

Zum Erfolg verdammt Die Digitalisierung der Energiewende

Dieter Fischer

Sparen ist angesagt, auch und gerade beim Energieverbrauch. Aber Sparen muss nicht mit Verzicht gleichgesetzt werden. Besser ist es, Ressourcen effizienter zu nutzen. Energie ist eine wesentliche Ressource für das Wohlergehen unserer Gesellschaft. Aber ihre Erzeugung führt zu oft unangenehmen Risiken und Nebenwirkungen, wenn nicht sogar zu riesigen Nebenwirkungen. So wenig Energieverbrauch wie möglich bei gleichbleibendem Nutzen zu schaffen, das ist die Herausforderung an Ingenieure und Techniker. Es schont die Umwelt und spart auch noch Geld.



In Deutschland braucht man für dringend benötigte Veränderungen erst einmal ein Gesetz, oder noch besser – gleich zwei. Die wurden 2016 verabschiedet: Das Gesetz zur Digitalisierung der Energiewende (GDEW) und das Messstellenbetriebsgesetz (MsbG). Sie enthalten beide die klare Forderung: „Alle Gebäudedaten sollen über eine gemeinsame, sichere Plattform mit gesicherten Übertragungswegen und zentral verwalteten Schnittstellen für externe Marktteilnehmer (EMT) zugänglich sein.“

Erst einmal Kosten sparen

Will man technisch etwas voranbringen, muss man hierzulande erst einmal die Kostenparer in den großen Konzernen begeistern. Und die Erfassung von Verbrauchsdaten ist so ein Kostenfaktor, den man durch Digitalisierung minimieren kann. Der Umweltschutzgedanke beruht dabei auf der vagen Hoffnung, dass der Verbraucher Energie spart, wenn er seine auflaufenden Kosten unmittelbar auf seinem

Intelligente Netzsteuerungen sind wichtig zur Synchronisation von Energieangebot und -nachfrage. Das bedeutet: Sichere und ständig verfügbare Übertragungswege sind unverzichtbar für die Energiewende (Foto: Enrique, pixabay)

Smartphone präsentiert bekommt.

Es verwundert also nicht, dass der Schwerpunkt der Entwicklung zunächst als Ziel hatte, Messdaten sicher und datenschutzkonform digital aus dem Gebäude zu bekommen.

BSI-Lösung zur Messdatenerfassung

Wird irgendetwas zwecks Rechnungsstellung messtechnisch erfasst, greift das Messstellenbetriebsgesetz (MsbG). Der Lieferant will schließlich rechtssicher verbrauchsabhängige Rechnungen schreiben. Es muss aber auch sichergestellt werden, dass die Cyberkriminalität weder Messdaten verfälschen, falsche Steuerbefehle einschleusen noch den Datenschutz aushebeln kann.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert in der Richtlinienreihe TR03109 das

Dieter Fischer ist Strategieberater im Bereich „Sicherer Datenzugang zur Gebäude-Infrastruktur mit Alarm- und Verbrauchssensorik“ bei TAS Sicherheits- und Kommunikationstechnik in Mönchengladbach

Smart-Meter-Gateway (SMGW) als zentrales Gerät zur Erfassung von Messdaten. Die Gegenstelle dazu in der Cloud ist der SMGW-Admin, der den Remote-Zugriff auf das SMGW überwacht und Meldungen an die zuständigen und verifizierten Empfänger weiterleitet.

Roadmap des BMWK

Die erste Generation der SMGW sollte nur die Basis für weitere Entwicklungsschritte sein. Zukünftig, so steht es im Gesetz und in der Roadmap des BMWK (Bild 1), sollen alle Daten, die von Geräten im Gebäude produziert oder zur Fernwartung von Anlagen genutzt werden, über ein gemeinsames Gateway übertragen werden. Dabei hat die Sicherheit gegen unbefugten Zugriff auf die Daten und die Gerätefunktionen oberste Priorität.

Die vom BSI und dem Gesetzgeber vorgegebene Sicherheitsarchitektur hat allerdings ihren Preis: unter einer halben Million Euro und mehreren Monaten Prüfzeit ist eine Zulassung nicht zu haben. Aber: Braucht die Energiewende eine andere Sicherheit als z.B. militärische Anlagen?

Digitalisierung trifft Sicherheit

Die Roadmap listet im Cluster 3 Themen auf, die bisher durch die Normen und Richtlinien der Alarmübertragungstechnik abgedeckt wurden. Brand- und Einbruchmeldeanlagen mit abgesicherter Übertragung zu Sicherheitsleitstellen, zu Polizei und Feuerwehr sind ja schon seit längerem in Gebäuden installiert. Hier soll wohl etwas zusammenwachsen, was bisher strikt getrennt behandelt wurde, auch bei der normgebenden Institution „Deutsche Kommission der Elektrotechnik im DIN und VDE“ (DKE).

Sicher, es ist sinnvoll, wenn alles in einem Gebäude, was Daten übermitteln will oder von extern steuerbar ist, über ein gemeinsames, sicheres Gateway mit dem Internet verbunden ist. Nur dieses eine flächendeckende Übertragungsnetz gibt

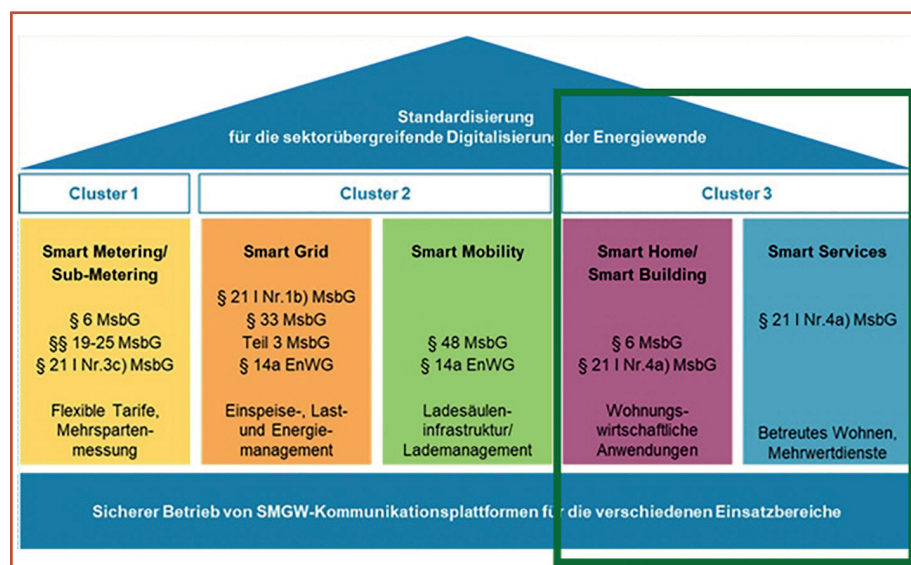


Bild 1: Die Roadmap des BMWK zur Digitalisierung der Energiewende: Zukünftig sollen alle Daten von Geräten, die im Gebäude Daten produzieren oder digital gesteuert werden können, über ein gemeinsames Gateway übertragen werden

es ja noch, egal, ob Festnetz oder Mobilfunk für die „letzte Meile“ genutzt wird. Nun treffen hier die unterschiedlichen Lösungsansätze, Normen und Richtlinien aus der europäischen und internationalen Standardisierung der Sicherheitstechnik auf die Richtlinien des deutschen BSI, insbesondere die der TR03109-Reihe.

Sicherlich, die digitale Souveränität unseres Gemeinwesens verlangt nach optimalem Zugangsschutz gegen kriminelle und feindliche Angriffe. Aber hier wurde ein Gateway für die Strommesstechnik geschaffen, ohne auf die bereits bestehenden Gateway-Richtlinien und Übertragungsweg-Normen für Gebäudeüberwachung und Personensicherung Rücksicht zu nehmen.

Anforderungen der Energiewende

Zwischen dem SMGW und dem SMGW-Admin wird für die Datenübertragung derzeit das öffentliche Internet genutzt. Im Objekt sind dabei DSL-Router, ONTs (Optical Network Termination) für die Glasfaser und Mobilfunkmodems Teil des Internetzugangs. Sie sind Angriffsversuchen aus dem Netz oder vor Ort unmittelbar ausgeliefert und ermöglichen böswilligen Angreifern, gezielt die Kommunikation zum SMGW zu unterbinden.

Für die reine Erfassung von Ver-

brauchsdaten ist das „nur“ ärgerlich. In naher Zukunft benötigen die nicht stabil verfügbaren Energiequellen wie Solarstrom und Windenergie aber zusätzlich rasch wirk-same Verbrauchssteuerungen, um keinen „Blackout“ entstehen zu lassen. Wenn aber für die Stabilität des Stromnetzes Schalt-handlungen wie z.B. Lastabwürfe in win-zigen Zeitfenstern zwingend erforderlich werden, ist das heutige SMGW-Sicherheits- und -Übertragungskonzept – vorsichtig formuliert – mehr als überarbeitungsbe-dürftig.

Alarmübertragungsanlagen

Zeitkritische Anwendungen und die Verfügbarkeitsüberwachung mit Redundanzoptionen, die in Alarmübertragungsanlagen Stand der Technik sind, werden in der Richtlinienreihe TR03109 nicht berücksichtigt. Dies verwundert gerade mit Blick auf die zukünftigen energiewirtschaftlichen Anforderungen. Die für die Anbindung von Mehrwertdiensten in der TR03109 definierte „CLS-Schnittstelle“ am SMGW ist so bei zeitkritischen Mehrwertdiensten wie betreutem Wohnen oder für die Anbindung von Alarmanlagen unbrauchbar. Die Nutzung gemäß Cluster 3 der Roadmap ist nach gegenwärtiger Normenlage sogar weitgehend unzulässig. Aber wie funktio-

nieren heute Alarmübertragungsanlagen?

Etablierte Rahmenbedingungen

Die Sicherheitstechnik hat die Aufgabe, Personen und Sachwerte zu schützen. Schnelles Handeln bei Brand oder Überfall kann Leben retten, bei Einbruch zumindest den Schaden in Grenzen halten. Schäden sind Kosten für Sachversicherer, also gibt es dort ein großes Interesse, für qualitativ hochwertige Sicherungs- und Alarmübertragungstechnik zu sorgen. Dazu gründete die Versicherungswirtschaft vor über hundert Jahren den VdS (Vertrauen durch Sicherheit), der nicht nur ein Regelwerk aus Richtlinien erarbeitet hat, sondern auch die Einhaltung dieser Vorgaben für Versicherungskunden überwacht.

Eine wesentliche Grundlage für schnelle und sichere Reaktion im Alarmfall ist das Zusammenspiel aller Hilfskräfte vom Ereignis bis zur Intervention. Diese „VdS-Sicherungskette“, basierend auf DIN/EN-Normen und VdS-Richtlinien, garantiert heute eine qualitativ hochwertige Gefahrenabwehr (Bild 2).

Überarbeitete und neue Normen

Die DKE als normgebende Stelle für die Energie- und Alarmkommunikation sowie der VdS mit seinem Richtlinienkatalog für die Sicherheitstechnik sind gefragt, die fälligen Anpassungen voranzutreiben. Für Hausbesitzer und Bewohner darf es keine unterschiedlichen, vielleicht sogar sich widersprechenden Vorschriften je nach Gewerk geben. Fällige Kosten dürfen auch nicht vernachlässigt werden: Entscheidend für die Akzeptanz von Produkten und Systemen, die dabei helfen, die Klimaziele zu erreichen, ist ein gutes Kosten-Nutzen-Verhältnis.

Es kommt also darauf an, dass durch die Digitalisierung der Energiewende keine zusätzlichen Kosten entstehen, vielleicht sogar für den Verbraucher – nicht

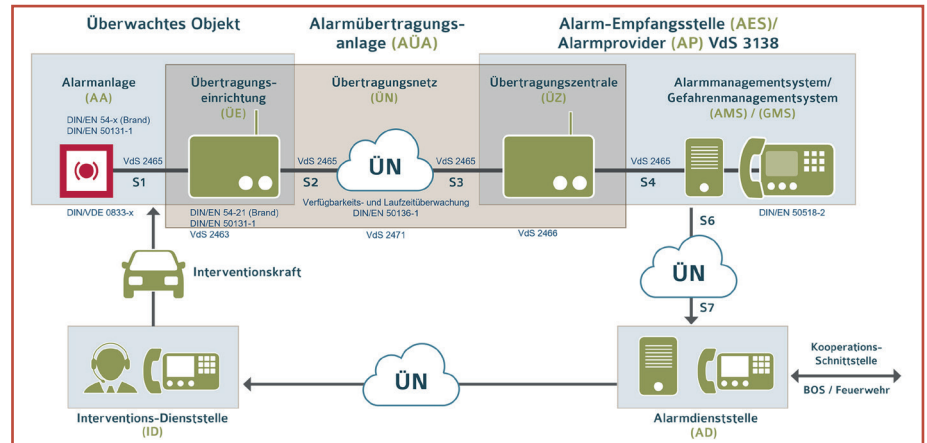


Bild 2: Die VdS-Sicherungskette garantiert, basierend auf DIN/EN-Normen und VdS-Richtlinien, eine qualitativ hochwertige Gefahrenabwehr – vom (Schadens-)Ereignis über das Management zur Intervention (Hilfeleistung)

nur für den Energieverkäufer – ein Kosten-senkungspotenzial generiert werden kann.

SMGW nur für den Elektroschrank?

Leider gab es zunächst für ein Forschungsprojekt, Energie- und Alarmkommunikation in Richtung einer gemeinsamen Plattform zu überarbeiten, beim BMWK keine Fördermittel. Wahrscheinlich wollte man die Markteinführung von SMGW für die Elektrozähler nicht stören. Aber die Zeit drängte. Mittlerweile besteht eine Installationspflicht für SMGW ab 6.000 kWh Jahresverbrauch Strom (größeres Einfamilienhaus) und für Liegenschaften mit steuerbaren Verbrauchseinrichtungen (z.B. PV-Anlagen ab 7 kW und Wärmepumpen). Das betrifft ca. 20 Mio. Gebäude in Deutschland. Wie viele davon haben heute aber schon eine Brand- und/oder Einbruchmeldeanlage mit sicherer Alarmübertragung?

WWNW – WärmewendeNordwest

So war das Bundesministerium für Bildung und Forschung (BMBF) bereit, einen anderen Aspekt der Energiewende zu fördern: die Wärmewende. „Für Raumwärme in Gebäuden wurden in Deutschland im Jahr 2018 26 % des gesamten Endenergieverbrauchs aufgewendet. Weitere 5 % entfielen auf den Bereich Warmwasser. Damit die Energiewende gelingen kann, brauchen wir daher auch eine Wärmewende“ (Zitatquelle:

Umwelt-Bundesamt).

Die Energienutzung für die benötigte Wärme muss also deutlich effizienter werden. Neben der Sanierung ist die Digitalisierung, also eine gesicherte Basis für die Datenübertragung und Steuerung, auch hier von zentraler Bedeutung. Im einem der WWNW-Forschungsfelder, dem Feld 2, sind fünf Partner zusammengekommen, um gemeinsam unter der Leitung der DKE und des Forschungsinstituts OFFIS (ein An-Institut der Universität Oldenburg) Lösungen für die Integration des SMGW in die VdS-Sicherungskette auszuarbeiten und in Normen und Richtlinien festzuhalten.

OFFIS hatte schon den Rollout des SMGW begleitet. Die Alarmempfangszentrale FSO, der Alarmübertragungsanlagen-Hersteller TAS und der VdS bringen die nötige Erfahrung mit dem Bestand von Alarm- und Notruftechnik ein. Das Wohnungsunternehmen GSG-Oldenburg wacht darüber, dass auch der Anwender als Hausbesitzer oder Mieter mit seinen Bedürfnissen nicht vergessen wird.

WWNW-Forschungsfeld 2

Es gilt also, das bereits erarbeitete Know-how der sicheren Übertragung von Brand-, Einbruch-, Überfall- und Personennotrufmeldungen in die Roadmap des BMWK zur Digitalisierung der Energiewende zu integrieren. Prinzipiell unterscheiden sich

die Anforderungen an die Sicherheit von SMGW und Alarmübertragungsanlagen nicht. Angriffe auf Netzrouter sind keine theoretische Möglichkeit, sondern eine reale Gefahr, gerne genutzt von Cyberkriminellen mit Erpressungsabsichten. Aber auch Terrorismus bis hin zum Cyberkrieg muss sicher verhindert werden. Generell kann man von folgenden Bedrohungen ausgehen:

- physische Zerstörung von Übertragungsgeräten;
- Austausch von Übertragungsgeräten;
- physische Zerstörung von Übertragungswegen;
- Blockade von Übertragungswegen (DoS);
- Funktionsveränderungen durch äußere elektromagnetische Strahlung;
- Funktionsveränderungen durch fehlerhafte Schnittstellenbeschaltung;
- illegaler Zugang zu gespeicherten Daten (DSGVO-Verstoß);
- Funktionsveränderungen durch illegalen Softwaretausch;
- Funktionsveränderungen durch illegale Konfigurationsänderung;
- Mitschneiden von Meldungen (Angriffsvorbereitung);
- Verändern oder Unterdrücken von Meldungen;
- unzulässige Schaltbefehle.

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 produzieren und nachzuweisen.

Schutz der Übertragungswege

Aber der beste Schutz nützt nichts, wenn die Datenübertragung selbst gestört wird. Das könnte schon ein Stromausfall sein. Gerade bei Stromausfall ist die Übertragung von Alarmen unverzichtbar. Alarmübertragungsgeräte haben heute einen

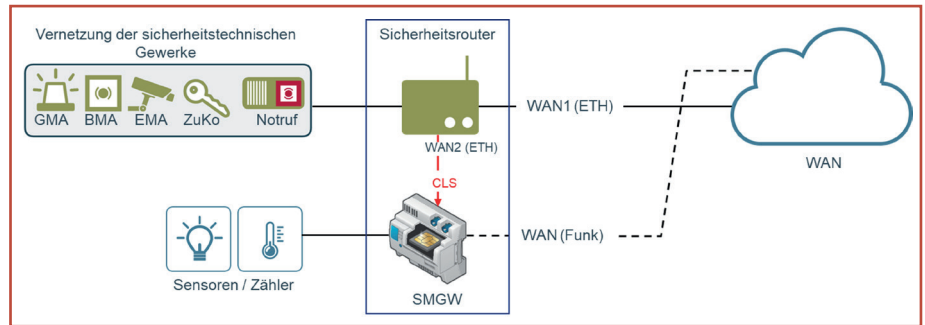


Bild 3: Nicht empfehlenswerter Lösungsansatz gemäß BMWi-Roadmap mit parallel angebundener Alarmübertragungstechnik: Die Übertragungseinrichtung aus der Sicherungskette übernimmt dabei zusätzlich Aufgaben eines Sicherheitsrouters

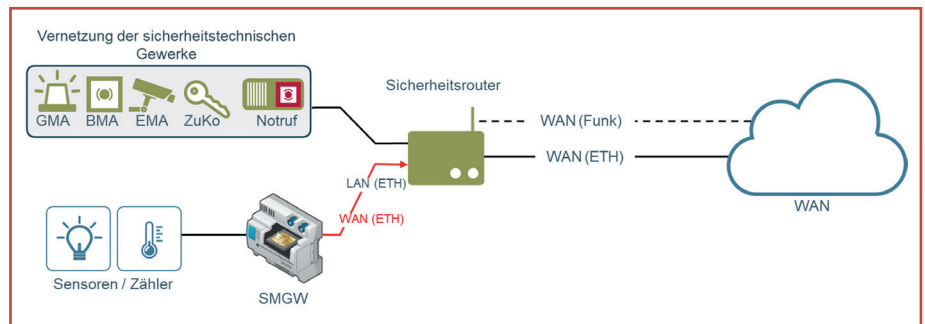


Bild 4: Lösungsansatz gemäß Forschungsergebnis: gemeinsamer Sicherheitsrouter für SMGW und Alarmer/Notrufe. SMGW und SMGW-Admin werden norm- und richtlinienkonform über die Übertragungswege der Sicherheitstechnik miteinander verbunden

batteriegestützten Funktionserhalt von bis zu 72 h, die Funktion des SMGW dagegen ist unmittelbar von der Stromversorgung abhängig. Auch ist es für die Notrufleitstellen wichtig, jederzeit die Funktion des Übertragungswegs überwachen zu können, um bei Ausfall Ersatzmaßnahmen einzuleiten.

SMGW und Alarmübertragung

Im Forschungsprojekt wurde zunächst, wie von der BMWK-Roadmap vorgesehen, der CLS-Kanal des SMGW als mögliche Verbindung der Gebäudesicherheitssysteme an das Netz betrachtet. Die Übertragungseinrichtung aus der Sicherungskette (Bild 1) übernimmt dabei zusätzlich Aufgaben eines Sicherheitsrouters, um im Notfall (Ausfall der SMGW-Übertragungsstrecke) auf einen alternativen Netzzugang zurückgreifen zu können (Zwei-Wege-Absicherung zur Erhöhung der Verfügbarkeit). Bild 3 zeigt diesen Lösungsansatz auf.

Dem Sicherheitsrouter fehlen hier jedoch Informationen über den physika-

lischen Status der Datennetzanbindung auf dem SMGW-Weg und somit über die Wahrscheinlichkeit einer erfolgreichen Alarmmeldungsübertragung. Das ist ggf. zeitkritisch. Die fehlende Notstromversorgung des SMGW reduziert zusätzlich die Verfügbarkeit des Übertragungswegs (EN 50136).

Weitere Probleme ergeben sich aus den Anforderungen, Remote-Infrastrukturen sowohl für das SMGW als auch den Sicherheitsrouter bis hin zu den nachgeschalteten Überwachungs-, Mess- und Steuerungssystemen bereitzustellen. Leider wurde bereits eine separate Lösung für das SMGW mittels „Smart-Meter-Gateway-Admin“ (TR03109-6) etabliert. Bei einer Übertragungstechnik von Alarmen aus sicherheitstechnischen Gewerken kollidiert diese Richtlinie mit den normativen Anforderungen der CLC/FprTS 50136-10 und der prEN 50710, da es den Verantwortungsbereich des dort definierten „Remote-Access-Infrastructure-Providers (RAISP)“ untergräbt. Die CLS-Schnitt-

stelle des SMGW erfüllt demnach nicht die Anforderungen an einen Alarmübertragungsweg.

Norm- und richtlinienkonform

Wie schon erwähnt, gibt es bei der Vernetzung sicherheitstechnischer Gewerke mit hilfeleistenden Stellen eine etablierte sichere Übertragungstechnik, basierend auf international anerkannten Normen und Standards. Es liegt also nahe, die Übertragung von Messdaten des Energieverbrauchs und „netzdienliche Schalthandlungen“ darin einzubinden, insbesondere unter dem Aspekt, dass die Sicherheitsanforderungen bezüglich Personen- und Sachwerteschutz gegenüber der Messdatenintegrität als gleichwertig betrachtet werden können (Bild 4). SMGW und SMGW-Admin werden norm- und richtlinienkonform über die Übertragungswege der Sicherheitstechnik miteinander verbunden.

Anstelle des DSL-Routers, Glasfaser-ONT, Breitbandkabel- oder Mobilfunk-Routers kommt hier ein Sicherheitsrouter mit direktem passiven Netzanschluss für alle Netzabschlüsse gemäß §70 Abs. 1 TKG zum Einsatz, der sowohl eine Übertragungseinrichtung im Sinne der Sicherheitskette als auch ein besonders sicherheitsgehärteter Netzrouter für das SMGW ist. Das SMGW kann nun auf alle Vorteile zurückgreifen, die eine Alarmübertragungsanlage bietet: hohe Verfügbarkeit durch redundanten Netzzugang und Notstromversorgung des Sicherheitsrouters, ständige Verfügbarkeitsüberwachung der Übertragungswege und gesicherte Fernwartungszugänge z.B. über die TAS Secure Platform. Ein SMGW-Admin wäre darin problemlos integrierbar.

Da die BSI-Richtlinien den Netzübertragungsweg nicht weiter beachten, wird die normkonforme Alarmübertragung nicht behindert, umgekehrt hat die Alarmübertragung auch keine Rückwirkung auf die richtlinienkonforme Funktion des SMGW und des SMGW-Admin (Bild 5). Lediglich

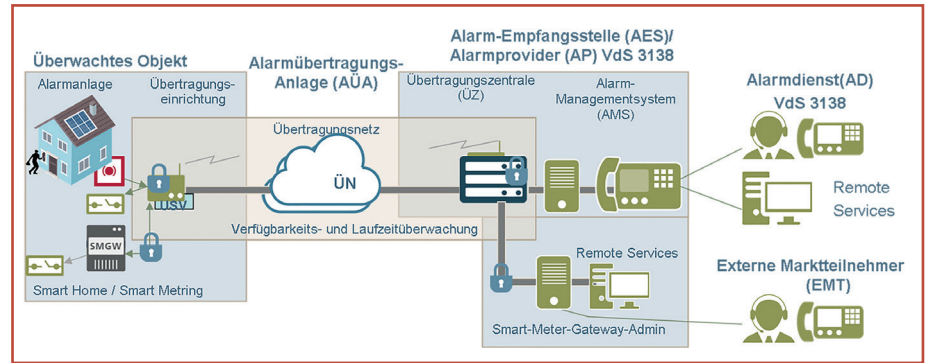


Bild 5: Gemeinsame Übertragungswege für SMGW und Sicherheitstechnik: Die normkonforme Alarmübertragung wird nicht behindert, umgekehrt hat die Alarmübertragung auch keine Rückwirkung auf die richtlinienkonforme Funktion des SMGW und des SMGW-Admin

für die Nutzung der CLS-Schnittstelle ergibt sich eine Wettbewerbssituation zwischen dem SMGW und den bereits verfügbaren Smart-Home-Schnittstellen des Sicherheitsrouters. Es bleibt ohnehin die Frage, ob das SMGW mit seinem Schwerpunkt auf die MsbG-konforme Messdatenerfassung zukünftig unbedingt noch Erweiterungen für Smart-Home-Anwendungen bereitstellen muss, die ja auch noch entwickelt werden müssen.

In vielen Gebäuden mit Brand- und Einbruchmeldetechnik ist heute schon eine Übertragungseinrichtung als Teil einer sicheren Alarmübertragungsanlage (AÜA) installiert; es muss also kein weiterer WAN-Anschluss für das SMGW eingerichtet und bezahlt werden. AÜA lösen auch das Problem, dass häufig eine stabile Mobilfunkverbindung zum Installationsort im Keller unmöglich ist. Dies wird beim derzeitigen Rollout der SMGW von Installateuren beklagt.

Normen unterstützen Innovationen

Bei der Digitalisierung der Energiewende müssen neben hoher Betriebssicherheit die Sicherheitsaspekte gegen unerwünschte und gefährliche Zugriffe immer Berücksichtigung finden. Elektronische Gateways und Router ins Internet stellen einen digitalen Hauszugang dar, der mindestens so gut gegen Einbruch (Cybercrime) geschützt werden muss wie die physische Haustür mit ihrem Türschloss. Trotz höchster Sicherheitsanforderungen muss dieser „elektronische Hauszugang“ jedoch mit akzeptablen Kosten bereitgestellt werden.

Gelingen kann das nur bei gemeinsamer Nutzung von vielen Gewerken im Gebäude (Sektorkopplung). Bereits installierte Sicherheitsinfrastruktur bei bestehenden oder von der Bauordnung vorgeschriebenen Alarm-/Brandmeldeanlagen mit standardisierten Schnittstellen, Funktionen und Sicherheitseinrichtungen könnte hier mithilfe eines preiswert zu realisierenden Upgrade zu einer sinnvollen Sektorkopplung beitragen. Dies wäre ein wesentlicher Beitrag zur Kostenreduktion bei gleichzeitigem Sicherheitsgewinn und könnte somit die Akzeptanz von Systemen zur CO₂-Reduktion deutlich erhöhen.

Im Rahmen des Forschungsprojekts WärmewendeNordwest ist nun geplant, die problemlose Funktion in real existierenden Gebäuden und Liegenschaften des Partners GSG nachzuweisen. Die technische Machbarkeit dürfte das weitaus geringere Problem sein gegenüber bürokratischen Regelungshürden. Die heutige TR03109 ist eine rein nationale deutsche Richtlinie. Ein gemeinsamer EU-Markt sollte doch eigentlich nationale Alleingänge verhindern. Europäische Normen können das sicherstellen. Es ist zu begrüßen, dass die Arbeitskreise der Energietechnik und der Sicherungstechnik im DKE mittlerweile bereits zusammengefunden haben. Aber auch die Mitwirkung des BSI und des BMWK sind unverzichtbar für den Erfolg. Und den brauchen wir nicht nur im Projekt für ein Gelingen der Wärmewende „als zentrale Säule der Energiewende“.