
Daniel H. Cote, PE, Senior Technical Specialist, McKim & Creed1*
Tim Baldwin, PE, Senior Vice President, McKim & Creed2
1McKim & Creed, Inc., 1365 Hamlet Avenue, Clearwater, FL 33756-3331
(*correspondence: dcoxe@mckimcreed.com, 727-442-7196)
2McKim & Creed, Inc., 1730 Varsity Drive, Suite 500, Raleigh, NC 27606-2689

KEYWORDS
DNP3, distributed network protocol version 3, cellular machine-to-machine, M2M, data plan, SCADA, modern advanced protocol, telemetry communications modernization, Ethernet

ABSTRACT
Reliable communication is the lifeblood of modern Supervisory Control and Data Acquisition (SCADA) systems. Many of our existing SCADA systems use private radio networks, but these networks are reaching the limits of their capacity. System maintenance can be labor intensive, and the Federal Communications Commission (FCC) continues to place restrictions on the spectrum by re-farming to narrower bands. Increasingly, utilities departments want to get out of the radio business.

So what is our best bet for communications in the future? Utilities are moving away from private radio networks toward machine-to-machine (M2M) solutions offered by cellular providers. These M2M data plans appropriately address the fundamental concerns of reliability, emergency response, ease of use and security. By offering data plans for $5 to $20 per month, they are extremely cost-effective.

But here’s a catch; these M2M plans also come with small data usage budgets, typically 5 to 25 MB per month. Can we do everything we want to do within these small data plans? SCADA typically uses very small amounts of data; however, the overhead associated with Ethernet Protocol and security measures makes data usage prediction difficult.

We conducted a ‘Proof of Concept’ (POC) test to simulate existing and future SCADA needs of an East Coast utility. Using modern advanced protocol—DNP3— we simulated normal data collection, as well as failures, where the protocol would automatically buffer and backfill historical data.

The data usage for all these scenarios was measured during the POC testing, so that we now have a comprehensive and realistic understanding of efficient data usage and a basis for moving forward into the upcoming SCADA upgrade.

Introduction

The Virginia Beach (Va.) Department of Public Utilities operates 406 sewage pumping stations and 33 water supply facilities of various sizes and descriptions. These systems have seen several generations of SCADA technology over the years. The existing SCADA system uses licensed UHF serial radio technology, along with unlicensed spread spectrum radios, to provide communications.
with the distributed RTUs and PLCs at the remote sites. The existing PLC and RTU hardware has become obsolete, and the data capacity of the existing radio system has nearly reached the limit of its data capacity. McKim & Creed was selected to engineer a Telemetry Communications Modernization Project to take the Virginia Beach Utilities into the future.

Stage ONE of this project, which was completed in 2010, provided a System and Goals Assessment phase. Some of the findings of this phase were as follows:

1. Flow monitoring and data collection capabilities need to be expanded to meet operational and engineering needs, regional standards and future needs.
2. PLC/RTU equipment standards need to be updated to eliminate outdated equipment.
3. Communications infrastructure needs to be upgraded to meet future needs.

Stage TWO of this project, which was completed in 2011, provided a Preliminary Engineering Report. Some of the highlights of this report were as follows:

2. Adopt a new PLC hardware standard. Three hardware platforms were chosen for evaluation.
3. Consider cellular machine-to-machine (M2M) data plans as the proposed communications infrastructure.

Stage THREE of this project, which is currently under way, includes a Proof of Concept (POC) test which provides the following:

1. Install each of the three proposed PLC hardware systems to provide side-by-side comparison of the proposed hardware and to provide owner experience for the purpose of comparison and evaluation in a broad range of criteria and test conditions.
2. Utilize the DNP3 protocol to provide a comprehensive understanding of the features, benefits, advantages and disadvantages of this protocol.
3. Install each of the three test PLCs on its own cellular M2M data plan to demonstrate the features and discover the pitfalls of SCADA using cellular M2M communications.

**Machine-To-Machine**

In recent years, cellular providers have increasingly encouraged the development of customers in small, data-only niche markets. These applications, known as “Machine-to-Machine” or M2M plans, include a surprising variety of applications, including traffic signals, vending machines, ocean buoys, kiosks, home health care monitoring and alarming devices, generators, pipelines, proprietary web-based SCADA applications, and a wide variety of conventional SCADA applications.

In large SCADA applications, the one objection to cellular communications has always been the historically high monthly recurring cost. In years past, the typical cost of cellular service for SCADA could be $50 per month or more, which can be generally unattractive for SCADA. At this price point, the public utilities department could typically build its own private radio network as a more cost-effective, long-term solution.

With the development of M2M solutions in the competitive cellular market, the price point for cellular communications can now be less than $10/month. At that price point, the financial aspect of cellular communications becomes much more attractive when compared with the cost of...
purchasing and maintaining radios, towers, cables, repeaters, path studies, and polling strategies, as well as the burdens of troubleshooting and repair.

There are a broad range of advantages and disadvantages when comparing cellular with privately owned system. This paper does not purport to evaluate these numerous aspects. This paper is intended to address the following: DNP3 protocol and M2M plan size.

![Figure 1: Comparison of data capacity and monthly cost.](image)

**So How Small Are These M2m Data Plans?**

Figure 1 shows typical examples of data capacity and monthly cost. Tier 1 data plans start as low as $1/month, with data usages of about 1MB. For our evaluation, we are targeting a price point of $10/month, which provides data usage of 25 MB/month. For comparison, the existing serial radio could be said to provide about 12 MB/month. This is based on polling hundreds of stations, so the effective serial data capacity is divided between stations. If 120 stations are polled in two minutes, the connectivity to any one station is limited to about one second every two minutes.

However, the data capacity of the M2M link is misleading because communication data is sent by Ethernet, which carries with it an additional burden of overhead, which will be explained in this paper. DNP3 protocol was chosen in order to maximize the useful capacity of a Tier 1 plan, so that the limited capacity of the data plan is efficiently utilized.

**Why Choose DNP3 Protocol?**

DNP3 is a well-established, open-standard protocol. It is widely used in power and gas utilities, and is gaining popularity in water and wastewater utilities. Some advantages include:

- Non-proprietary: Its use is not limited to specific equipment suppliers.
- Versatile: It is highly configurable to meet your needs.
- Efficient: For best use on small data plans.
- Automatic Backfill: Data is never lost.
- Compatibility with HMI: Third-party software is not needed.

DNP3 operation is based on the PLC’s ability to buffer and send events. An event is any analog measurement or digital change in state which needs to be communicated from the PLC to the SCADA host. Each event is time/date tagged so that the real time of the event is accurately known and is not dependent on when it arrives at the SCADA host.

Presented with permission of authors by ISA 2014
Presented at 2014 ISA WWAC Symposium; http://www.isa.org
As shown in Figure 2, up to 20,000 events can be stored in the PLC. These are retrieved by the SCADA host on any chosen time base, but the time base of the buffered data is never lost. Therefore, if communications are delayed because of unforeseen failures, the event data will eventually be retrieved when communications are restored; historical trends are backfilled and no data is lost.

Figure 3: Time-stamped trends of pump status and wet well level.

As shown in Figure 3, time-stamped data shows the exact time pumps start and stop, which is not typically available with conventional serial polling. Data quality is improved for purposes such as operational troubleshooting, hydraulic modeling or energy management.
In DNP3, data can be retrieved for trending in many different ways. In Figure 4, the measurement is made every 30 seconds, even though the RTU is polled only once every two minutes. With DNP3, you can have complete flexibility in the method of data collection, which is adjustable for every data point. As shown in Figure 4, the PLC can generate one event (reading) every 30 seconds or any time basis desired. This method can be wasteful of data plan utilization if a short time basis is chosen. Data collection every 30 seconds results in 2,880 events collected per day for that one signal.

In DNP3, data is often retrieved by dead band. It is thought to be wasteful of data plan capacity to send a reading if the signal value has not changed significantly, so the PLC is programmed to create events only when the value changes by a selected dead band. Figure 5 illustrates that a larger dead band generates fewer events, but it also results in a less informative trend.
Figure 6: Example of events generated using a smart dead band algorithm.

With all these examples, logging of data can be achieved in a variety of ways. When using an M2M data plan, the goal for efficient use of bandwidth is to provide informative data and trends using as few events as possible. In this test, we have experimented with logging data using a “smart” dead band algorithm. With conventional time based on dead band trends, as shown in Figures 4 and 5, it is disappointing that you often cannot capture the highest or lowest value. In the PLC you cannot predict the future, so that at any given moment the PLC has no way of knowing if the current value is the peak or if the signal will continue to rise. Therefore, events do not typically capture the peaks.

In this study, we have experimented with development of a smart dead band algorithm. As shown in Figure 6, the PLC is programmed to remember the previous maximum or minimum value since the last event was posted. Then, at a later time, the PLC can create an event which is time-stamped to occur in the past, when the peak actually occurred. Using this algorithm, the event trend can provide excellent usable process information while minimizing the number of needed events. Note that the trend in Figure 6 creates 260 events per day, while the events in Figure 4 and 5 require considerably more events to create less informative trends.

Ethernet Communications

Communications on M2M data plans require the data to be converted to Ethernet. When SCADA data is communicated using Ethernet, the usable content of the DNP3 protocol is encapsulated into the larger packets of the Ethernet protocol.
Figure 7: Ethernet communications illustrated as buses.

Figure 7 illustrates Ethernet communication of SCADA data. The bus represents the packet which must be sent by Ethernet. The DNP3 data is considered to be a passenger in the bus, known as the payload. Often, the packet is much bigger than the payload. This represents the overhead associated with Ethernet communications in SCADA.

Figure 8: A comparison of Ethernet overhead and DNP3 payload size in SCADA.

The measured typical data quantities of Ethernet overhead and SCADA payload are shown in Figure 8. Using this data, and experimenting with various data collection algorithms, we were able to provide real measurements of M2M data plan usage as follows:
The tabulation in Figure 9 shows the typical monthly data usage based on various event counts and on polling once every two minutes. An event count of 10 events per poll would result in a data usage of only 9 MB/month. Recall from Figure 1 that a Tier 1 data plan can support up to 25 MB/month, so event usage at or below 60 events per poll should be achievable using a Tier 1 M2M data plan. By examination of normal data needs and utilization of efficient algorithms of data collection, this data rate provides a very generous budget for anticipated data usage in SCADA.

**Problems Encountered**

Sometimes the behavior of communication systems and components can operate one way in a test environment, but can behave quite differently when deployed with real-world conditions. Figures 10 and 11 illustrate the problems encountered when the POC test equipment was deployed under real conditions. These provide some important lessons learned for Ethernet applications of SCADA on cellular networks.

The graph in Figure 10 illustrates the expected data usage for SCADA communications once every two minutes. “Wire Shark” software was used to capture the packets. Each poll consisted of three packets: read, response and confirm.
Figure 11: Data usage and protocol steps: unexpected results.

Compared to Figure 10, the graph in Figure 11 shows the actual data usage and protocol steps which were captured when the PLC was deployed on a cellular network. The data was successfully delivered, but data usage was higher than expected. Examination of the “Wire Shark” steps showed that the repeated retransmission of the “READ” command was triggered, causing unnecessary additional network traffic with each poll. This behavior of the Ethernet communications would cause significant waste of data plan usage, may result in upsizing the data plan to Tier 2, and could increase the data cost for 400 stations by more than $6,000 per month.

Finding the cause of this bad behavior was complicated because of finger pointing. Suspected causes ranged from the SCADA software, cellular network, PLCs, network IT, routers and firewalls, with each supplier blaming the others. After significant testing and research, the cause and cure for the unwanted behavior were revealed:

*The Transmission Control Protocol (TCP) retransmissions were caused by the behavior of the TCP Ethernet services of the Windows operating system in response to latency behavior of the cellular network.*

**Explanation**

TCP is a behavior of the Ethernet protocol that guarantees delivery of each data packet. Each packet sent using TCP is expected to be followed by an acknowledgement. TCP uses Return Trip Time (RTT) to measure the time between sending a packet and receiving the acknowledgement. TCP uses a time limit known as Return Trip Timeout (RTO) to decide how long to wait until the packet is assumed to be lost. Whenever a packet is considered to be lost, TCP immediately sends a duplicate packet (TCP Re-Transmission), and then doubles the RTO.

TCP is always striving to optimize the speed of transmission. This is accomplished by keeping the RTO as short as possible. TCP uses an algorithm known as SRTT to “smooth” the RTO, lowering it after each quick RTT to keep the RTO as short as possible, which is just a bit longer than the expected RTT. This SRTT algorithm is automatic and cannot be disabled.
The problem with cellular communications with SCADA is that the latency of the RTT behavior is not appropriate for TCP. With cellular communications, the first packet typically takes 2.5 seconds or longer to make a connection. Once the connection is made, the subsequent packets are very quick. However, if the line is quiet for more than 16 seconds, the cellular line goes dormant, and the next packet again requires 2.5 seconds to connect.

The dashed line in Figure 12 represents the RTO. During every poll, the SRTT algorithm shortens the RTT, so that as soon as the next poll is attempted, the longer packet RTT will cause multiple TCP retransmissions.

TCP is not suitable for SCADA communications on a cellular network.

Solution: Use User Datagram Protocol (UDP) instead of TCP. UDP is an alternate protocol used by Ethernet. UDP is judged to be less reliable than TCP because UDP does not guarantee delivery of packets. Instead, UDP sends packets as they are received, with no further action of monitoring or retransmission.

When UDP is used with SCADA, the responsibility for transmission of packets is no longer taken by the Ethernet protocol. Instead, the DNP3 protocol is used to guarantee data delivery.

**Conclusions**

- M2M data plans can be cost effective, but efficient operation requires careful attention to details.
- A versatile protocol such as DNP3 is needed for best results.
- TCP does not work well with M2M SCADA. PLC equipment and protocol must be able to guarantee data delivery using UDP.
List of Acronyms:
SCADA........................................Supervisory Control and Data Acquisition
FCC.............................................Federal Communications Commission
M2M............................................machine-to-machine
POC..........................................proof of concept
DNP3.........................................Distributed Network Protocol Version 3
UHF...........................................ultra-high frequency
RTU...........................................remote terminal unit
PLC..........................................programmable logic controller
MB.............................................megabyte
TCP..........................................Transmission Control Protocol
RTT............................................Return Trip Time
RTO...........................................Return Trip Timeout
SRTT.........................................Smooth Return Trip Time
UDP.........................................User Diagram Protocol

Daniel H. Cote, PE: For nearly 40 years, Dan Cote has specialized in water/wastewater design, instrumentation design, wastewater reclamation systems, SCADA systems, plant operations, communications and computer programming. He developed the comprehensive hydraulic model Forcemain©, which combines water system, gravity and forcemain wastewater systems, and reuse modeling with GIS integration in a single program. This hydraulic model is used by numerous cities and counties for both the water distribution and sewer system.

Most recently, Dan has focused on the sustainability aspects of SCADA technology, working to develop green techniques, programming, strategies and models that can cut power requirements, reduce costs and preserve resources.

Contact: dcote@mckimcreed.com