Reliable Power Monitoring is Critical to Successful 10G Deployment

A Technical Paper prepared for SCTE by

Tim Cooke
Director of Product Management
Amphenol Broadband Solutions
Chatham, VA
434-489-4713
tcooke@abs-go.com

Table of Contents

Title **Page Number**

List of Figures

Title **Page Number**

1. Introduction

As network speeds increase, and their elements move ever closer to end users, the need for good, reliable and steady power has never been greater. With the changing architectures of networks – copper, fiber, wireless, small cells, etc. it is equally important that power solutions be scalable and intelligent.

It is important, therefore, that modern power solutions provide usable data that not only tracks their own health, but also can collect and transmit information that allows an operations team to make better informed decisions on how to best manage the entire network. Voltage, amperage and temperature monitoring, for example, can provide actionable insight in the following ways:

1. Within a co-location facility – understand the actual power usage when access to the metering device or monthly power usage invoice is not available. Such information will prove useful for contract negotiations related to power consumption.
2. Provisioning analytics can determine at what time of day the highest power consumption takes place and offers the ability to tailor tasks for periods when power is less expensive and places a lesser demand on the grid.
3. Mitigation – with advanced monitoring, the ability to avoid disruption of services exists by enabling the ability to recognize and identify issues before a failure occurs.

Each of these areas, and more, may be improved through the effective use of power monitoring.

2. Technology Driving a Shift in Network Architecture

As technology, media, and other sectors push an ever-increasing number of modern applications in such diverse markets as residential, healthcare, entertainment, manufacturing, farming, transportation and hundreds of others, the speed and latency of traditional networks simply cannot keep up. There is a need for all forms of broadband networks – fiber, copper, wireless, etc. – to work together seamlessly to carry the information needed to allow the continued advancement of the promise of the IoT, autonomous vehicles, and hundreds of other applications yet to come.

With the accelerating complexity of available “connected” products, and even those that are only imagined now, it is important to find a common denominator that can bring some level of order or commonality. This may well be the fact that all of the parts, from the tiniest sensor inside a suburban home’s washing machine, to the complex computers that run statewide networks must be powered. This fact provides engineers with a methodology to monitor much of the energy health of 10G networks.

Meanwhile, in the increasingly automated and connected homes of today, power reliability and quality become ever more critical as IoT and connectivity demands increase. According to a recent analysis by Emergen Research, “The global power monitoring market size is expected to reach $5.86 Billion in 2028 and register a steady CAGR over the forecast period.”

Power monitoring equipment is now available for the homeowner to monitor and troubleshoot incoming power and power usage throughout the day. As solar and alternative energy sources become more affordable and utilized, the ability to monitor and ensure the requirements are being met, increases. As power monitoring capabilities move to the level of the homeowner, how much more critical is the system intelligence for the network power, whether HFC, DOCSIS 4.0, PON, EPON, etc. All of these levels related to power availability and quality are essential for post pandemic workers to stay connected and ensure network QoS for the rapidly changing work force.

With advanced monitoring, the ability to avoid disruption of services exists by enabling the ability to recognize and identify issues before a failure occurs. Through constant measurement and comparison against expected power thresholds, deteriorating power or other conditions can trigger the necessary actions to avoid intermittent, or even total loss of power. Such mitigation ensures reliable network service and the highest level of customer satisfaction.

3. 10G Speeds Demand Distributed Architecture

With remote work becoming the norm since the pandemic, the 10G initiative is being brought to the forefront quicker than originally anticipated and along with it, the need for clean, reliable power to service the network and the end-use products in the residence and elsewhere.

Distributed Access Architecture (DAA) migrates the intelligence and functionality that had once existed in head ends and data centers out much nearer to where these things are actually applied. In other words, the data remains closer to where it will actually be needed, decreasing the delay of making a round trip to the head end. (Figure 1)

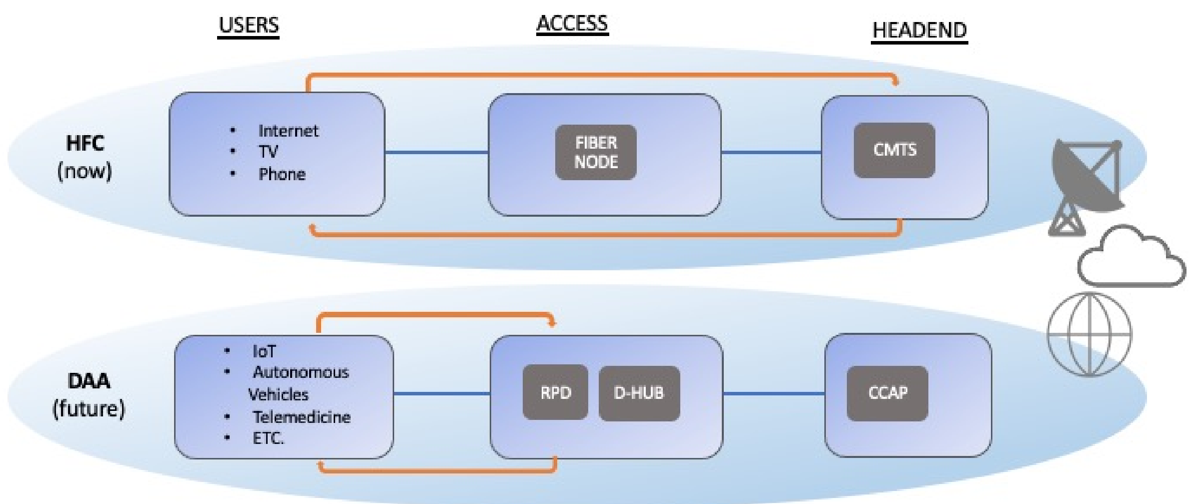

Figure 1 – DAA Migrates Intelligence & Functionality Closer to User

Consider autonomous vehicles. In this example, a future vehicle designed to operate at Level 5 (true driverless) will not only need to rely on the information available on-board the vehicle, but also such data as what traffic may be approaching from around a blind corner. This information is very location-specific, and therefore it would be inefficient to forward all of this to a central data repository at a head end merely to push it back to the vehicle.

With distributed access "local" information can stay local, lessening the burden on networks to carry every bit of information to and from a central hub. Thus, speed is increased, and latency reduced.

Moving nodes closer to end users will result in a network that is more complex. Equipment with the intelligence to move data within the node, as well as beyond, will be deployed. To support these intelligent nodes, basic infrastructure such as secure shelter, health monitoring, and intelligent power sources must be available.

As equipment is deployed deeper in networks, exponential growth of equipment locations naturally occurs. Each network element must have the ability to sense possible problems, and to transmit the need for support before a failure occurs. Imagine the possible problems in our autonomous vehicle scenario should a network failure occur. Like all other critical equipment, power panels should have such intelligence and capability.

4. Power Panel Design is Evolving

The main function of power panels, of course, is to provide the power needed by each piece of network equipment in a given site. Whether using fuses, circuit breakers, high-, medium, or low-current options, connectorized or lug outputs, or any of dozens of other technology options, the basic functionality of these panels is the provision of power to each piece of equipment that needs it.

The latest generation of power panels makes the integration of power management directly in the power platform easier than ever before. While power panels have provided the ability to monitor their own health in the past through simple alarm closures, the intelligence to report and, more importantly predict problems is now available within the panel itself.

Within the latest generation of power panels, power monitoring has been isolated from the provision of power itself, meaning that, depending on the design of the actual panel, monitoring devices, such as "hot swappable" cards, may go "bad" without interrupting the flow of power to critical equipment. Thus, the card may be removed for service or replacement without affecting services.

Power panels have had the ability to deliver simple alarm information via output contacts for some time. These output contacts have been tied into a network's alarm systems for decades. With the critical nature of traffic within every distributed node however, intelligent information that serves to predict problems before they occur is imperative.

Within a node, depending on its size, multiple panels may be required to supply the power necessary for all equipment to function at peak performance. In this case, the ability to "daisy chain" multiple panels over a serial cabling scheme which then use a single network connection to transmit critical data back to an operations center will simplify monitoring of multiple bays of equipment.

Intelligent power panels should monitor current at the individual circuit level, providing detailed information that is simply not available with feed-level monitoring or threshold alarming. By measuring parameters such as current per individual circuit, total input bus current, panel input voltage, temperature, and data from external probes, personnel now have access to a much more complete data picture, allowing operations to determine actual current usage, perform trend analysis, and gain critical insight into equipment performance. This data facilitates proactive action to avert disruptions to service as related to power and power quality.

5. From Alarm Closures to Predictive Analysis

Simple Network Management Protocol (SNMP) is a way to monitor network devices that are on an IP network. Information is requested by an SNMP Manager about the device and connected equipment and status. With baseline measurements and continuous updates, equipment performance can be tracked and controlled. Additionally, SNMP traps sends alerts instantly whenever an event occurs.

The SNMP manager interacts with a network device and its connected equipment. Through the local area network (LAN), an SNMP manager routinely requests information, such as power provisioning, remote site management and circuit threshold data from network devices. This information is recorded and stored via the SNMP manager and can be viewed in a user-friendly table or graph. The data collected can often be displayed by equipment type and location, performance and power usage, and typically monitors threshold levels which allows proactive maintenance with equipment, mitigating downtime by allowing maintenance to be scheduled on a routine basis.

SNMP Traps send instant alerts from the network device when an event occurs. The network device sends these messages without being prompted by a request from the SNMP manager. As soon as an event occurs an alarm is triggered indicating where the event occurred. Immediate access to equipment alarms can prevent unnecessary downtime. During an event, an SNMP manager promptly notifies the local technician who can then make repairs or prevent equipment damage

6. Using data to drive energy improvement in the network

Troubleshooting and prevention alone is a compelling reason for intelligently monitoring power supplies throughout the network. Still, with a growing emphasis on energy efficiency and cost savings, a compelling argument can be made to use data as a way to drive continuous improvement in energy usage in each individual location, as well as across entire networks. Consider each of these scenarios:

Within a co-location facility the ability to understand the actual power usage as measured by the service provider’s own equipment, allowing comparison to readings from the metering device or monthly power usage invoice as provided by the power company. Such information will, along with confirming usage, prove useful for future contract negotiations related to power consumption.

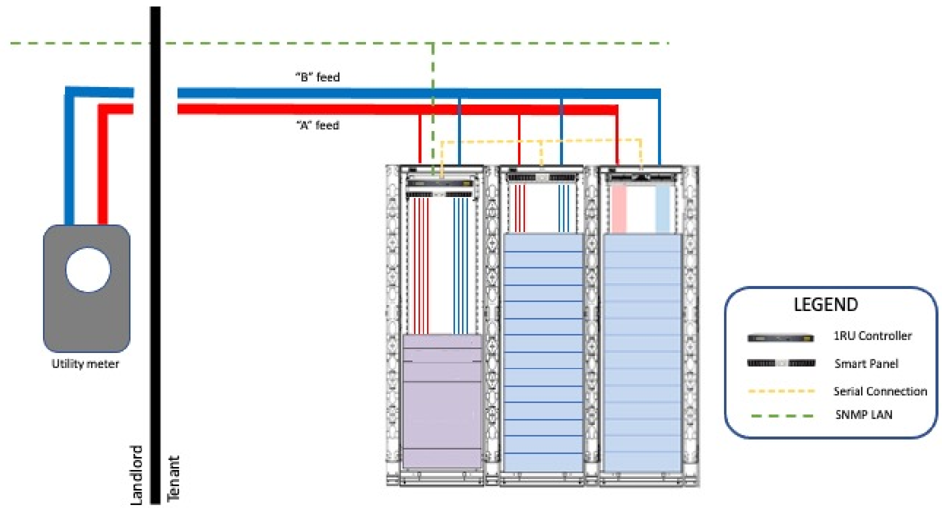

Figure 2 – Co-location Power Scenario

Perhaps even more critically, provisioning analytics will help determine the time of day or even day of the week when the highest power consumption takes place. This knowledge will contribute to better planning and cost savings by offering the ability to tailor tasks to occur during periods when power is less expensive. Further, the network provider will place a lesser demand on the power grid based on this information and planning.

7. Conclusion

With network speeds increasing exponentially, the need for good, reliable and steady power has never been greater, while changing network architectures indicate that it is equally important that power solutions be scalable and intelligent.

Modern power solutions must provide usable data that not only tracks their own health, but also can collect and transmit information that allows an operations team to make better informed decisions on how to best manage the entire network. Voltage, amperage and temperature monitoring can provide actionable insight in both the inside plant (ISP) and the outside plant (OSP), allowing engineers to determine key information such as time of day power consumption or, more importantly the ability to avoid disruption of services due to power loss.

Abbreviations

CAGR	compound annual growth rate
CCAP	converged cable access platform
CMTS	cable modem termination system
DAA	distributed access architecture
EPON	Ethernet passive optical network
HFC	hybrid fiber coaxial
IoT	internet of things
ISP	inside plant
LAN	local area network
OSP	outside plant
PON	passive optical network
QoS	quality of service
RPD	remote PHY device
SNMP	simple network management protocol

Bibliography & References

Power Monitoring Market Size to Reach USD 5.86 Billion in 2028, Emergen Research, June 2021

R. Abbi, et al "*Powering the future 10G access networks - An End-to-End Perspective",* SCTE Paper, 2020

R. Abbi, S. Dharanikota, "Powering the future of 10G Access Networks", SCTE Journal of Energy Management, September 2019

