SIEMENS
Ingenuity for life

IoT in Power Grids

Preparing Electrical Grids for Tomorrow's Challenges

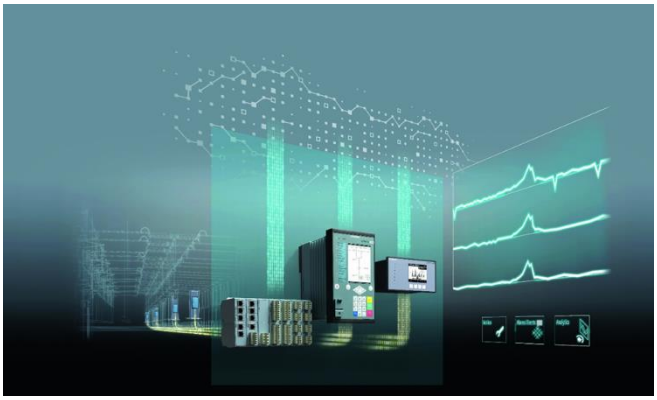
Writing the Next Chapter of Digital Communication

Ever since the adoption of digital protection relays in the 1980's, digital communication in power grids has become commonplace and gradually evolved over time to meet the growing needs of a more complex energy infrastructure. With the growing ubiquity of communication infrastructure, more and more devices are being upgraded to be able to communicate and thereby form a so-called "Internet-of-Things" (IoT), unleashing a torrent of innovation that has found its way from the consumer space to industrial automation, and by now has reached the shores of the energy industry. But how is IoT different from classic communication schemes and what additional value does it add in the context of power grids?

Looking back, communication in power grids has evolved along the path of increasing digitalization from serial protocols (still in use today) to the adoption of IP networks and integration of interoperable communication standards like IEC 61850. Meanwhile the Internet as the common infrastructure of all-IP-based communication has seen an explosion of bandwidth requirements as well as a steep increase in the number of end points connecting to the Internet. While the first wave of growth was driven by an increasing penetration of humans gaining access to smart phones, the next wave will be dominated by "things" (earlier called "machines") that either produce or receive data in line with their respective communication requirements.

The spectrum of IoT enabled devices is very wide, ranging from always-on communication to frequent connects and disconnects with small data payloads to only haphazard transmission on rare occasions. To accommodate this type of flexibility in communication, suitable protocols are needed to cover the widest possible number of use cases – hence the emergence of "IoT" protocols. Before we dive into further details, let's take a look at communication in a typical power grid today.

Contents



Since 2018 we at Siemens Digital Grid have begun to add IoT communication functionality to our substation automation and protection portfolio, thereby enabling additional data flows from the field- and substation automation level. The benefits of this new capability will unravel as electric grids experience increasingly dynamic situations, empowering our customers to gain deeper insights into what is going on in the grid using combined cloud/edge data processing solutions. Our entire fleet of SIPROTEC 5-based protection relays, bay controllers and fault recorders as well as SICAM A8000 RTUs and PQ Devices SICAM Q100/200 already benefit from this functional upgrade and will be complemented by additional offerings in the future. This Whitepaper outlines the basic motivation behind IoT in Power Grids and elaborates on some of the benefits as they can be discerned at this early stage.

Contents

IoT in Power Grids

Data and Communication in Power Grids

In the classic view of the power grid, there are essentially three tiers of control:

- The field device level
- The substation level
- The control center level

The field devices (IEDs) are located near the process and collect their input data from instrument transformers, hence they are the most productive sources of data in the overall architecture. IEDs communicate among each other to enable low-latency operations, as well as with the next higher layer, the substation automation level. Here a small configurable subset of data (approx. 15%) from the field devices is accumulated – still within the context of a single substation.

To manage power flows across the entire grid, the control center is the central point for Supervisory Control and Data Acquisition (SCADA System). On this level, only a few relevant data points from all substations in a grid are accumulated via distributed RTUs (Remote Transmission Units), analyzed and acted upon to maintain a stable energy supply.

Within this well-defined context, standardized communication protocols like IEC 61850-8, DNP3.0 as well as the classic IEC 60870-5 family have served us well to maintain stable energy flows and will continue to do so. Yet the landscape of energy production, transmission, distribution and consumption has become more sophisticated and will gradually develop into a structure as outlined in Image 2. While previously energy was produced at a few central locations, distributed energy generation with a strong focus on renewables as well as energy coupling between multi-modal grids has become a clear trend in the industry, thus requiring enhanced transparency and data processing capabilities in the distribution domain to maintain a reliable energy supply.

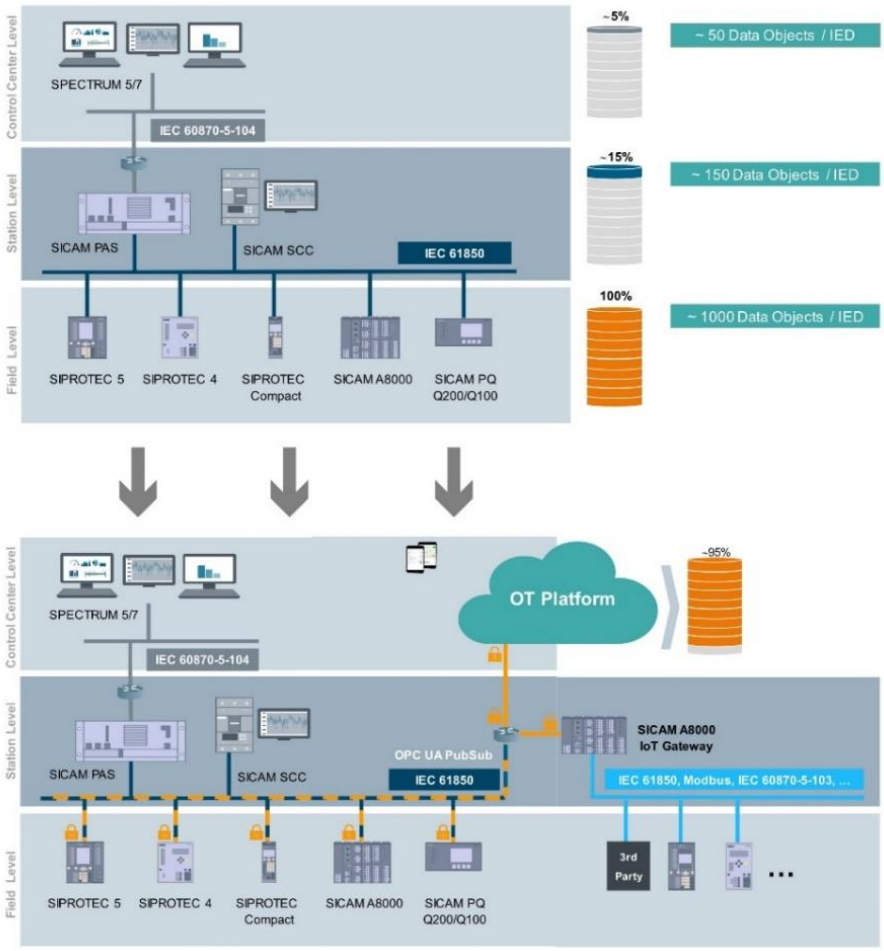


Image 1: Data Processing Layers in Power Grids

Factoring in all these changes, obviously there is a greater need for communication among all participants in the energy infrastructure. Perhaps the biggest paradigm shift in the new age of the "*Internet of Energy*" is the greater interdependence of all parts of the grid. In the old world, usage of data was restricted to the immediate hierarchy of the grid – in the new world, data from one corner of the grid may be needed to influence decisions outside of its

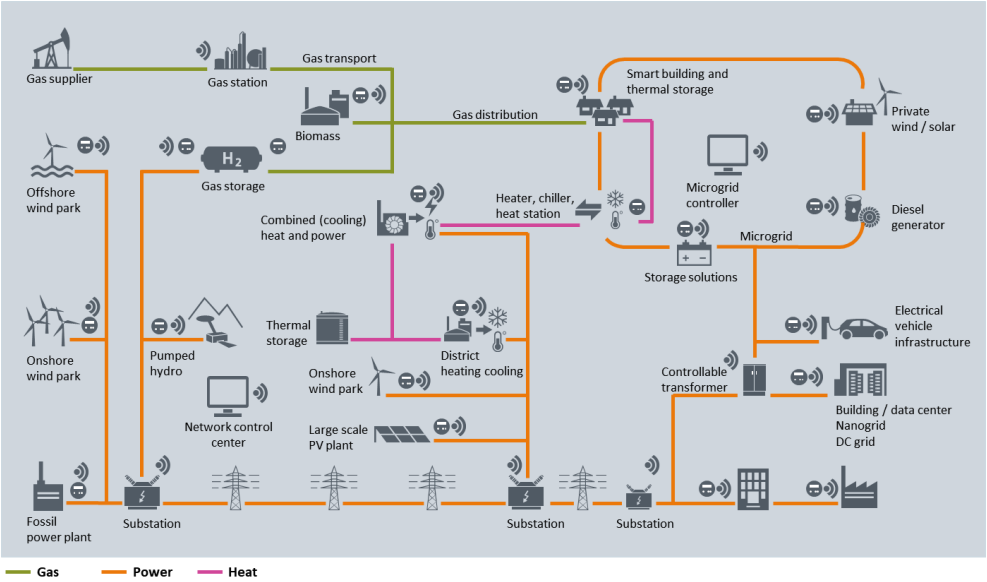


Image 2: Structure of Future Power Grids

classic "reporting line" – and include operational as well as non-operational types of data. Welcome to IoT communications!
Selecting one of the many available options for communication of things means finding a good trade-off between performance, scalability and ubiquity. Below are some key points that guided us in our decision-making process on how to implement IoT in Power Grids.

IoT in Power Grids

As we deal with huge quantity structures of "things", not all data can be sent at all times from all data sources to all receivers. As a first step it is essential to define a scalable architecture between the bottom and the top layers of the data pyramid – so we chose to adopt a publish-subscribe based communication model. This approach delivers many benefits, a few of them listed below

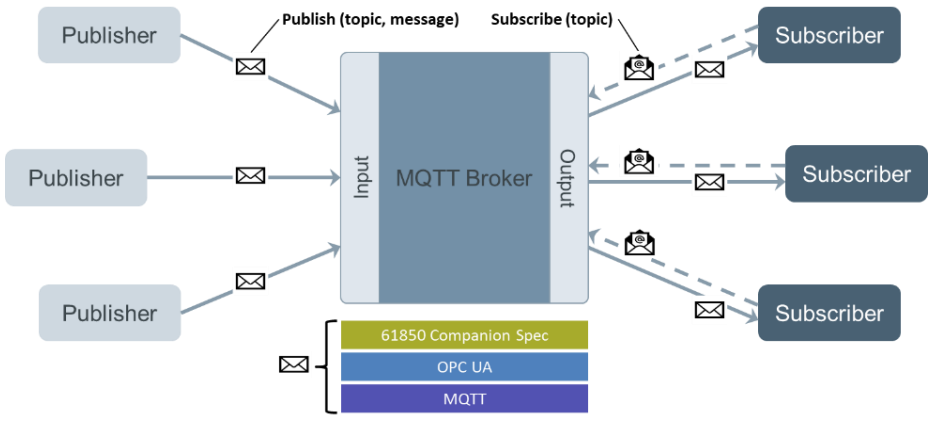


Image 3: Publish Subscribe Architecture

Independent decoupling and scaling
Through the publish-subscribe mechanism, sender and receiver nodes do not communicate directly but through a broker node. In this fashion they are decoupled and can operate and scale independently from each other. Nodes on either side of the broker can be added or subtracted without an impact on the overall communication system or a need for complex engineering procedures.

Elimination of Polling
Publisher nodes operate in a push-based mode and do no longer need to be actively polled from communication back-ends. Data is sent on immediately after measurement values are received.

Simplified Communication
The system no longer needs to maintain a registry of peers with compatible data types. Instead, messages are classified by topics which in turn can be subscribed to without knowledge of the originating publisher node.

Data Semantics

Beyond solving the network capacity problem, once a large number of distributed nodes in a widely dispersed network start sending their data, the implementation of proper data semantics is an essential prerequisite for the proper usage of data analytic methods. Each data point needs to be described with all essential attributes like device of origin, physical location, topology position, time stamp, measurement type, measurement value etc.. Only when the semantics are well-defined and openly accessible, it becomes possible to achieve cross-vendor interoperability and hence a wider adoption.

To this end we picked the evolved version of the well-established OPC UA standard named OPC UA PubSub (MQTT), which as the name suggests wraps the classic OPC UA payload inside an MQTT container. Furthermore, by also adopting and actively contributing to the related OPC UA 61850 companion specification we get both – a mature data semantic model together with a scalable publish-subscribe architecture.
By supplementing the traditional communication paradigms in power grids with IoT communications, new opportunities gradually come to light that add additional customer value. To capture this value, a range of applications within the framework of our **Grid Diagnostic Suite**[1] were introduced, addressing three different application scenarios:

- IoT for the energy transmission and distribution domain
- IoT for industrial power applications
- IoT for geographically dispersed devices in the context of secondary distribution automation.

IoT for Transmission & Distribution Systems

As mentioned earlier, digital communication inside a substation is not an innovation by itself. Our idea of IoT within this context however makes a great difference in the way the data is handled. First, we aim to look at a much bigger slice of data in relation to what is normally available on a substation automation or control center level. Second, we do not require any additional engineering. IoT for our customers should be as easy to deploy as plug & play and offer new functionality without any impact on an operational FAT/SAT approved substation. The essential features of a substation automation and protection system are to quickly and selectively trip circuit breakers in case of electric faults, execute configured switching sequences and report specific threshold violations and alarms. With the help of IoT and the corresponding bigger data space we are now able to expand this functionality to also recognize slowly evolving trends and anomalies in the grid that would not necessarily trigger any of the classic responses. Thus, we are now enabled to alert a grid operator ahead of time and avoid further problem escalations.
Our first application that demonstrates the new possibilities of IoT is our **SIPROTEC Dashboard**, enabling a grid operator to get a quick overview on the status of his entire device fleet deployed in multiple substations across the grid, including alerts on operational and security events. Furthermore, IoT also facilitates the automatic aggregation of classic data like fault records and alarm lists from across all substations to analyze events in the context of the entire grid, enabling features like multi-ended fault location and a sequence-of-events analysis to determine the actual root cause of a grid event.

Image 4: Screenshots of SIPROTEC Dashboard

IoT for Industrial Power

While most use case in the context of Industry and IoT refer to applications in the context of Industry 4.0, the benefits of energy management and systematic power quality monitoring are becoming more and more visible (see brochure "Power Quality in Production"[2])
To address this particular problem space, we offer the **PQ Advisor**, which is the first solution on the market that combines these two components in one package.
Leveraging on the advanced features of our power quality devices like the **SICAM Q200**, the PQ Advisor not only traces and optimizes energy consumption of individual production lines, but also checks power quality indicators like the presence of harmonics or the dynamics of power factors over time for entire fleets of PQ devices. Data analytic methods help us to further correlate the synchronous time-series data from a distributed set of data sources and identify possible sources for power quality degradation before they lead to defects in sensitive electronic equipment.

IoT for Secondary Distribution Automation

Outside the substation context, IoT connectivity enables previously silent stand-alone devices to communicate through wireless cellular or LPWAN networks, e.g. to aggregate data from classic fault sensor indicators over a wireless communication gateway into a cloud application to determine fault locations on overhead lines in distribution grids. Another use case is the remote monitoring of

[1] http://www.siemens.com/iot-energy-automation

[2] http://www.siemens.com/download?DLA03_2150

geographically dispersed secondary distribution substations that are hard to reach for service technicians.
Yet with all these data flows scaling up in the grid – where is all that data supposed to go?

OT Platform Options

One great benefit from the adoption of open standards for the communication layer is the freedom of choice when it comes to the decision for the most suitable IT platform. While many of the available commercial cloud platforms today will be able to deal with the raw data streams as such, the key decision point for a customer lies in the overall user experience. Some points stand out to consider:

- Easy scalability for future add-ons of communication nodes
- Automated workflows for secure commissioning and operations of IoT devices
- Full semantic description of IoT data
- API for customer specific application development

The **Grid Diagnostic Suite** was developed both to enable our customers to write their own applications as well as to create the best possible user experience, hence we put our focus on **Mindsphere** as the key cloud platform from Siemens for Industrial Data Analytics.
As the amount of actionable data-in-motion keeps growing, in the near future it will no longer be economically feasible to send all data straight into the cloud. Therefore, we foresee the deployment of a layered architecture with additional substation edge nodes that are able to ingest local high-frequency data streams and only transmit relevant bits of data into the cloud.
One key concern when it comes to large scale IoT deployments is of course the overall topic of cyber security. Considering the growing threat of cyber-attacks on critical infrastructure - how can we guarantee rock-solid operations in all parts of the grid?

IoT and Cyber Security

Regarding Cyber Security, the best recipe for success is a combination of well-tested and professionally implemented open standards combined with usability-centered workflows.
The security architecture is based on a X.509 public/private key infrastructure using digital certificates to establish trusted relationships between nodes in the grid. All users and devices that participate in grid communications must be authenticated, their scope of actions limited to an authorized set of access rights and data flows be encrypted by default.
The challenging part here is to rigorously apply all these principles to a network with a vast number of devices without creating complex manual workflows during installation or an excessive burden on the IT admins during operations.
Within the context of a substation, **SICAM GridPass** greatly facilitates the automated enrolment of new devices, including the distribution of communication certificates and the central administration of role-based access rules[3].
On the IoT level, a similar functionality is essential to provide our customers with a seamless experience – the first concepts for such a solution already exists in the form of cascaded entities of **GridPass** nodes, that each can handle allotments of up to 10.000 clients.
In summary we are convinced that the gradual adoption of IoT will increasingly add value to the Substation and Protection domain and shape its future towards a more responsive and flexible energy grid.

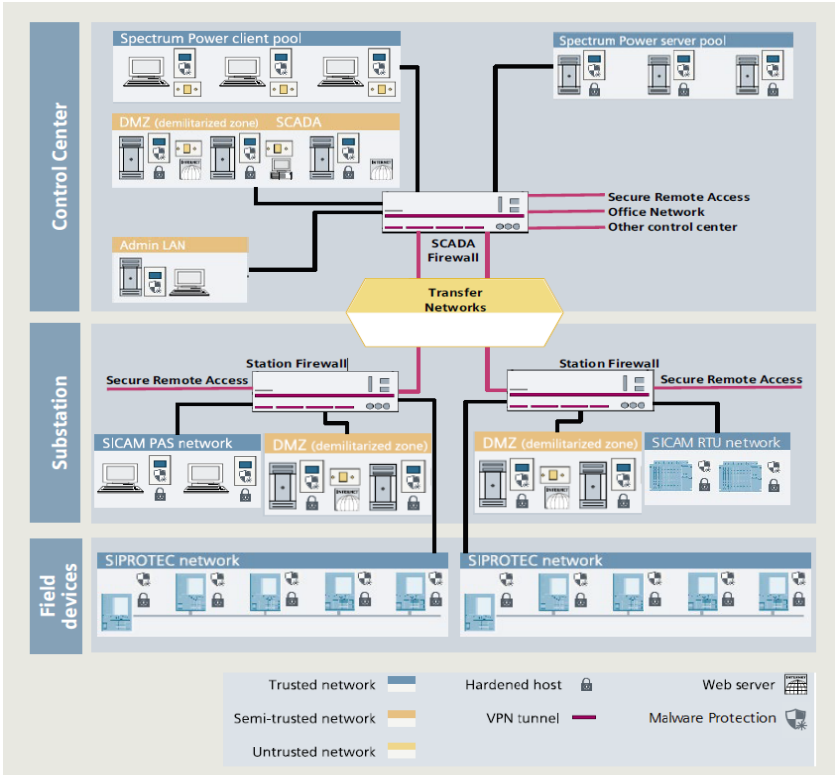


Image 5: Cyber Security Architecture for Power Grids

[3] http://www.siemens.com/gridsecurity

Abbreviations

FAT	Factory Acceptance Test
IoT	Internet of Things
LPWAN	Low-Power Wide-Area Network
OT	Operational Technology
PQ	Power Quality
SAT	System Acceptance Test

Markus Mediger
Portfolio Innovation Management
Business Unit Digital Grid
Siemens AG, Nürnberg