SCADA
Made Simple

Kelli Jamison – B L Anderson

What is SCADA?

- Various types of SCADA systems
- Differences between systems
- How SCADA applies to Water and Wastewater
- Mission’s Managed SCADA
- Questions and Answers

SCADA

- *Supervisory Control and Data Acquisition*
- SCADA systems were first used in the 1960’s
  - Coming from Telemetry that was first used in the 1830’s
  - Samuel Morse, Leonard Gale and Alfred Vail
- Monolithic (Large independent Mainframe)
- Distributed (WAN, LAN….Security Issues)
- Networked (Very Secure with todays Standards and Protocols)

What is SCADA *cont.*

- SCADA systems are used to monitor and control plant or equipment in industries such as:
  - Telecommunications
  - Energy, oil and gas refining
  - Transportation
  - *Water and Wastewater monitoring and control*
- SCADA systems can be relatively simple, such as ones that monitor environmental conditions of a small office building, or very complex, such as systems that monitor the activity in a nuclear power plant or *control a municipality's water system.*

What is SCADA *cont.*

- SCADA systems gather information such as:
  - Pump Runtimes
  - Water Levels
  - Amperage
  - Total/Free Chlorine
  - Flow
  - Pressure
  - Temperature
- …and transfer the information back to a central site (computer) where it is stored for alarming and reporting purposes

What is SCADA *cont.*

SCADA systems can monitor specific conditions such as:

- High or Low Level
- Pump Failure
- Intrusion
- Power Loss
- Generator Running
- Phase Loss
- High Temperature
- Excess Pump Starts
- Analog Thresholds

Thresholds can be set to cause alarms when readings are out of the norm

Types of SCADA Systems
Used in the Water and Wastewater Industry

- Auto Dialers
- LEO Satellite Systems
- Cellular Systems
- Client/ Server (traditional)
- Mission’s Managed SCADA

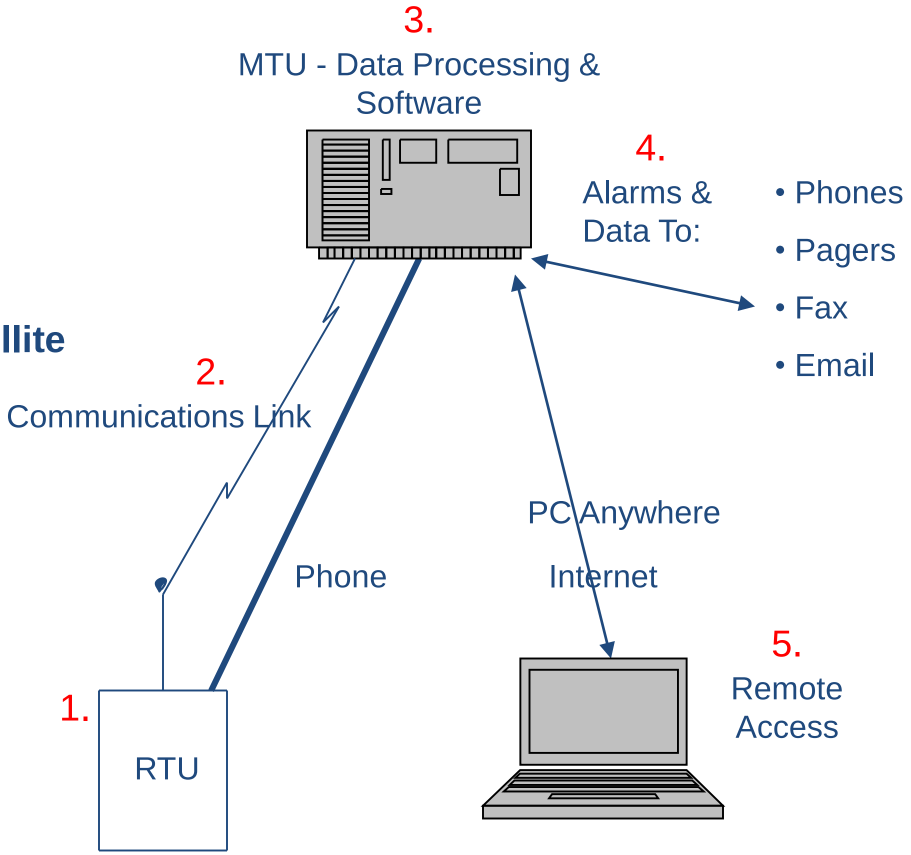
Differences Between Systems

- Method of transmitting data
- How often the data is transmitted
- Amount of data transmitted
- Where data is stored
- On going maintenance & support
- Cost!!!

Remember These Five Parts

Five Parts of Any Telemetry System

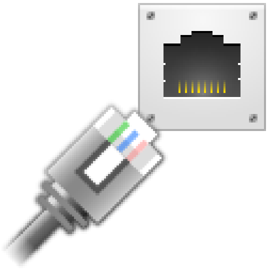
1. **RTU –** Radio Terminal Unit
   - **Custom or Standardized**
2. **Communications Link**
   - **Phone Line**
     - **Leased Or Dialup**
   - **Wireless**
     - **Cellular, spread spectrum, satellite**
3. **MTU -** Master Terminal Unit
   - **Software and Programming**
   - **Hardware and Data Bases**
   - **In House or Remote**
4. **Alarm System**
   - **Phone, Pager, Fax or Email**
5. **Remote Access**
   - **PC Anywhere**
   - **Web Access**
   - **Security**



Auto Dialers/Chatterbox

- Auto Dialer
  - Basic System
  - Easy installation
  - Requires a phone line
  - Local programming

- Leased line
  - Requires a dedicated phone line
  - Modem's
  - Unlicensed

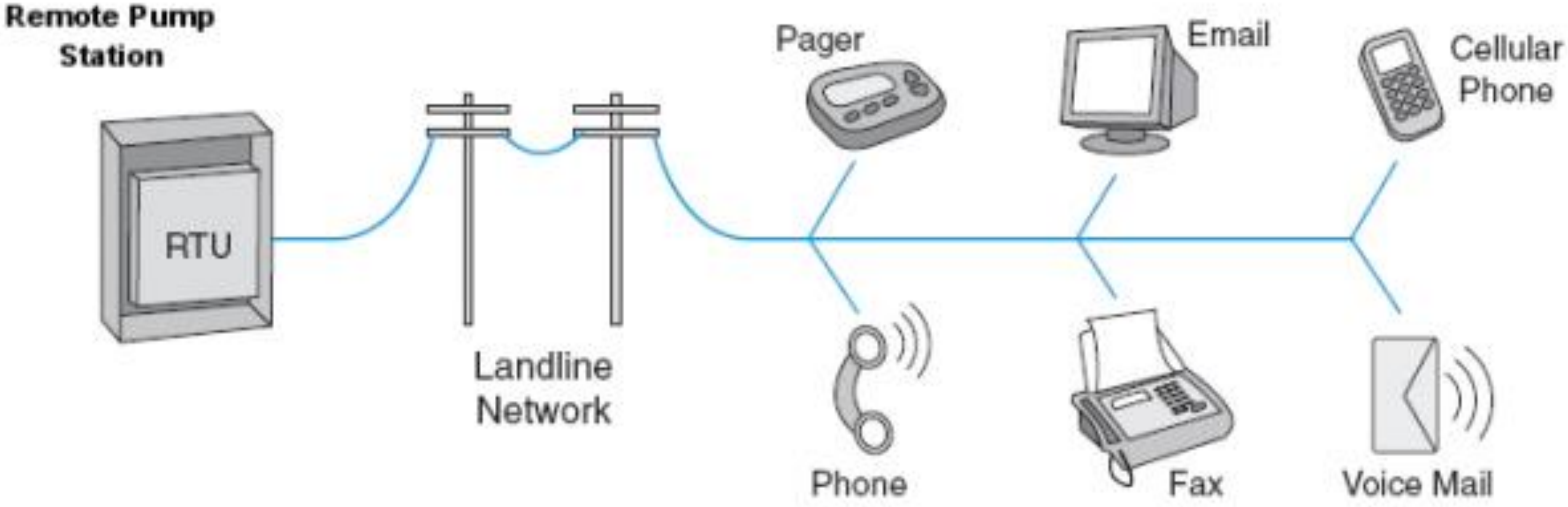


Auto Dialers/Chatterbox

- Good solution for basic alarms
- Need a dedicated phone line
  - You have to deal with the phone company if you want to move it!
  - Cost of the phone line $30-$60 per month
  - Lengthy time to re-establish service when natural disasters occur
- Minimal data storage for reporting purposes
- Limited features and functionality

Methods of Transmitting Auto Dialers

- Simple (Phone lines or Modems)
- No redundancy or watchdog for communication failures
- Have to rely on the phone company to reestablish connections
- Most still use (POTS) lines.

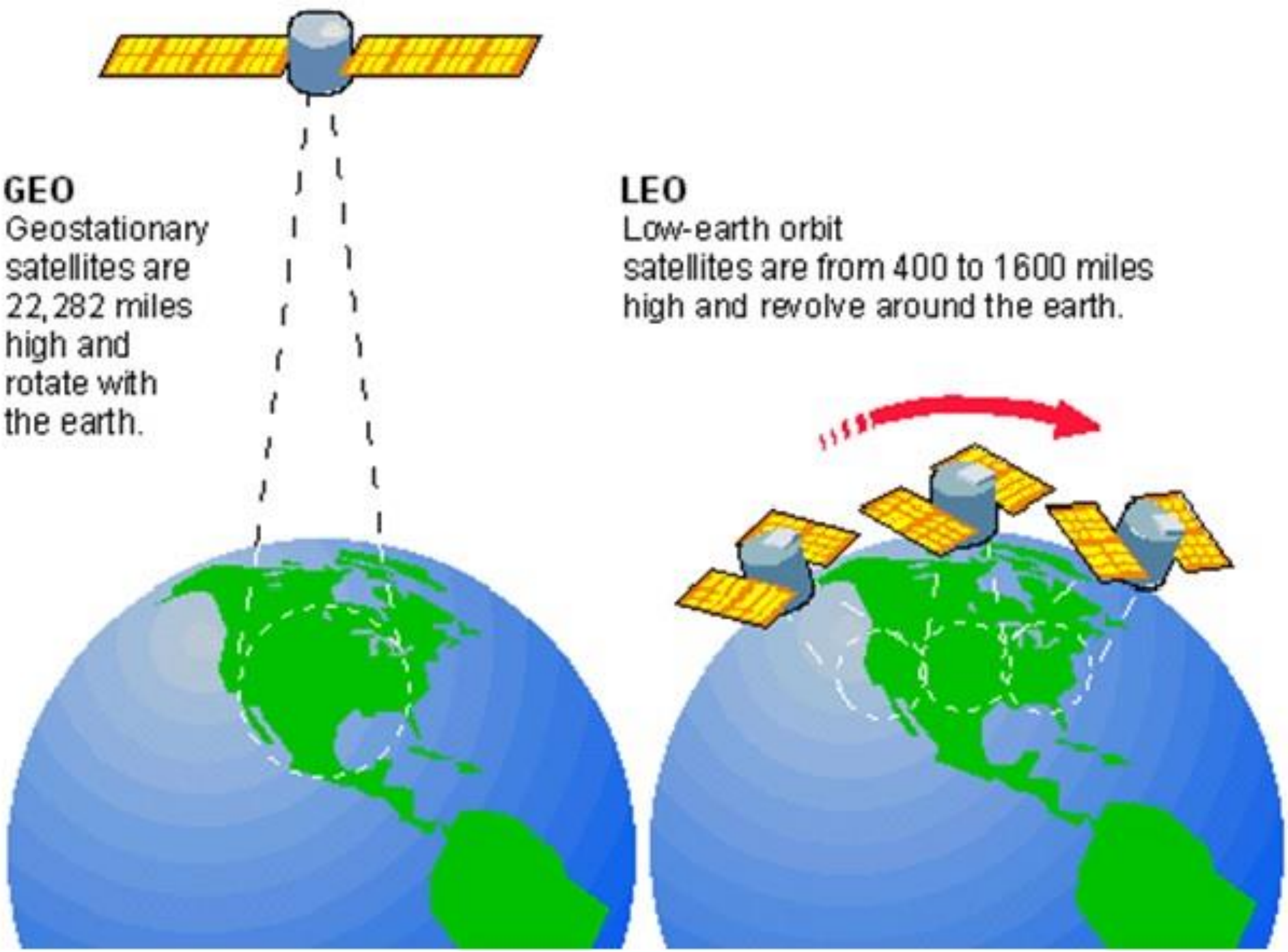

Remote Pump Station
RTU
Landline Network
Pager
Email
Cellular Phone
Phone
Fax
Voice Mail

LEO Satellite

- Several managed SCADA providers have chosen ORBCOMM as their data transmission partner.
  - ORBCOMM service has worldwide coverage
  - ORBCOMM is designed for very short messages.
  - ORBCOMM hardware is inexpensive
  - ORBCOMM antennas are unobtrusive

- Sounds great. Why would someone not use this? Why does Mission use cellular data?

LEO/GEO



GEO
Geostationary satellites are 22,282 miles high and rotate with the earth.

LEO
Low-earth orbit satellites are from 400 to 1600 miles high and revolve around the earth.

Cellular SCADA

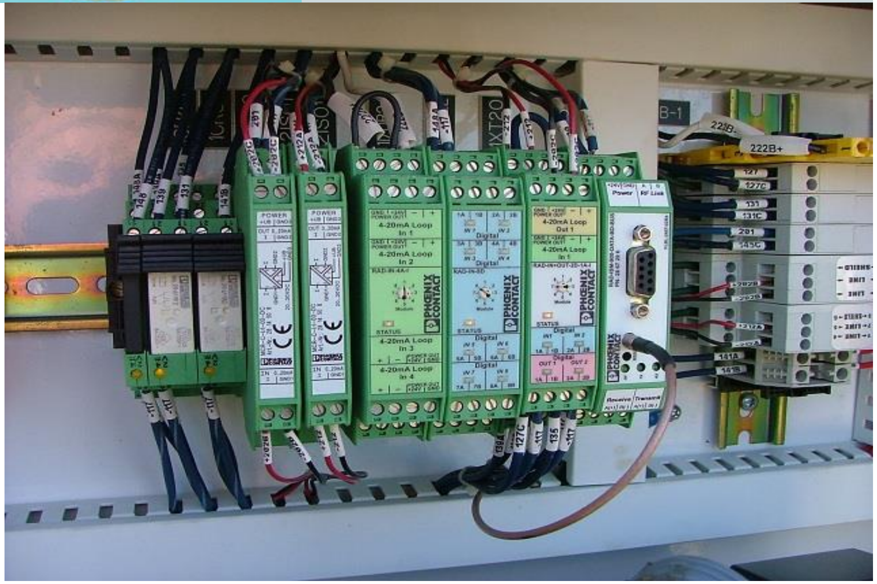
- Server hardware and software maintained by 3rd party (M2M, Kore Technology)
- Data is accessed on an unsecure website
- Say they can operate water systems
- Multiple vendors for hardware, cellular connectivity and the presentation of the data
- New features?
- Hardware has to be returned to the manufacturer to change radio technology
- Radio upgrades cost the customer

REMOTE TERMINAL UNIT
STATUS
ANTENNA
pb
Model: RT-1
6DI - 4AI - 2RO - Modbus Master / TCP
POWER
ETHERNET

OFF / ON
MIC
SPK
Buzzer Reset
GSM RTU
King Pigeon Hi-Tech.Co.,Ltd.
AD input
Rly drivable output
Switching input
RS232
DC9-28V
BEST-B2B.COM
Global trade start here

DPI 400
TONS
A1
A2
A3
C
Tx
Rx
Digital Process Indicator

WAGO

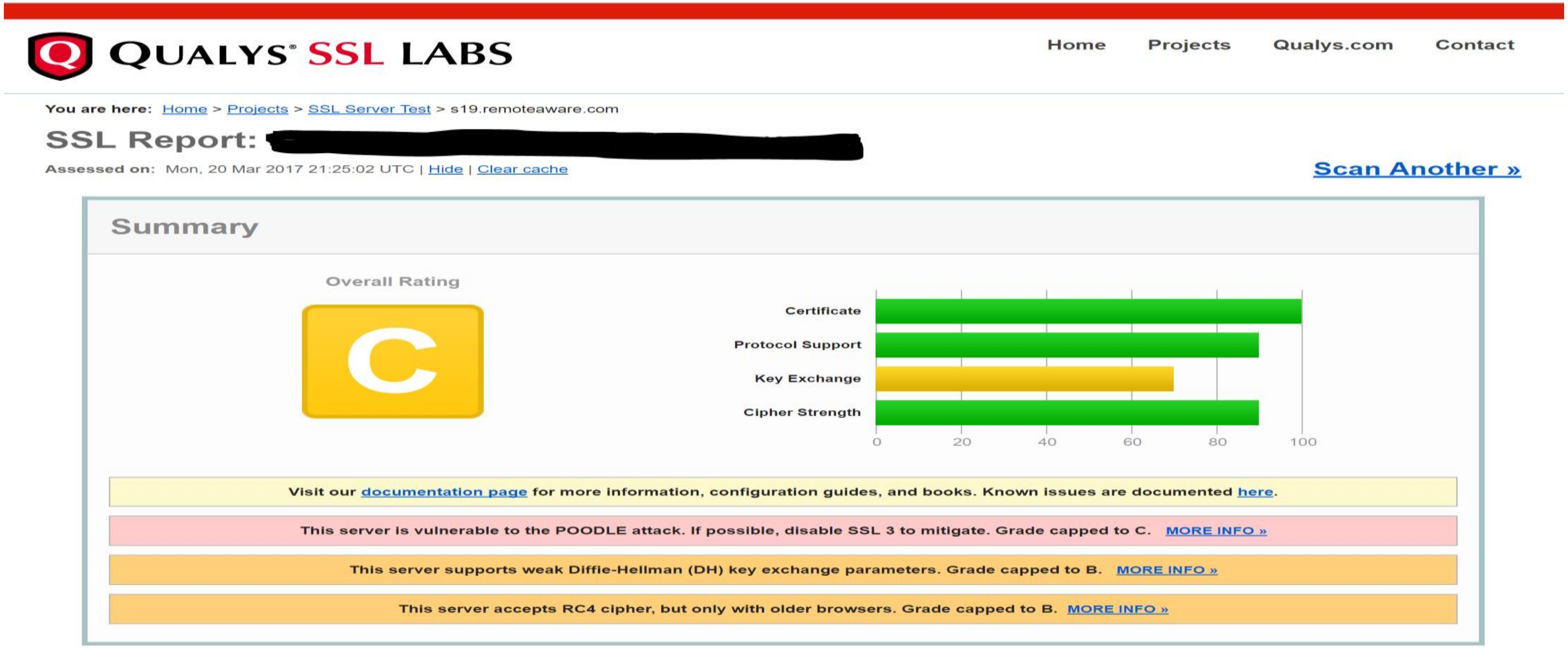

PHOENIX CONTACT
4-20mA Loop
Digital
222B+

Methods of Transmitting Cellular Systems

  - AWWA and Homeland Security minimum 1024-Bit SSL
- Mostly GSM some still CDMA/3G ($ adder) Sunset are coming!
  - Sprint “December 2021”
  - ATT GSM “3G 2/22/22”
  - Verizon CDMA “December 2022”
  - National coverage ???
- Several are Not on 4G/LTE/IoT
- Uses UDP (User Datagram Protocol)
- Doesn’t use “Socket Connections”
- Not an option for Control….Missed Data!!!

Methods of Transmitting Cellular Systems

- Unsecure website access
  - Most don’t offer this!
  - URL= http:



QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > s19.remoteaware.com

SSL Report: [redacted]

Assessed on: Mon, 20 Mar 2017 21:25:02 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

C

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. MORE INFO »

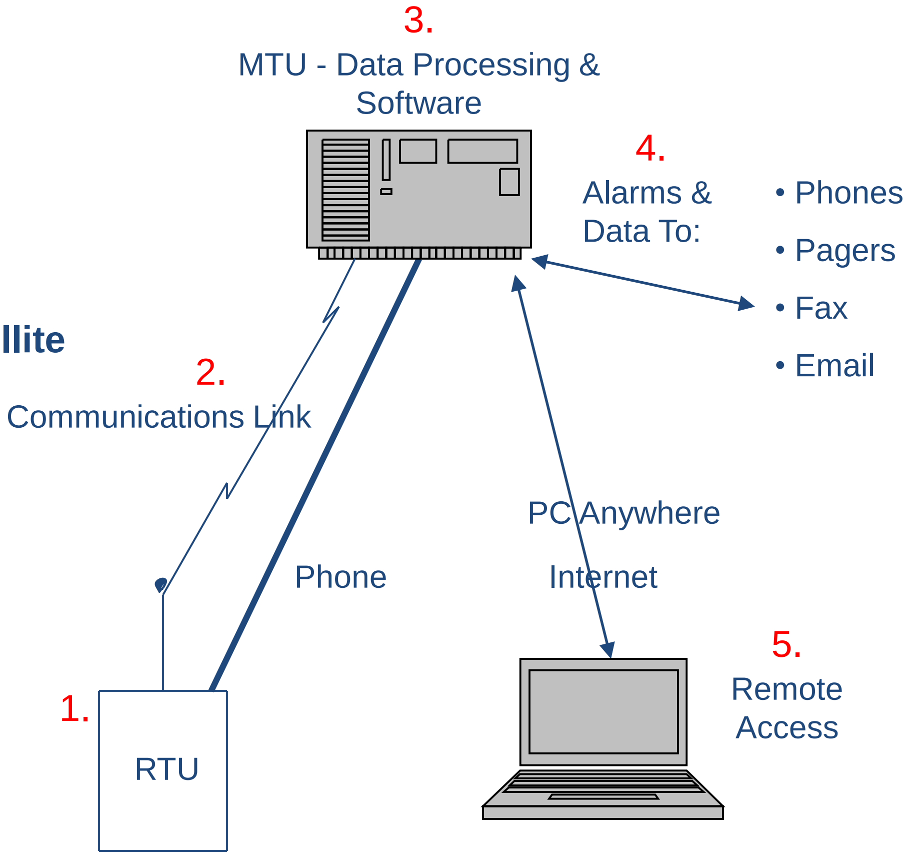
This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

This server accepts RC4 cipher, but only with older browsers. Grade capped to B. MORE INFO »

Remember These Five Parts

Five Parts of Any Telemetry System

1. **RTU –** Radio Terminal Unit
   - **Custom or Standardized**
2. **Communications Link**
   - **Phone Line**
     - **Leased Or Dialup**
   - **Wireless**
     - **Cellular, spread spectrum, satellite**
3. **MTU -** Master Terminal Unit
   - **Software and Programming**
   - **Hardware and Data Bases**
   - **In House or Remote**
4. **Alarm System**
   - **Phone, Pager, Fax or Email**
5. **Remote Access**
   - **PC Anywhere**
   - **Web Access**
   - **Security**



3. MTU - Data Processing & Software

4. Alarms & Data To:

- Phones
- Pagers
- Fax
- Email

2. Communications Link

Phone

PC Anywhere

Internet

1. RTU

5. Remote Access

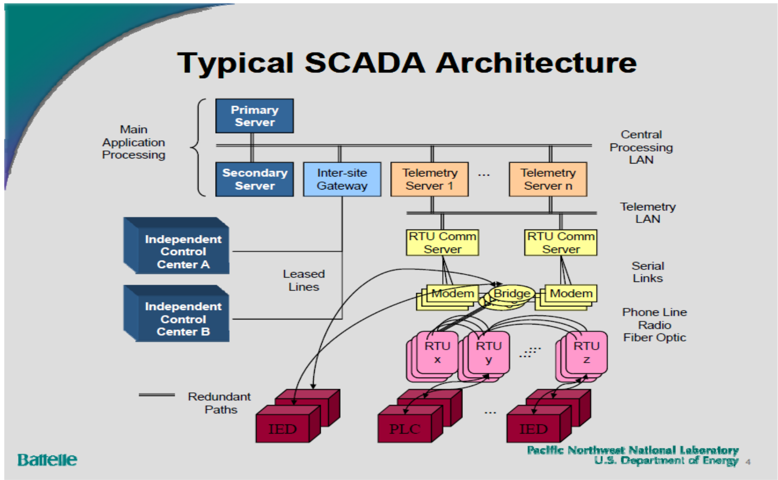
Methods of Transmitting Client/ Server

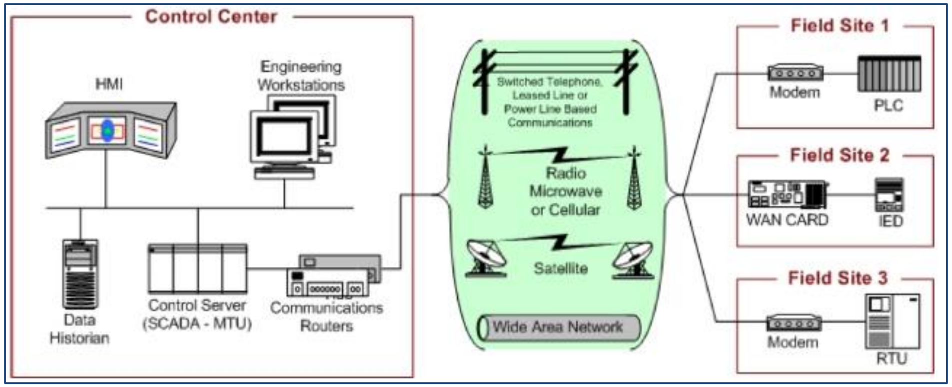
- Often proprietary software installed on user work-stations (servers/clients)
- Can be hard-wired between server and monitored location (Ethernet Radio, Serial, RTU)
- Optimal for advanced applications, i.e. oil, gas, electric, certain controlling applications
- IT department generally maintains servers
- Highly customizable but slow and costly to deploy
- 900MHz bleed over from other industries!

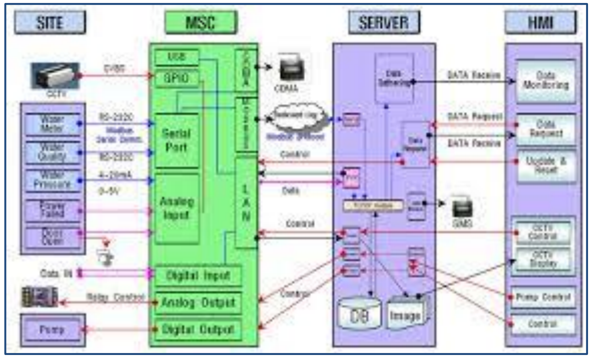
Client/ Server (traditional)

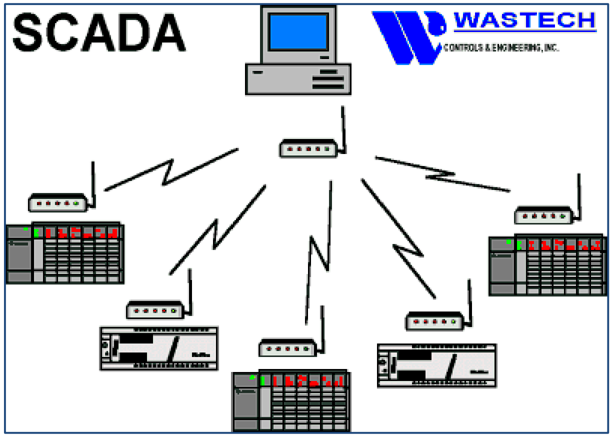
- Optimal for advanced applications, i.e. oil, gas, electric, certain controlling applications
- High number of inputs and outputs
- Generally custom designed
- Costly software
- Setup is time-consuming and requires specialized skills
- Reliability is dependent on private towers, or physical connections
- On going maintenance costs

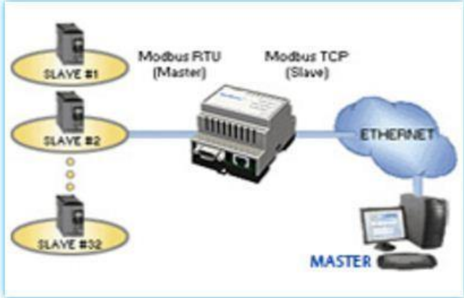
SCADA
Architecture Matters

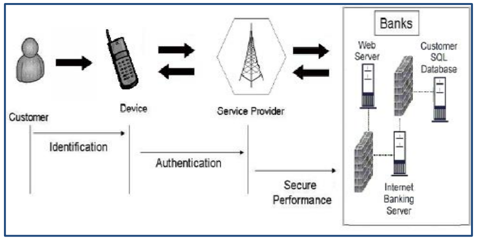

Typical SCADA Architecture



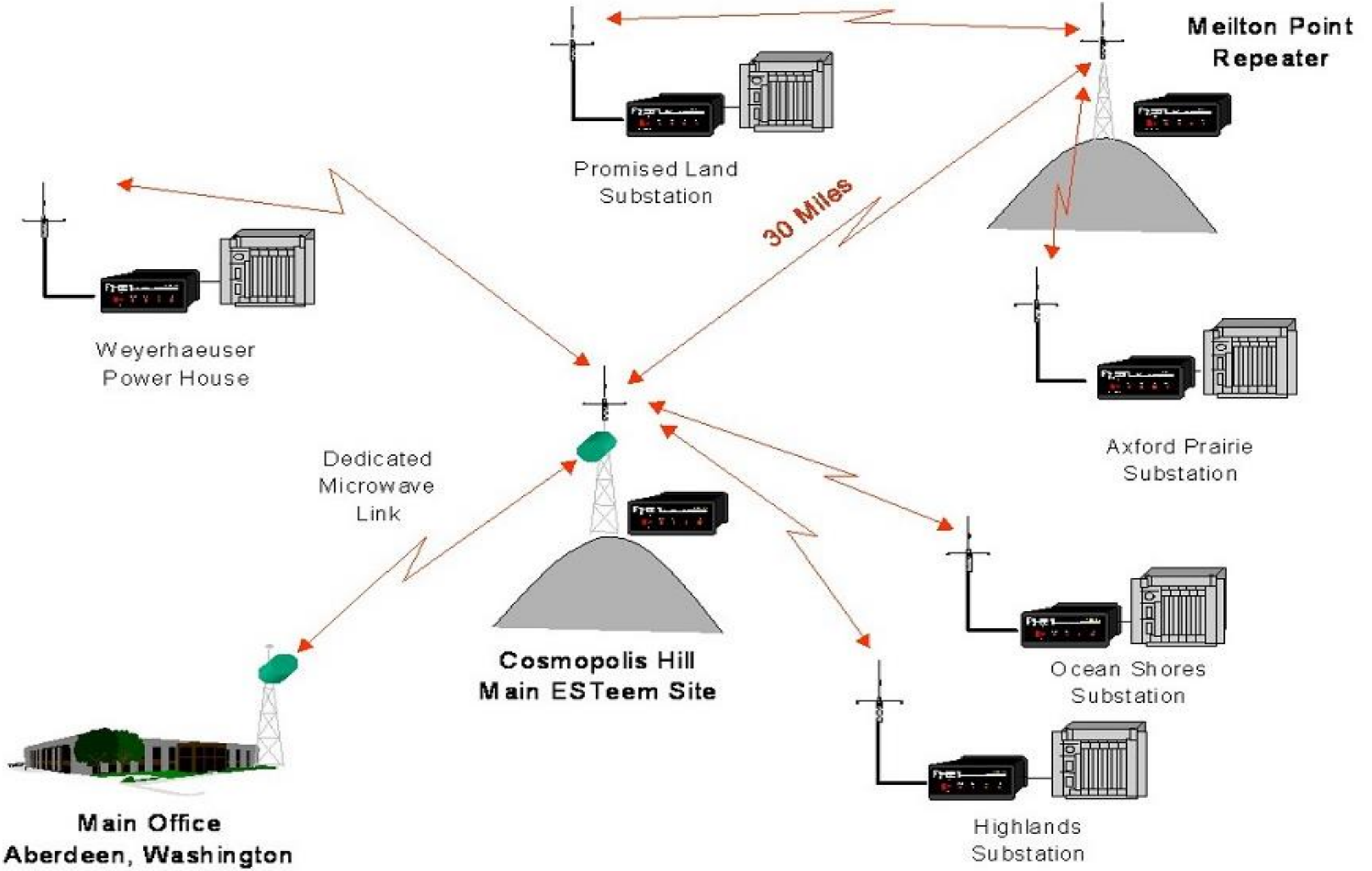




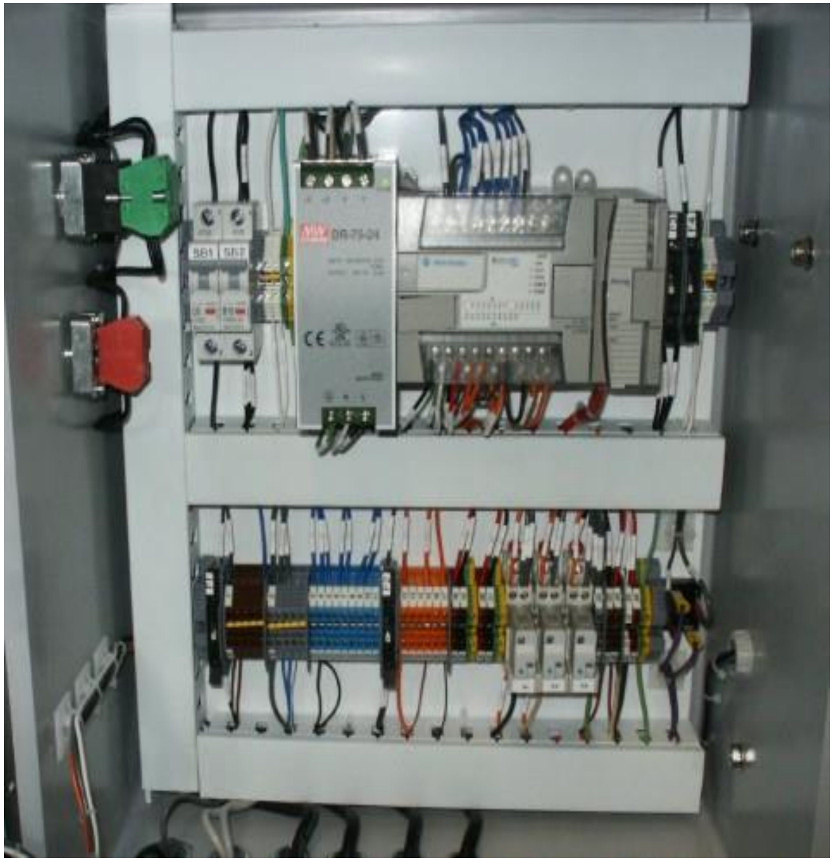




Complex systems with more penetration points can be more vulnerable

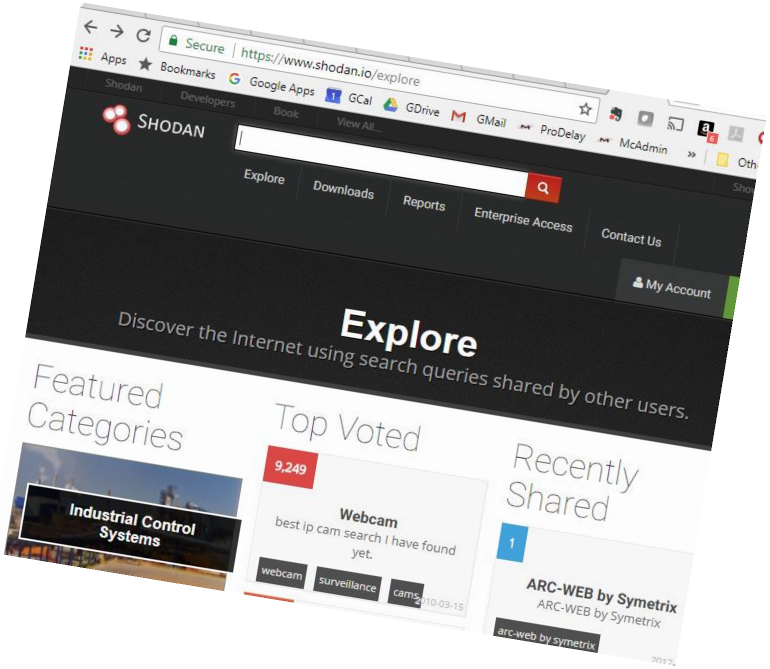

Meilton Point
Repeater
Promised Land
Substation
30 Miles
Weyerhaeuser
Power House
Axford Prairie
Substation
Dedicated
Microwave
Link
Cosmopolis Hill
Main ESTeem Site
Ocean Shores
Substation
Main Office
Aberdeen, Washington
Highlands
Substation

PLC-Programmable Logic Controller



Why Do PLCs get a Bad Rap?

- Date back to before cyber-security was an issue
- Last a long time
  - Source code, or passcode unavailable
- Extremely flexible/powerful
  - Perhaps too much so for some applications
- “Programmable”
  - Different vendors
  - Different staff
  - Different times in life cycle
- Showdan.io exposes some that weren’t programmed securely!



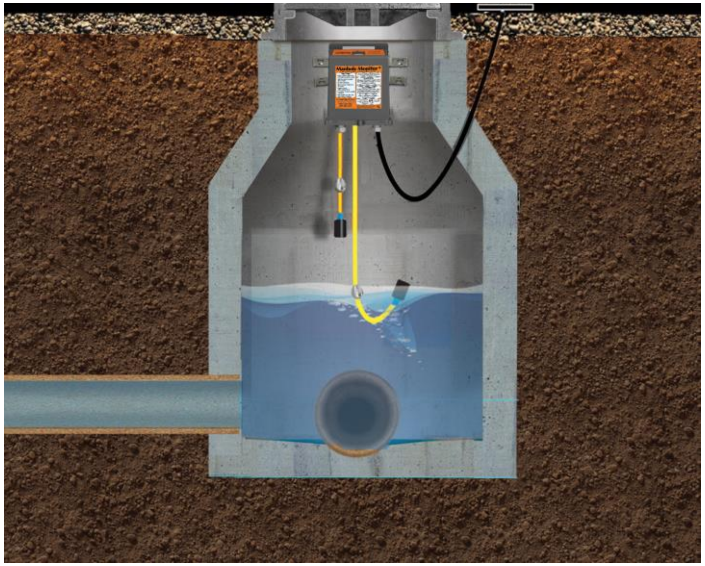
Discover the Internet using search queries shared by other users.

best ip cam search I have found yet.

Methods of Transmitting Mission's Way

- Website is 2048-Bit SSL certificates
  - URL= https:
  - SOC 2 Compliant
  - FedRamp Compliant
- 256-Bit AES (Advanced Encryption Standard)
  - Continuous "Socket Connections"
  - (MFA) Multi Factor Authentication
- National coverage (GSM- HSPA+ (4G)
- 3G, 4G or LTE
- Uses TCP IP (Transmission Control Protocol)
  - The only option for Control….Missed Data…..No Way!!!

Mission RTUs

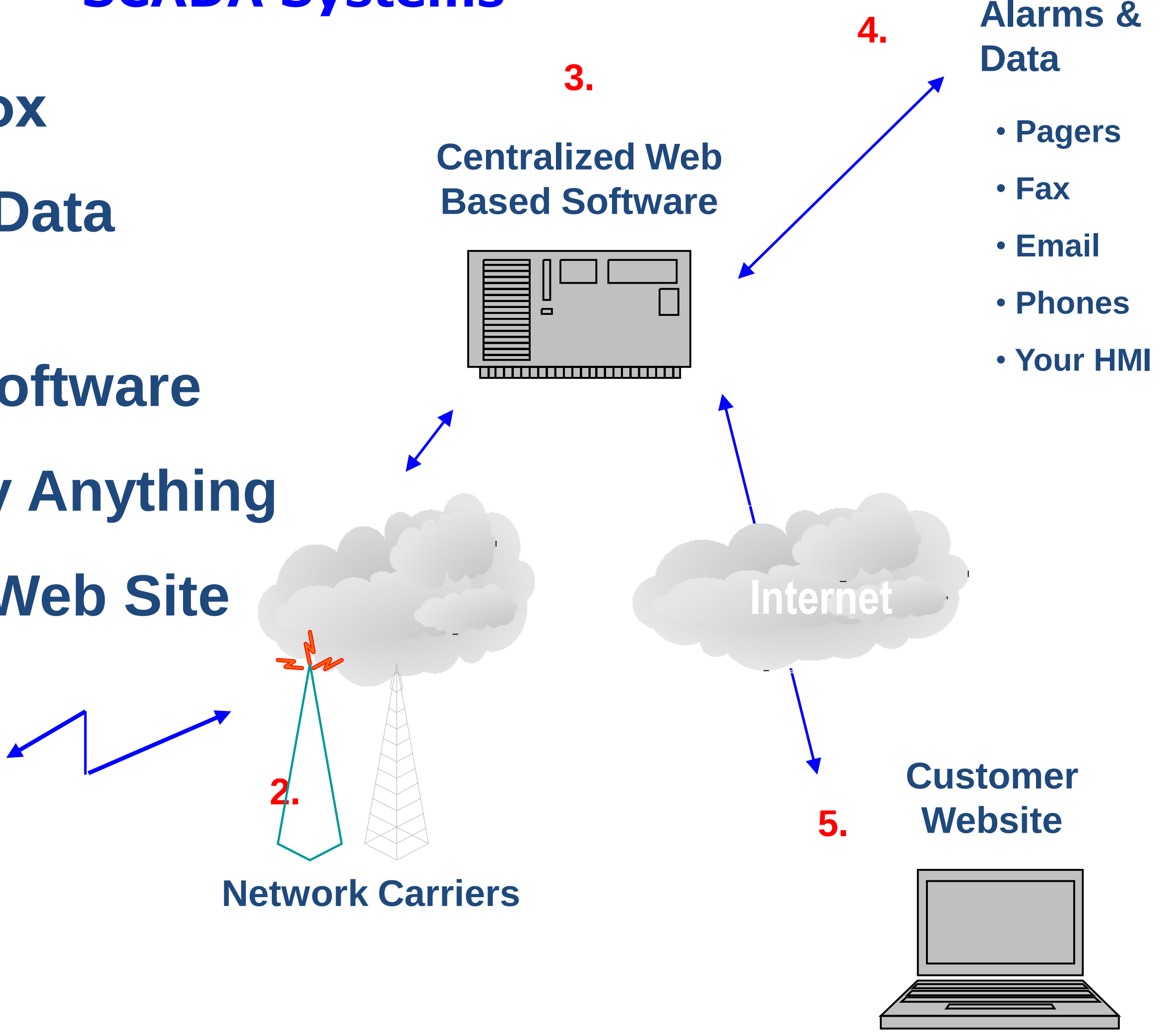


Basic Components of Internet Enabled Monitoring & SCADA Systems

1. Field RTU…The Box
2. National Wireless Data Networks
3. Centralized Web Software
4. Alarms To Virtually Anything
5. Secure Customer Web Site

1.

RTU



2.

Network Carriers

3.

Centralized Web Based Software

4.

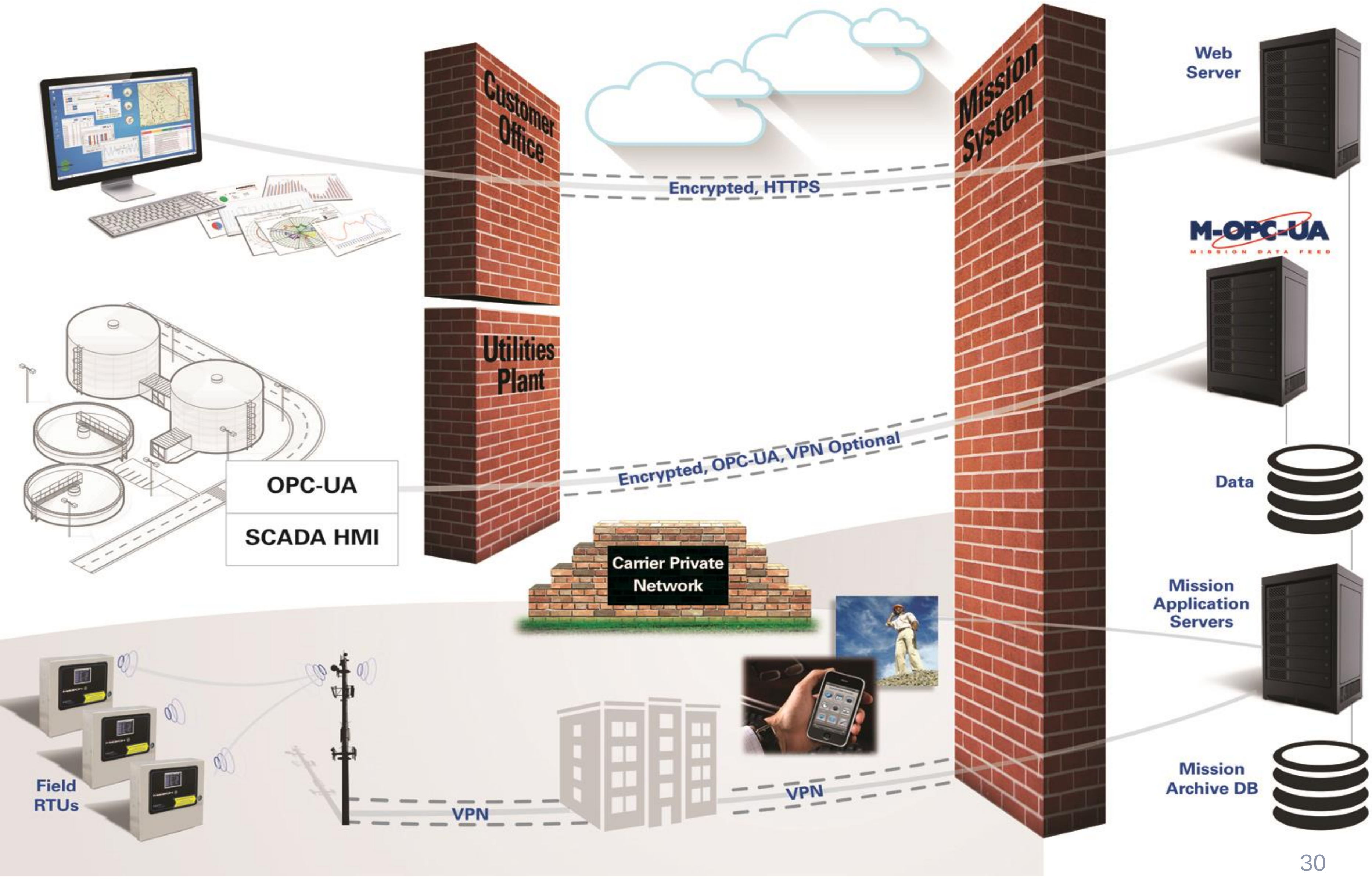
Alarms & Data

- Pagers
- Fax
- Email
- Phones
- Your HMI

5.

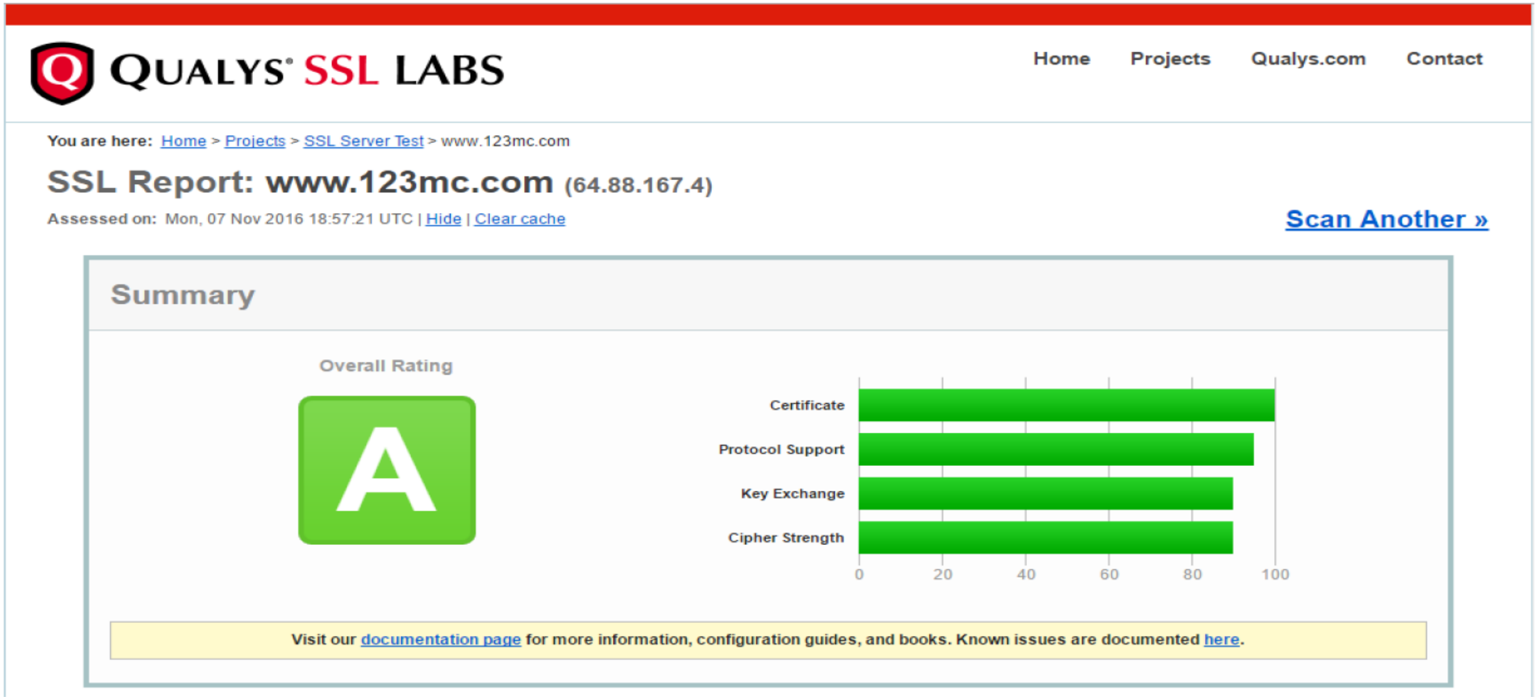
Customer Website

Mission Architecture



Methods of Transmitting Mission's Way

- Website is 2048-Bit SSL certificates
  - URL= https:



You are here: Home > Projects > SSL Server Test > www.123mc.com

SSL Report: www.123mc.com (64.88.167.4)

Assessed on: Mon, 07 Nov 2016 18:57:21 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A

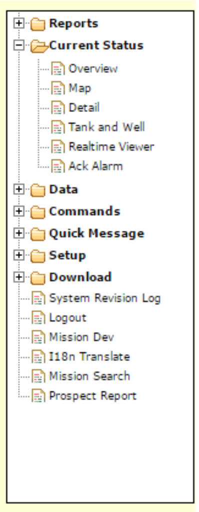
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

The Primary Applications

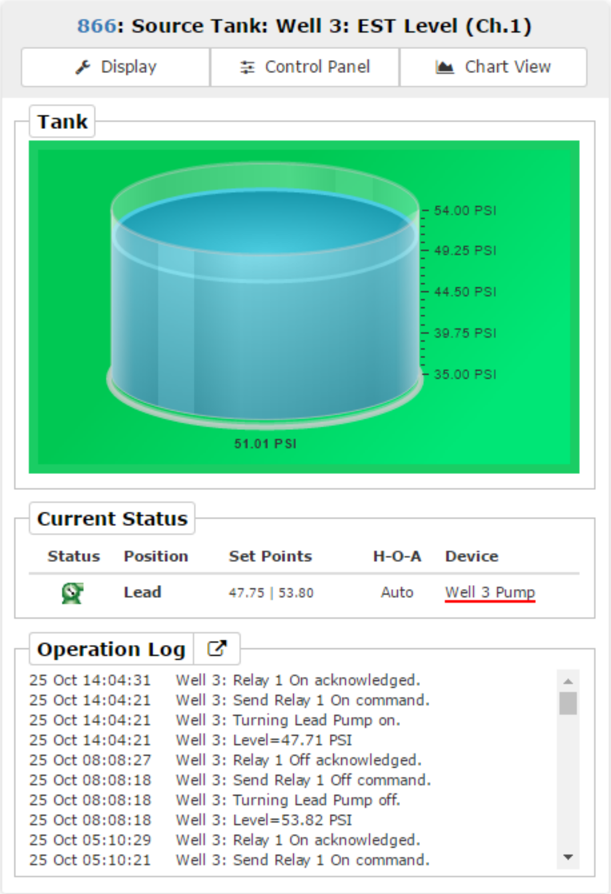
Tank
Lift Station
Well
Monitor
Remote Control
Comply
In-Sewer Level Alarm

Conserve Resources With Managed SCADA

Details With Each Click…



Tank and Well



Current Status

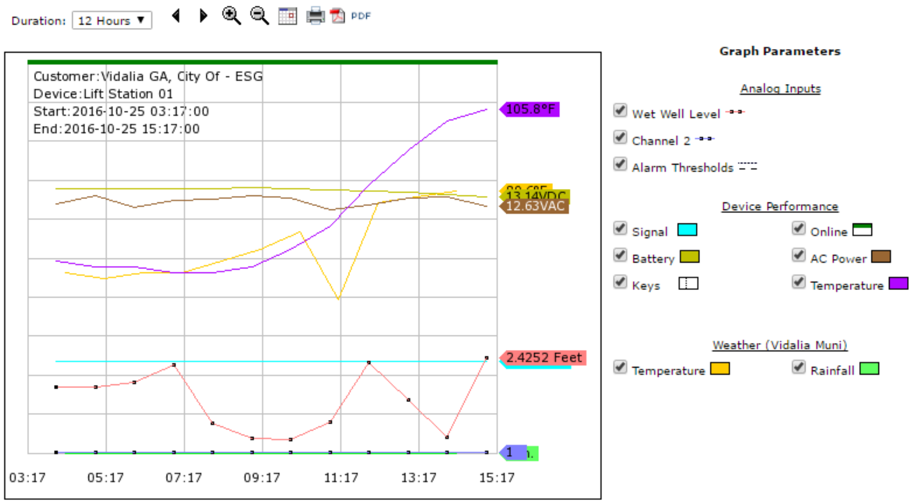
Status	Position	Set Points	H-O-A	Device
	Lead	47.75 | 53.80	Auto	Well 3 Pump

Operation Log

```
25 Oct 14:04:31   Well 3: Relay 1 On acknowledged.
25 Oct 14:04:21   Well 3: Send Relay 1 On command.
25 Oct 14:04:21   Well 3: Turning Lead Pump on.
25 Oct 14:04:21   Well 3: Level=47.71 PSI
25 Oct 08:08:27   Well 3: Relay 1 Off acknowledged.
25 Oct 08:08:18   Well 3: Send Relay 1 Off command.
25 Oct 08:08:18   Well 3: Turning Lead Pump off.
25 Oct 08:08:18   Well 3: Level=53.82 PSI
25 Oct 05:10:29   Well 3: Relay 1 On acknowledged.
25 Oct 05:10:21   Well 3: Send Relay 1 On command.
```

Analog Readings

Lift Station 01



Customer:Vidalia GA, City Of - ESG
Device:Lift Station 01
Start:2016-10-25 03:17:00
End:2016-10-25 15:17:00

Graph Parameters

Analog Inputs

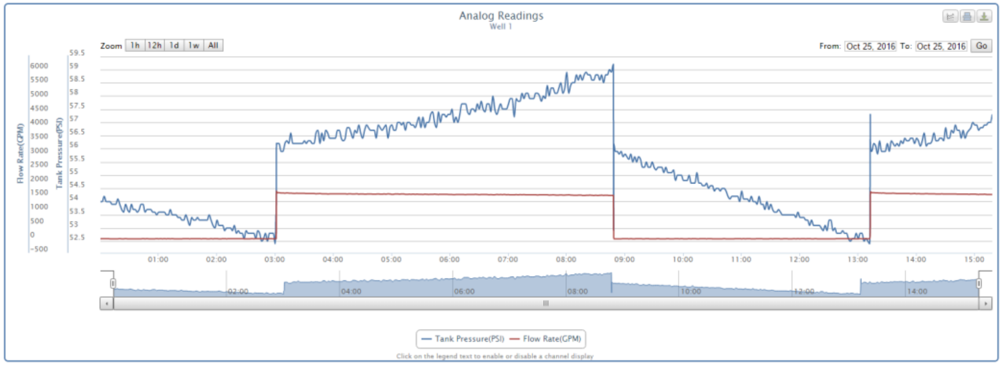
- ☑ Wet Well Level
- ☑ Channel 2
- ☑ Alarm Thresholds

Device Performance

- ☑ Signal
- ☑ Online
- ☑ Battery
- ☑ AC Power
- ☑ Keys
- ☑ Temperature

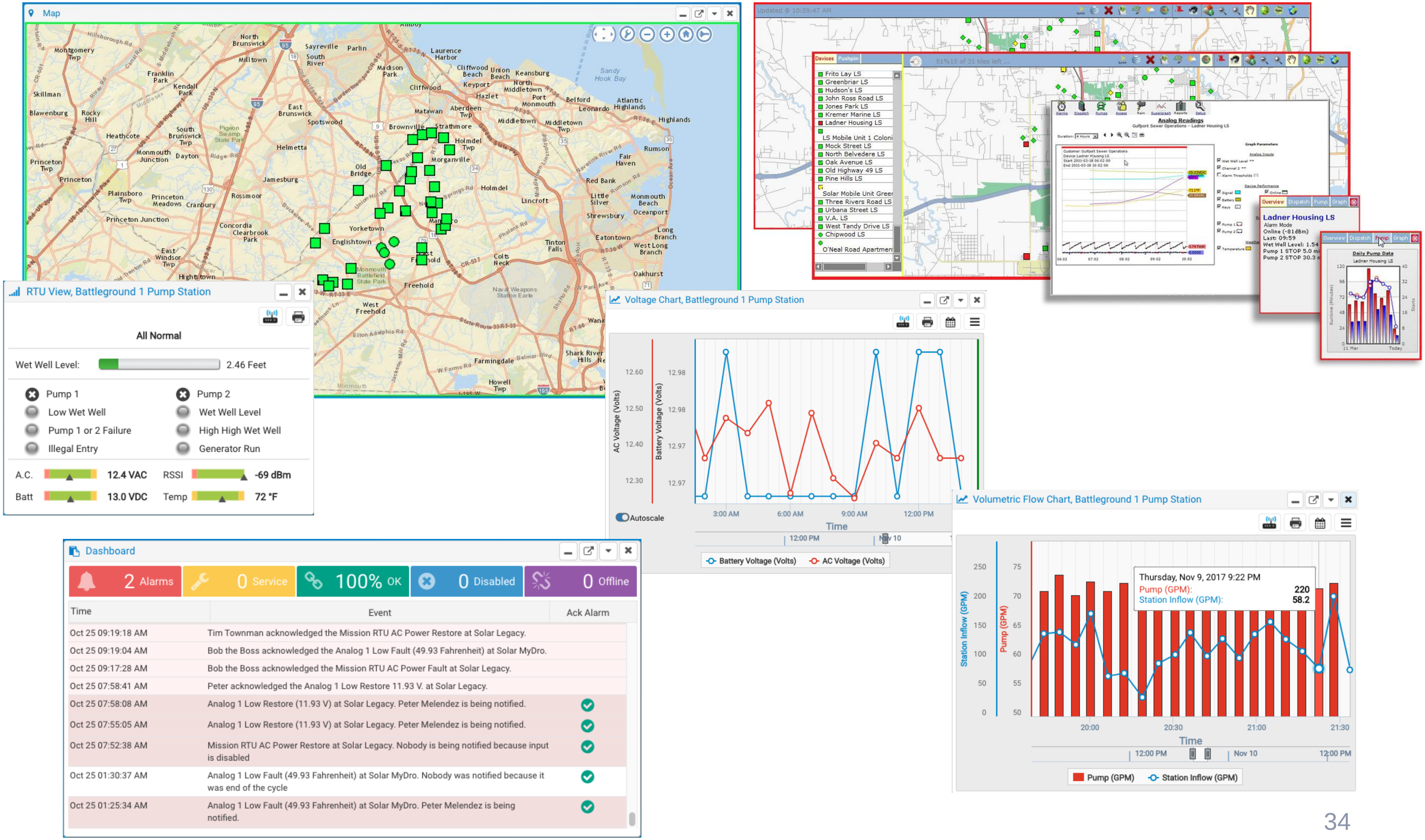
Weather (Vidalia Muni)

- ☑ Temperature
- ☑ Rainfall



MISSION COMMUNICATIONS

Your System Status At a Glance



RTU View, Battleground 1 Pump Station

All Normal

Wet Well Level: 2.46 Feet

☒ Pump 1	☒ Pump 2
● Low Wet Well	● Wet Well Level
● Pump 1 or 2 Failure	● High High Wet Well
● Illegal Entry	● Generator Run

A.C.	12.4 VAC	RSSI	-69 dBm
Batt	13.0 VDC	Temp	72 °F

Frito Lay LS
Greenbriar LS
Hudson's LS
John Ross Road LS
Jones Park LS
Kremer Marine LS
Ladner Housing LS
LS Mobile Unit 1 Coloni
Mock Street LS
North Belvedere LS
Oak Avenue LS
Old Highway 49 LS
Pine Hills LS
Solar Mobile Unit Greer
Three Rivers Road LS
Urbana Street LS
V.A. LS
West Tandy Drive LS
Chipwood LS
O'Neal Road Apartmen

Ladner Housing LS
Alarm Mode
Online (-81dBm)
Last: 09:59
Wet Well Level: 1.54
Pump 1 STOP 5.0 mi
Pump 2 STOP 30.3 m

Voltage Chart, Battleground 1 Pump Station

Volumetric Flow Chart, Battleground 1 Pump Station

Thursday, Nov 9, 2017 9:22 PM
Pump (GPM): 220
Station Inflow (GPM): 58.2

Dashboard

2 Alarms | 0 Service | 100% OK | 0 Disabled | 0 Offline

Time	Event	Ack Alarm
Oct 25 09:19:18 AM	Tim Townman acknowledged the Mission RTU AC Power Restore at Solar Legacy.	
Oct 25 09:19:04 AM	Bob the Boss acknowledged the Analog 1 Low Fault (49.93 Fahrenheit) at Solar MyDro.	
Oct 25 09:17:28 AM	Bob the Boss acknowledged the Mission RTU AC Power Fault at Solar Legacy.	
Oct 25 07:58:41 AM	Peter acknowledged the Analog 1 Low Restore 11.93 V. at Solar Legacy.	
Oct 25 07:58:08 AM	Analog 1 Low Restore (11.93 V) at Solar Legacy. Peter Melendez is being notified.	✓
Oct 25 07:55:05 AM	Analog 1 Low Restore (11.93 V) at Solar Legacy. Peter Melendez is being notified.	✓
Oct 25 07:52:38 AM	Mission RTU AC Power Restore at Solar Legacy. Nobody is being notified because input is disabled	✓
Oct 25 01:30:37 AM	Analog 1 Low Fault (49.93 Fahrenheit) at Solar MyDro. Nobody was notified because it was end of the cycle	✓
Oct 25 01:25:34 AM	Analog 1 Low Fault (49.93 Fahrenheit) at Solar MyDro. Peter Melendez is being notified.	✓

Is Cellular Reliable

- Direct relationships ATT “First Net”, Verizon, Sprint, Rogers, Tellus, Telenor
- GSM- HSPA+ (4G), Some still remain on CDMA
- Nationally maintained towers
- Radios are stationary
- Omni v. directional antennas
- Multi-Carrier Radios
- Connections monitored
- 99+% connectivity for 37,000+ RTUs and 4000 Utilities throughout the US & Canada!

Q & A