Achieving the promises of IoT with existing technology

Jacques Benoit, *Eaton*

***Abstract*— The "Internet of Things" (IoT) vision promises that organizations can achieve significant operational efficiency through cloud-based applications and Big Data analytics. This paper provides a brief discussion of the challenges of cloud-based applications for utility automation and alternative approaches already used in a number of utilities. The paper then provides an overview of real-world applications that have been deployed at utilities to collect and process data from substation devices for asset management, while co-existing with SCADA, and meeting cybersecurity requirements. The paper will discuss the architecture used for data acquisition and the challenges raised by managing very large numbers of data points. Finally, the author will briefly discuss how the data is put to use to provide improved operational efficiency.**

I. Introduction

Interest for the Internet of Things (IoT) continues to grow as can be witnessed from the ever growing flow of newsletters, conferences and event announcements making its way to our email inboxes. While the original IoT marketing message was all about connecting large number of devices, we can observe that the message is gradually shifting to the benefits that can be provided by putting to use all the data being produced by connected devices. Big data and analytics are now the key words driving IoT in different industry sectors.

While there is some skepticism towards IoT in the energy sector, we should keep in mind that utilities pioneered this vision by deploying large number of connected devices as part of their Smart Grid initiatives [1]. Through these projects utilities pursued the goal of adding intelligence to the electric network in order to improve its responsiveness, reliability and efficiency. The IoT vision can thus be considered as the next step since it starts out with intelligent devices and focuses on the benefits that can be provided by putting to use the large amounts of data produced by these devices.

In this paper, we will discuss how some utilities are already leveraging their communications infrastructure and putting data to use to improve their operations, achieving the benefits promised by IoT, with a focus on Condition Based Maintenance applications.

II. The IoT and utilities

Ironically, while IoT vendors seem to be focusing on the corporate boardroom, there are already numerous projects under way at different levels within utilities with the goal of leveraging the value of data being produced by devices. Utilities are thus busy pursuing goals similar to those of IoT, but without the hype.

Before we can discuss how utility projects achieve the promised benefits of IoT it is useful to review its defining concepts and technologies. Fundamentally, it is generally assumed that the IoT is based on the following [2]:

- Connected devices
- Cloud computing
- Big data and analytics

The popular press has propagated a vision of billions of devices connected through the public Internet and working together to provide value. While this could be feasible for some applications, cybersecurity and privacy concerns make it unlikely that utilities will choose this approach, except maybe for customer facing applications. For the foreseeable future, utility IT groups will continue to deploy devices through private "internets" based on a secure layered communications infrastructure.

Another key concept of the IoT is cloud computing. Handling the massive amount of data produced by a large number of devices is already challenging standard IT approaches based on physical servers and disk storage. The key concept of cloud computing is that computing and data storage resources are allocated as needed to virtualized applications sharing pools of servers and disks. Resources can thus be scaled according to demand, in a timely manner. This scalability is achieved by having numerous applications, and even customers, sharing the same pool of distributed resources. Again, this model raises security and privacy concerns since the control and management of the computing infrastructure is outsourced to a third party. Private clouds can address these concerns, but it will be a struggle for utility IT groups to migrate to complex virtualized solutions.

As we can see from the previous discussion, the communications model and cloud-based infrastructure of IoT are easily applicable to utility applications. However, the value of device data remains the same whatever technology is

Presented at Power and Energy Automation Conference, Spokane, WA, March 21-23, 2017

used. This value is achieved through analytics, which according to Wikipedia consists in the "discovery, interpretation, and communication of meaningful patterns in data" [3]. Since the volume of data can be very large, the processing requires special technology and analytical methods which are tagged "big data".

III. Big Data and Analytics

According to a study by a leading vendor of data historian software [4], the top reasons that companies invest in operational analytics are:

- To improve overall business performance
- To improve process efficiency
- To monitor asset health

Through analytics, companies can gain a better understanding of their operations and ultimately improve their performance and reliability. However, the whole process is incremental and starts out with gathering data to provide situational awareness, moving on to condition monitoring, and ultimately process optimization.

The analytics implementation process can thus be characterized by the following maturity levels:

- Descriptive Analytics: What happened?
- Diagnostic Analytics: Why did it happen?
- Predictive Analytics: What will happen?
- Prescriptive Analytics: How can we make it happen?

Analytics are applicable to utility projects which involve large number of connected devices. Advanced Metering Infrastructure (AMI) is the most commonly mentioned in the context of IoT. Originally deployed to reduce the costs of reading meters, AMI can also be used to provide a true real-time portrait of power usage and assist in network planning and fault analysis through Meter Data Management Systems (MDMS). Many utilities are also deploying communicating Faulted Circuit Indicators (FCI) to improve situational awareness through access to real-time network performance data.

In the rest of this paper, we will discuss asset health monitoring and Condition Based Maintenance (CBM), which are applications of analytics already being implemented and providing benefits to utilities.

IV. Condition Based Maintenance (CBM)

Assets used in the distribution network are typically run to failure. The business benefits of preventive maintenance are generally not offset by the cost of monitoring the health of the asset. However, there is a much better business case for assets installed in transmission and distribution substations. Most utilities have thus installed sensors and monitoring devices to monitor the condition of these assets, a first step towards Condition Based Maintenance (CBM).

The goal of Condition Based Maintenance (CBM) is to perform equipment maintenance only when it is necessary, instead of on a fixed schedule. With CBM, the maintenance schedule is driven by information provided by the equipment itself, or by specialized monitoring devices. Because of the cost of implementing CBM, it is generally used with critical assets such as breakers and transformers where the repair or replacement cost is significant, or when failure would have a significant impact on business.

For this paper, the author discussed with two major utilities that implemented CBM projects using readily available technology and software. In the following sections, we will discuss these projects, the business drivers, the technological choices, and the benefits.

V. CBM Business Drivers

CBM projects are generally undertaken as part of large enterprise-wide operational efficiency programs. With significant investments in technology being made to optimize operations and to compensate for the loss of expertise due to the aging work force, there is a strong drive to leverage technology in order to streamline processes and generally improve efficiency.

In the projects we reviewed, transformers were identified as the best target for CBM. In most utilities, large transmission transformers are rapidly approaching their expected life expectancy. Replacing transformers is an expensive operation with long lead times. The goal is thus to defer transformer replacement as long as possible, while preventing catastrophic failures.

The utilities we interviewed had deployed transformer monitoring devices and were performing oil analysis on a scheduled basis. Some gassing had been observed, but they did not have a clear picture of the condition of their transformers. Was it possible to push them further? Essentially what they required was real-time monitoring of the transformers in order to provide the equivalent of a “check engine” warning indicator.

The CBM projects thus aimed to deploy all necessary sensors and monitoring devices to collect the following types of data to provide a real-time indication of transformer condition:

- Oil Temperature: top oil, bottom oil, main/load tap changer (LTC) tank differential
- LTC tap positions and motor energy
- LV load current
- Ambient temperature
- On-line, 8-gas DGA
- Loss of cooling fans/pumps
- Bushing power factor monitor

While monitoring devices had been installed, they were often not connected and data values were captured manually by field technicians, if at all. The first step in the CBM projects was thus to connect sensors and diagnostic devices and make the data available to a centralized historical database in order to implement monitoring, alarming, and analytics applications.

However, retrieving data from a substation can be quite challenging. Until very recently, substation automation was limited to autonomous protection systems with limited communications capability, often through dedicated phone lines. A substation RTU collected some operational data and provided the capability for a SCADA master to perform control operations. While most utilities have upgraded, or are in the process of upgrading their communications systems to add bandwidth and network connectivity, this is often dedicated to SCADA/RTU.

VI. USING SCADA DATA FOR ANALYTICS

Vendors of data historians and analytics software often present architecture diagrams with SCADA as the source of data for analytics, as illustrated in Figure 1. But, as we have mentioned previously, the SCADA/RTU architecture is essentially dedicated to power system operations and generally does not contain the non-operational data necessary for CBM.

There are a number of reasons why non-operational data remains stranded at the substation level. From a technical perspective, SCADA may still be based on low bandwidth communications systems and would not be able to support the additional non-operational data. More important is the fact that SCADA is critical to operations. Implementation of the CBM system could interfere with SCADA, and would require numerous communications outages during implementation. Moreover, adding complexity and connecting more devices can only decrease the reliability of the system, which is not acceptable for a critical application such as SCADA.

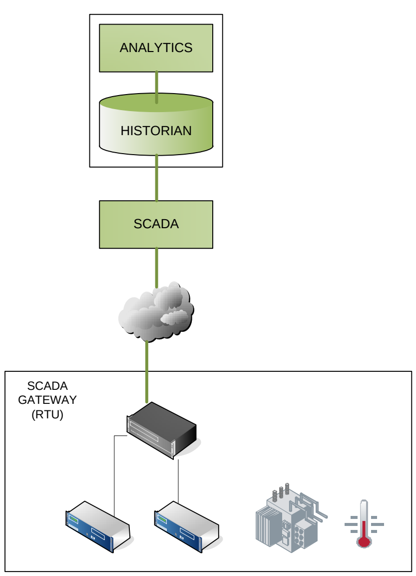

Figure 1: Non-operational data is generally not available to SCADA

VII. IMPLEMENTING A PARALLEL DATA PATH

The projects we reviewed thus started out by implementing a separate TCP/IP communications backhaul to retrieve non-operational data. This new data path was completely isolated from SCADA in order to prevent any disruption to operations.

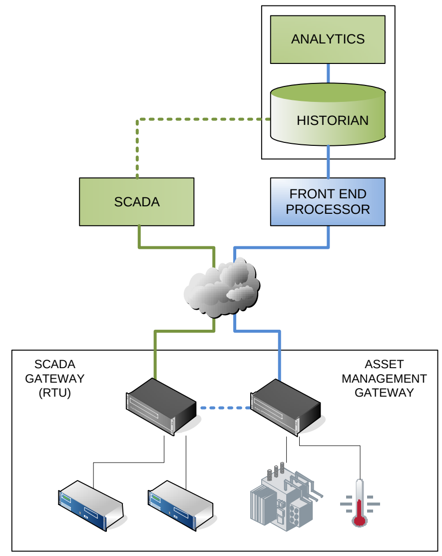

Figure 2: Parallel data path for non-operational data

A separate "asset management" data concentrator was deployed at the substation level to process the data from the various monitoring devices and sensors, and to handle the different protocols, using serial and networked links. At the enterprise level, a front-end-processor is used to concentrate the data being collected from all the substations, and to provide an interface to the data historian.

Retrieving the operational data required for analytics was achieved either at the substation level, by sharing data with the RTU/data concentrator, or at the enterprise level, through an interface to SCADA.

Since the projects involved implementing a modern networked communications infrastructure, it would seem possible to connect the data historian directly to the substation data concentrator, or even directly to the sensors and diagnostic devices. While this would be in alignment with the IoT vision of connected devices, it raises a number of issues from the cybersecurity, performance, and interoperability perspectives.

Typical sensors and monitoring devices are designed to be polled by a master system using protocols such as DNP3 or MODBUS. Having a data historian reach out to poll all the sensors and monitoring devices increases the number of logical connections, which increases the complexity of the system, and raises cybersecurity concerns. The complexity of the system is greatly reduced through the use of an enterprise level front-end-processor (FEP) connected to substation data concentrators that handle the scanning of devices and support the variety of standard and proprietary protocols used by the monitoring devices. With this architecture, there is a single network connection between the FEP and the data concentrator, resulting in simplified network design, and firewall rules.

Cybersecurity must also be taken into account. Best practices for control system architecture dictate the use of segregated network zones, enclosing systems of the same risk level, with well-defined conduits to manage data exchanges between zones [5]. From a NERC CIP perspective, protective relays may be considered BES Cyber Assets and need to be segregated with devices of the same criticality. Any device connected to the same network segment will thus be considered to be at the same criticality level, and will require the same protective measures, further increasing the complexity of the system [6].

For all of these reasons, the utilities implementing the CBM systems that serve as the basis for this paper chose to implement a parallel data path to retrieve data to be used for their monitoring and CBM applications.

VIII. Challenges

A. *Cybersecurity and NERC CIP*

As discussed, cybersecurity and NERC CIP compliance were major challenges in the implementation of the CBM projects. At one utility, the CBM project was essentially halted in mid stride when network connectivity to critical substations was disconnected for NERC CIP compliance. The adoption of CIP version 5 and the changes from critical assets to BES Cyber Systems, provided an opportunity to revise the substation network architecture and move the sensors and monitoring devices to an isolated low impact network segment. However, this resulted in an important loss of momentum for the CBM project.

B. *Organizational challenges*

In addition to cybersecurity, CBM projects face multiple organizational challenges. Cybersecurity is not the only factor to introduce delays and loss of momentum. Installing sensors and monitoring devices required outages which had to be planned months in advance, with the result that implementation moves very slowly, people lose interest or move on to new tasks, organizations and priorities change. It should be noted that both of the surveyed projects started in the 2008-2010 time frame and are still ongoing.

Implementing CBM requires coordinated efforts from multiple groups within the utility. The success of the project thus depends on the ability of the project leader to work with and coordinate all the involved parties, in addition to having sufficient understanding of the technologies involved. Implementing CBM also requires a change of culture and processes that may cause clashes with workers and unions.

C. *Technical challenges*

From a technical perspective, moving data from the substation to the data historian using the architecture described above was quite straightforward as the people involved were already familiar with the technology. The enterprise level front-end-processor was implemented using multiple data concentrators from the same vendor as the substation data concentrator. These data concentrators support a proprietary data exchange protocol which reduced the configuration effort by automatically propagating all available data points from one system to another. This could also have been achieved through the use of points lists as supported by DNP3 and IEC 61850.

However, the large number of available data points did introduce challenges. As can be seen in the Figure 2, the data is collected by a substation data concentrator, then by an enterprise-level front-end-processor, then by the data historian. The interface between each of these layers needs to be configured to set up to retrieve the required data points. Even with automatically generated points lists, multiple manual operations are required.

We observed two different strategies for handling data points. In one case, the utility chose to retrieve and archive all available data points, in order not to miss out on potentially useful data. This resulted in more than 500K data points to manage. With the enterprise level data concentrators and the interfaces to the data historian being limited to 64K data points each, care had to be taken in distributing the points. Adding a single point could cause a reshuffling of data points between interfaces if the maximum count is reached. This situation could potentially happen each time a new substation, or monitoring device, was brought online.

The alternative approach used by the other utility was to carefully select the data points to retrieve and archive. While this approach reduces the total number of points, it requires more analysis and design up front in order to create standardized device templates where only selected data points are transferred "up" the data acquisition path.

Additional configuration steps were also required to set up the interface to the data historian, remove any unnecessary data points added by the data concentrators, and provide the additional attributes necessary to correctly represent the values. Scripts were developed to handle this process automatically.

Interoperability is also proving to be a continuous challenge. Utilities work closely with vendors to implement the features required to meet their project objectives and to support new devices. However, this often results in the release of new software and firmware versions that may need to be retrofitted to already deployed devices, requiring unexpected and unplanned efforts.

D. *Improving the data collection process*

As described above, setting up the data acquisition process is a straightforward process. However, it was reported that it was cumbersome and time consuming. While some of the interfaces are self-configuring, there still remains too many manual steps, especially in the configuration of the data concentrators acting as a front-end-processor for the data historian. In the near future, the hardware data concentrators will be replaced by a software front-end-processor integrated with an IED Management system which should simplify the configuration process.

E. Adding meaning to the data

As a first step in the CBM project, the utilities developed dashboards to display data for each monitored transformer. The key requirement here is to use consistent naming conventions so that a dashboard template can be automatically mapped to the appropriate physical data points. This task was made possible through the use of tools provided by the data historian vendor that provide the capability to create a high level hierarchal model which is automatically mapped to data points through the use of regular expressions. By using a hierarchical mapping, it becomes possible to refer to a data point by its logical name, e.g. top temperature of transformer 1 of a given substation, whatever it's DNP3 index or MODBUS register address.

Through the use of tools provided by the data historian vendor a complete set of asset monitoring views were developed to navigate substations, overlay transformer images with real-time values and plot real-time trends, as illustrated in Figure 3 and Figure 4.

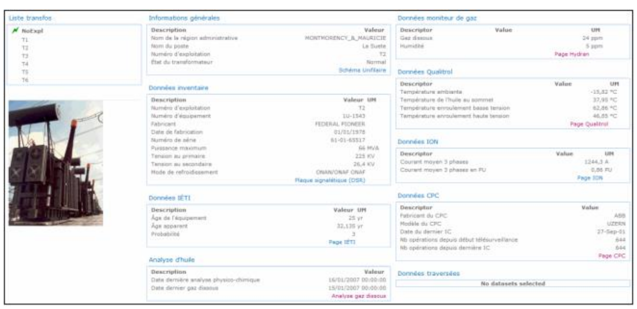

Figure 3: Sample transformer dashboard [7]

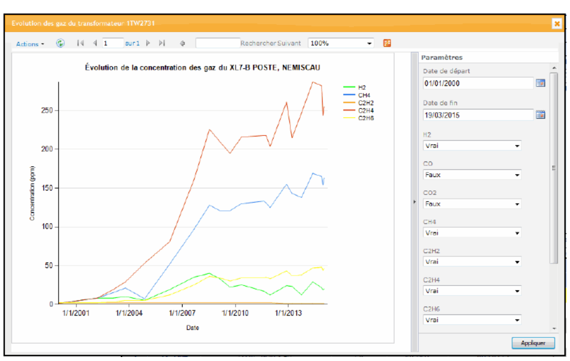

Figure 4: Sample dissolved gas concentration trending view[7]

IX. ANALYTICS

Dashboards and trends provide situational awareness and form the basis of condition monitoring and Condition Based Monitoring. By settings up basic alerts on thresholds and status changes, maintenance crews can be alerted automatically through emails or text messages whenever a situation arises, and act accordingly.

Additional analytical steps can further improve the value of data. For instance, it was observed that the retrieved data sets may contain non-consequential changes as a result of device settings changes. Also, algorithms can be implemented to correlate values and provide indications to maintenance crews on the future performance of the system. One of the utilities has been working with a research team in order to develop predictive algorithms.

X. NEXT STEPS

An important benefit of these projects was the deployment of a modern communications infrastructure. A number of additional initiatives have been undertaken to leverage the existence of the network infrastructure. The addition of IED Management software has provided secure remote access capability. One of the utilities is using the network to automate the process of retrieving event records from substation relays to provide faster fault location and merging the fault records to the historical data for further analysis.

XI. BENEFITS

In both utilities interviewed for this paper, the CBM project met its objectives and was considered a success. While there were measurable gains, this information was not shared with the author. But, it can be stated that transformer replacement was deferred and windshield time required for maintenance was reduced, resulting in significant financial savings.

Unfortunately, because of the duration of the projects the interviewed utilities felt that their projects didn't get the attention they deserved.

XII. CONCLUSION

The concepts of IoT, analytics, and big data are getting a lot of media attention, especially at higher levels within organizations. However, utilities are already deploying large numbers of intelligent devices and putting data to use to improve operational efficiency. In this paper, we discussed how utilities have been implementing Condition Monitoring and Condition Based Maintenance to reduce their operational costs and gain today the benefits that IoT promises for tomorrow.

XIII. REFERENCES

1. J. S. Katz, "IoT for Electric Power: Smart Grid was the Beginning", *IEEE Internet of Things Newsletter*, Jan. 2017. [Online]. Available:

http://iot.ieee.org/newsletter/january-2017/iot-for-electric-power-smart-grid-was-the-beginning.html
2. J. Benoit, "The Internet of Things and the Energy Sector: Myth or Opportunity", presented at the 2016 PEAC conference, Spokane, Wa, March 8-10, 2016.
3. "Analytics", Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Analytics
4. OSIsoft LLC, "Using Operational Data in Big Data Analytics", Oct. 12, 2016. [Online]. Available: http://pages.osisoft.com/BASurveyWebinarOD.html
5. Industrial communication networks - Network and system security, IEC TS 62443-1-1:2009.
6. Cyber Security – Electronic Security Perimeter(s), CIP-005-5.
7. N. Di Gaetano, ing., M. Daigle, ing., "Maintenance du réseau de transport électrique: Surveillance en temps continu à l'aide de SharePoint/PI WebParts et de PI Event Frames, " presented at the 2015 OSIsoft Regional Seminar, Québec, QC, Sept 2015.