RED TIGER SECURITY

Electricity for Free?
The Dirty Underbelly of SCADA and Smart Meters

Jonathan Pollet, CISSP, CAP, PCIP

July 2010

Table of Contents

Introduction

SCADA Systems control the generation, transmission, and distribution of electric power, and Smart Meters are now being installed to measure and report on the usage of power. While these systems have in the past been mostly isolated systems, with little if no connectivity to external networks, there are many business and consumer issuing driving both of these technologies to being opened to external networks and the Internet.

Over the past 10 years, we have performed over 100 security assessments on SCADA (Supervisory Control and Data Acquisition Systems), EMS (Energy Management Systems), DCS (Distributed Control Systems), AMI (Automated Metering Infrastructure), and Smart Grid systems. We have compiled very interesting statistics regarding where the vulnerabilities in these systems are typically found, and how these vulnerabilities can be exploited.

The purpose of this paper is not to disclose any specific exploits that will allow you to steal power from your neighbors, but we can give away enough meat in this paper to expose common vulnerabilities at the device, protocol, application, host, and network layers.

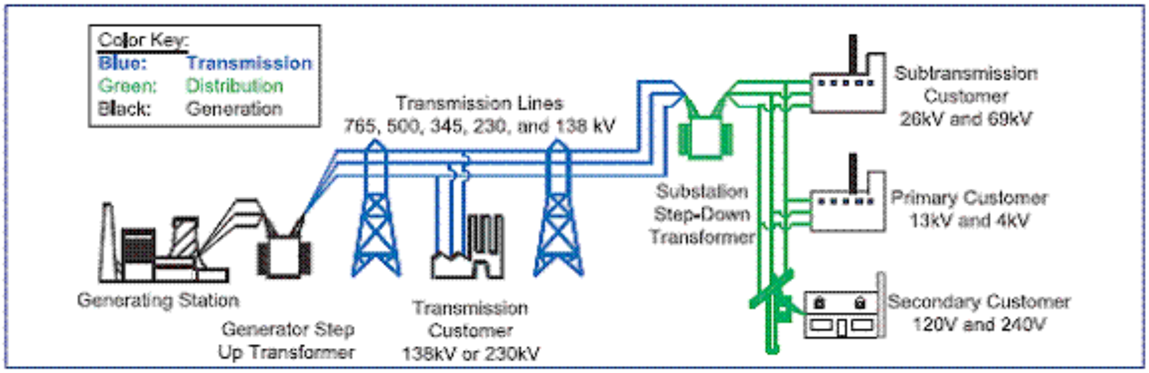
After performing hundreds of security assessments of systems that play a vital role in the production, transmission, and distribution of electric power, we now more than ever aware of the vulnerabilities that lie within these systems. The knowledge that we gained from these assessments out in the operational world has been combined with real incidence response experiences and the research that our team has done in this particular field of study.

We have seen PLCs (Programmable Logic Controllers), RTUs (Remote Terminal Units), as well as computing systems running HMI (Human Machine Interface) applications crash and fail when under high network traffic or malware. We have also participated in first responder's teams to cyber incidents that have caused immediate downtime and system failure for control systems that were compromised from worms, viruses, and malware. In several cases it was the Enterprise IT network traffic, heavy IT backup processes, or 3rd party network interconnections that were the cause of the SCADA incident.

The intent of this paper is to first provide a quick definition of how SCADA and Smart Metering systems are used in the generation, transmission, and distribution of power. Next, we will provide a summary of the 6-layer approach that we use to conduct vulnerability assessments of these systems. Lastly, we will summarize the vulnerabilities that we have found in these mission-critical systems to raise awareness to the need for increased hardening and security of these systems.

Power Generation, Transmission, and Distribution

Unlike other utility commodities like water or natural gas, electricity cannot be stored. Energy can also neither be created nor destroyed, only transformed into different types of energy. Electric Power Systems are typically grouped into three components. Power Generation covers the process of transforming various types of energy into electricity. Transmissions Systems step up the electricity to a higher voltage then transport and route the electricity over long distances for delivery to local markets. Distribution systems handle the process of stepping down electricity to proper delivery levels and distributing it to the final consumers of the power. The diagram below is a good example depicting these three components.



Color Key:
Blue: Transmission
Green: Distribution
Black: Generation
Transmission Lines
765, 500, 345, 230, and 138 kV
Subtransmission Customer 26kV and 69kV
Substation Step-Down Transformer
Primary Customer 13kV and 4kV
Secondary Customer 120V and 240V
Generating Station
Generator Step Up Transformer
Transmission Customer 138kV or 230kV

** graphic courtesy of NERC*

Power Generation

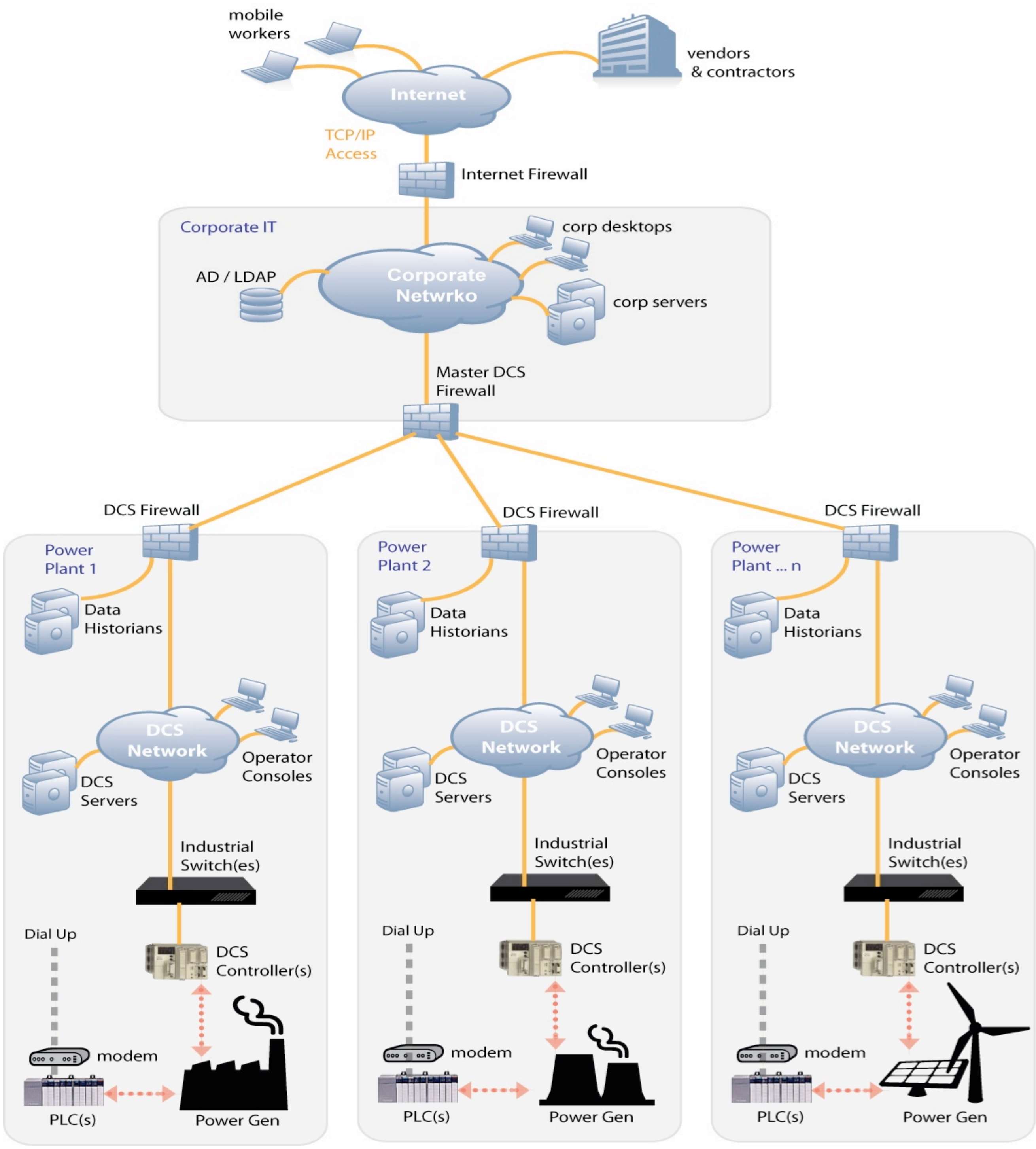
The Generation Process

Power generation is the process of converting non-electrical energy into electricity, and is the first step in the process of delivering power to consumers. Electricity is most typically generated at a power plant by electromechanical generators, which involve a spinning turbine to convert resident or stored energy into electricity.

Although there are many operational differences in the various forms of power generation from sources such as coal, natural gas, nuclear fission, flowing water, wind, and geothermal, all power generation operations share similar system components, including how the SCADA and control systems are connected back to Enterprise IT networks, the Internet, and other outside networks. Because of all of the generation systems are typically in one geographical location, and typically have little outside TCP/IP connections, of the three parts to the electric power industry, power generation tends to have less vulnerabilities than transmission and distribution systems. The diagram on the next page depicts a typical Power Generation network diagram, from the Internet down through the various Enterprise IT layers, to the physical equipment that produce electricity.

Typical Generation System Diagram

Power Generation - Typical Architecture



Power Transmission

The Transmission Process

Electric power transmission is the bulk transfer of electric power to the consumer. A power transmission network connects power plants, which are responsible for the generation of electricity, to substations. The substations in turn distribute electricity to industrial, commercial, or residential consumers.

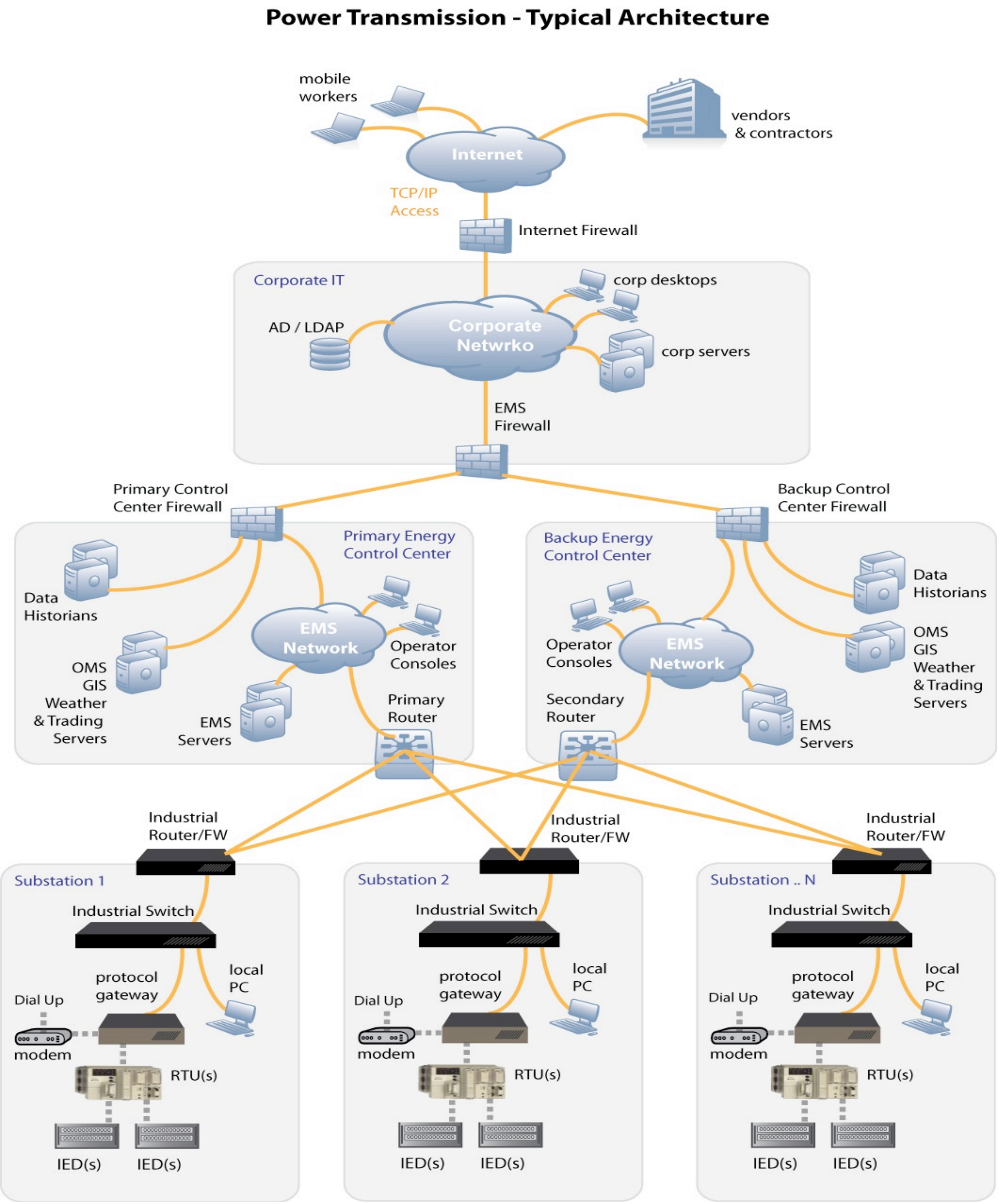
A power transmission network is also referred to as a “grid”. Multiple redundant power lines between points on the network are in place so that the power can be routed from any power plant to any load center through a variety of transmission routes based on the available path and cost of power.

The systems that reliably monitor and control the transport of electricity from power generation plants to the distribution load centers are called Energy Management Systems (EMS). These systems reside on the industrial control system or SCADA network. The EMS systems are typically only responsible for control of the power from after it is generated, up until it reaches the regional substations, where the DMS (Distribution Management Systems) then take over to manage the distribution and sale of power to individual customers.

EMS systems span large geographic areas, often rely on 3rd party telecommunications providers, and have connections to other business applications for some of the following functions: commodities marketing, weather monitoring, outage management systems (OMS), geographic information systems (GIS), protective relaying systems, and additional engineering applications for line efficiency calculations. For these reasons, EMS systems must be closely studied to insure that all components of the system are properly secured from external and internal threat vectors.

The diagram on the next page depicts a typical Power Transmission network diagram from the Internet, down through the various Enterprise IT layers, to the control room assets that monitor and control the flow of electricity. This network extends from the primary and backup control centers out to numerous regional substations that locally step down the voltage for local distribution.

Typical Transmission System Diagram



Power Transmission

The Distribution Process

As stated before, electric energy cannot be stored, so the amount produced through the electric generation process, and transmitted through the EMS (Energy Management Systems), must be immediately transported to a load where it can be consumed. Distribution Management Systems (DMS) utilize similar SCADA technologies as power generation and transmission systems. Distribution systems have the ability to remotely disconnect or shed large sections of load if required to protect the stability of the grid.

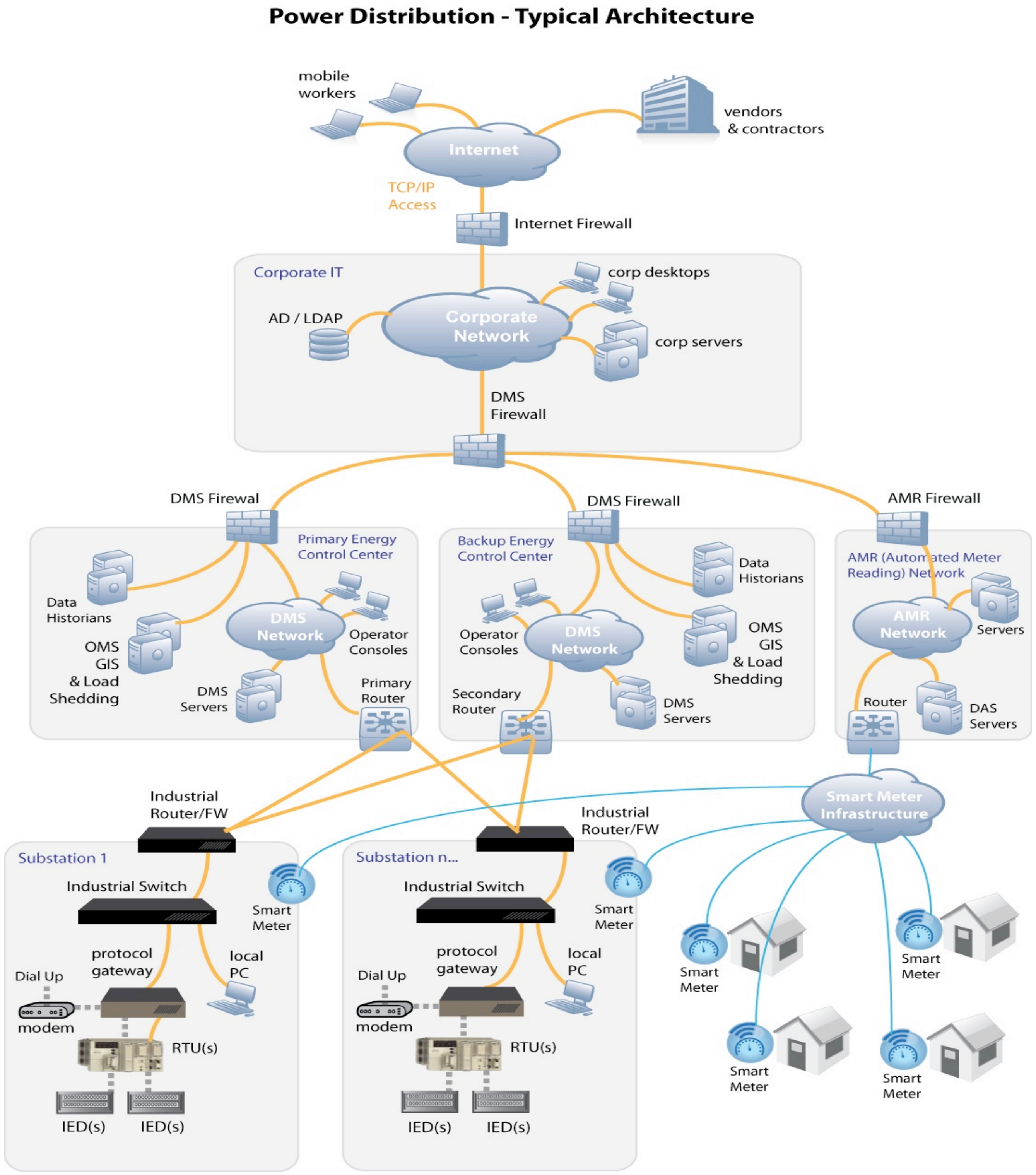
Distribution systems also have the requirement to monitor and bill off of the usage of the power. Prior to the movement to digitize power meters, the customer meter was an analog meter that was read manually by a meter reader technician. Over the past ten years, many power companies have invested in AMR (automatic meter reading) projects that either read the meter by rolling a truck through the neighborhood to locally electronically collect usage data wirelessly, or by remotely reading the meters through a variety of communication methods that include WiMax, Cellular, Broadband-over-Power, Power Line Carrier, or dual-use circuits shared by the DMS system.

At the end of 2009, the Obama Administration released billions of dollars under the federal stimulus act to drive technological innovation in the areas of clean technologies and smart-grid networks. The goal was to inject investments into the electric grid to break down the legacy barriers between generation, transmission, and distribution systems to eventually create a "Smart Grid" that can be used by power producers, transmitters, consumers, and researchers to facilitate a more robust and flexible power grid.

The first step in creating a "Smart Grid" involves converting the old analog electric meters into digital "Smart Meters" that can be polled remotely. This new injection of money into the electric industry fueled an entire industry of AMR and "Smart Meter" companies that manufacture digital meters than utilize a variety of communication methods for remote meter management and meter reading. These AMR systems are typically interconnected with the Distribution Management Systems, Enterprise IT systems, and other 3rd party networks.

The network diagram on the next page depicts a typical Power Distribution System, and common connection points with Enterprise IT systems, other outside networks, and Automated Meter Reading infrastructures.

Typical Distribution System Diagram



Methodology Used for SCADA Assessments

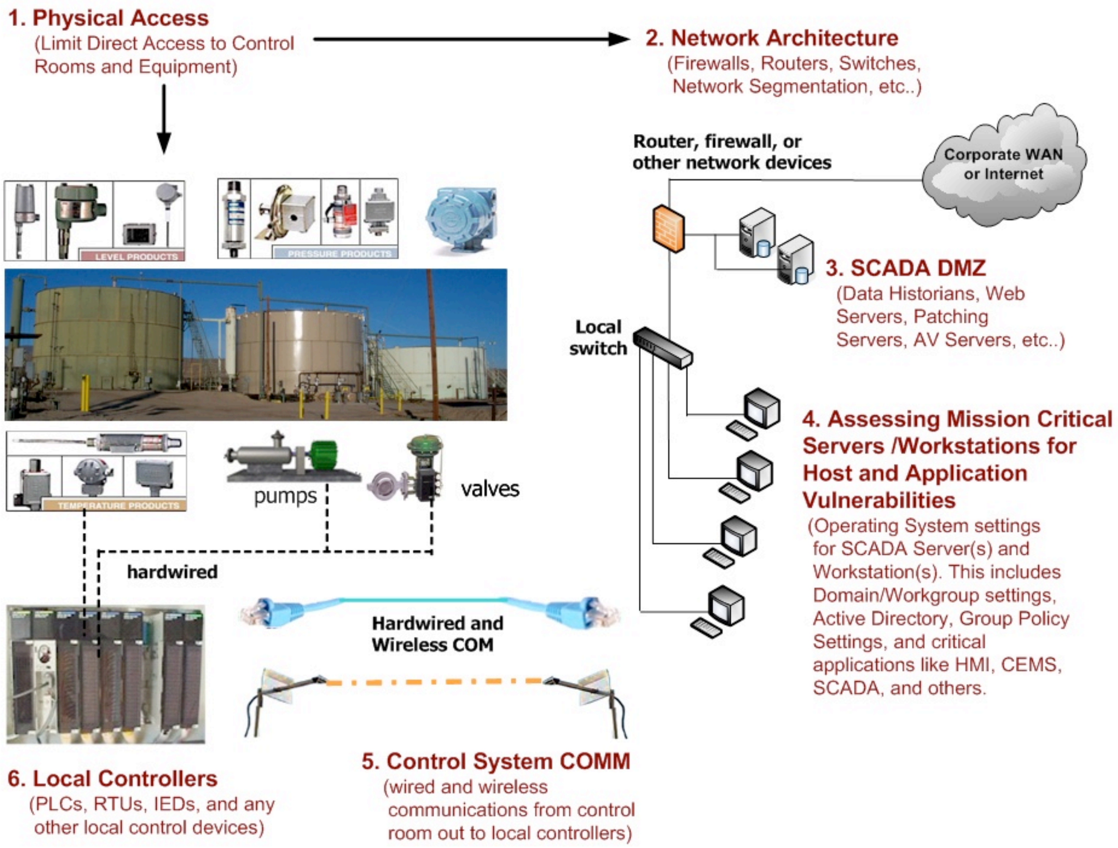
Red Tiger Security's Assessment Approach for SCADA

Over the past nine years of conducting security assessments of SCADA systems and performing research in the field of SCADA security, we have found that unless you use a defense-in-depth approach of assessing all components of the system, then small vulnerabilities can be used as threat vectors into the system.

Since we have been involved in the development and bench marking of several control systems security regulations and standards, we developed our assessment methodology in compliance with NERC CIP, ISA S99, and NIST 800-53 requirements for SCADA and Process Control Systems. We start with a review of the physical controls in place that restrict physical access to the systems used for monitoring and control. Then we use a "Follow-the-Wire" approach to analyze all of the digital components in the path from outside connections, through the network infrastructure, computing systems, applications, protocols, and lastly the field devices.

The diagram below shows how our six layer approach maps to the physical control systems network infrastructure, hardware, applications, protocols and field equipment.

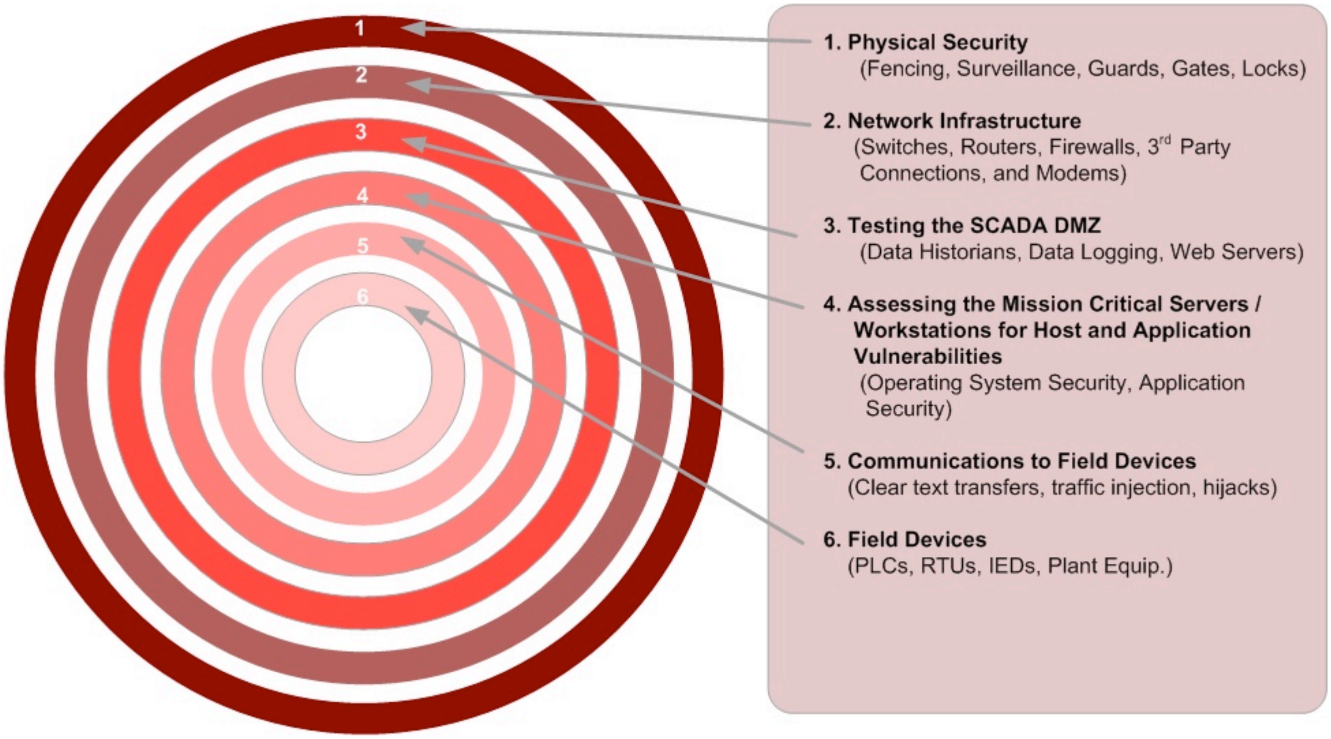
Control System Component Layers Involved in Security Audit


1. Physical Access
(Limit Direct Access to Control Rooms and Equipment)
2. Network Architecture
(Firewalls, Routers, Switches, Network Segmentation, etc..)
Router, firewall, or other network devices
Corporate WAN or Internet
3. SCADA DMZ
(Data Historians, Web Servers, Patching Servers, AV Servers, etc..)
Local switch
4. Assessing Mission Critical Servers /Workstations for Host and Application Vulnerabilities
(Operating System settings for SCADA Server(s) and Workstation(s). This includes Domain/Workgroup settings, Active Directory, Group Policy Settings, and critical applications like HMI, CEMS, SCADA, and others.
LEVEL PRODUCTS
PRESSURE PRODUCTS
TEMPERATURE PRODUCTS
pumps
valves
hardwired
Hardwired and Wireless COM
5. Control System COMM
(wired and wireless communications from control room out to local controllers)
6. Local Controllers
(PLCs, RTUs, IEDs, and any other local control devices)

Our assessment approach was designed to ensure that each protective layer helps secure the layer(s) below it. For example, the physical controls should protect access to the network infrastructure, which should restrict access over the network to the DMZ and host systems down in the control room environment. Since the field devices do more than just monitor the system, and are used for control functions, these are the most vulnerable and have the biggest impact to the reliability and availability of the system. That is why SCADA field devices must have the most protective controls in place.

This is the same methodology and approach that we use for assessments of DCS (distributive control systems), EMS (energy management systems), DMS (distribution management systems), AMR (automated meter reading) systems, and other mission-critical systems that have similar 24x7 uptime requirements and system components.

Six Layer SCADA Vulnerability Assessment Approach

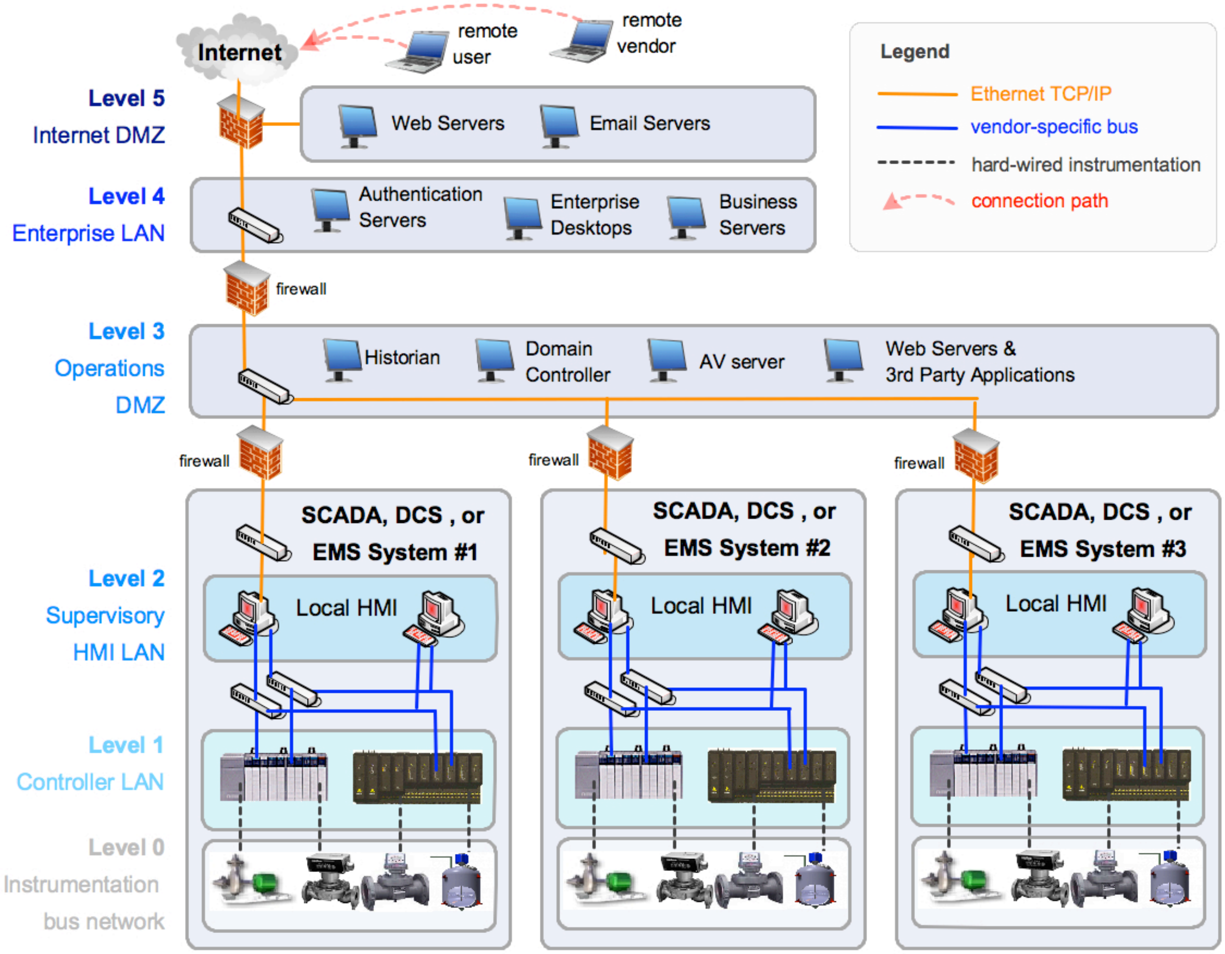


1. **Physical Security**
   (Fencing, Surveillance, Guards, Gates, Locks)
2. **Network Infrastructure**
   (Switches, Routers, Firewalls, 3rd Party Connections, and Modems)
3. **Testing the SCADA DMZ**
   (Data Historians, Data Logging, Web Servers)
4. **Assessing the Mission Critical Servers / Workstations for Host and Application Vulnerabilities**
   (Operating System Security, Application Security)
5. **Communications to Field Devices**
   (Clear text transfers, traffic injection, hijacks)
6. **Field Devices**
   (PLCs, RTUs, IEDs, Plant Equip.)

ISA S99 Model for Security Levels

The International Society of Automation (ISA) has drafted a standard for the security of SCADA and process control systems entitled the ISA S99 standard. This standard outlines specific security levels for each functional area of the system, then advocates the use of zones and conduits to separate, isolate, or provide security controls to challenge connecting from one security zone to another.

If we take a power generation system, like the typical one that we diagramed before, and then put all of the various functional components into the ISA model, we would find the most public systems such as Internet or Internet –facing systems at the top of the diagram at level 5. Then Corporate IT networks, DMZ networks for systems that need access from the SCADA networks, Supervisory HMI systems, Field Devices (controllers), and finally instrumentation and sensors last at level 0.



SCADA Vulnerability Statistics

Having a standard model for the various security levels in a SCADA, DCS, EMS, DMS, or AMR system is an important first step in classifying SCADA vulnerabilities. Once the model became part of the ISA S99 standard, we began to log SCADA vulnerabilities as to where in this model they were discovered.

After conducting over 100 assessments of SCADA and various types of control systems, our team eventually logged over 38,000 security findings and vulnerabilities from these assessments. In 2009, we were under contract from DHS to comb through these vulnerabilities and determine if trends in the data could help expose typical areas of vulnerability within SCADA systems, and the type of vulnerabilities most commonly found.

We Don't Need No Stinking SCADA 0-Days

When we set out to start capturing statistics on our vulnerability assessments, we wanted to know if these vulnerabilities that we are finding were already out in the public domain, and when these vulnerabilities were disclosed. We started entering the vulnerability disclosure date to the database, just to see if any interesting trends would develop. Some of the vulnerabilities that we found were not previously disclosed, and in some cases, the disclosure date was unknown, so we threw those records out. In a sample set of over 38,000 vulnerability records, we found that the average number of days between when the vulnerability was disclosed publically and when our team discovered the vulnerability **was 331 days.**

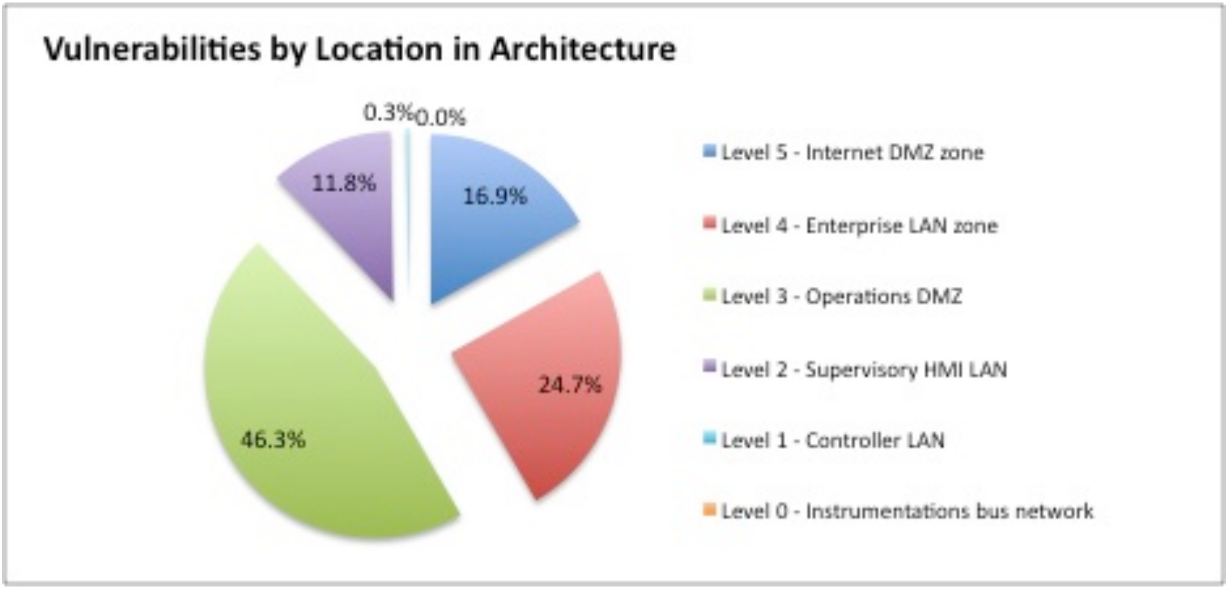
In some of the worst cases, we found vulnerabilities that had been disclosed over 1100 days before we found it, meaning that these **mission-critical SCADA systems were vulnerable to a known exploit for over 3 years before we found the problem.** It is well known that control systems are more difficult to patch than Enterprise IT systems, and the statistics in the data proves that we still have a patch management issue with critical infrastructure, especially when the patch has been available for on average of one year or more, and these systems are still popping up with old vulnerabilities. Which raises a serious issue, how many more critical infrastructure systems are working today like ticking time bombs with known vulnerabilities and exploits out in the wild that can take them down?

Where area of the SCADA System typically has the most Vulnerabilities?

Using the ISA99 model, are the vulnerabilities being discovered mostly at the Internet DMZ, Enterprise IT LAN, Operations DMZ, Supervisory HMI LAN, Controller LAN, or Instrumentation Bus?

To answer this question, we exported the complete data set of 38,753 vulnerabilities, parsed the data into columns, and added additional columns to help sort the data. Since we used an integer of 0 through 5 to represent where the vulnerability was located in the ISA S99 SCADA Security model, this allowed us to determine some statistics on where the vulnerabilities were discovered in a typical SCADA infrastructure. We were able to determine the actual count of how many times the value of 0, 1, 2, 3, 4, or 5 (ISA security levels) came up in the data set, and also calculate a percentage of that to the whole. The results from analyzing the data set are represented in the table and chart below:

SCADA Vulnerabilities by Location in the Network		**%**	**Count**
Level 5 - Internet DMZ zone		16.9%	6561
Level 4 - Enterprise LAN zone		24.7%	9567
Level 3 - Operations DMZ		46.3%	17957
Level 2 - Supervisory HMI LAN		11.8%	4554
Level 1 - Controller LAN		0.3%	105
Level 0 - Instrumentations bus network		0.0%	0
	Totals	100.0%	38744



Almost half of the total vulnerabilities were found in the DMZ between the Enterprise IT and SCADA systems. Often we find that SCADA system owners struggle with which group in their company has the ownership and responsibility for maintaining the systems in this part of the network.

It is usually very clear that the Enterprise IT systems are under the responsibility of the IT or MIS group, and the operational networks at the Supervisory HMI LAN and below are usually the responsibility of Operations or Engineering groups, but who maintains the systems in the middle?

Typically, the Operational DMZ networks are setup to share data with the Enterprise IT applications, and then left functioning for years without anyone maintaining them. Many of these contain embedded SMTP servers, database servers, web servers, and system components that are at risk to malware and network attacks.

The Operational DMZ network is the first stepping-stone from the Enterprise IT network, and is the most common threat vector for attacks against SCADA systems. Once access is made through the Enterprise IT network, then finding this Operational DMZ is a simple process. Almost all SCADA vendors use a design that places Data Historians, Web Servers, Reporting Systems, and other back-end servers in an area that is both accessible from the SCADA networks as well as the Enterprise IT networks.

Engineering and management personnel require access to near real-time and trended data from the SCADA systems to analyze the performance and efficiency of the SCADA systems. Marketing, Trading, and Business Modeling functions also need constant feeds of data from the SCADA systems to update systems that must interact with government, regulatory, business partners, customers, or other third parties.

Now we have found the "Perfect Storm" whereby the most connected area of the SCADA system also contains the most vulnerabilities, and is often overlooked by system administrators.

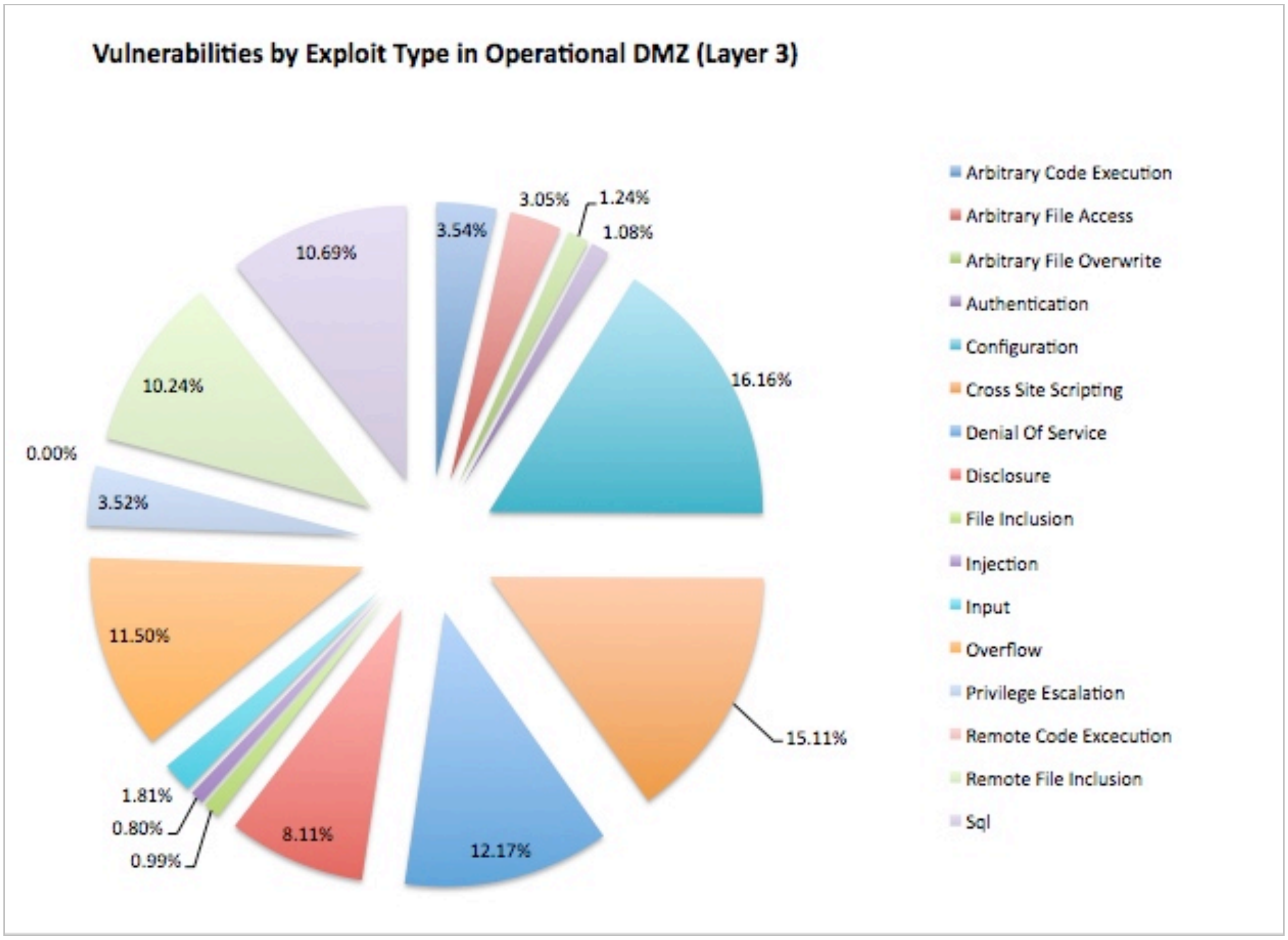
The next part of our research dealt with peeling back the next layer of the onion to classify these vulnerabilities by the type of exploit that would take advantage of these vulnerabilities.

SCADA, how can I own thee, let me count the ways

The Operational DMZ network is the last line of defense before any traffic hits the SCADA and Industrial Process Control systems, and in many cases, the servers, workstations, and applications in this middle area are all authorized and trusted by the SCADA systems. By dissecting the vulnerabilities in this level of the network, we can determine how the vulnerabilities at this level in the architecture can be exploited.

Our technicians and analysts had to first filter the SCADA vulnerability dataset for only those found in the Operational DMZ (Security Level 3), and then assigned a classification to each vulnerability based on the type of exploit that could be used to take advantage of the vulnerability. The classification dataset naturally fell into 16 different categories, and the results are disclosed in the table and chart below:

Exploit Type	**%**	**Count**
Arbitrary Code Execution	3.52%	658
Arbitrary File Access	3.03%	567
Arbitrary File Overwrite	1.23%	230
Authentication	1.08%	201
Configuration	16.08%	3004
Cross Site Scripting	15.04%	2809
Denial Of Service	12.11%	2263
Disclosure	8.07%	1508
File Inclusion	0.99%	185
Injection	0.80%	149
Input	1.80%	336
Overflow	11.45%	2139
Privilege Escalation	3.50%	654
Remote Code Execution	0.48%	90
Remote File Inclusion	10.19%	1903
SQL	10.64%	1987
	100.00%	18683



The underlining systems that control and monitor the generation, transmission, and distribution of electric power are utilizing similar computer networking components and architectures as Enterprise IT networks, yet they do not receive the same level of security maintenance or lifecycle planning.

These systems often are at least a year out of patch cycle, typically do not have any logging enabled, and rarely utilize any monitoring defense techniques like IDS, network, or host event monitoring. This does not even touch the topics relating to the security of the field devices, which are also very fragile and can be made to crash with simple PING commands. **See Appendix A for detailed results from the testing we did with an Ethernet-connected PLC.**

Now that we have exposed the dirty underbelly of the SCADA and Control Systems that govern the generation, transmission, and distribution of power, it is often a wonder why we haven't seen more incidents and security events with these systems. With that in mind, we next turn to the systems that are responsible for the tracking and billing for the usage of power to answer the question: Electricity for Free?

AMR and Smart Meter Vulnerabilities

AMR (Automated Meter Reading) Systems are structured in many ways like SCADA, EMS, DMS, and DCS systems. They have the same components at the network layer, utilize similar operating systems and applications, typically have proprietary protocols, and are geographically diverse in nature, since that rely on devices installed out at the customer location.

Through our own research and assessments of AMR systems in the field, we have found that AMR systems have vulnerabilities at various layers in the system:

- **Perimeter issues** > These systems are interconnected with business applications (billing, work-order, account management systems, etc..), AND also often connected to operational SCADA and Energy Management systems for load shedding and remote tripping.

- **Back-end Server/Application issues** > Similar web and database application vulnerabilities as business applications, less secure implementation of protocols, and old versions of application frameworks.

- **Too much trust in the Protocol** > Most AMI / AMR vendors are simply trusting that the 802.15.4 protocol security implementation will save them, and have not given much thought about scenarios when a communications mote is compromised.

- **End Devices have limited resources / weak stacks** > The meters themselves do not typically have the resources to handle security features. Basically, the hardware cannot handle more computationally demanding processes, like upgrading their encryption handling capabilities once deployed. Limited tamper-detection capabilities cited, but not found operational in testing.

Some have asked what an attacker could do given the vulnerabilities that we have experienced with AMR systems. We have verified that all of the following capabilities exist, and we have duplicated these in our own research:

- Data Enumeration (read real-time grid data)
- Host Enumeration (by scanning from the meter back to the head-end)
- Service Enumeration (determine what services are exposed)
- Change Data on the fly (manipulate and change usage and billing data at rest or in flight)
- Steal accounts and passwords (man-in-the-middle + wireshark)
- Damage core system components (bricking meters)
- Denial of Service (PING FLOOD, Malformed Packets, etc.. aimed at hardware or software)

Appendix B and C of this report contains the results from security testing performed on electric smart meters.

Summary Remarks

Power generation, transmission, and distribution systems all require functioning SCADA, EMS, and DMS systems that are available with 24x7 uptime. In the past, these systems were isolated systems that used serial protocols and obscure system components. SCADA engineers and specialized system integrators were the only ones that had any knowledge or tools to work with those legacy systems.

Recently, SCADA and Control Systems have evolved to the point where they are deployed with network infrastructure components used by Enterprise IT networks (Cisco, Juniper, 3COM, etc..). They also leverage the same Microsoft operating systems and .NET application frameworks. The vulnerabilities that were once only considered to be issues with Enterprise IT systems are now are the core of almost all modern SCADA systems. Together, with the requirement to connect these systems to external networks and the Internet, makes these systems even more vulnerable than ever. Lack of an aggressive administrative mindset has also left many of these systems, and the cyber health of our nations critical infrastructure, in a state of risk.

With so many known vulnerabilities (with existing working exploits) that exist in Operational DMZ and SCADA systems today, there is no need to develop new 0-day exploits, or spend numerous efforts on R&D researching new SCADA-specific exploits. Our national critical infrastructure, including the power generation, transmission, and distribution systems, are already vulnerable now, and require urgent action by asset owners and operators to diligently look under the rocks and weed out the vulnerabilities.

With the advancement of the “Smart Grid” and AMR systems, without the proper security precautions, the electric grid is now more vulnerable than ever. The research that we, and other independent security firms, have performed on Smart Meters and AMR systems expose vulnerabilities that can lead to a situation whereby electricity is free…for those who have the intent and motivation.

Appendix A - Test Results with Common PLC used in Power Generation

PING Testing

Red Tiger Security conducted a PING test against a well known PLC vendor that uses TCP/IP for communications with Power Generation Systems. The PING testing was ramped up from smaller packet size to larger packet size, until the maximum packet size was reached. Typically this test is ran by sending simultaneous PING packets at the following sizes to the target IP address:

- 60 byte
- 600 byte
- 6,000 byte
- 60,000 byte

The actual commands used to create and send the PING tests are provided in the results below, as well as the impact the command had on the performance of the PLC.

```
ping -f -s 60 (target IP Address)

PING 11.128.66.170 (11.128.66.170): 60 data bytes
.....................................................................................................................................
.....................................................................................................................................
..............................................................................................................................
--- 11.128.66.170 ping statistics ---
601 packets transmitted, 150 packets received, 75% packet loss
```

(The device lost communications and was unreachable on the network. The device was not reachable by SCADA scans, but came back up in a few seconds after the attack was over.)

```
ping -f -s 600 (target IP Address)
PING 11.128.66.170 (11.128.66.170): 600 data bytes
.....................................................................................................................................
.....................................................................................................................................
.....................................................................................................................................
......
--- 11.128.66.170 ping statistics ---
497 packets transmitted, 32 packets received, 93% packet loss
```

(The device lost communications and was unreachable on the network. The device was not reachable by SCADA scans, but came back up in a few seconds after the attack was over.)

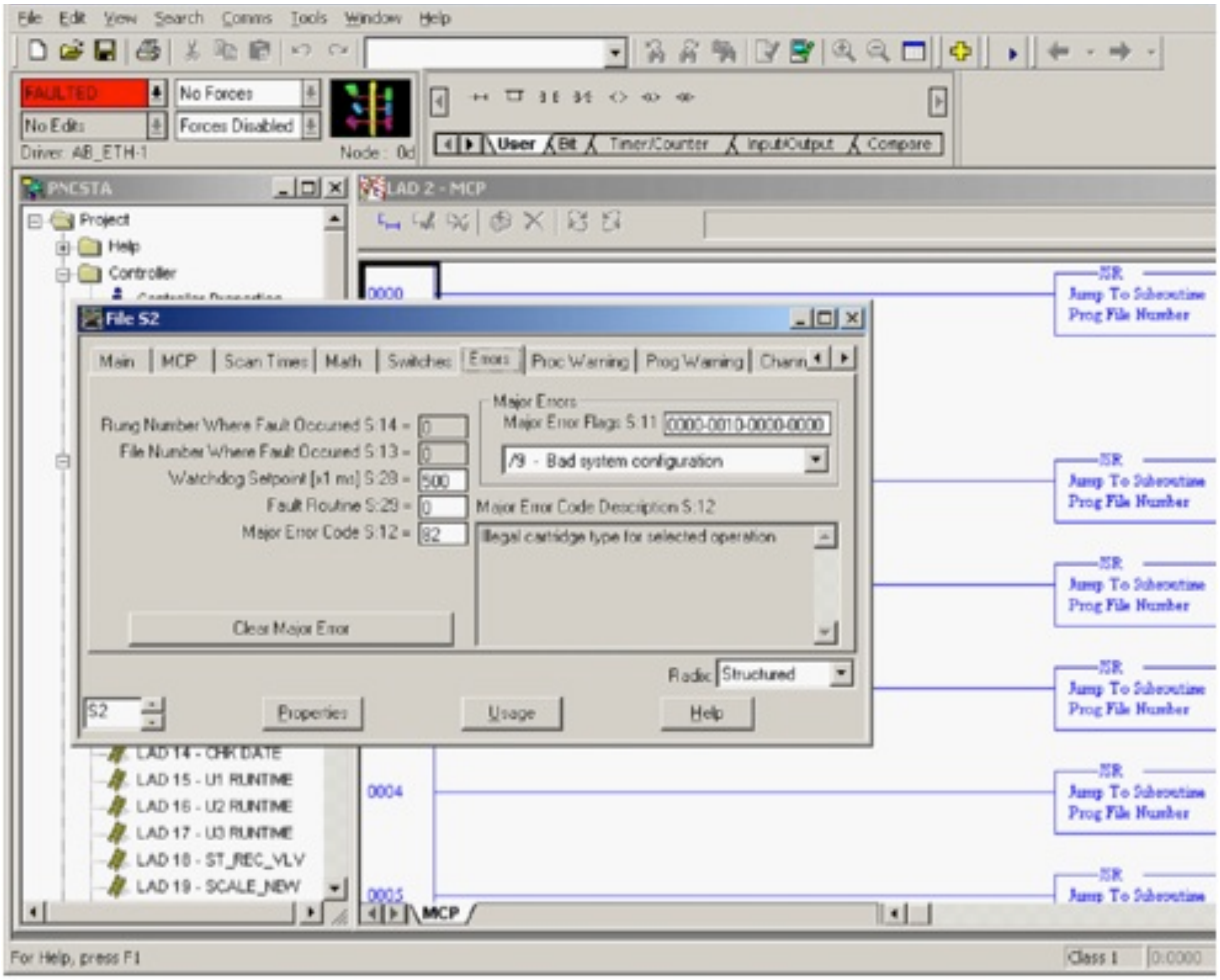
```
PING 11.128.66.170 (11.128.66.170): 6000 data bytes
.........................................................................................................................................................
.........................................................................................................................................................
.........................................................................................................................................................
...........................................................
--- 11.128.66.170 ping statistics ---
518 packets transmitted, 0 packets received, 100% packet loss
```

(The device lost communications and was unreachable on the network. The device was not reachable by SCADA scans, and it went from a RUN to a FAULTED state. **All configuration was lost, and we had to recycle power, then transfer the configuration back to the device over a serial connection to restore its operation.)**

```
PING 11.128.66.170 (11.128.66.170): 60000 data bytes
.........................................................................................................................................................
.........................................................................................................................................................
.........................................................................................................................................................
.........................................................................................................................................................
.........................................................................................................................................................
......................................................
--- 11.128.66.170 ping statistics ---
819 packets transmitted, 0 packets received, 100% packet loss
```

(The device lost communications and was unreachable on the network. The device was not reachable by SCADA scans, and it went from a RUN to a FAULTED state. **All configuration was lost, and we had to recycle power, then transfer the configuration back to the device over a serial connection to restore its operation.)**

We used the programming software to monitor the health of the PLC while using the PING test scenarios. The screen shot below shows to status of the PLC when it failed under a simple PING test.



File S2

Rung Number Where Fault Occured S:14 = 0
File Number Where Fault Occured S:13 = 0
Watchdog Setpoint [x1 ms] S:28 = 500
Fault Routine S:29 = 0
Major Error Code S:12 = 82

Major Errors
Major Error Flags S:11 0000-0010-0000-0000
/9 - Bad system configuration

Major Error Code Description S:12
Illegal cartridge type for selected operation

Radix: Structured
S2

Appendix B - Test Results with Typical Power Meter used in AMR systems

PING test

Red Tiger Security conducted a similar PING test against a well-known power meter that uses TCP/IP for transmitting meter data. The team also tested the software application that was poling the meter. The PING testing will be ramped up from smaller packet size to larger packet size, until the maximum packet size is reached. Typically this test is ran by sending 1000 simultaneous PING packets at the following sizes to the target IP address:

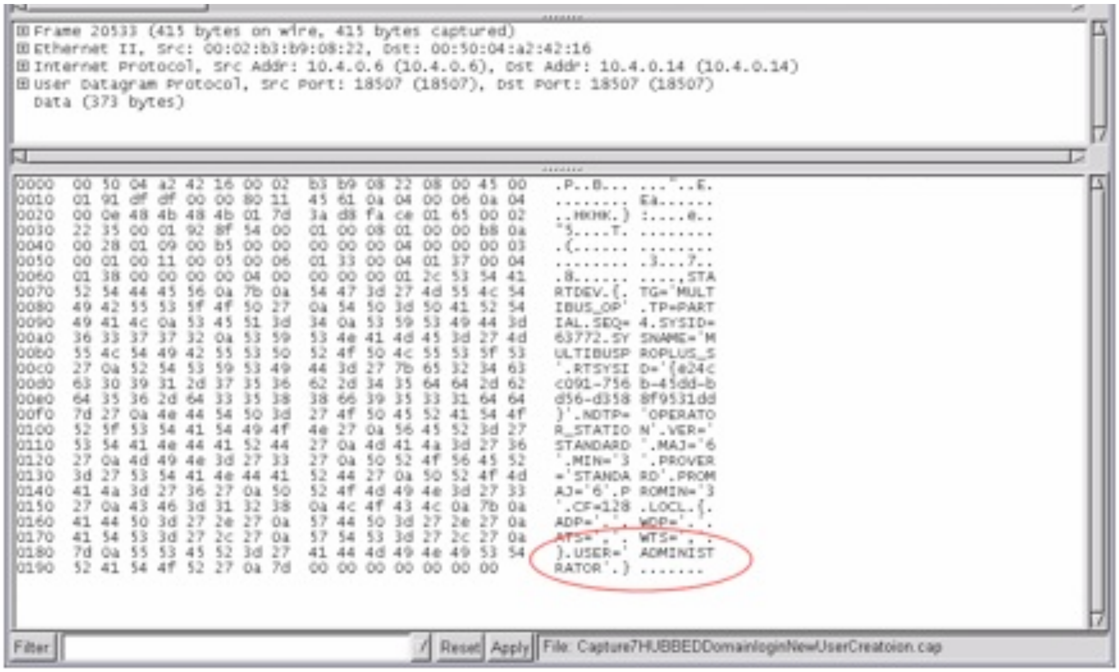
- 60 byte
- 600 byte
- 6,000 byte
- 60,000 byte

The actual commands used to create and send the PING tests are provided in the table below, as well as the results that the test had on the meter.

command	type	Result test had on Meter Operation
ping -f 137.20.5.86 -s 60	Ping Flood with 60 byte size payload	This test crashed the METER. After the attack was turned off, it took about 3 minutes for the METER to recover on its own.
ping -f 137.20.5.86 -s 600	Ping Flood with 600 byte size payload	This test crashed the METER. After the attack was turned off, it took about 3 minutes for the METER to recover on its own.
ping -f 137.20.5.86 -s 6000	Ping Flood with 6,000 byte size payload	This test crashed the METER. After the attack was turned off, the METER never recovered on its own. **The METER had to be rebooted, and then the configuration had to be reloaded into the METER through a serial cable.**
ping -f 137.20.5.86 -s 60000	Ping Flood with 60,000 byte size payload	This test crashed the METER. After the attack was turned off, the METER never recovered on its own. **The METER had to be rebooted, and then the configuration had to be reloaded into the METER through a serial cable.**

Appendix C - Some Smart Meter Vendors Send Username/Password in the Clear

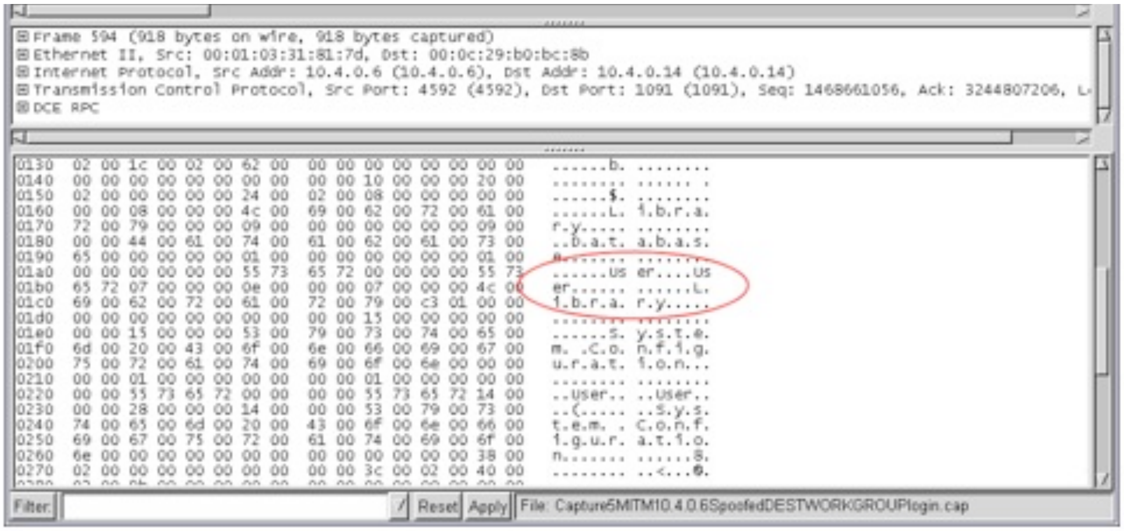
In some of our other testing of metering systems that use Ethernet protocols, we have found that many of these protocols send the usernames and passwords to log into the meters in the clear over the network. A simple network sniffing software like Wireshark can pickup this information as shown in the figures below.



```
⊞ Frame 20533 (415 bytes on wire, 415 bytes captured)
⊞ Ethernet II, Src: 00:02:b3:b9:08:22, Dst: 00:50:04:a2:42:16
⊞ Internet Protocol, Src Addr: 10.4.0.6 (10.4.0.6), Dst Addr: 10.4.0.14 (10.4.0.14)
⊞ User Datagram Protocol, Src Port: 18507 (18507), Dst Port: 18507 (18507)
  Data (373 bytes)
```

```
0000   00 50 04 a2 42 16 00 02  b3 b9 08 22 08 00 45 00   .P..B... ..."..E.
0010   01 91 df df 00 00 80 11  45 61 0a 04 00 06 0a 04   ........ Ea......
0020   00 0e 48 4b 48 4b 01 7d  3a d8 fa ce 01 65 00 02   ..HKHK.} :.....e..
0030   22 35 00 01 92 8f 54 00  01 00 08 01 00 00 b8 0a   "5....T. ........
0040   00 28 01 09 00 b5 00 00  00 00 00 04 00 00 00 03   .(...... ........
0050   00 01 00 11 00 05 00 06  01 33 00 04 01 37 00 04   ........ .3...7..
0060   01 38 00 00 00 00 04 00  00 00 00 01 2c 53 54 41   .8...... ....,STA
0070   52 54 44 45 56 0a 7b 0a  54 47 3d 27 4d 55 4c 54   RTDEV.{. TG='MULT
0080   49 42 55 53 5f 4f 50 27  0a 54 50 3d 50 41 52 54   IBUS_OP' .TP=PART
0090   49 41 4c 0a 53 45 51 3d  34 0a 53 59 53 49 44 3d   IAL.SEQ= 4.SYSID=
00a0   36 33 37 37 32 0a 53 59  53 4e 41 4d 45 3d 27 4d   63772.SY SNAME='M
00b0   55 4c 54 49 42 55 53 50  52 4f 50 4c 55 53 5f 53   ULTIBUSP ROPLUS_S
00c0   27 0a 52 54 53 59 53 49  44 3d 27 7b 65 32 34 63   '.RTSYSI D='{e24c
00d0   63 30 39 31 2d 37 35 36  62 2d 34 35 64 64 2d 62   c091-756 b-45dd-b
00e0   64 35 36 2d 64 33 35 38  38 66 39 35 33 31 64 64   d56-d358 8f9531dd
00f0   7d 27 0a 4e 44 54 50 3d  27 4f 50 45 52 41 54 4f   }'.NDTP= 'OPERATO
0100   52 5f 53 54 41 54 49 4f  4e 27 0a 56 45 52 3d 27   R_STATIO N'.VER='
0110   53 54 41 4e 44 41 52 44  27 0a 4d 41 4a 3d 27 36   STANDARD '.MAJ='6
0120   27 0a 4d 49 4e 3d 27 33  27 0a 50 52 4f 56 45 52   '.MIN='3 '.PROVER
0130   3d 27 53 54 41 4e 44 41  52 44 27 0a 50 52 4f 4d   ='STANDA RD'.PROM
0140   41 4a 3d 27 36 27 0a 50  52 4f 4d 49 4e 3d 27 33   AJ='6'.P ROMIN='3
0150   27 0a 43 46 3d 31 32 38  0a 4c 4f 43 4c 0a 7b 0a   '.CF=128 .LOCL.{.
0160   41 44 50 3d 27 2e 27 0a  57 44 50 3d 27 2e 27 0a   ADP='.'. WDP='.'.
0170   41 54 53 3d 27 2c 27 0a  57 54 53 3d 27 2c 27 0a   ATS=','. WTS=','.
0180   7d 0a 55 53 45 52 3d 27  41 44 4d 49 4e 49 53 54   }.USER=' ADMINIST
0190   52 41 54 4f 52 27 0a 7d  00 00 00 00 00 00 00      RATOR'.} .......
```

File: Capture7HUBBEDDomainloginNewUserCreatoion.cap



```
⊞ Frame 594 (918 bytes on wire, 918 bytes captured)
⊞ Ethernet II, Src: 00:01:03:31:81:7d, Dst: 00:0c:29:b0:bc:8b
⊞ Internet Protocol, Src Addr: 10.4.0.6 (10.4.0.6), Dst Addr: 10.4.0.14 (10.4.0.14)
⊞ Transmission Control Protocol, Src Port: 4592 (4592), Dst Port: 1091 (1091), Seq: 1468661056, Ack: 3244807206, L
⊞ DCE RPC
```

```
0130   02 00 1c 00 02 00 62 00  00 00 00 00 00 00 00 00   ......b. ........
0140   00 00 00 00 00 00 00 00  00 00 10 00 00 00 20 00   ........ ...... .
0150   02 00 00 00 00 00 24 00  02 00 08 00 00 00 00 00   ......$. ........
0160   00 00 08 00 00 00 4c 00  69 00 62 00 72 00 61 00   ......L. i.b.r.a.
0170   72 00 79 00 00 00 09 00  00 00 00 00 00 00 09 00   r.y..... ........
0180   00 00 44 00 61 00 74 00  61 00 62 00 61 00 73 00   ..D.a.t. a.b.a.s.
0190   65 00 00 00 00 00 01 00  00 00 00 00 00 00 01 00   e....... ........
01a0   00 00 00 00 00 00 55 73  65 72 00 00 00 00 55 73   ......Us er....Us
01b0   65 72 07 00 00 00 0e 00  00 00 07 00 00 00 4c 00   er...... ......L.
01c0   69 00 62 00 72 00 61 00  72 00 79 00 c3 01 00 00   i.b.r.a. r.y.....
01d0   00 00 00 00 00 00 00 00  00 00 15 00 00 00 00 00   ........ ........
01e0   00 00 15 00 00 00 53 00  79 00 73 00 74 00 65 00   ......S. y.s.t.e.
01f0   6d 00 20 00 43 00 6f 00  6e 00 66 00 69 00 67 00   m. .C.o. n.f.i.g.
0200   75 00 72 00 61 00 74 00  69 00 6f 00 6e 00 00 00   u.r.a.t. i.o.n...
0210   00 00 01 00 00 00 00 00  00 00 01 00 00 00 00 00   ........ ........
0220   00 00 55 73 65 72 00 00  00 00 55 73 65 72 14 00   ..User.. ..User..
0230   00 00 28 00 00 00 14 00  00 00 53 00 79 00 73 00   ..(..... ..S.y.s.
0240   74 00 65 00 6d 00 20 00  43 00 6f 00 6e 00 66 00   t.e.m. . C.o.n.f.
0250   69 00 67 00 75 00 72 00  61 00 74 00 69 00 6f 00   i.g.u.r. a.t.i.o.
0260   6e 00 00 00 00 00 00 00  00 00 00 00 00 00 38 00   n....... ......8.
0270   02 00 00 00 00 00 00 00  00 00 3c 00 02 00 40 00   ........ ..<...@.
```

File: Capture5MITM10.4.0.6SpoofedDESTWORKGROUPlogin.cap