Konzept zur Untersuchung des dynamischen Verhaltens von Messsensoren in Energienetzen mit hohen Anforderungen an die Systemsicherheit

Yiyang Su*, Jörg Neumann**

* Yiyang Su, Arbeitsgruppe 8.52 "Metrologische IKT-Systeme"

** Jörg Neumann, Arbeitsgruppe 8.52 "Metrologische IKT-Systeme", E-Mail: joerg.neumann@ptb.de

Einleitung

Für das effektive Betreiben von Smart Grids müssen eine große Menge von Messdaten und Steuerinformationen übertragen werden. Aktuelle lokale Mengen an verbrauchter oder eingespeister elektrischer Energie werden hierbei von den intelligenten Messsystemen und Zählern als wichtige Eingangsgrößen bereitgestellt. Für den Betrieb von Smart Grids spielt insbesondere die sichere Datenübertragung eine bedeutende Rolle, die als Thema im Rahmen des European Metrology Research Programme (EMRP) im Forschungsprojekt ENG63 GridSens Sensor network metrology for the determination of electrical grid characteristics in einem eigenen Arbeitspaket Security and standardisation näher untersucht wird. Dieses Projekt mit einer Laufzeit von 3 Jahren wurde im Sommer 2014 gestartet.

Die sich aus dem Fachbereich Metrologische Informationstechnik der PTB und dem Institut für Elektrische Energietechnik und Energiesysteme der Technischen Universität Clausthal zusammengesetzte Arbeitsgruppe hat sich zum Ziel gesetzt, ein sicheres verteiltes Messsystem in einem Niederspannungs-Microgrid zu entwickeln und aufzubauen. Neben der Systemsicherheit wird vor allem auch die Veränderung des dynamischen Verhaltens des Gesamtsystems durch zusätzliche Sicherheitskomponenten untersucht. Zu den Schwerpunkten der Arbeiten gehören:

- Bewertung vorhandener Sicherheitslösungen,
- Entwicklung eines generischen Datenmodells,
- Untersuchung von dynamischen Eigenschaften der Sicherheitslösungen und
- Erarbeitung konkreter Lösungsvorschläge für den Bereich der Zustandsbestimmung in Smart Grids.

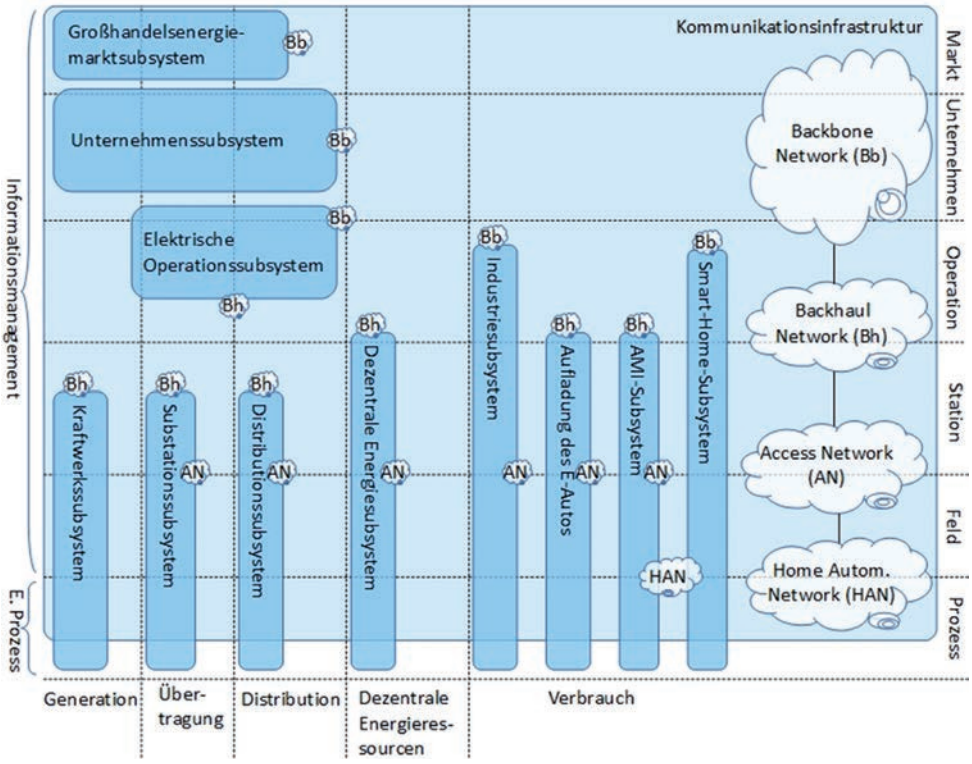

Bild 1:
Smart-Grid-Komponenten [1]

Im Folgenden wird eine Übersicht zu Sicherheitsaspekten im Smart Grid geben sowie der aktuelle Stand der Arbeiten in dem Forschungsprojekt beschrieben.

Sicherheitsaspekte in Smart Grids

Traditionelle Energienetze zeichnen sich dadurch aus, dass die Energie von zentralisierten Energieerzeugungsanlagen erzeugt und an die Endverbraucher transportiert wird. Die Energieflüsse sind unidirektional und die Kontrollstrukturen zentralisiert. Mit der wachsenden Anzahl von dezentralen Energiequellen innerhalb der Energienetze werden neue Kommunikationstechniken und Kontrollsysteme benötigt. Die Vielfalt der heterogenen und miteinander vernetzten Systeme zeichnen sogenannte Smart Grids aus.

In der CEN-CENELEC-ETSI Smart-Grid-Koordinationsgruppe wurde ein allgemeines Modell entwickelt [1], welches die Smart-Grid-Komponenten und die energiewirtschaftlichen Prozesse abbildet. Dieses enthält sowohl die Komponenten der elektrischen Prozesse, bestehend aus Generation, Übertragung, Distribution, dezentrale Energieressourcen und Verbrauch als auch die des Informationsmanagements. Eine vereinfachte Form ist in Bild 1 dargestellt.
Das Informationsmanagement wird hierbei in fünf Zonen untergliedert:

- Feld: Gesamtheit der Einrichtungen, die das Stromnetz schützen, kontrollieren und überwachen können,
- Station: Aggregation der Informationen aus dem Feld,
- Operation: Bewertung des Netzzustandes und generieren von Steuerinformationen in der jeweiligen Domäne,
- Unternehmen: Beinhaltet die wirtschaftlichen und organisatorischen Prozesse sowie Dienstleistungen und Infrastrukturen der Unternehmen und
- Markt: Bildet die Marktvorgänge bezüglich der Energieumwandlungskette ab.

Unterschiedliche Subsysteme werden mit vielfältigen Vernetzungstechnologien über verschiedene Kommunikationswege verbunden. Eine große Menge von Messdaten und Steuerinformationen werden zwischen diesen übertragen. Ein Angriff auf diese Daten stellt ein potenzielles Sicherheitsrisiko dar. Zum Beispiel, im Bereich der elektrischen Operationssubsysteme werden verschiedene Supervisory Control and Data Acquisition (SCADA) Systeme eingesetzt, die über Netzwerke mit anderen Untersystemen (z. B. Substations- und Distributionssubsystem) gekoppelt sein können. Eine detailliertere Ansicht über die Verbindung zwischen elektrischem Operationssubsystem und Substationssubsystem ist in Bild 2 dargestellt. Die Messdaten werden aus den angeschlossenen Geräten akquiriert und der Zustand des Energienetzes vom SCADA-System bewertet.

Diese Informationsnetze könnten über Cyber-Attacken angegriffen werden bspw. über passive Angriffe, wie dem Abhören des Netzwerkes, um an Informationen zu gelangen oder durch aktive

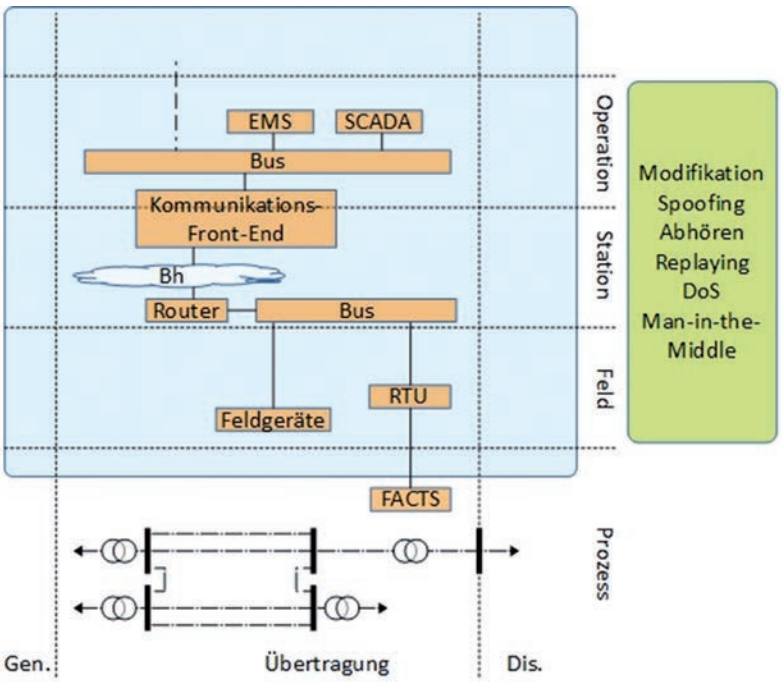

Bild 2:
EMS-/SCADA-System [1]

Angriffe, die die Funktion des Smart Grids stören sollen. Mit dem Unterdrücken oder Einspielen falscher Daten [2, 3] können bspw. ein oder mehrere SCADA-Systeme angriffen werden, die letztendlich zu einer falschen Bewertung des Energienetzes führen.

Um einen zuverlässigen Betrieb des Smart Grids zu gewährleisten, ist ein sicherer Informationsaustausch eine unabdingbare Voraussetzung. Für den Schutz von Messdaten und Steuerinformationen in Smart Grids lassen sich die folgenden Sicherheitsanforderungen definieren [4]:

- **Integrität** bezeichnet den Schutz der Daten vor Modifikation und Replay-Angriff,
- **Authentizität** weist die Urheberschaft nach,
- **Nicht-Bestreitbarkeit** verhindert, dass die Urheberschaft abgestritten werden kann, und
- **Vertraulichkeit** bietet Schutz vor unbefugtem Abhören.

Über diese Sicherheitsanforderungen hinaus, welche insbesondere die Messdaten und Informationen betreffen, können für verteilte Messsysteme weitere Schutzziele definiert werden. So stellt die Verfügbarkeit des Netzwerks ein wichtiges Schutzziel dar [5].

Durch die Nutzung kryptografischer Verfahren bei der Datenübertragung und Archivierung können alle vier genannten Schutzziele erreicht werden. Um eine langfristige Sicherheit zu gewährleisten und Kompatibilität zwischen den verschiedenen Systemen sicherzustellen, sollten genormte bzw. standardisierte Verfahren eingesetzt werden. Je nach Anwendungszweck werden hierzu symmetrische (DES, AES) oder asymmetrische (RSA, ECC) kryptografische Verfahren in den Kommunikationsprotokollen von Smart Grids eingesetzt.

In den betrachteten Netzwerken werden teilweise Übertragungsprotokolle genutzt, die ursprünglich für eine effiziente Übertragung von Mess- und Steuerungsdaten entwickelt wurden. Die Fragen der sicheren Datenübertragung im Sinne der oben genannten Schutzziele spielte eine untergeordnete Rolle. Typische Vertreter sind das Distributed Network Protocol (DNP3) sowie die Normenserien der IEC 60870 und IEC 61850.

Um das Schutzniveau der Kommunikation zu erhöhen, wurde es notwendig, das Thema der IT-Sicherheit in einer gesonderten Norm, der IEC 62351 zu behandeln. Diese erweitert die im TC 57 beschriebenen Kommunikationsprotokolle um eine Sicherheitsschicht. In Bild 3 ist die Verknüpfung der Kommunikationsprotokolle (Bild 3 linke Seite) und der in der IEC 62351 beschriebenen Maßnahmen (Bild 3 rechte Seite) zur Gewährleistung einer sicheren Datenübertragung dargestellt.

In der IEC 62351 werden auch die unterschiedlichen Anforderungen an das dynamische Verhalten der Systeme berücksichtigt. In weniger zeitkritischen Anwendungen können Datenübertragungsprotokolle nach der Manufacturing Message Specification (MMS) verwendet werden. Darüber hinaus kann die Kommunikation auf der Transportschicht mittels Transport Layer Security (TLS) verschlüsselt werden.

Der zweite Einsatzbereich ist die sichere Datenübertragung innerhalb von zeitkritischen Prozessen. Hier liegt der Schwerpunkt der Datensicherheit auf der Authentizität der Daten. Als Beispiele können die Generic Object Oriented Substation Events (GOOSE) und Sampled Values (SV) aus der IEC 61850 genannt werden. Aufgrund der Anforderungen, wie z. B. der erforderlichen Reaktionszeit von 4 ms, der Notwendigkeit der gleichzeitigen Datenübertragung an mehrere Teilnehmer (Multicast) und eventuell geringer CPU-Leistung

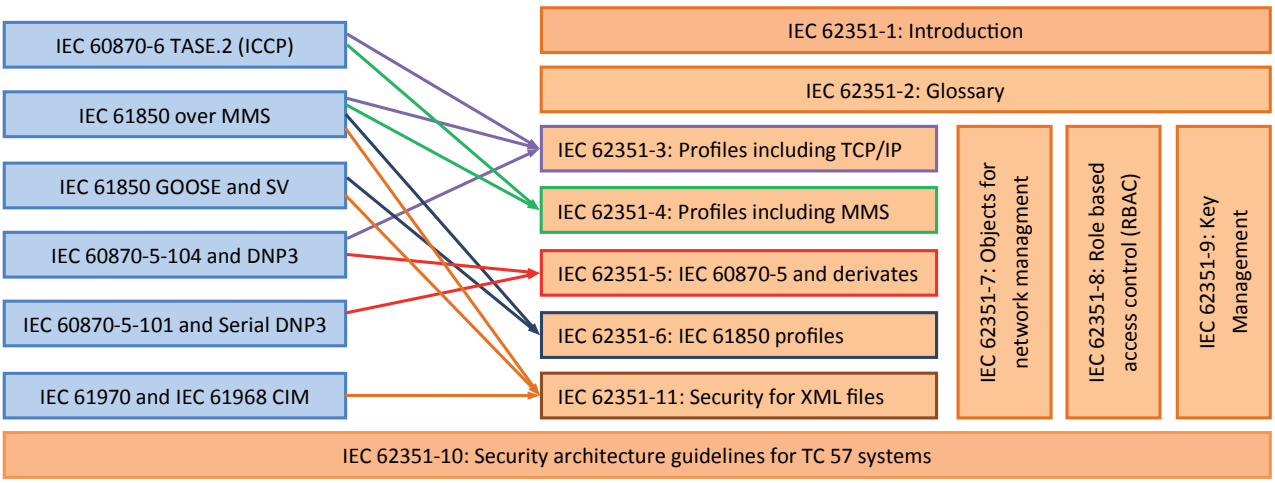

Bild 3:
Anwendungsbereich der IEC 62351 [6]

der Geräte, wird eine Verschlüsselung der Kommunikation nicht empfohlen. Die Datensicherheit wird u. a. durch ein Erweitern der Nutzdaten Protocol Data Unit (PDU) von GOOSE/SV Elementen mit Authentifizierungsinformation, die durch Hash-Funktion SHA256 und RSA-Algorithmus berechnet werden, erreicht.

Forschungsprojekt „ENG63 GridSens“ – aktueller Stand

Im EMRP-Projekt sollen einige der hier aufgezeigten Kommunikationsprotokolle untersucht werden. Ein Schwerpunkt hierbei ist die Datenmodellierung unter dem Blickwinkel der Zustandserfassung im Smart-Grid. Die zu erfassenden Messwerte sind mit einem geeigneten Datenübertragungsprotokoll zu übertragen. Die verschiedenen Datenübertragungsverfahren sollen daraufhin untersucht werden, ob sie den oben genannten Sicherheitsanforderungen genügen bzw. ob sie durch entsprechende Protokollerweiterungen auf ein entsprechendes Sicherheitsniveau gebracht werden können.

Durch die Verwendung kryptografischer Verfahren bei der Datenübertragung ist damit zu rechnen, dass sich die dynamischen Eigenschaften des Gesamtsystems verändern. Der Einfluss auf die Systemeigenschaften wie Latenz-, Reaktions- und Antwortzeiten ist hier Untersuchungsgegenstand. Für diese Analysen wurde ein universelles Messgerät konzipiert (Bild 4) und in einer ersten Variante realisiert.

Ein handelsüblicher Sensor wird über seine Schnittstelle an einen frei programmierbaren µController angeschlossen. In diesem erfolgt die Protokollwandlung auf das zu untersuchende Datenübertragungsverfahren. Die sicherheitsrelevanten Funktionalitäten werden in einem Kryptomodul abgearbeitet. Über ein GSM-Modem bzw. einen Ethernetanschluss kann mit verschiedenen Netzwerken kommuniziert werden. Die Ansteuerung des Sensors und das Triggern von Ereignissen zum Bestimmen des dynamischen Verhaltens des Systems erfolgt über die digitalen Ein- oder Ausgänge.

Bei der Verwendung asymmetrischer Kryptografieverfahren unter Verwendung von Zertifikaten ist der Aufbau einer Public-Key-Infrastruktur notwendig. Die Struktur der PKI ist in Bild 5 dargestellt.

Eine Besonderheit dieser PKI besteht darin, dass in der Rolle der Antragsteller keine Personen, sondern technische Geräte auftreten. Die Grundelemente der PKI wurden bereits entwickelt. Es gilt, sie an die realen Anforderungen beim Einsatz von Messgeräten anzupassen. Neben der sicheren Messdatenübertragung müssen die verschiedenen Lebenszyklen des Gerätes, der Zugriffsschutz auf das Gerät, Archivierung der Messdaten und die Möglichkeiten der Verifikation berücksichtigt werden.

Die Akzeptanz von Verfahren und Systemen hängt in großem Maß von ihrer Praxistauglichkeit ab. Deshalb erfolgt die Entwicklung in enger Zusammenarbeit mit dem Institut für Elektrische Energietechnik und Energiesysteme der Technischen Universität Clausthal. In dem dort vorhandenen Versuchsnetzwerk können die entwickelten Methoden getestet werden.

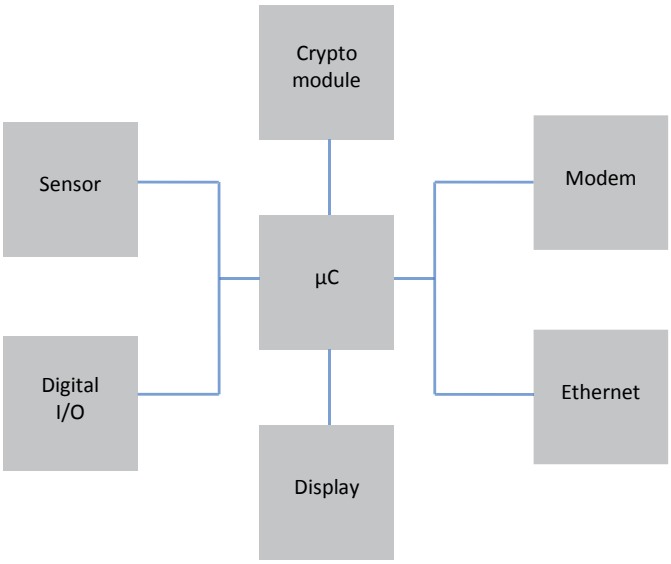

Bild 4:
Struktur der universellen Messeinrichtung

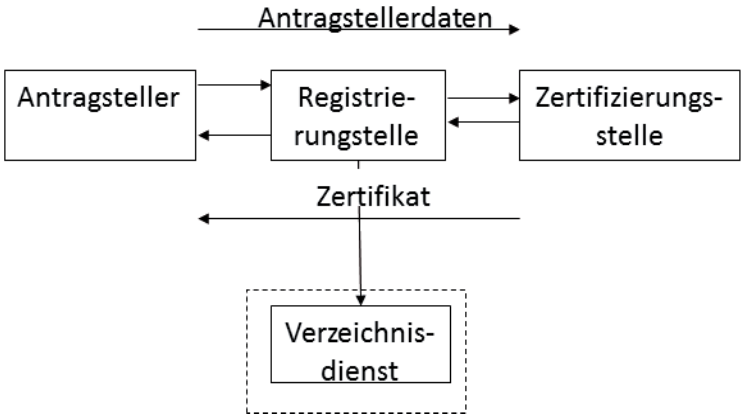

Bild 5:
Struktur der Komponenten PKI

Zusammenfassung

Im Rahmen des EMRP-Forschungsprojekts ENG63 GridSens: Sensor network metrology for the determination of electrical grid characteristics wurde ein eigenes Arbeitspaket Security and standardisation eingerichtet, das partnerschaftlich vom Fachbereich Metrologische Informationstechnik der PTB und dem Institut für Elektrische Energietechnik und Energiesysteme der Technischen Universität Clausthal bearbeitet wird. Ziel ist es, ein sicheres verteiltes Messsystem in einem Niederspannungs-Microgrid zu entwickeln und aufzubauen. Neben der Systemsicherheit wird sich der Frage der Veränderung des dynamischen Verhaltens des Gesamtsystems durch zusätzliche Sicherheitskomponenten besondere Aufmerksamkeit gewidmet.

Literatur

[1] CEN-CENELEC-ETSI Smart Grid Coordination Group, „First Set of Standards“, 2012

[2] P.-Y. Chen, S. Yang, J. McCann, J. Lin und X. Yang, „Detection of false data injection attacks in smart-grid systems“, Communications Magazine, IEEE, Bd. 53, Nr. 2, pp. 206-213, 2015

[3] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih und Z. Han, „Detecting False Data Injection Attacks on Power Grid by Sparse Optimization“, IEEE Trans. Smart Grid, Bd. 5, Nr. 2, pp. 612-621, 2014

[4] J. Wolff, R. Bösel, N. Zisky und D. Richter, „Sicherung von Messdaten in verteilten Messsystemen“, Verteilte Messsysteme, pp. 193-206, 1993

[5] H. Karl und A. Willig, Protocols and architectures for wireless sensor networks, John Wiley & Sons, 2007

[6] CEN-CENELEC-ETSI Smart Grid Coordination Group, „Smart Grid Information Security“, 2014