IOT BASED SMART GRID COMMUNICATION FOR METROPOLITAN ELECTRICITY DISTRIBUTION NETWORKS

Author & Presenter: Gerhard Brown (Pr Eng) B Eng Electrical/Electronic Engineering with endorsement in IT, B Sc Information Technology – Principal Professional Officer in the Energy and Climate Change Directorate of the City of Cape Town

1. Introduction

Smart Grid technology has emerged due to a need for electricity grids that can accommodate changes in the ways humans generate, transfer, distribute and use electrical energy with energy efficiency and reduced carbon emissions in mind. To address this need utilities have to shift their focus to consumer participation, renewable electricity generation and storage accommodation, asset optimisation, self-healing grids and resistance to attacks. Conventional grids are developed using a centric approach that consist of relatively few, very high-output, generating plants interconnected by transmission systems supplying many substations, that in turn supply a huge number of distribution points. This approach relies on centralised designs where electricity flows unidirectionally through transmission and distribution lines from power plants to the consumers.

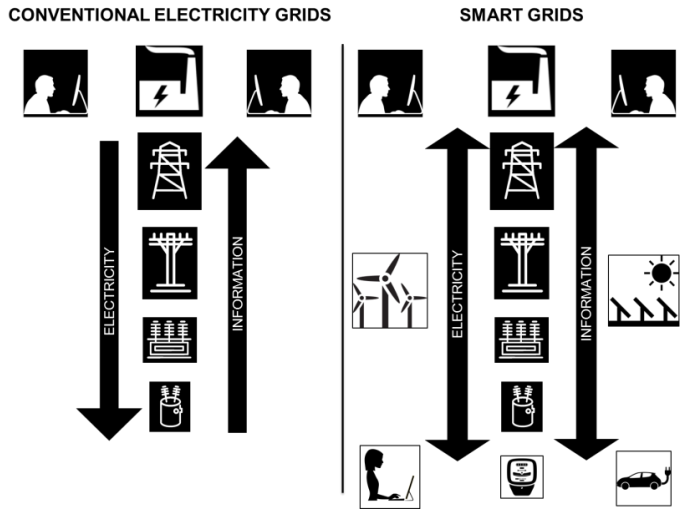

Figure 1: Conventional Electricity Grids and Smart Grids. [1]

Grid data and information is also concentrated in central locations and only partially in substations, while consumer equipment is totally passive. A new approach is needed for reliable, flexible, efficient, economic, and secure electricity provision. This new Smart Grid approach uses more data and widely distributed intelligence embedded in local electricity production. It makes use of two-way electricity and information flows enabling more participation and collaboration for all grid users and therefore depends a complex two-way communication infrastructure, sustaining power flows between intelligent components, sophisticated computing and information technologies as well as advanced business applications. The difference between conventional electricity grids and Smart Grids is illustrated in Figure 1.

Smart Grids create opportunities for utilities to leverage the benefits of new technologies such as smart sensors, renewable energy generation, electricity storage, electric transportation and advanced metering infrastructure (AMI) more effectively. Implementing Smart Grid technologies comes with many challenges however, most of which stem from the fact that Smart Grids can be classified as complex systems in systems engineering terms [2] because they are vast and very dynamic.

Data communication is the cornerstone of any Smart Grid system and as more data generating devices are added to the grid, more opportunities emerge for Smart Grids to use this data in specific applications. These devices can provide data that can be used to determine energy production, grid efficiency, asset condition and consumer behaviour. For applications to have access to this data, it has to flow to various points in a massive communication network that is often just as complex as the grid it supports. Major challenges therefore exist

in design, implementation, operation and maintenance of Smart Grid Information Communication Technology (ITC) networks that have to be addressed by further research.

2. Smart Grids

2.1. Smart Grid Design

In its fundamental form, a Smart Grid design can be presented as a framework consisting of four layers as illustrated in Figure 2. These layers are integrated to work in unison for the Smart Grid to perform optimally.

The energy infrastructure layer represents the grid technology responsible for electricity generation, transmission, distribution and ultimately consumption. It also includes the devices that generate and use grid data to perform specific functions. The communication infrastructure layer is responsible for transferring data in the Smart Grid over networks using ICT, while the Information Technology layer represents the elements that deal with the data structuring, processing and storage. Users utilise grid data and information to perform or automate certain grid functions using various Smart Grid applications, represented by the top layer of this framework.

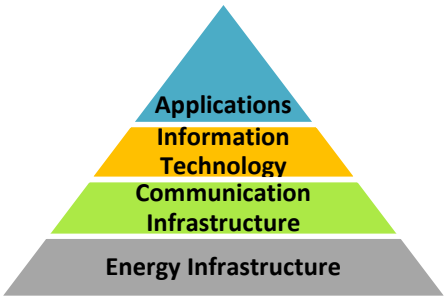

Figure 2: Smart Grid framework adapted from [1], Fig. 1, pg. 29

A more detailed reference architecture for Smart Grids was developed by the CEN-CENELEC-ETSI Smart Grid Coordination Group [3]. Their reference architecture includes the Smart Grid Architecture Model (SGAM) presented as a three dimensional framework with five interoperability layers on the Y-axis, five grid domains on the X-axis and six grid zones on the Z-axis and is shown in Figure 3.

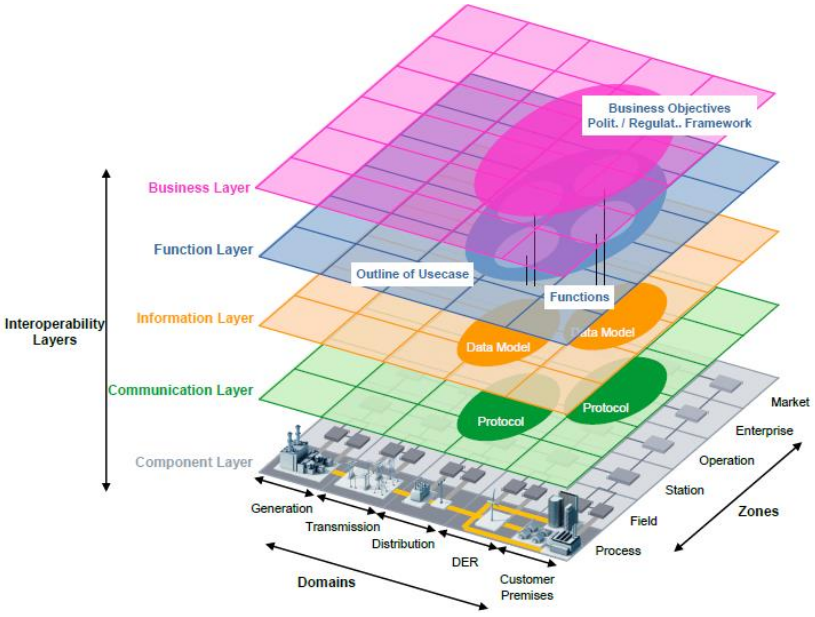

Figure 3: SGAM Framework [3]

This framework builds on the four layer framework by adding a fifth layer called the business layer that considers the objectives of the Smart Grid. As an example one may consider the business objective to monitor the condition of assets in a distribution grid. To meet this objective a Smart Grid design should include the monitoring application users will use, the data models and communication protocols needed to support these applications, as well as the components in various grids zones that will be monitored using collected grid data. Each one of these interoperability layers usually contains a series of complex designs that require regular review and change as the objectives an organisation aims to achieve evolve.

It is for this reason that a Smart Grid should be designed to be as flexible and adaptable as possible. Besides the energy infrastructure, which is usually already established, the data communication systems are the most complex and capital intensive parts of any new Smart Grid development. These communication systems form the crucial links between Smart Grid components and the users that monitor and control them. The communication infrastructure therefore requires the same level of management and oversight as the grid infrastructure itself.

2.2. Smart Grid Communication Networks

Various organisations such as the IEEE, IEC and NIST are working towards standardising communication in Smart Grids. Figure 4 shows a high level model of the IEEE's proposal for end-to-end Smart Grid communications. This model divides the Smart Grid communication network into three sections: a WAN, a distribution section and a customer section.

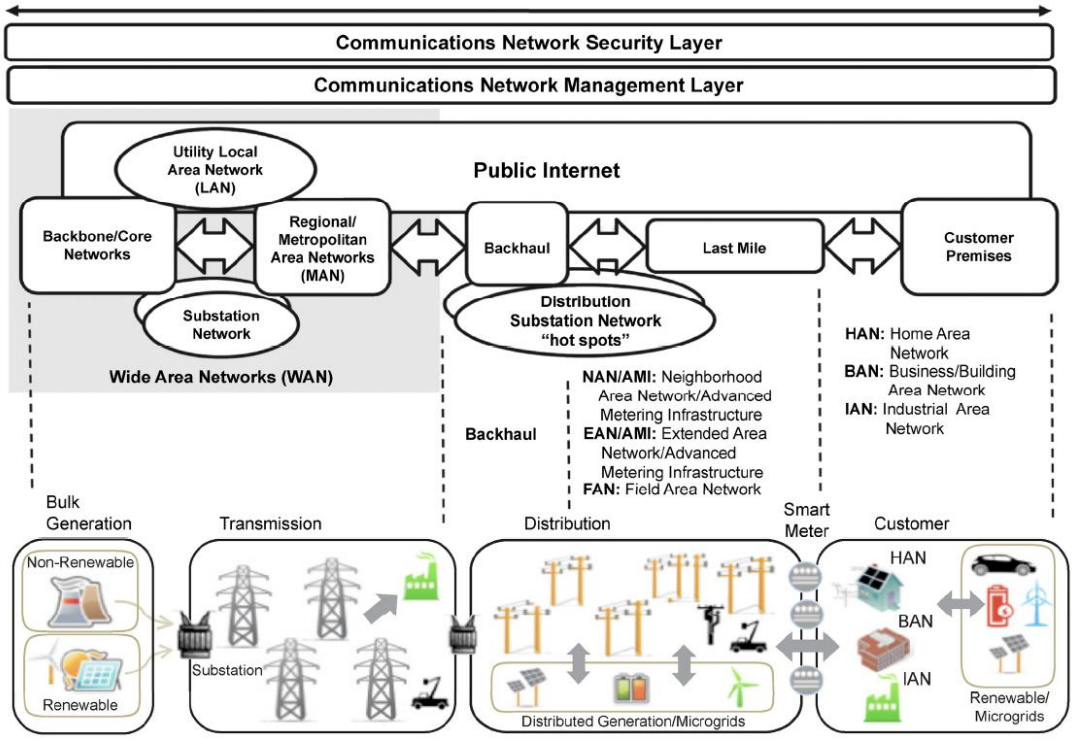

Figure 4: End-to-End Smart Grid Communications Model [4]

Because electricity grids are spread across wide geographical areas they make use of wide area networks (WANs) to connect generating units and transmission networks with distribution networks. The WAN usually consists of a high-bandwidth backbone communication network that handles long-distance data transmission interfacing with various plant networks, substation networks, MANs and a utility's LANs. Electricity distribution networks consisting of NANs, EANs, FANs and AMI networks make use of a backhaul network to interconnect networks in distribution substations, microgrids and distributed generation plants to the Smart Grid communication network while the customer section includes HANs, BANs and IANs for connection of customer appliances, equipment and devices. Smart meters communicate either through the distribution networks or customer networks, depending on a utility's design standards.

The communication network in an electricity distribution grid acts as a bridge between a utility's WAN and its customers' networks and therefore becomes a crucial part of the end-to-end communication network. Consisting of many sub-systems, equipment and components the distribution network is often the largest and most complex part of the utility communication network. Electricity distribution grids vary from location to location as grid designs have to cater for thousands of customer's that are densely clustered in towns and cities as well as those in rural areas with only a few widespread customers. Metropolitan areas often contain the most intricate collection of distribution grid designs that tend to follow a hierarchical network topology with main substations at the top and smaller localised distribution equipment such and mini-substations, ring main units (RMUs) and low voltage distribution panels at the bottom.

Conventional communication networks that support electricity distribution applications such as SCADA and SAS often follow similar hierarchical topologies. Historically, these network designs favoured dedicated wired connections over wireless technology resulting in grid designs where power cables are often installed with accompanying communication cables. Many metropolitan electricity distribution grids therefore have existing

communication infrastructure in place, although some of these installations may be based on dated technology not capable of meeting the requirements for some Smart Grid applications especially those that rely on big data.

Some of the critical areas where these conventional data communication networks fall short are network management and security. In addition to grid operations, data communication needs to be monitored regularly to identify anomalies and to allow network administrators to do fault analysis and correction, performance management, and network provisioning while controlling the quality of service. Administrators also have to set security policies that can prevent unauthorised access, misuse, modification, or denial of a computer network and network-accessible resources. This can include policies for access control, behavioural analytics and installing antivirus and antimalware software. If data is stored remotely, storage management is required to manage storage resources and data structures while device management applications may be required to manage smart devices connected to the gird as well as their interactions. These functions may be straightforward to implement and perform on smaller single application networks, but because of the complex nature of most Smart Grid networks administering these networks can become a mammoth task.

3. The Internet of Things (IoT)

3.1. IoT Frameworks

Rapid advances in telecommunication, IT and manufacturing have led to many new innovative ways that allow computers, tablets, smart phones and other smart sensor devices to communicate, bringing with it different architectures and frameworks for IoT [5]. Similar to the framework for Smart Grids, most of them find unity in the presentation of an architecture that contains three layers as a minimum: An application layer for applications that provide services to users; a network layer representing the interconnection between devices and applications while responsible for all data transfers between these elements; and a device layer representing devices able to generate, store, transfer and process data or execute control actions.

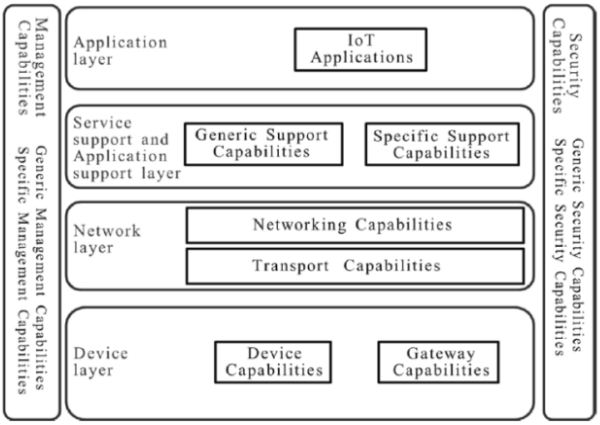

Figure 5: ITU-T IoT Reference Model [6]

Building on this, some standard reference models such as the International Telecommunications Union's (ITU's) IoT reference model shown in Figure 5 adds a service and application support layer as well as multi-layer capabilities for crucial functions such as management and security. Applying this IoT architecture in ICT system designs creates new opportunities to transform physical "things" into equivalent software representations and to automate "actions" using software algorithms. Examples of how these software defined approaches have improved our daily lives can be observed in the abundance of mobile devices and device applications for personal use as well as the emergence of new IoT based home automation, self-driving cars and the creation of virtual environments using augmented or virtual reality.

This virtualisation of the real world has also found new applications in industry, especially in the IT and telecommunication industries. IoT paradigms such as cloud computing have already contributed significantly towards alleviating some of the problems associated with resource allocation, utilisation and management in massive data networks. Cloud computing is however facing new challenges regarding flexibility, dependability and security. The Software Defined Systems (SDSys) paradigm addresses these challenges by adding software components that help to abstract physical hardware from other layers. This abstraction provides opportunity for system administrators to more easily construct and manage their systems through flexible software layers.

A popular example of this abstraction is found in Software Defined Networking (SDN). Conventional networks rely on hardware such as network switches to manage network traffic with pre-programmed control functions configured on the physical device according to network policies. These control functions execute in the switch's control plane, controlling the data flowing through the network switch's data plane. Network switches

have limited visibility of the entire network, impacting the overall network performance. Any changes to the network configuration or network policies that require changes to these control functions require network administrators to manually reconfigure each switch individually. In SDN, control functions run as applications in logically centralised SDN controllers.

These SDN controllers provide the network administrators with a global network view, as well as programmatic interfaces to allow direct control of the network's forwarding devices using SDN applications. This architecture therefore decouples the control plane from the data plane, allowing the switches to become simpler traffic forwarding devices that allow the SDN switches to run on normal computer hardware while the SDN controllers can run on general purpose servers or even as a distributed set of servers using cloud computing principles with more scalability. The difference between conventional networking and SDN is illustrated in Figure 6.

Network Functions Virtualisation (NFV) is another IoT framework that complements SDN as it decouples network functions from hardware so they can run in software on virtual machines (VMs). Because the network functions are virtualised software applications, they can be dynamically created, configured, migrated and replicated, thereby eliminating the need for physical, on-site installations of hardware. Using NFV, network functions such as network address translation (NAT), firewalling, intrusion detection, domain name service (DNS) and caching can be deployed as Virtualised Network Functions (VNFs) on substrate infrastructure that includes the hardware resources (computation, storage and networking). A virtualisation layer, which can be realised by VMs or container virtualisation, provides virtual computation, storage and networking resources.

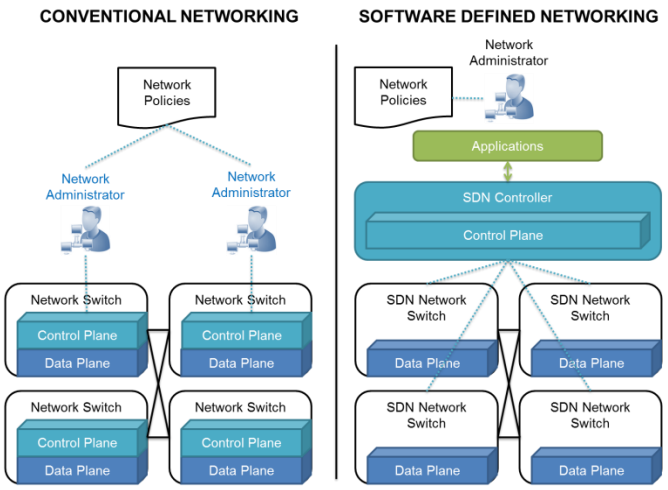

Figure 6: Conventional Networking and SDN [7]

This approach of abstracting network functions using software layers can also be applied to other functions such as storage management (SDStore), security management (SDSec) and device management (SDIoT) to name a few possibilities.

3.2. Machine-to-Machine Communication (M2M)

M2M is a combination of various technologies, including wireless sensor networks (WSN), cyber-physical systems (CPS) and the Internet of Things (IoT), that enable machines such as computers, embedded processors, smart sensors, actuators and mobile devices to communicate with each other with limited intervention by humans, thus automating and optimising the processes these machines support. M2M relies on data communication achieved through standardisation of the communication interfaces that can exist between machines in a network. This is usually implemented by the introduction of a middleware layer in the communication network architecture that supports standardised data models, encoding and serialisation of data for exchange between machines through services. This approach is shown in Figure 7.

Two organisations have made significant contributions to M2M standardisation. ETSI published their first M2M standards in 2011, focussing on horizontal service platforms and related Application Interfaces (APIs) that aim to improve and maintain globally applicable, access independent technical specifications for M2M, with an initial focus on the Service Layer. The global oneM2M organisation also released a series of standard M2M specifications in 2014. The oneM2M standard describes Application Entities that make use of a set of service functions common to the M2M environment that can utilise underlying network capabilities and can interact with each other.

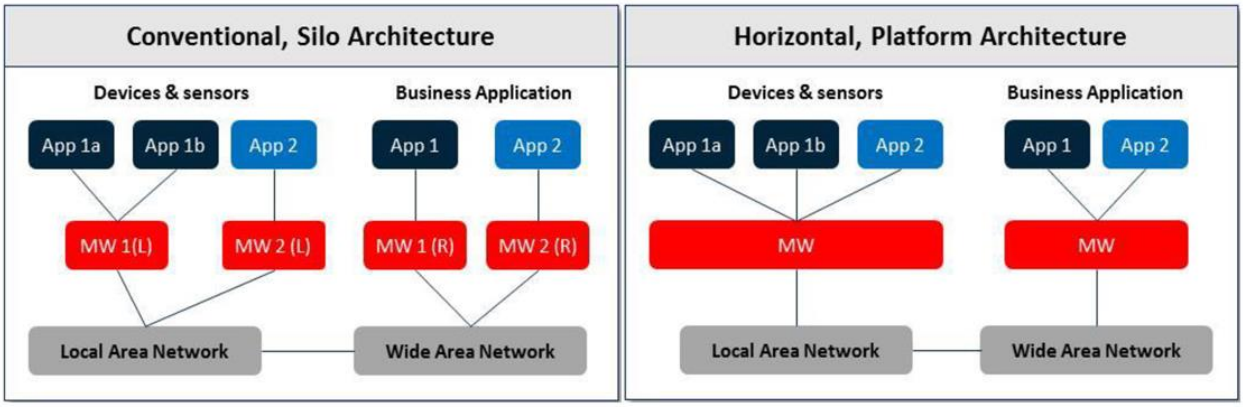

Figure 7: Conventional Silo Architecture vs. Horizontal Platform Architecture used in M2M Communication [8]

An example of a reference implementation of the oneM2M standard available as open source software is OpenMTC. The OpenMTC reference architecture consisting of Internetworking Proxies (IPEs), Gateways and a Backend is shown in Figure 8.

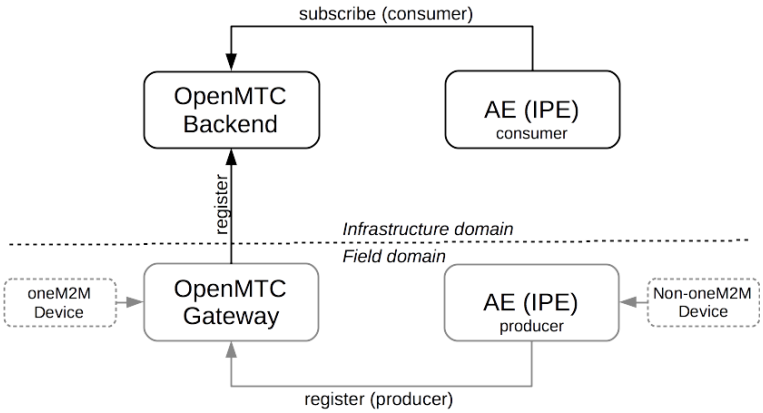

Figure 8: OpenMTC reference architecture [9]

The IPEs are application entities that translate data from one domain to another. An example of an IPE could be an application that reads out sensor values from sensor devices by using a vendor-specific binary interface and translates it to a common standard such as oneM2M.

A Gateway is a M2M software node that is central to a particular field domain, such as a section of a grid in a suburb or industrial area allowing it to collect data from various IPEs. Local applications in this domain can access resources via the Gateway without the need to interact with a central server. It is possible to create a hierarchy of Gateways in a grid network allowing data to travel from one part of a field domain to another.

A central Backend server acts as the M2M root node within a hierarchy of Gateways and is the main software node within the infrastructure domain. The Backend provides access to data and services to a central group of applications such as other IPEs or industrial and enterprise applications at a control centre or grid administration offices.

4. IoT in Smart Grids

Smart Grid technology can have various applications in electricity distribution. Most of these applications are focussed on monitoring and control of the grid or specific grid elements, while others support grid objectives such as revenue collection and energy management. Table 1 summarises some of the most common Smart Grid applications with their network performance requirements.

Because all Smart Grid applications rely on data communication, the use of SDN and NFV in Smart Grids has received a lot of research attention. This focus can be attributed to the past successes of these paradigms in

data centres, WAN and enterprise networks. The benefits of implementing SDN and NFV in Smart Grids include:

- Simplified network management by providing remote monitoring and control of ICT network devices and network activity.
- Reduced dependence on specialised network hardware and the amount of effort required for remote fault finding and network maintenance.
- The ability for different Smart Grid applications or users to have different network views while sharing the same physical network infrastructure, known as network slicing.
- The ability to configure Smart Grid networks to become contextually aware and automate actions that support grid stability.
- The ability to create self-healing networks with network resilience features such as fast failover recovery (FFR).
- The ability to automate network optimisation, improve network traffic flow and reduce network congestion using load balancing applications.
- The ability to virtualise protocol conversion functions on available computer hardware, controllable from a network management application that allows the ICT network to adapt quickly to connection requests from unrecognised networks or devices using unrecognised protocols. Protocol conversion is vital for incorporating exiting grid networks based on existing grid communication standards, for example substation networks based on IEC 61850 communication standards.

In addition to these benefits, other IoT frameworks also hold potential benefits for Smart Grid implementations. SDSec has been shown to be a viable solution for intrusion prevention, data security and malicious attack detection and prevention, while SDStore offers various improvements over Cloud Storage approaches, especially when used in conjunction with multi-access edge computing (MEC).

M2M standards offer a means for standardising the communication interfaces and data models used in Smart Grid networks. By implementing M2M middleware on devices at appropriate points in the network edge and core, the Smart Grid will not only become much more flexible in terms of the machines and applications that can interface with it, it will also be much easier to deploy and maintain. This is because M2M makes use of common libraries that provide common functions for diverse use-cases and allows developers to focus on applications, rather than underlying communication. M2M also promotes cross-sharing of resources and data between different applications and devices that creates new opportunities for solving many grid problems and improving existing functionality.

Application	Bandwidth	Latency	Reliability
Substation Automation	9.6 – 56 kbps	15 ms – 200 ms	99% - 99.999%
Overhead Transmission Line Monitoring	9.6 – 56 kbps	15 ms – 200 ms	99% - 99.999%
Wide-Area Situational Awareness	600 – 1500 kbps	15 ms – 200 ms	99% - 99.9999%
Distribution Automation	9.6 – 56 kbps	20 ms – 200 ms	99% - 99.999%
Distribution Management	9.6 – 100 kbps	100 ms – 2 sec	99% - 99.999%
Home Energy Management	9.6 – 56 kbps	300 ms – 2 sec	99% - 99.9%
Renewable Distributed Energy Resources	9.6 – 56 kbps	300 ms – 2 sec	99% - 99.99%
Demand Response Management	14 – 100 kbps per node	500 ms – 5 min	99% - 99.99%
Advanced Metering Infrastructure	10 – 100 kbps per node	2 sec	99% - 99.99%
Outage Management Systems	56 kbps	2 sec	99%
Electrical Vehicles and Vehicle to Grid	9.6 – 56 kbps	2 sec – 5 min	99% - 99.99%
Enterprise Asset Management	56 kbps	2 sec – hours	99%
Meter Data Management Systems	56 kbps	2 sec – hours	99%

Table 1: Network requirements for Smart Grid Applications

Adapted from [1], Table 1, pg. 38

5. Reference architecture for an IoT based Smart Grid ICT network

In support of streamlining designs for Smart Grid ICT networks, a five layer reference architecture for IoT based Smart Grid designs is presented in Figure 9. The five layers in this proposed architecture include:

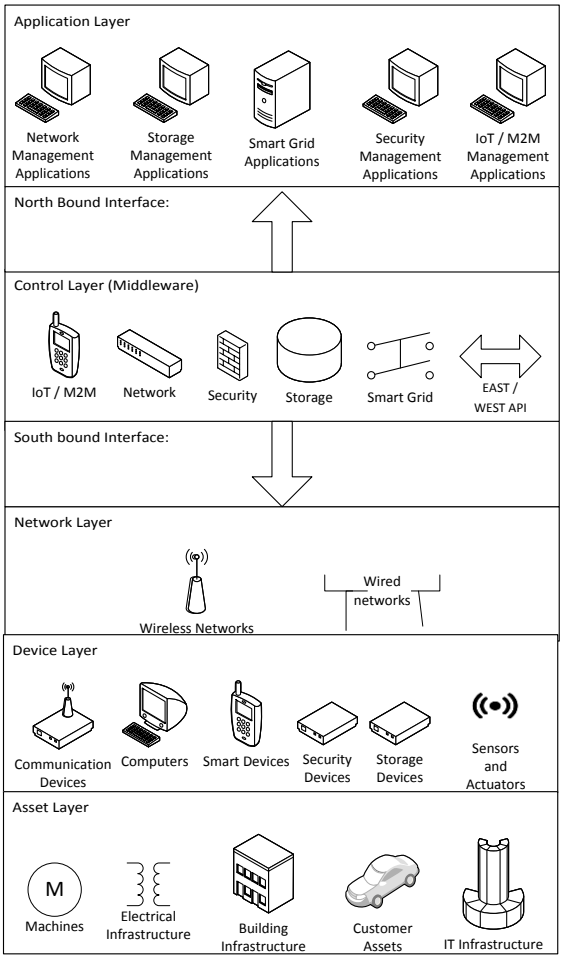

Figure 9: IoT based Smart Grid reference architecture

The Asset Layer

All assets that are fitted with sensors and actuators, and that interface with the Smart Grid network using processing devices, are described in the asset layer of this reference architecture. This layer usually consists mainly of electrical infrastructure, but also includes buildings and other infrastructure that support grid operations. Because the distribution network acts as the main grid interface for customers, this layer can also contain customer assets that produce and use data where data communication network integration is required.

The Device Layer

In most modern electricity grids Smart Substation devices are used to provide data processing, storage and communication capabilities to the grid. Other substation technologies that offer similar features can include Intelligent Electronic Devices (IEDs) and Remote Terminal Units (RTUs) usually implemented with systems such as SCADA or SAS. The device layer represents all these devices that allow grid infrastructure to interface with the Smart Grid ICT network to exchange data. These devices interface with sensors and actuators connected to grid infrastructure that measure and control temperatures, current flows, voltages, vibration, pressure, motion or positions of things like doors or switches. The embedded processing capabilities in these devices can be used to translate or filter collected data and trigger control actions.

The device layer also includes PCs, laptops, servers or other computer devices that are used as hosts for specific applications. These applications can include the software required for SDSys implementation, M2M middleware or applications that support specific gird functions such protection settings management. Other hardware in the device layer may include network devices such as switches, routers and gateways as well as security devices and storage devices.

The Network Layer

The network layer represents the data communication interfaces between all networked devices. Design of the network layer starts with selecting the optimum communication mediums while considering performance requirements, available infrastructure and potential risks in network coverage areas. Wired communication mediums such as copper, PLC and fibre provide the advantages of physical connections between devices that are less susceptible to interference and more secure, although they are usually more costly to install in large coverage areas. Wireless communication is more flexible and can cover greater distances if long range wireless communication methods such as Low Powered Wide Area Networks (LPWAN) or cellular networks are used. In most cases a combination of wired and wireless networks needs to be considered to cater for different requirements in different parts of a Smart Grid.

The network layer design should also define the different networks that will exist in a Smart Grid. Metropolitan distribution grids will likely include a MAN with a high performance backhaul network that connects different networks across a metropolitan area. NANs will be established in specific neighbourhoods where gird assets are located, while EANs and FANs may be used to connect assets in more rural areas. Some customers' HANs, BANs and IANs may also require interface with the Smart Grid communication network. Communication standards and protocols used in Smart Grid networks also need to be considered in network layer design. Most Smart Grid devices will come with a predetermined set of communication standards they support and communication networks will have to be designed to interface with heterogeneous devices from

different manufacturers. Protocol conversion can be implemented using gateway devices or virtualised translation applications. Interface requirements with other networks such as enterprise networks and the internet also need to be considered in the network layer design.

The Control Layer

The control layer represents the capabilities that support the Smart Grid services and applications by controlling and interacting with the underlying layers. SDSys controllers and M2M middleware are great examples of functions that reside in the control layer. The control layer elements rely on southbound interfaces to interact with devices in the device layer via the network layer. The Openflow protocol is an example of a southbound interface used to control network switches in a SDN implementation. Different control layer elements can also interface with each other using east and west bound interfaces.

The Application Layer

The application layer defines the various applications implemented in the Smart Grid network, aligned to the functions grid operators perform to meet specific objectives. Smart Grid applications can be divided into two categories. Functional Smart Grid applications perform functions linked directly to the Smart Grid objectives such as grid monitoring and control, metering, grid protection or data acquisition for analytics to support decision making. Support applications manage systems that support the Smart Grid applications. Examples of these are network management, storage management, security management and device management applications. Northbound interfaces such as the REST API are used to connect the control layer elements with applications in the application layer.

6. Example of an IoT based Smart Grid Design for a Metropolitan Electricity Distribution Grid

An application of this reference architecture in a design for a metropolitan electricity distribution Smart Grid is presented in Figure 10.

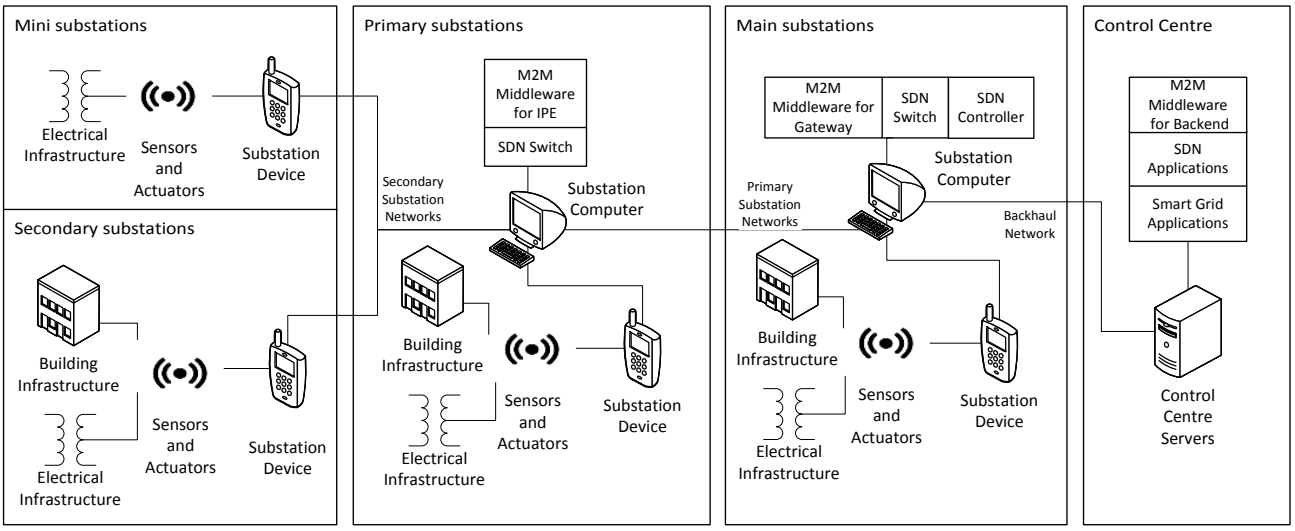

Figure 10: Example of a system architecture for an IoT based Smart Grid implementation

Assuming specific requirements best addressed by SDN and common M2M services, a city's electricity distribution network consisting of Mini-, Secondary-, Primary- and Main substations is designed to be connected in a network consisting of a MAN, backhaul, smaller NANs and substation networks in specific grid sections. These networks use a combination of wired and wireless communication mediums. Each substation in the Smart Grid is equipped with sensors and actuators connected to substation devices with embedded processors and storage. These devices connect to substation computers located in Primary substations that act as Internetworking Proxies (IPEs). The substation computers also serve as local SDN switches for the greater SD-MAN. Main substations also include a substation computer, but these computers are configured to offer M2M Gateway services in addition to SDN switching. The Main substation computers also act as SDN controllers for the respective grid sections in their areas, monitoring and controlling the SDN switches in the

network. The use of multiple SDN controllers in a network eliminates the risk of controller failure disabling a network. All Main substations connect to a Control Centre through the backhaul network. The servers in the control centre offer the services of a M2M Backend and also host the SDN applications used for monitoring and controlling the Smart Grid ICT networks. Smart Grid applications that control field devices and make use of the data acquired from sensors in the field are also hosted on the Control Centre servers.

7. Conclusion

Smart Grid technology is needed to improve our electricity grids so that they can accommodate the rapid change from electricity consumers to electricity "prosumers" and the introduction of disruptive smart technologies. The uptake of Smart Grid technology depends on the development of methods that will simplify the design, implementation, operation and maintenance of their complex ICT networks.

IoT offers many opportunities that improve on conventional grid ICT network implementations, especially in metropolitan electricity distribution grids that consist of designs with the potential for vast numbers of sensors and actuators. Decoupling the management and orchestration of crucial grid support functions, such as networking, from field hardware simplifies grid operations and maintenance. This results in reduced operating expenditure and reliance on specialist ICT expertise to perform these functions. In addition, streamlining the design of Smart Grid ICT networks through standardised and repeatable functions and approaches simplifies Smart Grid implementation, making these systems less capital intensive for utilities to develop. The benefits of using IoT frameworks in Smart Grid designs should therefore be a prioritised consideration for any electricity utility.

8. Acknowledgements

The author acknowledges the research guidance and support received by the Telkom Centre of Excellence (CoE) in Broadband Networks & Applications in the Department of Electrical Engineering at the University of Cape Town whilst pursuing his MSc (Eng) studies in the areas of Smart Grids and IoT. He also acknowledges the guidance and support from members of the City of Cape Town's Energy and Climate Change Directorate.

9. References

[1] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "A Survey on Smart Grid Potential Applications and Communication Requirements.", Industrial Informatics, IEEE Transactions on 9, no. 1, pp. 28–42, 2013.

[2] M.Uslar, S. Rohjans, C. Neureiter, F. Pröstl Andrén, J. Velasquez, C. Steinbrink, T. Strasser, "Applying the Smart Grid Architecture Model for Designing and Validating System-of-Systems in the Power and Energy Domain: A European Perspective", Energies, 12(2), 2019.

[3] CEN-CENELEC-ETSI Smart Grid Coordination Group, "Smart Grid Reference Architecture", 2012.

[4] IEEE 2030, "IEEE Smart Grid Interoperability Series of Standards", 2011.

[5] R. Minerva , A. Biru, D. Rotondi, "Towards a definition of the Internet of Things (IoT)", IEEE Internet Initiative, 2015.

[6] ITU-T, "Overview of the Internet of things", Recommendation ITU-T Y.2060 of Series Y: Global Information Infrastructure, Internet Protocol Aspects And Next-Generation Networks: Next Generation Networks – Frameworks and functional architecture models, 2012.

[7] ITU-T, "Framework of software-defined networking", Recommendation ITU-T Y.3300 of Series Y: Global Information Infrastructure, Internet Protocol Aspects And Next-Generation Networks: Future Networks, 2014.

[8] oneM2M, "Solving the IoT Platform Challenge", Executive Briefing, November 2015.

[9] The OpenMTC website. Available at https://www.openmtc.org/index.html, accessed 2019.