



Sektorkopplung auf Basis sicherer Gateways und Router



GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Whitepaper

Sektorkopplung auf Basis sicherer Gateways und Router
Offenbach

Autor*innen:

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

Disclaimer:

Dieses Whitepaper wurde in dem durch das vom Bundesministerium für Bildung und Forschung (BMBF) 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 BMBF.

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: Destina / stock.adobe.com, p. 16: Day Of Victory Stu. / stock.adobe.com,

Inhaltsverzeichnis

1.	Sichere Gateways und Router auf Grundlage für Mehrwertdienste (SiGRun)	6
1.1	Forschungsfeld 2 im Kontext zum Gesamtvorhaben WWNW	7
1.2	Beschreibung des Forschungsfeldes 2 (Status Quo)	8
1.3	Die Akteure aus WWNW-FF2	9
2.	Normungskontext	10
2.1	Internationale Institutionen	10
2.2	Relevante DKE Gremien	11
2.3	Nationale Institutionen	11
3.	Digitale Architektur	12
3.1	Gegenüberstellung der zwei lokalen Lösungsansätze	12
3.11	Lösungsansatz „Grundidee BSI – CLS – Schnittstelle für Smart-Home“ 1	12
3.1.2	Lösungsansatz „SMGW nutzt sichere Übertragungswege gem. DIN EN-Norm“	13
3.2	Anforderungen an die Plattform	14
3.3	Wieso Lösungssatz nach 3.1.2?	14
4.	Handlungsempfehlungen	15
5.	Ausblick	16
A	Internationale Institutionen	17
B	Relevante DKE Gremien	19
C	Nationale Institutionen	21
	Literaturhinweise	23

Abkürzungsverzeichnis

BMA	Brandmeldeanlagen
BMBF	Bundesministerium für Bildung und Forschung
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)
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
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
SMGW	Smart-Meter-Gateway
TAS	Telefonbau Arthur Schwabe GmbH & Co. KG
TC	Technical Committee
TR	Technische Richtlinie
VDE	VDE Verband der Elektrotechnik Elektronik Informationstechnik e. V.
VdS	VdS Schadenverhütung GmbH
WAN	Wide-Area-Network
WWNW	BMBF-Förderprojekt WärmewendeNordwest
ZuKo	Zutrittskontrollsystem

Executive Summary

Dieses Whitepaper ist im Rahmen des BMBF-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.

Prinzipiell unterscheiden sich die Anforderungen an die Sicherheit von SMGW und Alarmübertragungsanlagen nicht. 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 zugelassenen SMGW als auch VdS- anerkannte Alarmübertragungsgeräte nach DIN EN-Normen wurden gegen alle diese Bedrohungen gehärtet. Es unterscheiden sich lediglich die Methoden, Sicherheit zu erreichen und nachzuweisen (BSI-TR vs. DIN EN-Normen).

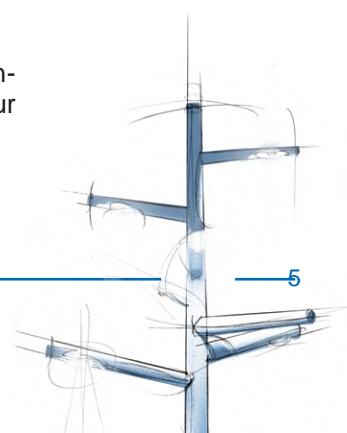
Obwohl für den eigentlichen Übertragungsweg über öffentliche Netzbetreiber hinweg bisher in den BSI-TR keinerlei Vorgaben enthalten sind (WAN-Schnittstelle), ergibt es Sinn, hochverfügbare und schwarzfall-resiliente Übertragungswege zu nutzen, wie sie in der physischen Absicherung schon lange Stand der Technik sind. Alle Daten, in einem Gebäude, die bisher nicht in einem SMGW erfasst werden und über das WAN transportiert werden müssen, sollen 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 EN50136 um die Übertragung von Energiedaten des Energiesektors
- Erweiterung des Scopes der VdS-Richtlinien um die Übertragung von Energiedaten des Energiesektors
- Anpassung der internationalen Energienormung im IEC TC57 um die Möglichkeit die Energiedaten via Sicherheitsrouter über eine sichere Plattform zur Verfügung zu stellen. 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 Sichere Gateways und Router auf Grundlage für Mehrwertdienste

Das Forschungsfeld 2 (FF2) aus dem BMBF-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 ebene Gebäudeüberwachung bereits nutzen und diese 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“ Energienetzes. 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 Bedarfe der elektrischen Energiewirtschaft.

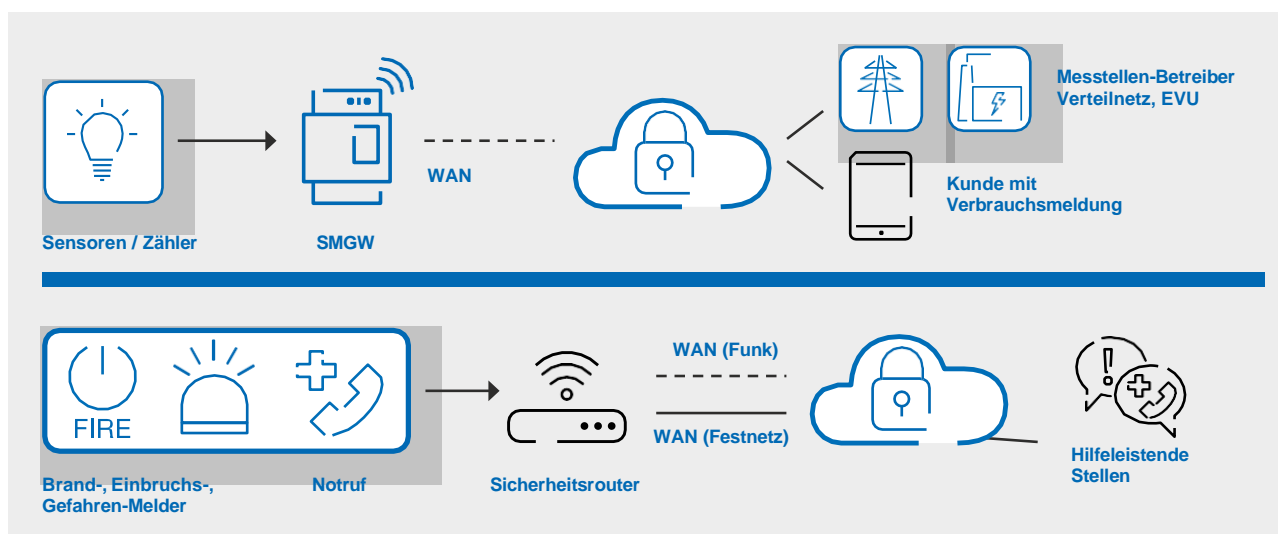


Abb.1: Getrennte Übertragungsplattformen für Energiezähler und alle anderen Gewerke
Für eine erfolgreiche Sektorkopplung müssen alle im Gebäude vorhandenen

104 Gewerke mit einbezogen werden können. Hierbei müssen alle anfallenden Daten,
105 Meldungen sowie Aktoren mit ihren technischen und sicherheitsrelevanten
106 Anforderungen mit in die Betrachtung einbezogen werden.
107 Mithilfe geschlossener Datenmodelle und offener Schnittstellen über die gesamte
108 Prozesskette wird erst ein Zusammenschluss verschiedener Sektoren möglich.
109 Eine weitgreifende Vernetzung könnte helfen, übergreifende Anforderungen, wie
110 z.B. das Optimieren von Energieverbräuchen, zu ermöglichen. Die Eindeutigkeit
111 und Sicherheit der Daten müssen hierfür jedoch zu jeder Zeit gewährleistet sein.
112 Übertragene Daten dürfen auf der kompletten Übertragungsstrecke keinen
113 Interpretationsspielraum lassen und müssen eindeutig sein. Unter Einhaltung der
114 herausgestellten Strukturen und Schnittstellen ist es möglich, dass verschiedene
115 Unternehmen ein Teil des Prozesses werden können.
116

117 Weiter schützenswert sind Daten über Netzzustand, Erzeugung und Verbrauch in
118 Energienetzen sowie von Alarmzuständen im Gebäude. Um Angriffe auf das
119 System und resultierende Datenlecks zu vermeiden, wird im kompletten
120 Erhebungsprozess „Privacy & Security by Design“ gelebt. Praktische Vorgaben für
121 die sichere Umsetzung bieten hierbei die technischen Richtlinien des BSI (BSI-
122 TR-03109) und die Richtlinien des VdS für die Alarmübertragung, die es im
123 Zusammenhang mit den relevanten Normen und Standards zu vereinheitlichen gilt.

124 1.1 Forschungsfeld 2 im Kontext zum Gesamtvorhaben WNW

125 Im Zuge des Gesamtvorhabens spielt das Forschungsfeld 2 eine wichtige Rolle in der
126 Strukturschaffung sicherer Datenübertragung verschiedenster Liegenschaften. Der Fokus liegt
127 auf der sicheren Übertragung sicherheitskritischer Alarmmeldungen an hilfeleistende Stellen
128 und Interventionsdienste. Hinzu kommen standardisierte Übertragungswege von
129 Energiemessungen, die parallel zu den Alarmübertragungswegen an die hierfür vorgesehenen
130 Stellen angebunden sind. Wichtig für die Behandlung energierelevanter Messungen sind unter
131 anderem die technischen Richtlinien des BSI mit Vorgaben für intelligente Messsysteme und
132 deren sicheren Betrieb (BSI-TR-03109). Ziel des Forschungsvorhabens im Zuge von WNW
133 ist es, Lösungen für die Sektorkopplung zu erarbeiten und dabei Anpassungsvorschläge für
134 die Synchronisation der BSI-TR-03109 mit den etablierten Verfahren der Alarm- und
135 Notrufübertragungstechnik zu geben. In WNW wird hierbei im Feld ein sicherer Router
136 eingesetzt, der verschiedenen Akteuren mittels einer sicheren Plattform die Möglichkeit bietet,
137 Teil dieser Infrastruktur zu sein (siehe Kapitel 3). Aufgrund einer Microservice¹ Architektur
138 haben alle Anbieter der Plattform die komplette Datenhoheit, da alle Anwendungen getrennt
139 von den übrigen Systemen funktionieren. Die sichere Übertragungstechnik kann bei
140 energetischen Optimierungen des Gebäudes installiert werden und somit eine sichere
141 Infrastruktur schaffen, die die notwendigen Gewerke vereint. Dies bietet einen gemeinsamen
142 Mehrwert für Wohnungswirtschaft, Sicherheitstechnik und Bewohner.²
143
144

155
156
157
158
159
160
161
162

1 Mikroservice Architekturen bestehen aus Gesamtlösungen, welche sich aus mehreren kleinen Anwendungen zusammensetzen. Die Anwendungen 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

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

163

1.2 Beschreibung des Forschungsfeldes 2 (Status Quo)

164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188

Das WNW-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. Diese haben im Zuge des Smart Meter Gateway Rollouts technische Richtlinien und ein Schutzprofil verabschiedet, die es einzuhalten gilt, um die Sektorenkopplung 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. Diese Änderungen gilt es in Fachgremien zu kommunizieren.

Hierzu sind Teilziele ein wichtiger Faktor. Zunächst werden die Anwendungsfälle aus den zu vereinigenden Bereichen beschrieben. Im weiteren Verlauf werden Möglichkeiten dargeboten, die bestehenden Infrastrukturen in eine gemeinsame Plattform einzubringen.³



189
190
191
192
193
194
195
196
197
198
199
200
201

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

1.3 Die Akteure aus WNW-FF2

203

Das FF2 zeichnet sich durch Partner verschiedenster Branchen aus, die gemeinsam die Aufgabenstellungen bewältigen und die optimalen Lösungen für die Sektoren finden.

204

205

Vertreten sind Partner aus Normungsgremien, wie die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik (DKE), sowie Prüf- und Zertifizierstellen, wie die VdS Schadenverhütung GmbH.

206

207

208

209

Die **DKE** ist die in Deutschland zuständige Organisation für die Erarbeitung von Normen, Standards und Sicherheitsbestimmungen im Bereich der Elektrotechnik, Elektronik und Informationstechnik. Sie

210

211

212

vertritt deutsche Interessen im Europäischen Komitee für Elektrotechnische Normung (CENELEC) und in der Internationalen Elektrotechnischen Kommission (IEC).

213

214

215

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.

216

217

218

219

220

221

222

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.

223

224

225

226

227

228

Die Überwachung der im Projektkontext verbauten Technik übernimmt die **Fernwirk-Sicherheits-systeme 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.

229

230

231

232

233

234

235

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.

236

237

238

239

240

241

242

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.

243

244

245

246

247

248

249

250

251

252

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 Partnern aus der Wissenschaft das Konsortium, welche die gewonnenen Learnings weiterentwickeln und fundiert untersuchen können. Das Aufbauen auf den gewonnenen Erkenntnissen können somit zu einem stetig entwickelnden Multiplikator für Normung und Unternehmen werden

253

254

255

256

257

258

259

260

261

262

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

263

264

2 Normungskontext

Alle Beteiligten in einem Gebäude mit Daten und Steuerungsbedarf benötigen eine effiziente und sichere Übertragung, die durch eine gemeinsame Infrastruktur erreicht werden kann. Um die Ziele im Projekt zu erreichen, ist die Einbindung der Normung nicht wegzudenken. In diesem Kapitel wird der Zusammenhang zwischen WWNW und den relevanten Gremien und Institutionen, die in Bezug auf die Infrastruktur tätig sind, näher dargestellt.

2.1 Internationale Normungsgremien

Folgende internationale Gremien erachten wir für die „Sektorkopplung“ als relevant:

Abkürzung	Beschreibung
IEC/TC 13	„Electrical energy measurement and control“, CLC/TC 13 WG1 „Electricity metering – Payment systems“, CLC/TC 13 WG2 „Data models and protocols for additional functionality of and data exchange in interoperable multi-utility smart metering systems“
IEC/TC 57	„Power systems management and associated information exchange“, WG 15 „Data and communication security“
CEN/TC 72	„Brandmelde- und Feueralarmanlagen“
IEC/TC 79	„Alarm- und elektronische Sicherheitssysteme“
IEC/TC 23	„Electrical accessories“
CLC/TC 205	„Home and Building Electronic Systems (HBES)“
SyC AAL	Active Assisted Living“
IEC/SyC Smart Energy	„Smart Energy“
CLC/TC 8X	„System aspects of electrical energy supply“

Tabelle 1: Relevante internationale Gremien für die Sektorenkopplung

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



284

2.2 Relevante DKE Gremien

285
286

In der DKE erachten wir folgende Gremien für die „Sektorkopplung“ als relevant:

Abkürzung	Beschreibung
DKE/K 461	„Messeinrichtungen und -systeme für Elektrizität“
DKE/K 713	„Gefahrenmelde- und Überwachungsanlagen“
DKE/K 716	„Elektrischen Systemtechnik für Heim und Gebäude (ESHG)“
DKE/K 801	„System Komitee AAL“
DKE/K 901	„Smart Energy“
DKE/K 952	„Netzleittechnik“
TBINK/AK_BMWK_BSI	„Koordinierung im Umfeld intelligenter Messsysteme“

287
288
289
290
291
292
293

Tabelle 2: Relevante DKE Gremien für die Sektorenkopplung

Ausführliche Beschreibungen der in Tabelle 2 benannten DKE Gremien sind im [Anhang B](#) zu finden.

2.3 Nationale Institutionen

294
295
296
297
298
299
300
301
302
303

Folgende nationale Institutionen erachten wir für die „Sektorkopplung“ aus Sicht unseres Projektes u. a. als relevant:

- VdS Schadenverhütung GmbH
- Bundesamt für Sicherheit in der Informationstechnik
- DIN-Normenausschuss Feuerwehrwesen

Ausführliche Beschreibungen der Institutionen sind im [Anhang C](#) zu finden.



304
305
306
307

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.

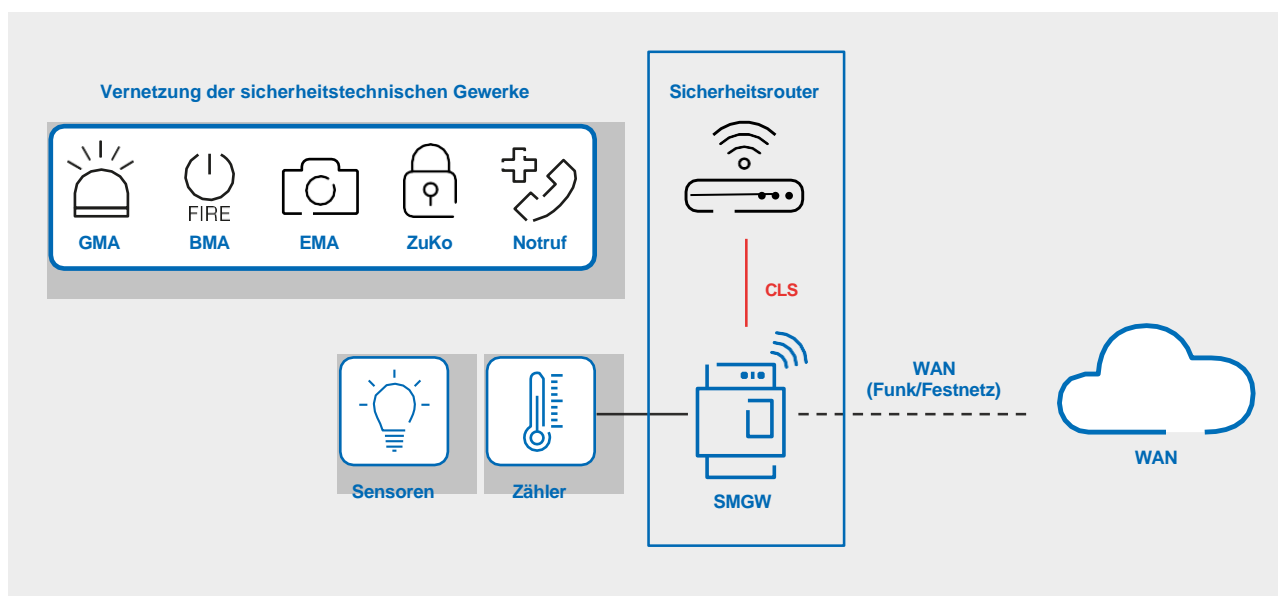


Abb.2: Anbindung Sicherheitstechnik gem. BMWK-Roadmap zur Energiewende

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.

Der in diesem Abschnitt beschriebene Lösungsansatz (siehe Abbildung 2) hat in Verbindung mit Sicherheitsanwendungen folgende Nachteile:

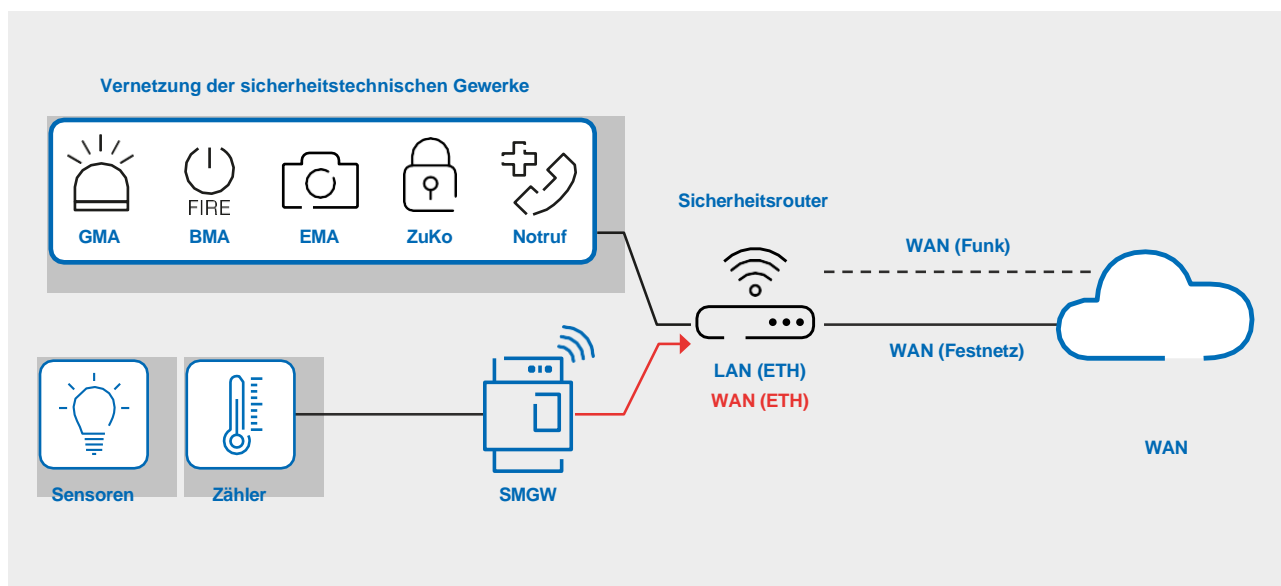
- Mindestens ein zusätzlicher, unabhängiger Übertragungsweg ist weiterhin erforderlich
- Keine klare Verantwortungsabgrenzung
- Keine einheitliche Remote Access Infrastruktur
- Der Sicherheitsrouter kann die Verfügbarkeit der CLS-Übertragungsstrecke nicht erkennen

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,

348
349
350
351
352
353

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.

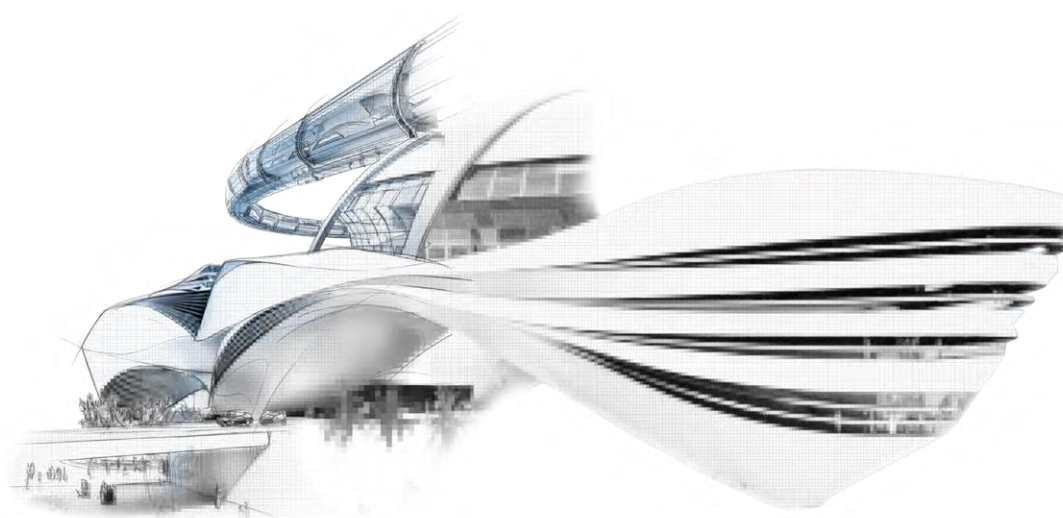


354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396

Abb.3: Nutzung der sicheren und redundanten Übertragungstechnik für alle Gewerke

Der in diesem Abschnitt beschriebene Lösungsansatz hat also mehrere Vorteile gegenüber dem Lösungsansatz nach 3.1.1.1:

- Nutzung redundanter Netzzugänge über DSL, Funk, LWL
- 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
- Nutzung der etablierten, standardisierten Sicherungskette des VdS im Sinne der Sektorkopplung
- Nutzungsmöglichkeit auch für zeitkritische Übertragung Schalthandlungen

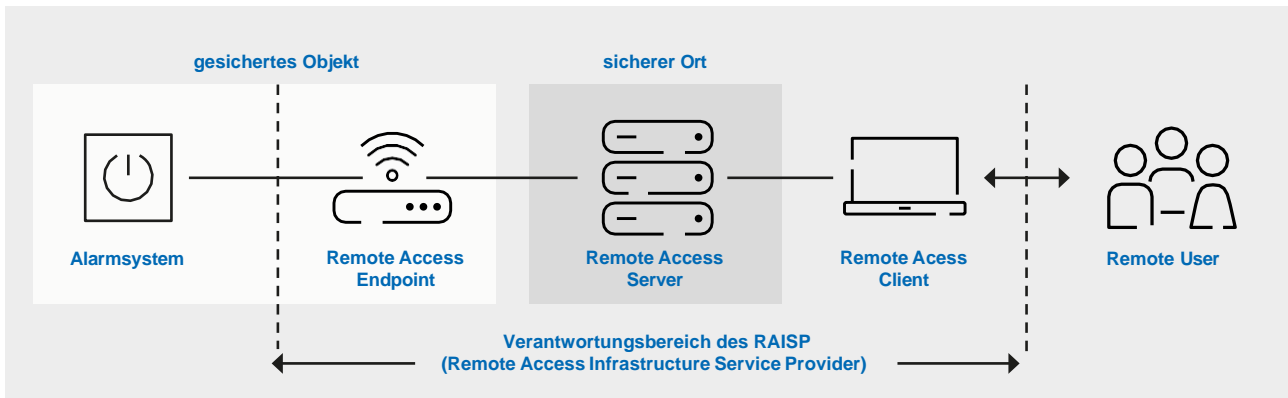


397

3.2 Anforderungen an die Plattform

398
399
400
401
402
403
404
405
406

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 Fernzugriffen 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.



407

Abb.4: Remote Access Infrastruktur

408
409

3.3 Wieso Lösungssatz nach 3.1.2?

410
411
412
413
414
415
416
417
418
419
420
421
422

Prinzipiell unterscheiden sich die Anforderungen an die Sicherheit von SMGW und Alarmübertragungsanlagen nicht. 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 zugelassenen 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 (BSI-TR 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 angebotenen Endgeräte (wie EMA, BMA, Sprechstellen, Personennotruf, IoT-Gateways)
VS7	Direkter Netzzugang gem. Telekommunikationsgesetz (TKG) §73 Abs. 1 (passiver Netzabschluss)
VS8	Weltweite/ Europaweite Normierung

423
424

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 Übertragungstrecke 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 vorgeschrieben sind, müssen hier zudem keine neuen Geräte installiert, sondern vorhandene Infrastrukturen genutzt werden. Dieses Vorgehen leistet einen zusätzlichen Beitrag zu CO₂-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, sondern es kann auf Lösungen zurückgegriffen 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.

Durch Hinzuziehen ergänzender Netze der Alarmübertragungstechnik und

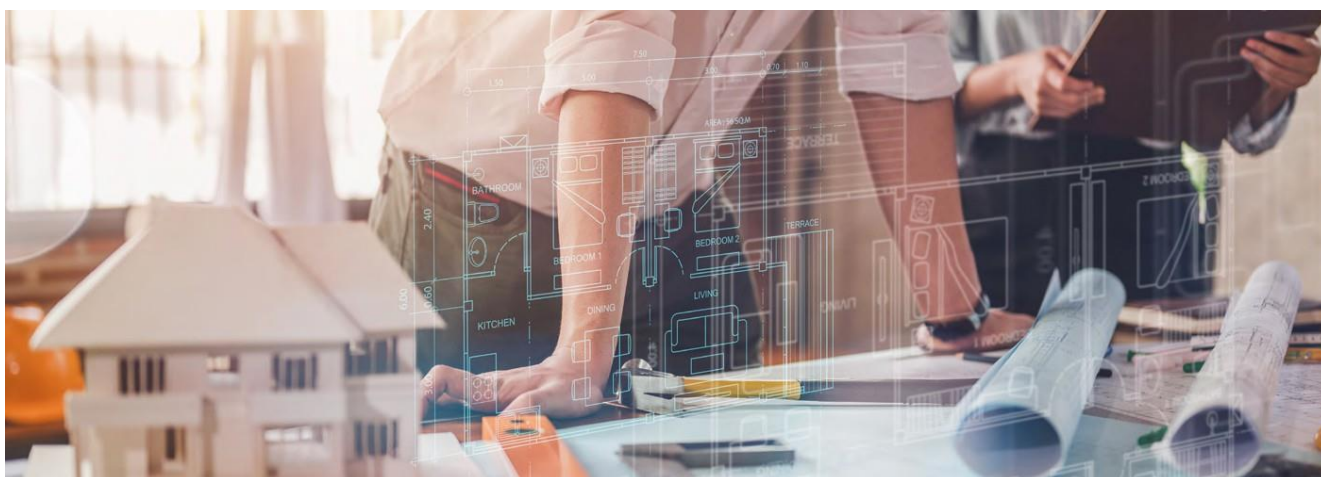
468
469
470
471
472

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 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	Klare Verantwortungszuweisung bei Verbindungsstörungen
VH5	Kurzfristige Erweiterbarkeit um Anwendungen für KRITIS-Infrastrukturüberwachung sowie Smart-Home und AAL mit Sicherheitsbedarf
VH6	Bereits etablierte Plattform für Servicedienstleistungen

473
474
475
476
477
478

Tabelle 5: Vorteile Handlungsempfehlungen des Projektes



479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499

Anhang A: Internationale Institutionen

IEC/TC 13

Die IEC/TC 13 beschäftigt sich mit der Normung auf dem Gebiet der Wechsel- und Gleichstrommessung und -steuerung elektrischer Energie, für intelligente Messgeräte und -systeme, die Teil intelligenter Netze sind und in Kraftwerken, entlang des Netzes und bei Energieverbrauchern und -erzeugern eingesetzt werden, sowie die Ausarbeitung internationaler Normen für Zählerprüfgeräte und -verfahren. Ausgeschlossen: Normung für die Schnittstelle von Messgeräten für Verbindungsleitungen und industrielle Verbraucher und Erzeuger (abgedeckt durch TC 57).

IEC/TC 57

Die IEC/TC 57 behandelt die Ausarbeitung internationaler Normen für Geräte und Systeme zur Steuerung von Energieversorgungssystemen, einschließlich EMS (Energy Management Systems), SCADA (Supervisory Control And Data Acquisition), Verteilungsautomatisierung, Teleprotection und zugehörigem Informationsaustausch für Echtzeit- und Nicht-Echtzeit-Informationen, die bei der Planung, dem Betrieb und der Wartung von Energieversorgungssystemen verwendet werden. Das Management von Stromversorgungssystemen umfasst die Steuerung innerhalb von Leitstellen, Umspannwerken und einzelnen Primärgeräten, einschließlich der Fernsteuerung und der Schnittstellen zu Geräten, Systemen und Datenbanken, die möglicherweise nicht in den Anwendungsbereich von TC 57 fallen. Die besonderen Bedingungen in einer Hochspannungsumgebung müssen berücksichtigt werden.

IEC/TC 79

Die IEC/TC 79 beinhaltet die Ausarbeitung internationaler Normen für den Schutz von Gebäuden, Personen, Gebieten und Grundstücken gegen betrügerische Handlungen, die darauf abzielen, unerlaubt in einen Ort einzudringen oder etwas mitzunehmen oder zu benutzen, sowie gegen andere Bedrohungen von Personen.

Der Geltungsbereich umfasst unter anderem Geräte und Systeme, die entweder von gewöhnlichen Personen oder von geschulten Personen in den folgenden Anwendungen im privaten und nicht privaten Bereich verwendet werden:

- Zugangskontrollsysteme;
- Alarmübertragungssysteme;
- Videoüberwachungssysteme;
- Kombinierte und/oder integrierte Systeme, einschließlich Brandmeldeanlagen;
- Brandmelde- und Feueralarmsysteme;
- Einbruch- und Überfallmeldeanlagen;
- Entfernte Empfangs- und/oder Überwachungszentralen;
- Soziale Alarmsysteme.

IEC/TC 23

Das IEC/TC 23 koordiniert zwischen den verschiedenen Unterausschüssen des TC 23 und mit anderen technischen Gremien innerhalb und außerhalb der IEC von Aspekten der Sicherheit, EMV, Koordination, Leistung, Kompatibilität, Interoperabilität, Austauschbarkeit, Energieeffizienz und Terminologie für elektrisches Zubehör, die zum globalen Management der elektrischen Energie beitragen. Ausarbeitung von Normen für elektrisches Zubehör und zugehörige Systeme, für Wechsel- und Gleichstrom, für den Haushalt und ähnliche Zwecke,

wobei das Wort „ähnlich“ Orte wie Büros, Geschäfts- und Industriegebäude, Krankenhäuser, öffentliche Gebäude usw. einschließt.⁵

4 <https://www.iec.ch/technical-committees-and-subcommittees#tclist>, Abruf: 14.02.2024

CEN/TC 72

„Brandmelde- und Feueralarmanlagen“ Das CEN/TC 72 (Technisches Komitee CEN 72) ist ein technisches Entscheidungsgremium innerhalb des CEN-Systems, das an der Ausarbeitung von Normen im Bereich der Brandmeldeanlagen in und um Gebäude in der Europäischen Union arbeitet. Ziel der Normen ist es, die grundlegende Anforderung „Sicherheit im Brandfall“ der Bauproduktenverordnung 305/2011 zu erfüllen.⁶

CLC/TC 205

„Home and Building Electronic Systems (HBES)“ CLC/TC 205 „Home and Building Electronic Systems (HBES)“ bietet Normen für alle Aspekte elektronischer Systeme in Haushalten und Gebäuden im Zusammenhang mit der Informationsgesellschaft. Dieses TC befasst sich hauptsächlich mit den notwendigen Leistungsanforderungen und den erforderlichen Hardware- und Softwareschnittstellen und nicht mit Gerätenormen.⁶

SyC AAL

System Committee „Active Assisted Living“ Der Systemausschuss SyC AAL soll eine Vision des Active Assisted Living schaffen, die der Entwicklung des Markttest entspricht. Dabei soll die Normung gefördert werden, die die Benutzerfreundlichkeit und Zugänglichkeit von AAL-Systemen und -Diensten ermöglicht. Auch die herstellerübergreifende Interoperabilität von AAL-Systemen, - Diensten,- produkten und - Komponenten soll gegeben sein.⁵

IEC/SyC Smart Energy

System Committee „Smart Energy“ Im IEC/SyC Smart Energy wird Normung im Bereich der intelligenten Energie Koordination und Anleitung auf Systemebene in den Bereichen Smart Grid und Smart Energy, einschließlich der Interaktion in den Bereichen Wärme und Gas behandelt. Umfassende Konsultation innerhalb der IEC-Gemeinschaft und der breiteren Stakeholder-Gemeinschaft, um den TCs und anderen Standardentwicklungsgruppen innerhalb und außerhalb der IEC einen Gesamtwert auf Systemebene, Unterstützung und Anleitung zu bieten. Kontaktaufnahme und Zusammenarbeit mit der SEG Smart Cities und zukünftigen SEGs sowie der zukünftigen Systems Resource Group.⁵

CLC/TC 8X

„System aspects of electrical energy supply“ Vorbereitung des erforderlichen Normenrahmens und Koordinierung der Entwicklung von CE- NELEC-Normen in Zusammenarbeit mit anderen TC/SCs, um das Funktionieren von Elektrizitätsver-sorgungssystemen in offenen Märkten zu erleichtern. TC8X deckt auch die Hochspannungs-Gleichstrom-Übertragung (HGÜ) für Gleichspannungen über 100 kV ab.⁶

Anhang B:

Relevante DKE Gremien

DKE/K 716

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

DKE/K 713

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.⁷

DKE/K 952

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 952.⁷

DKE/K 901

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

677 nicht nur IEC-Normung, sondern auch externe und an der Normung beteiligte
678 Gruppen wie Behörden und Konsortien mit ein. Darüber hinaus setzt sich das
679 Komitee mit dem Thema Digitalisierung auseinander: Insbesondere Blockchains
680 im Energiesektor werden durch eine Task Force bearbeitet.⁷

681
682
683 6 (DKE, o.A.)

684 **DKE/K 461**

685 Normung im Bereich der Messung und Steuerung von elektrischer Wechsel- und Gleichstromenergie für
686 intelligente Messeinrichtungen (Smart Meters) und Systeme, die Teile intelligenter Netze (Smart Grids) bilden,
687 für die Anwendung in Kraftwerken, in Netzen und bei Endverbrauchern und -erzeugern sowie die Erarbeitung
688 internationaler Normen für Zählerprüfeinrichtungen und -verfahren. Zu den Themenfeldern rund um die
689 Messgeräte gehören Geräteabmessungen, Messbereiche, Messunsicherheitsfestlegungen, Wirkungen von
690 äußeren Einflüssen, wie Temperatur, Spannungsqualität oder Magnetfelder, Kommunikationsprotokolle oder
691 auch Sicherheitsfestlegungen und Zuverlässigkeitsanforderungen. Die Normungsarbeit der dem DKE/K 461
692 zugeordneten Arbeitskreise trägt maßgeblich dazu bei, dass nicht nur jedes Gerät an sich funktioniert,
693 sondern dass die Wertschöpfung im gesamten Systemverbund gehoben werden kann, indem die einzelnen
694 Geräte zuverlässig und interoperabel miteinander kommunizieren können.

695 Tätigkeiten: Auch im Jahr 2016 war die Arbeit des DKE/K 461 stark durch die
696 vorgesehene Einführung von Smart Metering in Deutschland geprägt. Im
697 Mittelpunkt standen dabei Normungs- und Standardisierungsarbeiten rund um das
698 sogenannte Smart Meter Gateway und hier besonders dessen Schnittstellen. So
699 wurden die Arbeiten am Entwurfs-Manuskript für „Leitungsgebundene LMN-
700 Protokolle“ abgeschlossen und veröffentlicht. Diese Arbeiten erfolgten in enger
701 Abstimmung mit dem VDE FNN.⁷

702 703 **DKE/K 801**

704 Nach Gründung des System Committees auf IEC-Ebene wurde auf nationaler
705 Ebene das System Komitee AAL (DKE/K 801) gegründet. AAL-Technologien sind
706 technische Hilfsmittel, die Menschen im Alltag und im Beruf unterstützen, ihre
707 Gesundheit bewahren und fördern sowie Folgen von Krankheit und Verletzung
708 mildern, kompensieren oder beheben. Sie zeichnen sich durch eine Vielfalt von
709 Technologien und Komponenten aus, weshalb ein systematischer Ansatz in der
710 Normung und Standardisierung benötigt wird. Themenübergreifende Schnittstellen
711 zu verwandten Domänen (z. B. Smart Home) und funktionale Anforderungen in
712 Zusammenarbeit mit relevanten Gremien, Konsortien und Foren sollen identifiziert
713 werden, um beispielsweise die Interoperabilität sicherzustellen. Dieses Ziel des
714 System Komitees AAL wurde bei der ersten Sitzung des Gremiums im August
715 2014 bestätigt. Das Gremium beschäftigt sich u. a. mit folgenden Themen:
716 Verknüpfung von AAL bezogenen Normungsaktivitäten in unterschiedlichen
717 Technologiefeldern und Berücksichtigung des ausgeprägten Systemcharakters von
718 AAL-Technologien, Barrierefreiheit von AAL-Produkten und –Systemen,
719 Zugänglichkeit zu AAL-Systemen, User Interfaces, Usability,
720 herstellerübergreifende Interoperabilität von AAL- Systemen, - Produkten und –
721 Komponenten, Schnittstellen zu Smart Home, E-Health und E-Mobility, Use Cases
722 und Use Case Architecture, Integrationsprofile, Datenschutz und Sicherheit im
723 Umfeld von AAL, Nutzeranforderungen, Qualitätskriterien und Wearable Smart
724 Devices. Außerdem wird das Thema „Dienstleistungskette für
725 Gefahrenmeldungen im sozialen Betreuungswesen“ behandelt. ⁷

726 727 728 **DKE/TBINK/AK_BMWK_BSI Koordinierung im Umfeld intelligenter Messsysteme**

729 Informationsaustausch zum Thema „Metering und zugehörige Technologien im
730 Umfeld intelligenter Messsysteme“.

731 Koordination bei Kommentierungen zu „Metering und zugehörige Technologien im
732 Umfeld intelligenter Messsysteme“, (BSI, BMWK, BNetzA etc.).⁷

733
734 7 (DKE, o.A.)

Anhang C: Nationale Institutionen

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 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.

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

791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806

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.⁸

807
808
809
810
811
812
813
814

DIN-Normenausschuss Feuerwehrwesen

Der DIN-Normenausschuss Feuerwehrwesen (FNFW) ist aus dem Fachausschuss für Normung der Feuerwehrräte im Normenausschuss der Deutschen Industrie entstanden, dessen Gründung auf das Jahr 1920 zurückgeht. Der Zuständigkeitsbereich erstreckt sich von der Feuerwehrausrüstung über die Feuerwehrfahrzeuge, die Brandmelde- und Löschanlagen sowie Feuerlöschgeräte bis hin zu baulichen Anlagen und Einrichtungen für Feuerwehren und umfasst weiterhin das Gebiet der Sicherheit und des Schutzes des Gemeinwesens.⁹

815

Die Arbeitsausschüsse kooperieren auf europäischer und internationaler Ebene mit den CEN-Gremien:

816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848

- CEN/TC 72 „Brandmelde- und Feueralarmanlagen“

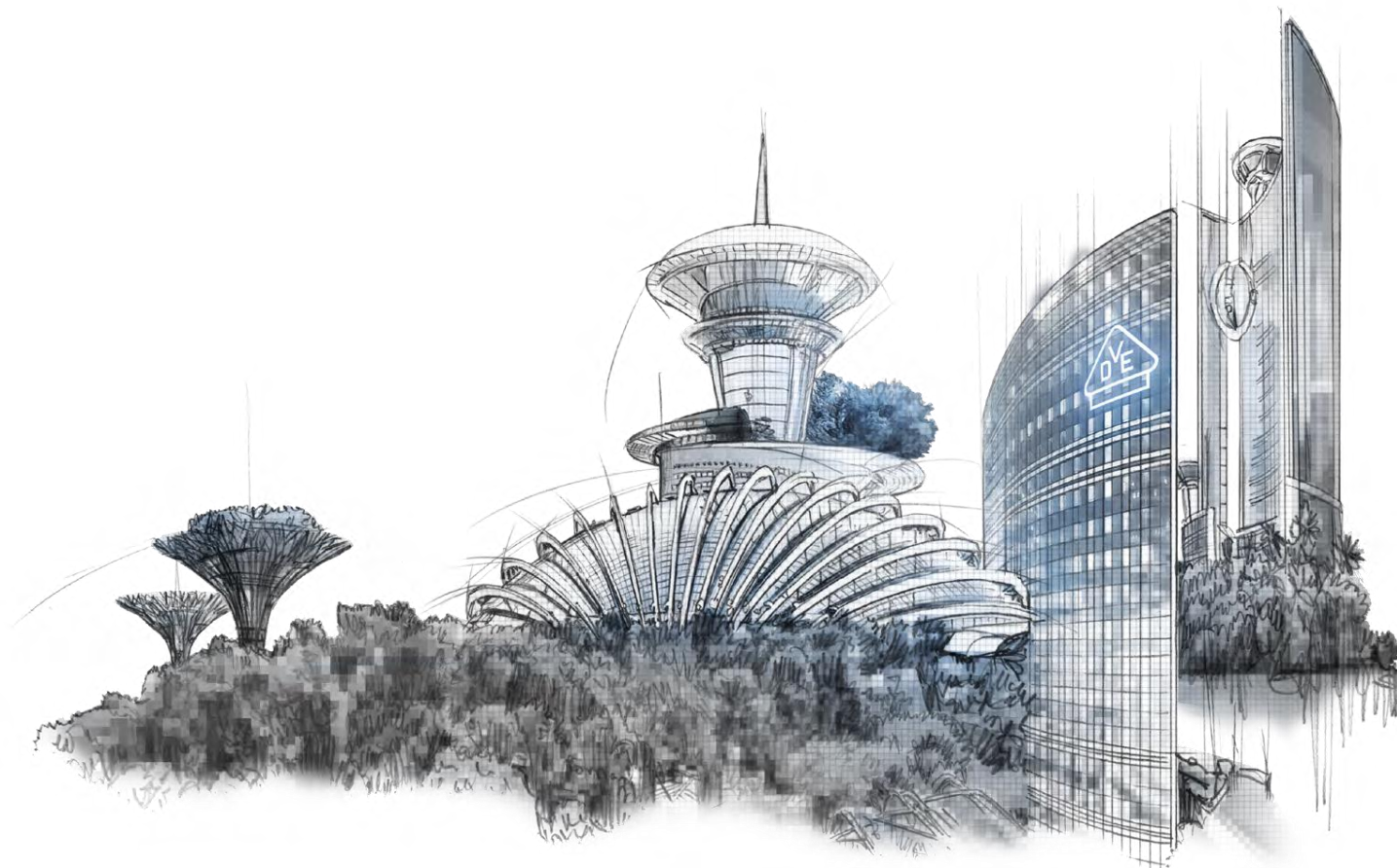
849
850
851
852

⁸ https://www.bsi.bund.de/DE/Home/home_node.html, Abruf: 14.02.2024

⁹ <https://www.din.de/de/mitwirken/normenausschuesse/fnfw>, 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