung und der Förderung des Wettbewerbs in sogenannten Netzmärkten. Eine weitere Aufgabe ist die Moderation von Schlichtungsverfahren. Die Bundesnetzagentur ist außerdem Aufsichtsstelle für Vertrauensdiensteanbieter nach der eIDAS-Verordnung.

Im Aufgabenbereich Energie ist sie für die Regulierung zu § 14a EnWG verantwortlich und trifft Vorgaben zu Kommunikation und Prozessen zu Steuerung über das SMGW.

12 https://www.bsi.bund.de/DE/Home/home_node.html, Abruf: 14.02.2024

Literaturhinweise

- Richtlinie VdS 2463: 2019-04 Übertragungseinrichtungen für Gefahrenmeldungen
- Richtlinien-Reihe VdS 2465 Übertragungsprotokoll für Gefahrenmeldungen
- Richtlinie VdS 2471: 2015-06 Übertragungswege in Alarmübertragungsanlagen
- BSI/BMWK: Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nach dem Gesetz zur Digitalisierung der Energiewende



VDE Verband der Elektrotechnik
Elektronik Informationstechnik e.V.
DKE Deutsche Kommission
Elektrotechnik Elektronik Informationstechnik
Merianstraße 28
63069 Offenbach

Tel. +49 69 6308-0
dke@vde.com
www.dke.de

DKE