EFM Data Communications – Problems and Solutions

Rusty Fields – Professional Services Engineer
Weatherford Int'l / CygNet Software
1040 Schlipf Road, Katy, Texas 77493

Introduction

Natural gas companies in all segments – upstream, midstream, transmission and distribution – have deployed Electronic Flow Measurement (EFM) devices on a massive scale. Since the information contained within the EFMs is crucial to the company's operations, robust and reliable systems to communicate with EFMs are required.

The EFM data needs of some departments are mission-critical. Gas controllers need real-time information to safely and effectively operate large stations and systems. They need to know what is happening now. Other departments can live with near real-time data. They need to know what happened over the last couple of hours, for example. Finally, some departments might only need daily and monthly data.

EFM data communication systems must be flexible.

Data Overload

The EFM data communications system for a major gas transmission system with thousands of EFMs and RTUs must handle huge volumes of data. Interestingly, the department with the most time-critical need for data, Gas Control, often needs the least amount of data from the EFM devices. Gas controllers need the data in real-time but they don't need a lot of it. They need to see pressures, temperatures, today's volume, yesterday's volume, and often little more.

However, the gas measurement department, with the least time-sensitive demand for data, needs the most data. Why? Because the AP! 21.I standard, as implemented by most gas companies in the United States, requires that EFMs create large files of hourly and daily data, event logs, and other audit trail information for each measurement tube. An EFM at a multi-run station with station totals and other information.

What is RF communication like in the field?

To understand and improve success in the collection of SCADA and EFM data you must first understand what's in the field, their frequencies and communication methods.

Frequency ranges typically utilized in the field are 900 MHz and 2.4 GHz. These frequency ranges were released as "junk band" or public use by the FCC in the 1980's and 1990's. These frequencies were adopted by everything from cell phone manufacturers, wireless home phones, two way handheld radios and many more.

Statistics indicate that there are currently between 750,000 and 1,200,000 radios deployed in the oil and gas fields across the U.S. and sales expectations for 2013 are upwards of 100,000.

In the O&G world we can expect a great many of these to impact us in the Bakken play.

As frequency increases the signal is easier to deflect so as you move from 900 mhz radios to 2.4ghz you can expect to deal with more signal deflection and interference from towers, tree's buildings etc. Simply put, the signal is easier to block and redirect than the older 900 mhz range.

Radio technology is now making it easier to select a frequency and ports, and manage them. However, many installing radios continue to use the default RF network and ports. This causes adjacent properties to conflict with each other because they constantly try to negotiate and establish connections with sites that are not within your companies operation. A radio "traffic jam"!

In a perfect world, each company in each field would have their own assigned IP's, TCP port range and RF network range. But since we don't live in that world, one company will pick ranges that work for them, and place towers and repeaters as they require them. Many times this increases the failure rate for another company so they make changes or add repeaters etc. and the fight continues perpetually. Signal to noise ratios decrease shortening RF range and increasing failures.

A visual example pertinent to many

The Wattenburg field in Northeast Colorado is a prime example of RF ranges that have been continuously reduced over the last several years from as far as 32 miles to now less than a 6 mile range. Some companies are more successful than others in defending their ranges. However, overall success is declining and the noise floor is increasing thereby causing communication problems for field engineers and EFM data collection.

***So what can you do about the problem*?**
How do you recognize, and monitor for predictive failures caused by this pattern of behavior?

1. Review templates for data being requested that is unused in the point schema and remove.
2. Count those bytes…know what is going out and coming in and out!
3. Monitor request response times, transaction sizes, retries and trend for degradation and predictive failure monitoring.
4. Understand the environment you are working in and streamline your RF network to avoid conflicts with neighboring properties.
5. Be creative about statistical data reporting and monitoring.
6. Monitor and track scheduled tasks and reduce overlapping requests, or duplication.

Envision the similarities between airline flight concentrations and radio traffic. How successful would Air Line Carriers be if they operated with their own individual agendas, standards and requirements? Our air ways would be in total chaos!

Similarly, Oil & Gas fields are operating in "Chaos" due to unlicensed wireless radio transmissions!

Common problems and troubleshooting

1. Unable to poll a group of devices

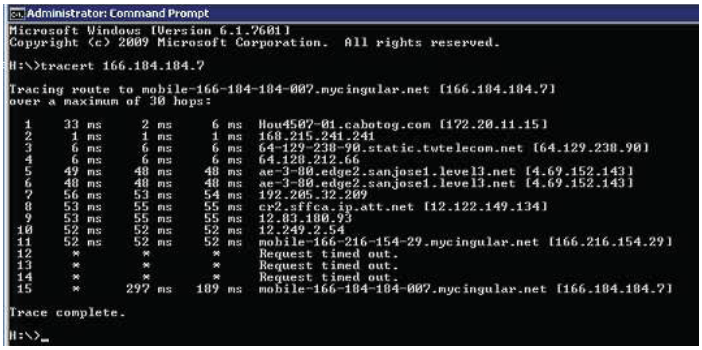
Questions to ask yourself

- What is the common element?
- Are they in the same master radio?
- Are they on the same multi-drop physical com line?
- Are they the same device type?
- Are they making it out to master radio?

So how do you find the answers
In your SCADA software find the IP address being used In the com device setup.

PING the master radio modem IP address
If Successful the corporate and com provider networks are OK

If the PING is unsuccessful
TRACERT to the master radio modem IP address and see where the connection is broken.
NOTE not all hops on the comm provider network will show up, some devices do not responds to ICP packets, link ping and TRACRT.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

H:\>tracert 166.184.184.7

Tracing route to mobile-166-184-184-007.mycingular.net [166.184.184.7]
over a maximum of 30 hops:

  1    33 ms     2 ms     6 ms  Hou4507-01.cabotog.com [172.20.11.15]
  2     1 ms     1 ms     1 ms  168.215.241.241
  3     6 ms     6 ms     6 ms  64-129-238-90.static.twtelecom.net [64.129.238.90]
  4     6 ms     6 ms     6 ms  64.128.212.66
  5    49 ms    48 ms    48 ms  ae-3-80.edge2.sanjose1.level3.net [4.69.152.143]
  6    48 ms    48 ms    48 ms  ae-3-80.edge2.sanjose1.level3.net [4.69.152.143]
  7    56 ms    53 ms    54 ms  192.205.32.209
  8    53 ms    55 ms    55 ms  cr2.sffca.ip.att.net [12.122.149.134]
  9    53 ms    55 ms    55 ms  12.83.180.93
 10    52 ms    52 ms    52 ms  12.249.2.54
 11    52 ms    52 ms    52 ms  mobile-166-216-154-29.mycingular.net [166.216.154.29]
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *      297 ms   189 ms  mobile-166-184-184-007.mycingular.net [166.184.184.7]

Trace complete.

H:\>_
```

Find the last successful hop whatever the next hop is will be the one broken.

IE you get to your DMZ router but can see nothing on the telecom provider network then you have a connection broken at between the DMZ router and the provider.

IF this is successful as in the example above then you need to research what is connected to the remote modem.

Typically will be a MASTER RADIO and or a TERMINAL SERVER. These are connected to the slave radios or local hardware via a wired connection.

Point being understand the physical layout of how devices are connected in the field and how they connect to your SCADA system.

What if the EFM collection system communication sends the request and data comes back but it's not correct or clean?

BAD / dead is not the same a dirty communication

What if a request is sent and you see the com bytes go out and you see a response come back but it then times out?

At this point you need to understand the protocol being used, Totaflow, Fisher, ModBus etc.. at least enough to know if the response is from the correct RTU or another device.

This can be caused by duplicate names or addresses in the field. Or a piece of hardware corrupting the data in the transmission.

A simple solution is to start rebooting the hardware from the RTU to the master radio polling after each is rebooted and locate the problem child.

I have recently seen terminal servers get corrupted after a storm and begin sending bad data. After rebooting everything else we rebooted the terminal server on the line and communications was restored.

Knowing the hardware and path is critical to your success in communications troubleshooting.

Knowing the communications protocol and being able to decipher it is also very important!

In the end RF communications world is cluttered, noisy and problematic with minimal diagnostics available at the SCADA level. So what do you do about it?

SNMP polling can provide critical information about the health of the hardware in the field,

A free tool available is SNMPGET available online.

OPC polling engines like Kepware also have this driver. Many options are available to monitor hardware at this level and will take some research on your side to pin down a solution that works for you..

What about DIGITAL OILFIELD?

Digital oilfield in its simplest form provides a network in the field in the same manner that your network is managed and maintained in the office using WIFI and ETHERNET communication.

More and more new measurement devices are coming with Ethernet and WIFI capability.

In short you will have a network in the field that will look like it is a part of your office network.

Even if connections to the RT's , Measurement and control devices connect via RF.

Many of the same hurdles will exist, you're still reliant on the communications provider to connect the two networks and hardware still exists that allows it to work.

What I believe is great about it will be how manageable it is and how it provides connectivity for Security, Video, VoiceOver IP phones etc.. We already know how dependable it can be since we use that technology at home, in the office and on our cell phones right now!

A few things to remember

Communications get sick before they fail. Monitor for slowness, errors, connection failures and act before they completely go down.

Balance your communication needs and revisit them every quarter to make sure the SCADA and Measurement polling are not polling for more data or more frequently than required.

Be creative with monitoring and alarming

Understand your communications world END to END.

Learn the basic fundamentals for all your field devices and protocols.

Know you can find improvements that will impact the success or failure of the SCADA system and Measurement data quality with some creative efforts.