

Informationssicherheit bei intelligenten Energienetzen

Information Security in Intelligent Energy Networks

Schlagwörter wie Smart Metering, Smart Grid oder Smart Home finden sich seit geraumer Zeit in den Fachpublikationen und der Tagespresse. Die intelligenten Energienetze der Zukunft, die sogenannten Smart Grids, gelten zusammen mit erneuerbaren Energien und Speichersystemen als wichtigste Säule bei der Weiterentwicklung der Energieversorgung.

Slogans such as smart metering, smart grid or smart home have been found in the trade publications and the daily press for some time now. The intelligent energy networks of the future, the so-called smart grids, stand in conjunction to renewable energy and storage systems as an important pillar in the development of energy supplies.

Als erster Schritt gilt die Einführung der Zähldatenermittlung und Zählerfernauslesung (Smart Metering), bedingt sie doch den flächendeckenden Aufbau von Kommunikationsnetzen. Sobald die Infrastruktur zur Vernetzung von Geräten zur Verfügung steht, wird das Thema Smart Home an Bedeutung gewinnen, indem SmartSensor- und Mess-Systeme zur Steigerung der Energieeffizienz und Wohnqualität sowie zur Verbesserung der Sicherheit in Wohn- und Nutzgebäuden entwickelt und eingesetzt werden. Bereits heute hat jeder Verbraucher die freie Wahl des Messstellenbetreibers und Messdienstleisters und kann nach seinem Wunsch z. B. eine monatliche Energieabrechnung erhalten.

Auslastung der Energienetze optimieren

Aus Sicht der Energieversorger bietet sich die Chance, über intelligente Zähltechnik die Verbraucher in ihr Energiemanagement einzubinden und somit die Auslastung der Energienetze zu optimieren. Durch kostengünstig verfügbare Energieangebote, die einen Anreiz zur Energieeinsparung oder Steuerung des Energieverbrauchs liefern, soll der Verbraucher zu einem ökonomischen und ökologischen Verhalten motiviert werden. Mit dieser Zielsetzung wird klar, dass „Smart Metering“ weit mehr ist als nur die elektronische Erfas-

sung von Verbrauchsdaten. Vielmehr sind davon ein Vielzahl von Betriebsprozessen zur Erfassung, Übertragung, Speicherung, Archivierung, Verarbeitung und Abrechnung von Verbrauchsdaten wie auch für die Energiebeschaffung und die Steuerung des Energieverbrauchs betroffen.

Datenschutz

Neben ökonomischen und ökologischen Aspekten ist aber auch der Datenschutz in den Vordergrund gerückt. Das Bundesdatenschutzgesetz (BDSG) stellt personenbezogene und personenbeziehbare Daten unter seinen Schutz. Die Energienutzung ist gerade in einer hochtechnisierten Gesellschaft ein Spiegelbild des menschlichen Lebens. Durch die individuellen Lastprofile, die durch das Smart Metering erstellt werden, kann ein Rückschluss auf Lebensgewohnheiten, ja sogar auf den tagesebenen Ablauf, gezogen werden. Allgemein besteht daher kein Zweifel, dass Verbrauchsdaten zu den schützenswerten Daten der Verbraucher zählen.

Verschlüsselung

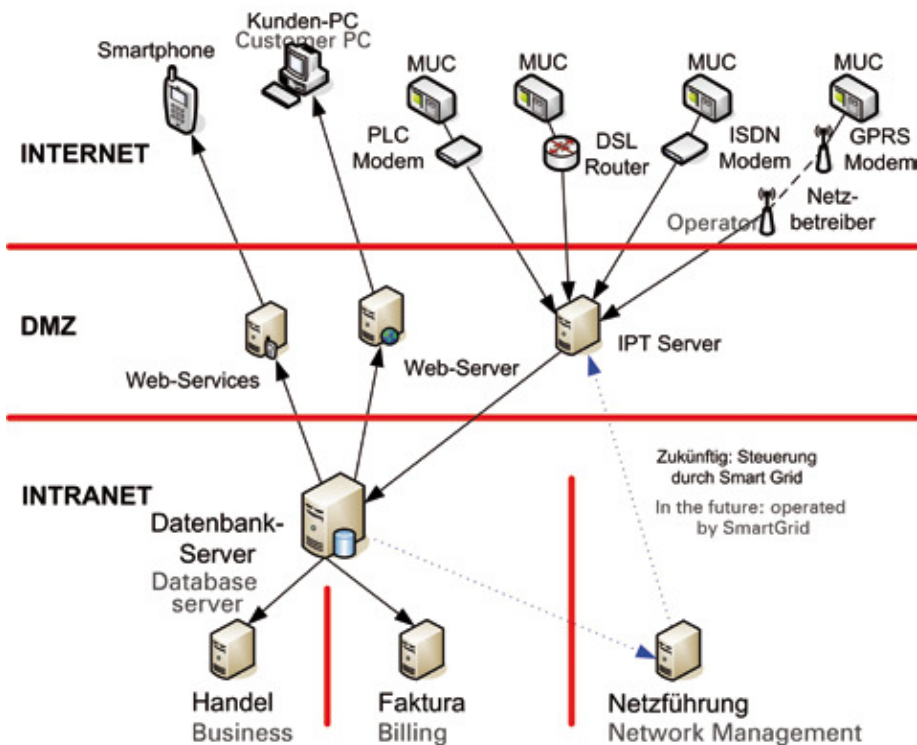
Dies wurde im Forum Netztechnik/Netzbetrieb des VDE offensichtlich übersehen. In Form eines Lastenhefts ist unter <http://www.vde.de/de/fnn/dokumente/seiten/hinweise.aspx> eine Referenzplattform zur einheitlichen Datenerfassung für Gas,

Strom, Wärme und Wasser (MUC – Multi-Utility-Communication) veröffentlicht. In der Anforderungsmatrix steht zum Thema "Datensicherheit, Zugriffsschutz" folgende Aussage: "Eine Verschlüsselung der Übertragung ist nicht notwendig". Es erstaunt also nicht, dass verschiedene am Markt befindliche MUC-Produkte, die als Ersatz für die heute installierten elektromechanischen Ferraris-Zähler zum Einsatz kommen, keine Software für Verschlüsselung besitzen. Auch die zur Verfügung stehende Prozessorleistung ist völlig ungeeignet, um die komplexen kryptografischen Operationen, wie sie für die Ver- und Entschlüsselung von sicheren Kommunikationsvorgängen notwendig sind, in angemessenen Zeiträumen durchzuführen.

Effiziente und effektive Sicherheitsarchitektur

Die TTS Trusted Technologies and Solutions GmbH betreut langjährig einige Kunden im Energiesektor. Dabei wird das Thema Smart Metering ganzheitlich im Sinne der Informationssicherheit behandelt und alle in den Geschäftsprozessen involvierten Anwendungen, System- und Netzwerkkomponenten berücksichtigt.

Es hat sich gezeigt, dass Smart Metering auf eine effiziente und effektive Sicherheitsarchitektur angewiesen ist, da zu den einzelnen Verbrauchern jeweils Netzwerk-



Einsatzszenario Smart Metering mit Darstellung verschiedener Sicherheitszonen.

Smart Metering deployment scenario, with representation of different security zones.

kopplungen realisiert werden und dabei alle beteiligten Kommunikationspartner bzw. ihre Unternehmensnetze voreinander zu schützen sind (siehe Abbildung). Die zum Einsatz kommenden zentralen (wie etwa Datenbank-Server, Faktura-System oder Web-Server) wie auch dezentralen Systeme (z. B. DSL-Modem, MUC) müssen abgesichert werden, stets den aktuellen Sicherheitsstand berücksichtigen und mit rigiden Zugangs- und Zugriffsberechtigungen versehen sein. Neben einer Überwachung der Systeme ist zu gewährleisten, dass die Übermittlung von Daten die vorherige Authentisierung des Kommunikationspartners verlangt. Bei einer derartigen Vielfalt an Sicherheitsaspekten ist es erforderlich, das Thema Informationssicherheit schon in der Konzeption der Smart Metering-Lösung zu berücksichtigen. Durch die Ausarbeitung eines Sicherheitskonzeptes sind die notwendigen Sicherheitsmaßnahmen zu ermitteln und anschließend in eine problemadäquate Sicherheitsarchitektur zu integrieren.

The introduction of remote meter reading and meter evaluation (smart metering) are the first steps, since they determine the building of wide-area communication networks. Once the infrastructure for net-

working equipment is available, the smart home topic gains in importance through the development and implementation of smart sensor systems and measurement systems designed to improve residential energy efficiency and quality of living, thus enhancing safety in domestic and non-residential buildings. Already today, every consumer has the free choice of metering service providers and billing providers and may demand a monthly energy bill at his own request, for instance.

Optimizing the utilization of energy networks

From the utility providers' perspective, using smart metering provides the opportunity to engage consumers in their energy management, therefore optimizing the utilization of their energy network. Available cost-effective energy offerings provide incentives to save energy and control energy consumption so that consumers are motivated to exhibit economic and ecological behaviour. With this objective, it is clear that "smart metering" is much more than just the electronic recording of consumption data. Rather, it involves a variety of operating processes for recording, transmission, storage, archiving, processing and billing of consumption data as well as for energy procurement and the monitoring of energy consumption.

Data privacy

Besides economic and ecological aspects, the focus on data protection has increased. The German Federal Data Protection Act (BDSG) provides protection for personal-related and personally identifiable data. Energy consumption, particularly in a highly technological society, is a mirror of human life. Personalised load profiles created by smart metering can reflect human life and can even go as far as a showing precise daily processes. In general, there is no doubt that consumption data is among the most sensitive data to consumers.

Encryption

This was apparently overlooked in the network engineering / network operation forum of the VDE (Germany's Association for Electrical, Electronic and Information Technologies). A specification was published, found under <http://www.vde.de/de/fnn/dokumente/seiten/hinweise.aspx>, which serves as a reference platform for the uniform collection of data for gas, electricity, heat and water (MUC – Multi-Utility Communication). The requirement matrix therein emphasises the points of "data security, access control," in the following statement: "An encryption of transmission is not necessary." It is therefore not surprising that various MUC products on the market that are installed

today to replace the electromechanical Ferraris meter do not offer software for encryption. Also, the available processing power is totally unsuitable for the complex cryptographic operations needed for the encryption and decryption of secure communication processes carried out at appropriate intervals.

Efficient and effective security architecture

For many years, TTS Trusted Technologies and Solutions GmbH have served several customers in the energy sector. In doing so, the topic of smart metering is treated holistically in terms of information security and is included in all integrated business processes involving applications, system components and network components.

It is clear that, in order to ensure smart metering efficiently and effectively, a security structure is necessary since network links are implemented in each individual consumer system to protect all participating communication partners as well as the individual corporate networks from each other (see also Figure 1). The central command stations (such as database servers, billing systems or web servers) as well as decentralized systems (e.g. DSL modems, MUC) must guarantee to unfailingly take into account the current security levels and rigid entry and access authorisations. In addition to monitoring the systems it is crucial that prior to the submission of data, authorisation must be approved by the communication partner.

With such a variety of safety issues, it is necessary to take information security into account early on in the concept development of a smart metering solution. Through the development of a security concept the necessary security measures must be determined and then integrated into a security structure adequate to the problem. ▲

Contact

Dr. Jörg Cordsen

TTS Trusted Technologies and Solutions GmbH

Email: joerg.cordsen@tts-security.com
www.tts-security.com

Modulares GSM-Meldesystem für Security-Anwendungen

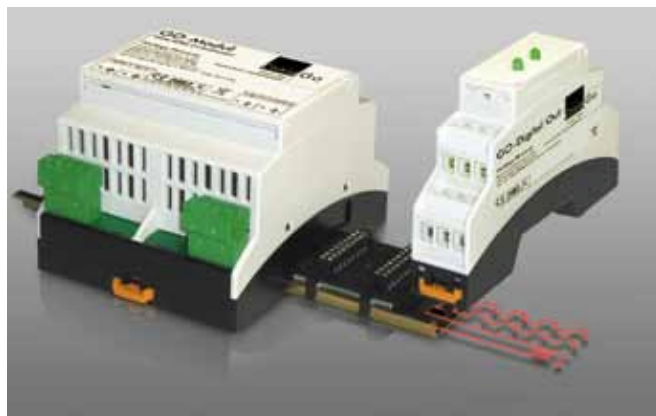
Modular GSM Alarm System for Security Applications

Security-Anwendungen über GSM-Meldeanlagen können sowohl SMS als auch GPRS-Datenübertragung nutzen und setzen sich im Markt mehr und mehr durch.
Security applications by GSM as a short message or by GPRS have become more and more common in the market.

Die GSM-Technik hat in Sicherheitsanwendungen seit Jahren Einzug gehalten. Bekannt sind Geräte verschiedenster Ausführungen, z.B. die seit Jahren bewährten GSM-Meldemodule der Typen Advanced GSM Modul und GSM Scout. Diesen Geräten ist zueigen, dass sie über eine festgelegte Anzahl von Meldelinien oder auch Messeingängen für Analogsignale verfügen. Problematisch wird das, wenn Anlagen später an andere Anforderungen angepasst werden sollen oder erweitert werden müssen. Hier setzt das Konzept der GO-Module an. Die Neuheit bei der ConiuGo GmbH besteht darin, dass man sich das Meldegerät aus einer GO-Zentrale und bis zu 16 GO-Modulen nach Bedarf zusammenstellen kann. Das

schafft ein bislang unbekanntes Ausmaß an Flexibilität und Investitionssicherheit.

Die Kommunikation der Module untereinander und mit dem Zentralmodul erfolgt dabei über eine Busschiene, die praktischerweise direkt in die Hutschiene zur Montage der Geräte integriert werden kann. Die Vorteile dieses Konzepts liegen auf der Hand: Man kann die GSM-Meldeanlage jederzeit erweitern und zusätzliche Module ergänzen. Im Reparaturfall arbeiten die nicht betroffenen Module weiter, auch die mit einer Reparatur verbundenen Kosten bleiben erfreulich niedrig. Investitionssicherheit und Flexibilität entstehen auch, weil man einzelne Module jederzeit



Das GO-Modul besteht aus einem Zentralgerät mit bis zu 16 Zusatzmodulen. So ist Flexibilität für den Anwender garantiert. The innovative GO-Module consists of a central unit and up to 16 additional modules for input- /output- functions. A high degree of flexibility is guaranteed for the users application.