DLMS Direct Connect Whitepaper

Innovative, secure and interoperable functionality for Power Line Carrier based infrastructures

elster

1 Introduction

Power Line Carrier (PLC) based systems are proving an attractive and cost-effective solution for Smart Metering deployments in the residential domain. In Europe, PLC solutions have already been implemented widely in some countries, while others are at an advanced stage of planning for large-scale roll-out. The installed base in Spain (based on PRIME Alliance technologies) numbers in the millions, and ENEL, a utility in Italy, says that it has reached full roll-out coverage. France is currently preparing for a residential Smart Meter deployment using a Linky system with either G1 or G3 that will also rely heavily on PLC infrastructure. Furthermore, a group of manufacturers now offers an interoperable PLC solution based on IDIS PLC standards. The latter is successfully meeting the requirements of utilities in emerging markets such as the MENA region. IDIS standards also employ a unified data model, meaning it supports several types of physical transmission media, making it attractive for utilities operating in markets where there is no single dominant player.

While typical approaches to PLC-based Smart Meter Systems are identical, there are differences in the underlying technology employed in each market – namely in respect of the physical modulation of and access to the carrier signal itself. For example, G3 in France and PRIME in Spain are both based on Orthogonal Frequency Division Multiplexing (OFDM), while G1 and IDIS technology rely on Spread Frequency Shift Keying (S-FSK). Both allow the transmission of information over a power line. However, the signal modulation and available bandwidth are different. The co-existence of these technologies on a single carrier is problematic due to interference. Thus, it is advisable that only a single system be deployed in any given area.

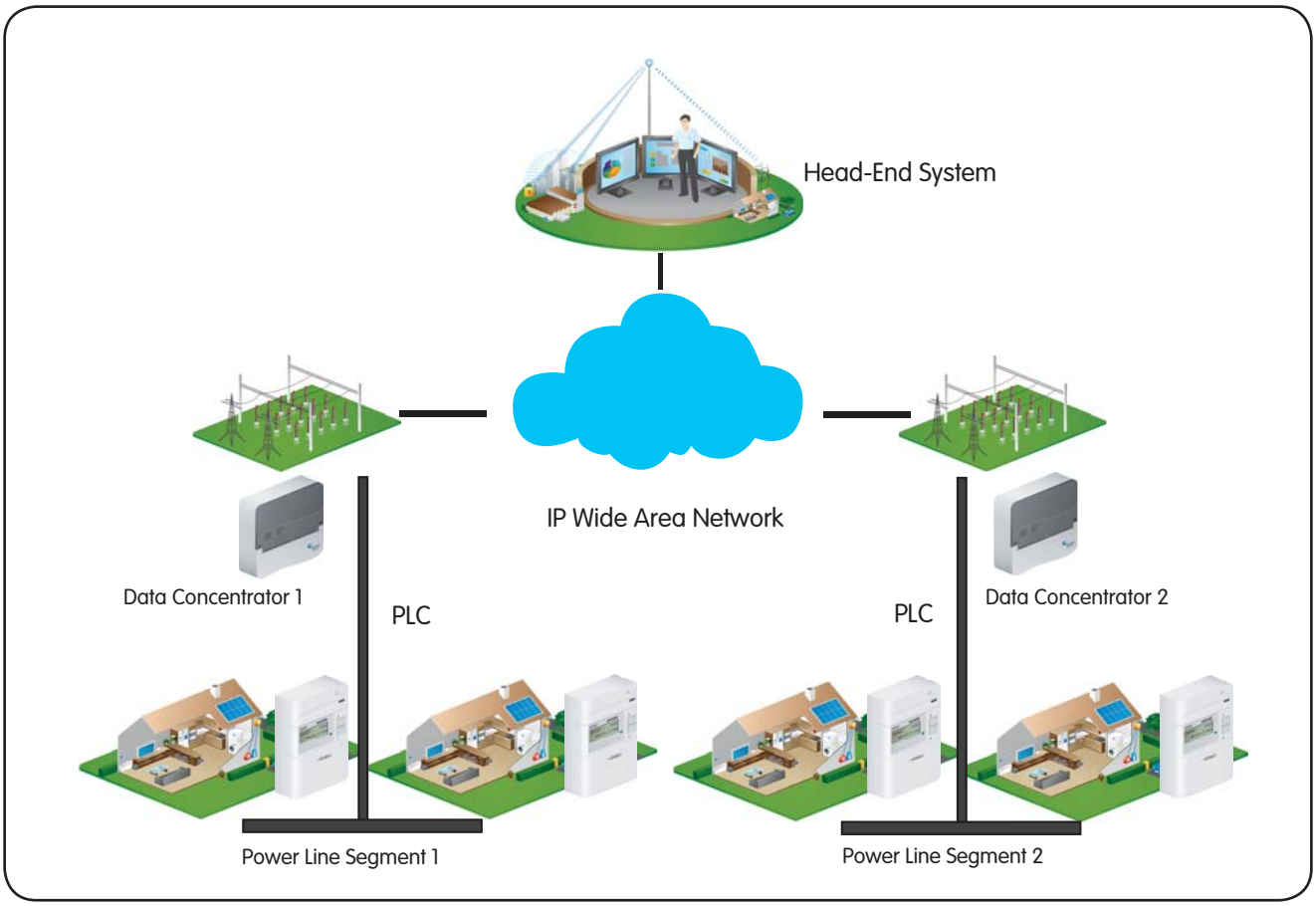


Figure 1: General building blocks of a PLC-based Smart Metering System

Figure 1 outlines the general building blocks of a PLC-based Smart Metering System. Data is collected from the metering end-point and is transported over the power line to an intermediate node, the Data Concentrator (DC), which is typically located either at or close to a sub-station on the grid. From here, various communication media are available to transport the information towards the Head-End System – for example, GPRS (wireless) or Ethernet.

The options for the Application Layer protocol – i.e. the protocol that provides the interface for the processes required by the use case – are diverse. A popular choice thus far has been to use the DLMS/COSEM protocol between meters and Data Concentrators. DLMS/COSEM is an international standard covering data exchange for meter reading, tariff and load control. Proprietary protocol implementations are no longer common for meter to Data Concentrator communication, but there is no well-defined standard for the Wide Area Network (WAN) connection, which is the connection between the Data Concentrator and Head-End System.

Unlike in deployments where a reading is taken directly from the metering end-point using a direct GPRS connection, in a PLC domain a Data Concentrator is always present and requires managing as an additional component in the network. Besides performing the routine task of collecting data from metering end-points, security management can be a requirement either because additional credentials are needed to manage the device, or to allow the Data Concentrator to access the meters securely. Moreover, in terms of network resilience, a Data Concentrator can represent a single point of failure, or impede scalability in instances where a single Data Concentrator is the only node routing information between metering end-points and the Head-End System.

In this paper, Elster elaborates on the different elements that require attention within a PLC-based Smart Metering infrastructure, and presents the DLMS Direct Connect concept as a technology enhancement to conventional Data Concentrators that will resolve several of the key challenges posed by current Smart Metering architectures.

2 Overview of Concepts

2.1 Data Concentrator

The main task of Data Concentrators is to collect information (readings, events, alarms) from metering devices, process the obtained data and, in a subsequent communication, transmit the acquired data to the Head-End System.

Figure 2 outlines the detailed architecture and building blocks of a conventional PLC system using Data Concentrators. The communication link between Data Concentrator and Head-End System is provided by a Wide Area Network (WAN), which is IP-based. The link between the Data Concentrator and the meters uses PLC technology. On top of the PLC communication, the DLMS protocol is most commonly used at the Application Layer. In DLMS terminology, the meter is the 'DLMS server', and the Data Concentrator represents the 'DLMS client'.

Data Concentrators perform the routine tasks of a Smart Metering System. They can query all meters autonomously for readings, events and alarms. This is possible even without a persistent connection to the Head-End, as some Data Concentrators might not have 'always-on' WAN connectivity – for example, if a dial-up solution has been implemented for cost reasons. A Data Concentrator can also pre-process the information acquired from the meters and compress the data prior to transmitting it to the Head-End in order to minimize the overhead in terms of bandwidth and computational effort.

The PLC segment of the network represents a shared medium, generally allowing only one network component to transmit data at a time while enabling multiple parties to receive the signal. This characteristic is essential in scenarios where large sections of the same data stream have to be transmitted to all nodes, or to a larger group of nodes. For example, this capability is necessary when performing firmware updates, with the new firmware image being broadcast to all Smart Metering end-points simultaneously.

Some markets require that the Data Concentrator is supplied with embedded integrated metering functionality, such as the ability to measure the 3-phase current and issue an alert in case of failure, default, and deviation, versus nominal voltage.

However, all of these different possibilities suggest that the DLMS would also be best employed as an Application Layer protocol for the WAN connection. In the past, utilities have directly specified WAN protocols in accordance with their own demands, which has impeded any attempts at standardization in the WAN and thus the associated benefits of standardization have not been realized.

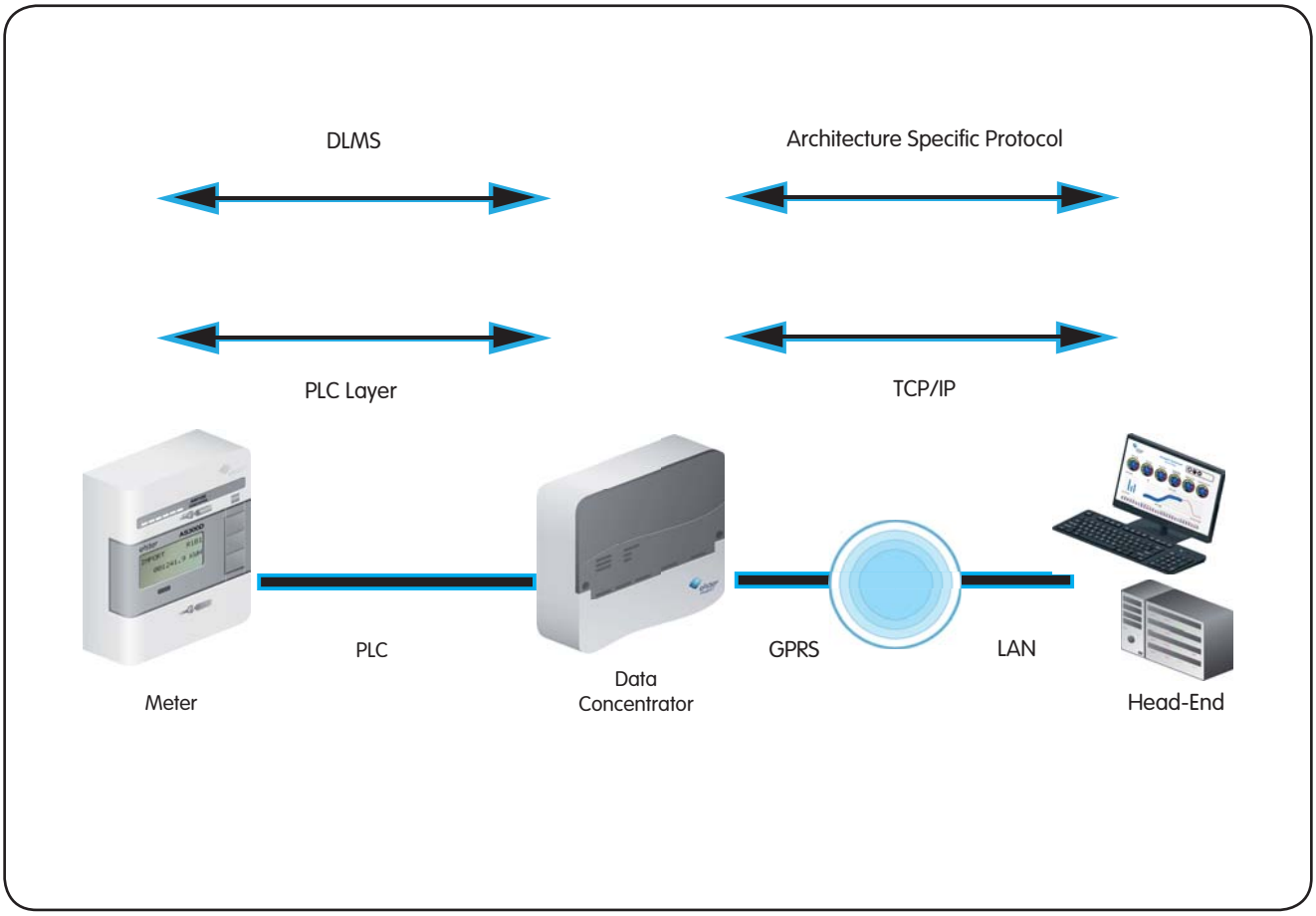


Figure 2: Detailed architecture and building blocks of a conventional PLC-system

Nevertheless, there has recently been a more coordinated effort to define a standard WAN protocol to address the needs of the market rather than the requirement of a single utility. This has been led by the PRIME Alliance and the IDIS association. However, more work is required, leaving the question of a standardized WAN protocol unaddressed.

Due to the nature of PLC architectures, a Data Concentrator also needs to manage maintenance of the metering end-points. This could include administering changes such as tariff updates on the Smart Meters, or any security-related tasks, with key updates or changes to access rights being of particular concern. Moreover, the role of a Data Concentrator needs to be considered for any operations affecting end-to-end security, such as a remote disconnect.

Currently, there is no Data Concentrator model that includes a solution addressing all of these requirements. This is where the implementation of the 'DLMS Direct Connect' concept can make a significant contribution.

2.2 The DLMS Direct Connect Enhancement

Figure 3 outlines the modifications applied by DLMS Direct Connect approach. It extends the Application Layer protocol from the meter at one end, across the Data Concentrator, and all the way to the Head-End System. In other words, it enables for direct, end-to-end DLMS communication between the Head-End and metering end-points.

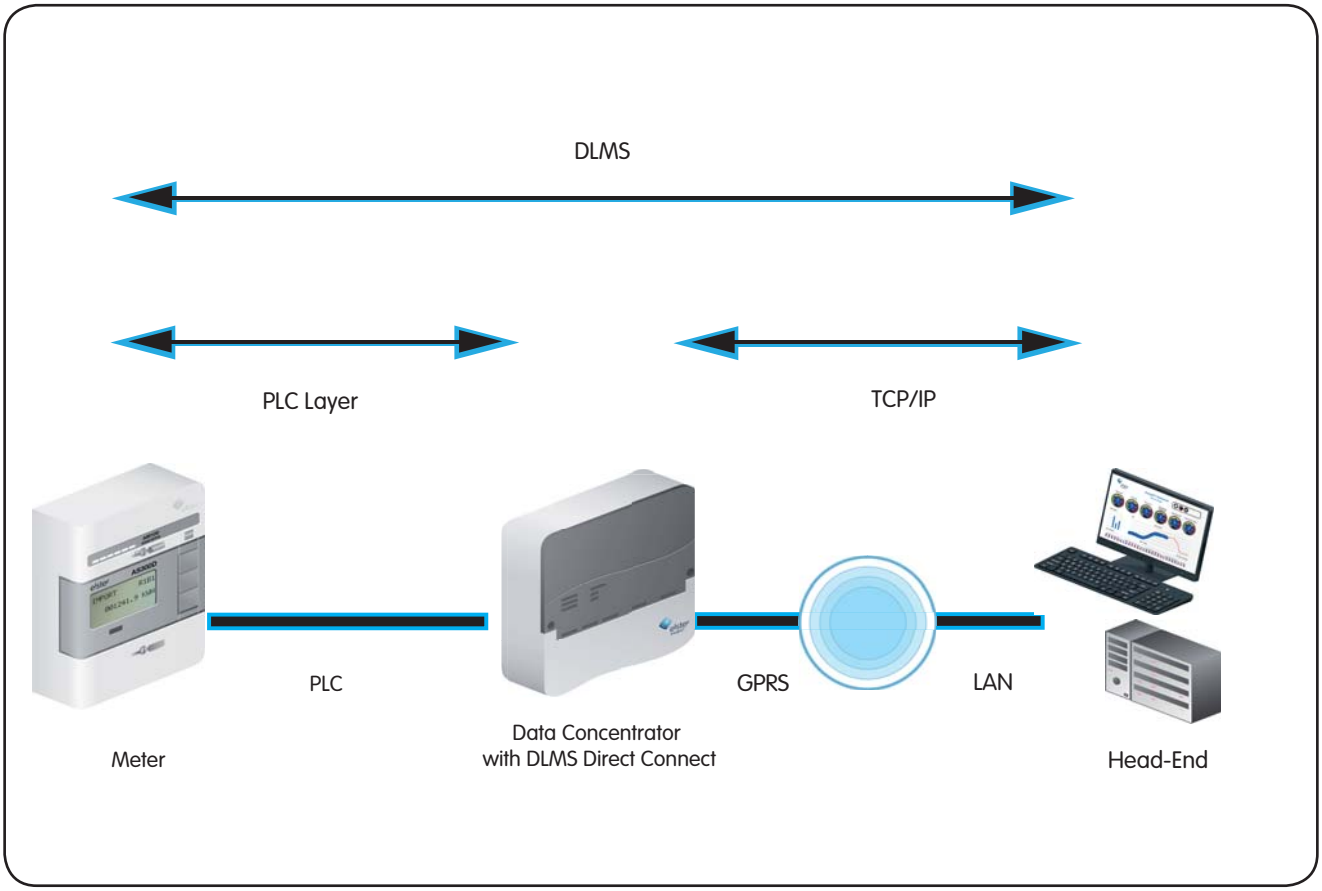


Figure 3: DLMS Direct Connect concept modifies the Data Concentrator to allow for a transparent connection directly between the Head-End and the meters

Using this model, the meter remains as the DLMS server, but the Head-End now assumes the role of the DLMS client, meaning that the Data Concentrator becomes an intermediate node. As such, the device need only route metering information between the client and the server, significantly reducing the complexity of operations performed at the Data Concentrator.

This functionality allows utilities to address the requirements of their specific use case more efficiently. Crucially, it means that both modes of operation – i.e. conventional Data Concentrator and a DLMS Direct Connect functionality – can in principle co-exist in one device. This makes for a more flexible implementation in respect of the potential use cases, which are explored in more detail in the following chapter.

3 Key Use Cases for the DLMS Direct Connect Approach

The following chapter outlines the key use cases for implementing DLMS Direct Connect functionality.

3.1 Configuration Management

In a PLC-based system, as with any other networked system, the configuration of all devices has to be maintained. However, keeping track of meter settings would go beyond the day-to-day routine of Data Concentrators simply acquiring information from the metering points.

One specific requirement is the propagation of a new tariff structure to the devices. In this case, the tariff update command has to be compiled by the Head-End and distributed to the Data Concentrators using the WAN protocol. The Data Concentrator is then required to transform the received command into individual DLMS commands that would update the tariff structure on the metering end points and finally, forward the instructions to the individual meters themselves.

It should be noted that any changes either to the DLMS command structure or to the WAN protocol would require a change to the Data Concentrator functionality, which is in most cases equivalent to performing a firmware update.

Often, settings need to be configured individually at each device. This is the case when maintaining system security properties such as updating keys or generating new certificates, changing access rights or authorization levels. To perform any of these tasks, established security keys are required. This means that the Data Concentrator must hold all of the necessary credentials for the meters to be able to carry out the given task.

With the DLMS Direct Connect concept, only the Head-End System needs to hold the credentials that would authorize the configuration. In this scenario, the Head-End is able to set the individual configurations directly at the meter level using DLMS commands. No translation between the Head-End, the Data Concentrator, and the meter is required, and no credentials such as DLMS security keys need to be held at the Data Concentrator.

This reduces the complexity of the network significantly, since the DLMS Direct Connect provides an easy way to administer the network. Furthermore, the management of security keys for an entire meter population is simplified because they are stored at a central server point (i.e. in the Head-End). This allows utilities to benefit from more robust protection on the network, easier maintenance and efficient management of the security credentials.

3.2 End-to-End Security

Establishing true end-to-end security is an important design objective for state-of-the-art Smart Metering architectures and is considered an important building block to achieve security by design. Furthermore, this is a legal requirement in several European Member States. In the UK for example, the Department of Energy and Climate Change (DECC) will mandate an end-to-end security architecture. This requires that all critical commands are protected when in transit between the utility's central system and the meters on the wall. A similar decision was taken in Germany with the "BSI Gateway" that will only allow for a TLS protected channel between the Head-End System and the in-home gateway. Utilities in the Netherlands have also been investigating the end-to-end security model for some time. The DLMS Direct Connection provides a neat solution for addressing end-to-end security requirements.

One of the highest priorities (and highly-debated use cases due to security concerns) for strong end-to-end protection is the Remote Disconnect functionality of Smart Metering architectures. If the architecture design is not robust, an attacker could potentially manipulate a data concentrator to trigger the disconnection of electricity supply. A large-scale disconnect across multiple households would not only cause inconvenience to the residents in those locations, but may also lead to issues with the grid itself – such as a power outage – or even threaten the stability of the grid.

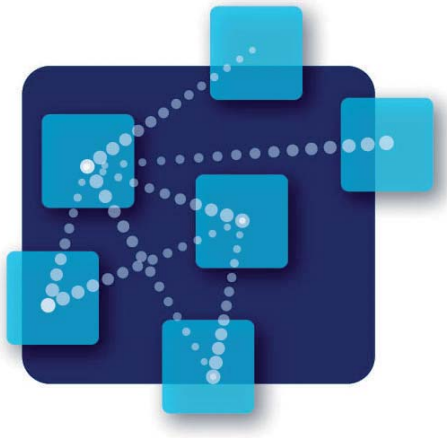
In markets where end-to-end security is mandated, a conventional Data Concentrator model cannot be implemented without additional safeguards. Discussions on this topic have taken place, but to little avail. Options include the addition of a dedicated hardware component (Secure Element) to the Data Concentrator to allow for the secure storage of keys, as well as the introduction of digital signatures.

One of the main arguments for employing DLMS Direct Connect functionality is to establish an end-to-end security relationship between the Head-End and the meter. As such, this approach not only reduces complexity, but enhances overall security of the system. Critical commands can be protected end-to-end, from the Head-End to the meters using DLMS security functionality.

3.3 Firmware Updates

Remote firmware updates are an important requirement for Smart Metering Systems, as this capability allows utilities to introduce new functionality to network devices or resolve any issues discovered following commissioning of the system (i.e. 'bug fixing'). What's more, the ability to carry out remote firmware updates is critical to maintain system security (security updates) in light of ever-evolving security threats.

Firmware updates are often administered using an individual activation command. While a firmware image could be distributed in the conventional manner using a Data Concentrator, or even broadcasted to individual nodes to minimize bandwidth consumption, the activation of the firmware image should be triggered with a command protected end-to-end. Here also, DLMS Direct Connect functionality would allow for this in an efficient and secure manner.



4 Business Benefits of the DLMS Direct Connect Approach

Establishing the business case for a Smart Meter deployment represents a challenging task that requires multiple factors to be considered.

Under the terms of the Third Energy Package, EU Member States must perform a cost-benefit analysis as a foundation for conducting a consistent, credible and transparent economic assessment of the long-term costs and benefits of the roll-out of Smart Metering.

More cost efficient and effective solutions such as DLMS Direct Connect functionality will be important for utilities looking to demonstrate clear benefits such as a lower overall cost of the architecture.

DLMS Direct Connect functionality would allow utilities to significantly reduce the costs associated with system design, deployment and maintenance, due to the following key characteristics.

4.1 Interoperability

Aside from achieving interoperability, standardising communication protocols provides a huge benefit in terms of reduced costs. Establishing a standard, introduces economies of scale and allows utilities to source from multiple vendors. They benefit from greater choice, sustainability of supply, and a reduction in overall implementation and operational risks. In addition, these standards help to improve products and services over time, as multiple companies accumulate knowledge and feed their commercial experience back into further developing or refining the standard. Ultimately, having standards, increases the chance of long-term success.

In current Smart Metering architectures, the Data Concentrator is located between the Head-End System and the meters, and therefore employs two different interfaces that must be defined correctly: an interface towards the WAN; and one towards the PLC domain. While the lower layers of the OSI model are defined for both – an IP link for the WAN interface; and the respective PHY/MAC protocol for the PLC domain – the higher layers are less well defined.

The DLMS Direct Connect model addresses the need for suitable standards for the Wide Area Network (WAN) and the PLC domain by extending DLMS from the meters into the WAN domain towards the Head-End System. As such, DLMS provides an international standard for meter communication, eliminating the need for network operators to maintain proprietary protocols on their own.

4.2 Advanced Security

It has been suggested that Smart Meters using PLC to operate over the electrical network pose a greater threat if compromised, since end-user premises could be disconnected from the grid should an attacker compromise the network. In addition, there are risks relating to data privacy, and the disclosure of an end-user's energy consumption patterns to unauthorized third parties.

This is why it is important to recognize that the Data Concentrators in current Smart Metering architectures are managing all the security credentials necessary to communicate with each individual meter. Given that a Data Concentrator is typically installed near the distribution transformer, either on a pole or in the substation, neither of which can be considered a secure location, a compromised Data Concentrator would enable an attacker to disconnect the network domain.

Defending against these threats with a conventional Data Concentrator model would require a significant investment in security architecture.

Relying on a DLMS Direct Connect however, ensures end-to-end security and can reduce the required security investment. Without any credentials present at the Data Concentrator, security critical operations can be performed via the DLMS Direct Connect, eliminating the need for additional physical protection at the Data Concentrator. This also removes the cost of integrating a Secure Element.

4.3 Scalability & Resilience

The DLMS Direct Connect approach is proven to be highly scalable, supporting the connection of up to 1,200 network devices. A network based on the DLMS Direct Connect can therefore reduce the amount of intermediate nodes required to manage end devices.

A huge advantage of the DLMS Direct Connect model is the potential to achieve high network resilience, as it enables implementation of a second standby node in the network that could take over the data routing should the primary device fail. Alternatively, both devices could operate simultaneously if necessary. There is no need for complex schemes to support redundant Data Concentrators in the same segment of the network, which further reduces the administrative costs of the infrastructure.

5 The Elster Implementation

Elster has implemented the DLMS Direct Connect on the company's RTU+Server2 hardware platform – a flexible baseline that enables the implementation of different communication technologies.

The RTU+Server2 may be installed at utility substations, with the goal of enabling a distributed processing system for utilities that want to pre-process interval data at the substation level. Acting as a concentrator for an entire neighborhood, this solution allows communication costs to be spread over a huge number of end-points while providing Head-End software functionalities and offering new services.

In Elster's communications portfolio, there are already two variants of the RTU+Server2 supporting the DLMS Direct Connect concept: the G3 Gateway; and the IDIS Gateway. The main difference between these two devices is the communication technology employed at the link layer – i.e. the PLC media (OFDM, or S-FSK).

The implementation of the DLMS Direct Connect specifies a data model for DLMS/COSEM that allows addressing multiple logical devices through one physical DLMS device. In doing so, the RTU+Server2 allows the creation of logical devices for every DLMS meter that is connected via PLC.

In scenarios where every meter is reachable via IP communication, as would typically be the case in a GPRS deployment (meters with built-in GPRS modems), the Head-End System can communicate directly with the meters. However, direct communication may not be possible if the meters are on a dedicated network. In such a configuration, every meter would have its own address specified inside the private meter network (for example by PLC, RS232, or wireless node identifiers), depending on the technologies and protocols employed. Addressing these devices from outside of the private meter network is impossible, because the Head-End System cannot connect directly to them.

As with other Smart Metering devices, a Data Concentrator is connected to the private meter network and has its own internal address within this network. It also has a DLMS server running. The concentrator however, has a secondary network interface that allows it to connect to the WAN. Therefore, it is reachable from the Head-End System too.

The RTU+Server2 is now enabled to pass DLMS packets from the WAN interface to the meter interface (LAN), allowing it to reach every device on the PLC network from the Head-End System. In order to achieve this, every meter gets its own address during the registration process at the RTU+Server2, depending on the technology employed. In most cases, these addresses are only known in the RTU+Server2 itself. In order to communicate from the Head-End System to a device on the private network, the Head-End System requires an addressing format understandable to DLMS.

The RTU+Server2 keeps a list of the devices on the network and maps each device to a unique 'SAP' address. The Head-End System can obtain a list of every SAP address connected to the network from the RTU+Server2, and is then able to iterate over each logical device and set up an association to obtain COSEM data directly from the device.

6 Conclusions

DLMS Direct Connect enhances the conventional Data Concentrator model in PLC networks and resolves key challenges posed by current Smart Metering architectures. This has been demonstrated in several European deployments of the technology, where utilities have successfully realized substantial cost benefits and efficiencies, while meeting mandated requirements in respect of security by design:

- DLMS Direct Connect provides a simple means of enabling direct communication between the Head-End System and metering end-points. Simplicity is assured as DLMS Direct Connect uses the international DLMS standard, meaning no proprietary protocol is required.
- DLMS Direct Connect also simplifies communication, firmware upgrades, and device management, driving down the costs associated with administering and managing the network.
- Standard interfaces for upstream and downstream communication ensure true interoperability, simple management and reduced provisioning, make DLMS Direct Connect a perfect fit for large-scale roll-outs.
- True end-to-end security. With direct communication between the Head-End and all metering end-points, communication can be authenticated and encrypted end-to-end. The management of security keys for an entire meter population is simplified because they are stored at a central server point. As a result, utilities benefit from protection on the network, easier maintenance and efficient management of the security credentials.

Crucially, DLMS Direct Connect functionality is provided as an enhancement to existing Smart Metering implementations, enabling utilities to protect their existing investments while realizing new levels of efficiency and security.

With EU member states required to undertake a cost benefit analysis of Smart Meter roll-outs, DLMS Direct Connect provides a compelling option for those looking to achieve a positive assessment.

.

Elster GmbH, Sterinern Strasse 19-21, Mainz-Kastel, Germany ,www.elster.com