

# Mit Sicherheit ein hoher Aufwand: Der Prozess der Gateway-Administration im Überblick

Michał Sobótka und Lars Weber

*Rund 4,5 Mio. intelligente Messsysteme (iMsys) müssen in den kommenden Jahren installiert werden. Um dies wirtschaftlich umsetzen zu können, kommt es darauf an, den Rollout-Prozess möglichst effizient und vor allem hochintegriert abzubilden. Das gilt auch, wenn die Gateway-Administration über einen externen Dienstleister abgewickelt wird. Worauf im Gesamtprozess zu achten ist, beschreibt der vorliegende Artikel.*

Die Herausforderungen beim iMsys-Rollout beginnen schon lange vor der Installation der ersten Geräte. Denn zunächst gilt es, den realen Ist-Zustand im eigenen Netzgebiet zu kennen. Das bedeutet, dass alle potenziell auszutauschenden Geräte identifiziert und den betroffenen Mess- und Marktlokationen – die künftig den klassischen Zählpunkt ersetzen – zugewiesen werden müssen. Und noch wichtiger: Es ist zu entscheiden, welche Messeinrichtungen und -systeme zum Start tatsächlich betrachtet werden. Schließlich sieht das Interimsmodell vor, das mindestens 10 % aller Systeme in den ersten drei Jahren auszurollen sind.

Welche Zählpunkte im Fokus stehen sollen und ob es nicht sinnvoll sein könnte, gleich mehr als 10 % auszurollen, bleibt der Entscheidung des grundzuständigen Messstellenbetreibers (gMSB) – also in der Regel dem Netzbetreiber – überlassen. Aus Sicht des Gateway-Administrators ist schon dieser erste Prozessschritt essenziell. Nach der Auswahl der Zähler richten sich deren Stammdaten, die später für den Administrationsbetrieb benötigt werden.

Auch für den Beschaffungs- und Konfektionierungsprozess der Geräte ist die Erfassung des Ist-Zustandes die wesentliche Voraussetzung. Denn anders als beim guten, alten Ferraris-Zähler kann ein intelligentes Messsystem nicht einfach installiert werden. Es besteht aus verschiedenen Komponenten wie der modernen Messeinrichtung, dem Gateway und einer SIM-Karte, der wiederum ein entsprechender Vertrag zuzuordnen ist. Alle Geräte benötigen zudem die feste Zuordnung zu einer Mess- und Marktlokation, sonst können sie nicht in Betrieb genommen werden. Ebenfalls ist vorab zu klären, ob das Gateway am geplanten Installationsort per GSM kommunizieren

kann oder ob andere Kommunikationswege installiert werden müssen.

All diese Informationen fließen in Vorbereitung der Bestellung zum Gateway-Administrator, der daraufhin die sog. VP2-Konfigurationsdatei erstellt. Diese ist Basis für den Elektronischen Bestellschein und die Gütezertifikate. Über sein Gegenstück, den Elektronischen Lieferschein, wird das intelligente Messsystem dann direkt im stammdatenführenden System des MSB sowie im IT-System des Gateway-Administrators angelegt.

Von diesem Zeitpunkt an müssen diese Daten zwischen Systemen wie SAP IS-U oder andere ERP-Systemen und der IT des Gateway-Administrators beidseitig synchron gehalten werden. Bei größeren Mengengerüsten ist dazu eine tiefe Integration der Systeme des Gateway-Administrators mit den stammdatenführenden Systemen auf Seite des MSB unverzichtbar.

Bei kleineren Mengen – insbesondere während der dreijährigen Interimsphase – ist es dagegen durchaus möglich, dies auch teilautomatisiert umzusetzen, etwa über den Austausch von standardisierten CSV-Dateien. In diesem Zusammenhang wurde von GWAdriega ein „Startpaket“ entwickelt. Der Vorteil: Der Prozess kann in wenigen Wochen statt in Monaten produktiv gesetzt werden. Und eine Skalierung bis hin zur späteren Vollintegration ist jederzeit auch während des laufenden Betriebs möglich.

## **Echtzeitkommunikation für die Inbetriebnahme notwendig**

Könnte der bisherige Prozess der Installation von Ferraris-Zählern noch papierbasiert abgewickelt werden, ist dies künftig nicht

mehr möglich. Denn ohne eine mobile Anbindung des Monteurs ist der iMsys-Rollout kaum umsetzbar. Und das nicht nur, weil einzelne Arbeitsschritte eng ineinandergreifen. Besonders bei der Inbetriebnahme sollte möglichst wenig Zeit verloren gehen.

Ein Problem ist hier die sog. „Pairing-Lücke“. Das ist die Zeit, die zwischen der Installation und dem Pairing von Zähler und Gateway vergeht. In diesem Zeitraum werden keine Verbrauchsdaten erfasst und können auch nicht über das Gateway übertragen werden. Denn der digitale Zähler als Messeinrichtung und das Gateway werden zunächst als separate Systeme in den Verteilerschrank eingebaut.

Danach muss das Gateway über den Gateway-Administrator entsprechend konfiguriert und mit den notwendigen Sensor-, Kommunikations- und Auswerteprofilen ausgestattet werden. Erst dann werden die aktuellen Messdaten vom digitalen Zähler an das Gateway übergeben, dort korrekt gespeichert und mit einem Zeitstempel versehen. Anschließend erfolgt der Versand über den Gateway-Administrator an die vorher definierten Marktpartner und deren Messdaten-Management.

Deswegen ist eine Echtzeitkommunikation im Rahmen des Workforce Managements zwischen dem stammdatenführenden System und der IT des Gateway-Administrators künftig absolut sinnvoll – auch für die Monteure vor Ort. Denn sie können wenige Minuten, nachdem sie den Prozess der Inbetriebnahme angestoßen haben, an die nächste Installation gehen. Die restliche Konfiguration erfolgt dann vollautomatisiert und ist spätestens nach 10 bis 20 Minuten abgeschlossen – immer vorausgesetzt, die

Kommunikationsstrecke zwischen Gateway und Gateway-Administration steht.

Zwar könnte der während der Pairing-Lücke angefallene Verbrauch an Energie theoretisch rekonstruiert werden, doch die Verfahren dafür sind aufwendig. Auch ließen sich die iMSys vorkonfektionieren, um Zeit zu sparen. Doch das ist fachlich wenig sinnvoll, da erst am Zählerplatz die Einbausituation vollständig bewertet werden kann.

### Herausforderung Zertifizierung

Die Integration der Datenflüsse ist also eine wesentliche Voraussetzung und muss – speziell im Fall einer tiefen Integration – frühzeitig in Angriff genommen werden, egal ob die Gateway-Administration im eigenen Hause oder über einen externen Dienstleister wie GWAdriga abgebildet wird.

Im letzteren Fall kann der Aufwand aber deutlich gesenkt werden. Nicht nur, weil ein Full-Service-Dienstleister in der Regel einen erprobten Standardprozess inklusive standardisierter Schnittstellen zu den stammdatenführenden Systemen anbietet, auf den der gMSB einfach aufsetzen kann. Auch das umfangreiche Zertifizierungsverfahren für den Prozess der Gateway-Administration sowie die verwendeten IT-Systeme entfällt vollständig.

Und dieses hat es durchaus in sich: Kernstück der Zertifizierung ist das Informationssicherheits-Managementsystem (ISMS) nach ISO 27001 und TR03109. Im Rahmen des Zertifizierungsverfahrens werden sowohl die interne Dokumentation der Prozesse als auch die mit der Gateway-Administration verbundenen gelebten Prozesse sowie der physische Standort, an dem auf dem System gearbeitet wird, inklusive der für die Administration vorgesehenen Arbeitsplätze und vor-Ort-IT-Installationen genau unter die Lupe genommen. Dazu gehört u. a. auch die Prüfung der Wirksamkeit des Notfallkonzepts.

Hier musste GWAdriga bspw. nachweisen, dass selbst bei einer Unzugänglichkeit oder Zerstörung der Geschäftsräume, etwa durch Feuer oder einen Anschlag, der Betrieb der GWA-Strukturen weiterhin möglich ist. Zur Zertifizierung gehörten zudem mehrere Penetrationstests, bei dem ein professioneller Hacker versuchte, in die unterschiedlichen Teile der GWAdriga-Systeme einzudringen und die Kontrolle über diese zu erlangen, bzw. Schaden anzurichten.

Solche Penetrationstests werden regelmäßig im laufenden Betrieb wiederholt, weil sich durch Updates der Systeme trotz großer Sorgfalt theoretisch immer wieder Angriffspunkte ergeben können und die Norm dies vorsieht. Auch die von GWAdriga eingesetzten Softwarelösungen BTC | AMM Gateway Manager und BTC | AMM Meter Data Manager sowie der Betrieb in den Rechenzentren der BTC AG mussten nach den Vorgaben der Technischen Richtlinie BSI TR 03109-6 und -4 basierend auf ISO 27001 zertifiziert werden.

### Sichere Datenflüsse müssen garantiert werden

Eine weitere Anforderung ist die BSI-konforme vertrauliche Übertragung der Zertifikate und Daten, die höchsten Anforderungen gerecht werden muss. Vergleichbar ist hier das Sicherheitsniveau der Anbindung der Geldautomaten an die Bankensysteme. Hier hat sich GWAdriga für die Zusammenarbeit mit Worldline, dem europäischen Marktführer für Zahlungsverkehrs- und Transaktionsdienstleistungen, entschieden.

Mithilfe der Worldline-Lösung Energy Security Suite wird die komplette Kommunikation zwischen den Smart Meter-Gateways und der zentralen Applikation lückenlos End-to-End verschlüsselt. Die erforderlichen Zertifikate für die sichere Kommunikation zwischen den Geräten werden von Atos durch die BSI-zertifizierte Atos Smart Grid CA ausgestellt. Worldline und Atos erfüllen dabei nicht nur alle gesetzlichen Vorgaben, das System von Worldline lässt sich darüber hinaus vollständig und nahtlos in die eingesetzten Softwarelösungen BTC | AMM Gateway Manager und BTC | AMM Meter Data Manager integrieren.

Die WL Energy Security Suite beinhaltet alle Funktionen für die Kommunikation mit den Smart Meter-Gateways und liefert dabei die Funktionen der TR3109-4. Sie wird mit dem Worldline Hardware Security Modul (ASM) Crypton CS4 betrieben.

Damit lässt sich eine in sich geschlossene, autarke Sicherheitsumgebung aufbauen, die physikalisch von der Applikationsplattform getrennt werden kann. Das Management der Zertifikate auf den Gateways wird über den PKI Manager abgewickelt (PKI: Public Key Infrastructure). Die Lösung ermöglicht es, die Zertifikate zu prüfen, Zertifikatsanfragen an die Atos Smart Grid CA weiterzuleiten und die verwalteten Zertifikate mit den heruntergeladenen PKI-Sperrlisten abzugleichen.

### Auf die Menge kommt es an

Wie deutlich wird, sind die technischen Anforderungen im Bereich der Gateway-Administration nicht zu unterschätzen. Aber auch die Wirtschaftlichkeit ist ein wichtiger Faktor. Erforderlich ist dazu nicht zuletzt ein entsprechendes Mengengerüst: Ergebnis der Berechnungen, die die Gesellschaftsunternehmen von GWAdriga unabhängig voneinander angestellt haben, war, dass der Gesamtprozess erst ab einem Gesamtvolumen von rund 400.000 auszurollenden iMSys tatsächlich wirtschaftlich umzusetzen ist. Das bezieht sich nicht nur auf die Prozesskosten. Auch aufseiten der Beschaffung der Geräte sind sie Skaleneffekte enorm. Schon aus diesem Grund ist es absolut sinnvoll, über die Auslagerung der Gateway-Administration nachzudenken.

*Dr. M. Sobótka, Geschäftsführer und L. Weber, Leiter Operations GWAdriga GmbH & Co. KG, Berlin*  
[m.sobotka@gwadriga.de](mailto:m.sobotka@gwadriga.de)