

REMOTE METER READING OF RESIDENTIAL CUSTOMERS, QUALITY ASSURANCE OF THE METERING DATA

Henrik Weldingh
DEFU – Denmark
HW@danskenergi.dk

ABSTRACT

An expected large-scale introduction of remote reading of domestic electricity meters in Denmark has prompted the development of rules and procedures for keeping a suitable and documented quality of the measurement data. This work also addresses the potential threat against the IT security which a multi-terminal system like the AMR system represents. The article describes the basis and contents of the work, which is expected to be finished during 2007.

INTRODUCTION

AMR or AMM, i.e. remote metering of residential customers attracts a growing interest these years both from the political side, from the energy authorities and from the utilities, even if only little interest is being shown from the user-side.

A number of positive arguments are forwarded, often with a basis in considerations for energy conservation through end-use efficiency or for the establishment of an end-user market for electricity.

It could also be mentioned that the EU directive on energy efficiency and services [Ref 1] in its Article 13 states, that the member states shall ensure, that the final customers are provided with "...individual meters that accurately reflect the final customer's actual energy consumption and provide information on actual time of use." This is in some countries interpreted as a requirement for remote reading of domestic meters.

In Denmark, as indeed in many other countries, no political decisions have been made which demand remote reading of domestic customers, even though the authorities show much interest in the subject.

According to the Danish rules, measurements of the electrical energy are the DNO's responsibility.

A number of DNO's have on their own decided to invest in remote reading of all customers. Multiple promising and interesting possibilities are opened with the establishment of remote reading but the main argument is beyond any doubt the gain in operational efficiency.

In economical analysis of AMR systems, costs and benefits tend to be almost equal and the result sensitive to capitalisation factors which can only be judged with much uncertainty. Nevertheless it can be observed, that by the end of 2006, 15 % of all domestic meters in Denmark are in the process of being replaced by remote read meters and a fair guess indicates, that 50 % will be reached within the next few years.

Remote reading of meters is of course by no means a new operation to the Danish DNO's. Large customers have been remotely read for years, and the market rules demand all hourly billed meters with a yearly consumption in excess of 100 kWh to be read remotely. The reading of these meters is traditionally done by a very simple system with limited information transfer capability. The number of such meters is limited, typically few percent of the total meter population for a DNO.

When it comes to remote reading of domestic customers however, then alone the number of meters to be installed and operated represents its own set of problems.

In order to realize the stipulated efficiency benefits, it is essential that the received metering data have a documented high quality. This can not be regarded as automatically achieved, even if the number of faults in the installation phase is kept to a minimum: Remote meter reading implies the transmission of data over a public network i.e. an open network with free access for everyone and thus with possibility for corruption of the information. It can also not be automatically assumed, that the customer will accept the remote readings. Even though it is possible to solve a disagreement of a reading by direct reading of the meter, then any efficiency gain will be ruined if that happens too often.

Thus the system must be designed and operated in such a way that the quality of the measurements is sufficient and documented.

The Danish DNO's, in close cooperation with the System Operator Energinet.dk, have initiated the development of a sensible set of rules to achieve this. During this work two other important issues became evident:

The establishment of remote reading implies that each customer on his premises has a terminal installed, i.e. the meter with a direct connection to the IT system of the meter operator and to other meters. This represents a threat which must be addressed even if only an extremely small part of the users will attempt to misuse the system.

The system for remote reading, which must be rolled out in a limited span of time, implies that all existing meters are replaced by new ones. This gives a meter population with an extremely narrow age-distribution. This is different to what is normal practice, at least in Denmark, and must be reflected in the maintenance and replacement plans.

QUALITY ASSURANCE OF METERING DATA

Meter readings are legal data i.e. data on which money

transactions are based and must thus be treated at a suitable level of security. In the development of the Danish set of rules, the work by WELMEC, the European Cooperation in Legal Metrology, is used as basis:

WELMEC guide 7.2 on software [Ref 3] contains in its extension T a set of rules for transmission of legal data via communication networks.

The guide, which is developed for utility instruments, operates with several risk classes, A to F, where electricity meters belong to class C.

The guide also distinguishes between open and closed networks. The networks used for remote reading of meters are exclusively of the open type, characterised by the fact that arbitrary participants and devices with arbitrary functions can connect to the network. The identity and functionality of a participating device and its location may be unknown to other participants.

The Guide formulates 8 rules, from T1 to T 8:

T1: Completeness of transmitted data

The transmitted data must contain all relevant information necessary to present or further process the measurement result in the receiving unit.

T2: Protection against accidental or unintentional changes

Transmitted data shall be protected against accidental and unintentional changes.

T3: Integrity of data

The legally relevant transmitted data must be protected against intentional changes with software tools.

T4: Authenticity of transmitted data

For the receiving program of transmitted relevant data, it shall be possible to verify the authenticity and the assignment of measurement values to a certain measurement.

T5: Confidentiality of keys

Keys and accompanying data must be treated as legally relevant data and must be kept secret and be protected against compromise by software tools.

T6: Handling of corrupted data

Data that are detected as having been corrupted must not be used.

T7: Transmission delay

The measurement must not be inadmissibly influenced by a transmission delay.

T8: Availability of transmission services

If network services become unavailable, no measurement data must get lost.

Each rule contains examples of acceptable solutions, requirements for control and guidance for validation of the chosen solution.

These documentation and validation rules are used in the Danish work as basis for the requirement. The choice between the different acceptable solutions is free for the contractor of the system.

Definition of the data set

In order to be complete, the data set from each metering point must contain the following:

- Energy from the verified register of the meter
- Measurement unit for the energy. (kWh if nothing else is specified)
- Factors like transformer ratios etc.
- Real time for the measurement. Must be specified with a suitable accuracy. The tolerance of the time is ± 15 sec.
- Unambiguous identification of the location for the measurement; both a meter (terminal) id and a customer id may be relevant.

The individual parts comprising the dataset may have different origin. The identification of the customer may for example require the coupling of a terminal id with a meter id and a customer id. The procedures for the establishment of the metering point, change of meters etc. are extremely important for the quality assurance of this point.

Solutions and validations

The guide gives examples of acceptable solutions.

Protection against unintentional and intentional changes could be based upon checksums over data, like for example the CRC-16 algorithm.

In order to secure the integrity of the data, the initial vector of the CRC-register and the generator polynomial must be known only to the programs generating and verifying the checksums and must be treated with the same secrecy as keys.

In the validation of such a measure, it must be checked that the secret data are kept secret against spying with simple SW tools.

The checksum calculation demands some data handling power, which not always may be available at the meter; the domestic meter really being a price-optimised product. Other solutions are however also acceptable.

To secure the authenticity of the data set, for example to prevent the use of accessing the network with a "false" meter, the origin of each measurement data set must be identified without ambiguity. Acceptable solutions could be based on a unique (current) identification number allocated to each data set or on another form of unambiguous signature.

Another possibility, more difficult to handle and validate, is to check all data in the received data set for plausibility.

A certain and important question is to keep the keys and accompanying data secret and protected against compromise by software tools. Again, the moderate

level of risk taken into account, only protection against simple software tools is devised.

Finally, extension T contains some considerations for transmission delays and availability of transmission services.

These are normally not of great concern for integrating measurements like measurement of electrical energy, especially not if the data set contains a time stamp.

DATA SECURITY

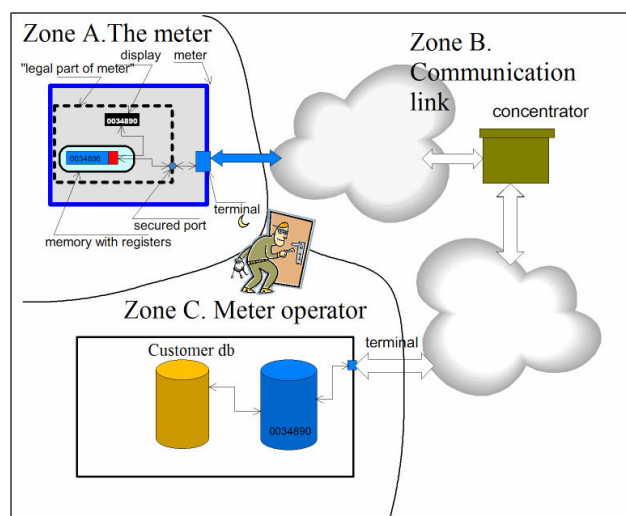


Figure 1 Data transfer from meter to meter operator

The provisions mentioned in the preceding section will secure that the data set is transmitted correctly from the meter to the meter operator, that the meter which transmits the signal is the “legal” meter from the specific metering point, and that the signal, on its way from the meter to the meter operator is not intercepted or corrupted.

It will not secure that the signal can be kept confident. More threatening is, however, the fact that each meter (terminal) represents a direct channel into the IT system of the meter operator, to any part of the data transmission system, to other meters and to the meter itself.

The system for remote reading of domestic meters can be regarded as especially critical in this respect for mainly two reasons:

1. The thousands of remote terminals (i.e. the meters) which are located with easy access and without any supervision in private dwellings.
2. The fact that this situation will remain for many years.

One can argue, that it is difficult to see any rational reason for misuse or attack on the system, except perhaps for corrupting own meter reading. But experience shows, that if such possibility exists, attacks will come eventually.

Even though the acceptable level of security is much lower than that of for example a home banking system, it is necessary to consider the security risks and establish suitable countermeasures.

The literature has lots of recommendations of how to establish data security. In the Danish work, it was decided to use ISO/IEC 17799, Code of practice for information security management [ref 2].

The AMR system can be divided into three zones, as shown in figure 1. Zone B depends of the chosen system, which for example could be based on GSM links directly from the individual meters to the meter operator or on PLC communication from the meters to concentrators in the 10/04 kV secondary substations and GSM links from here to the meter operator, as illustrated in Fig. 1.

The system is broken down into its individual components, as shown in Table 1, where they are linked to the relevant section and paragraph in ISO/IEC 17799. For this process see [Ref 4]

		Section in ISO/IEC 17799
Hardware	Physical Connection	9.2.1, 11.3.2, 11.4.4
	Communication media	9.2.3
Software	General	10.4.1, 10.10, 11.1, 11.2, 11.3.1, 11.3.2
	OS	11.5
	Application	11.6
	Networkservices	10.6.2, 11.4.1, 11.4.2, 11.4.2
Information (data)	General	10.10, 11.1, 11.2, 11.6
	Storage	10.7
Communication		10.6.1, 10.8.1, 10.8.4, 11.4.6, 11.4.7

Table 1

As can be seen, the relevant parts of the standard are the following four sections:
 Section 9, Physical and environmental security
 Section 10, Communications and operations management
 Paragraph 10, Monitoring
 Section 11, Access control

When going into the details it appears that many of the recommendations of the standard in zone C i.e. at the meter operator can be considered fulfilled by the normal IT security of a utility.

A number of security recommendations in Zone A will in the same way automatically be fulfilled, if the requirements in chapter 4 are fulfilled and the meter for example is in accordance with EU’s metering directive.

The establishment and operation of the remote meter reading system raises however some new security aspects:

The communication network has its own security problems. If operated by a “professional” company like the normal telecom operator, security problems are automatically dealt with, but the operator must of course be informed of the

character of the (data) communication in connection with the transfer of metering data. If the meter operator establishes his own communication network e.g. PLC connections to data concentrators in the secondary substations, then both the PLC communication and the concentrators represent special security problems, which must be addressed accordingly.

The communication link to and from the meter represents a new entrance to the IT network of the meter operator, which must be properly protected by firewalls etc. like the normal external links, the internet.

The operation of the meters may call for the establishment of a new hierarchy of access controls: The meter manufacturer, the verification laboratory, the meter operator, the DNO installing the meter etc.

ISO/IEC 17799 addresses this problem and stresses the importance of a tightening of the security procedures and management for all parts involved in the establishment or operation of the metering system.

Monitoring of the system for detection of unauthorized information processing activities is recommended. All information security events should be recorded. Operator logs and fault logging should be used to ensure that information system problems are identified.

This applies not only to zone C, but if possible, also to zone A, for example by an event logger in the meter, which records all changes and which cannot be reset.

RELIABILITY AND DURABILITY OF THE METER

One of the consequences of the establishment of AMR is the replacement of all meters with new ones. The reliability and durability of the (new) meters are of course extremely interesting in this respect. Information of the operational performance of electronic meters are collected systematically in many countries as in Denmark [Ref 5], but one must bear in mind that an AMR system comprises not only the meter, but also the communication terminal, the reliability and durability of which is not known.

The establishment of an AMR system has in itself the possibility for a better supervision of the meter population, through the direct access to each meter.

This can be utilized in the quality assurance system for the meters, where the existing system based on fixed time in operation can be replaced with dependability management systems, where a given availability of the meter is the quality factor. [Ref 5]

CONCLUSION

The establishment of remote reading of domestic customers represents a major investment in new technique for the DNO's but has the perspective of considerable operational and other benefits. To realize the efficiency benefits, however, it is essential that the received metering data have a documented high quality. This can not be regarded as automatically achieved

As the establishment of AMR involves a very large number of new installations, it is absolutely important, that the procedures for the establishment are sound and that they contain some form of control of especially the user i.d.

Remote meter reading implies that data are transmitted over a public network. This means "free" access for everyone and with a possibility for spying or corruption of the information. And further, this opens the access to the IT system of the meter operator.

It is important to establish rules and procedures for the metering system to secure and document the quality of the received legal data. In the establishment of these, it is of vital importance that the rules not in any way imply such procedures that the operational gain by the establishment of remote reading is threatened.

Danish DNO's in cooperation with the System Operator are in the process of establishing a set of rules, which aim to fulfil these demands, based on a combination of WELMEC recommendations and ISO/IEC standards.

The system is planned to be in force during 2007.

REFERENCES

- [1] DIRECTIVE 2006/32/EC of the European Parliament and of the Council of 5 April 2006 on Energy end-use Efficiency-.
- [2] ISO/IEC 17799 Information Technology – Security techniques – Code of practice for information security management. Second edition 2005-06-15
- [3] WELMEC 7.2 Issue 1. Software Guide (Measurement Instrument Directive 2004/22EC), May 2005.
- [4] Lars Nordström. Assessment of Information Security Levels in AMR Infrastructures. *Energy Forum Conference "Automatic Meter Reading in Utilities. Stockholm, September 27-28, 2006*
- [5] Henrik Weldingh. Reliability and Dependability Management for Domestic Electricity Meters *CIRED 18th International Conference on Electricity Distribution. Turin 2005.*