Using Radios for SCADA, Protection and System Automation

Topics Covered

- Application Considerations
- Cyber Security
- O&M Considerations
- Radio Configurations
- Types of Radios
- Path Analysis
- Radio Case Studies

Radio communications in the OT world – When does it make sense?

- Difficult terrain
- Remote locations
- Right of way issues
- Cost constraints
- Short construction time

Application Considerations

- Pros
  - Cost (usually, depends on project specifics)
  - Viable when fiber is not
  - Faster construction time
  - Has adequate bandwidth and speed for OT needs
- Cons
  - Can experience issues when line-of-sight is lost
  - Limited to distances of around 40 miles
  - May require more initial set up and troubleshooting effort
  - May require additional O&M capabilities

Cyber Security

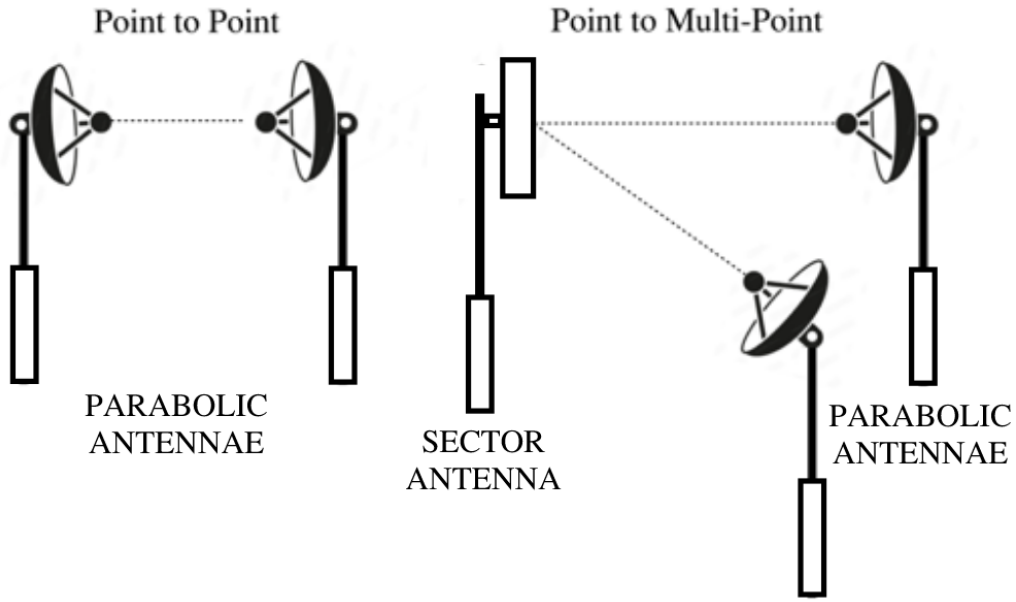
- Wireless Security
  - Encryption: AES 256
  - Radio whitelist by MAC ID
  - Optional FIPS 140 certification
- Network Level Security
  - Turn off non-secure remote connection protocols
    - Telnet, HTTP, SNMP V3 are examples of non-secure protocols
    - SSH, HTTPS are examples of secure protocols
- Set strong passwords and remove unused accounts

Operations and Maintenance Considerations

- RF Interference
  - Requires regular monitoring of wireless links
- System maintenance considerations
  - Must maintain line of sight
    - Tree trimming and vegetation control
    - Future construction may obstruct LoS
- Wildlife
  - Nesting
  - Bird strikes

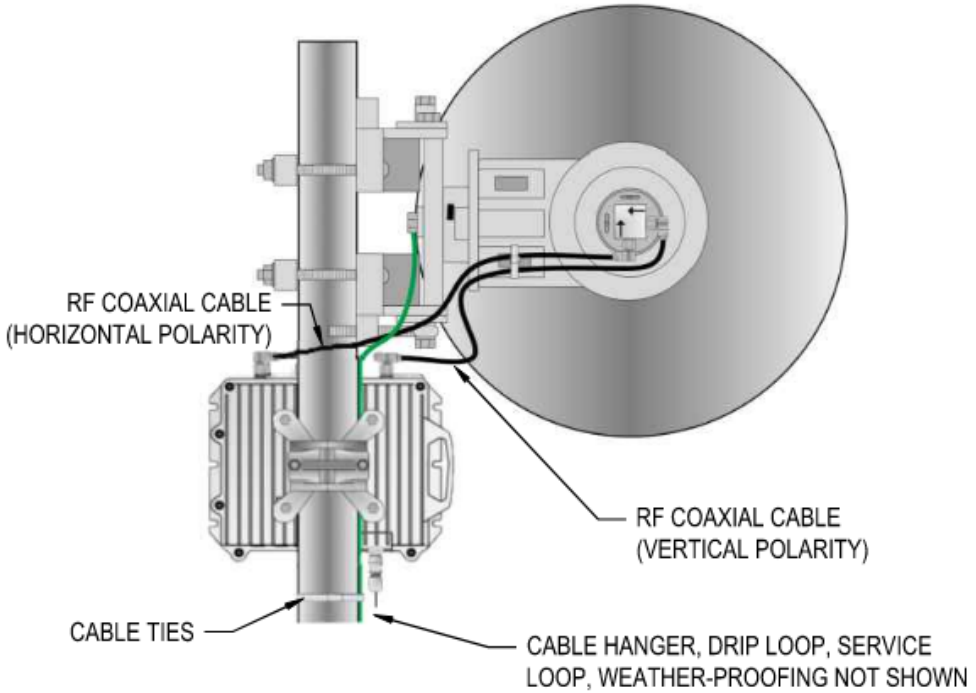
Radio Configurations Considered

- Point to Point (PTP)
  - One sector controller and one receiver
  - Utilized parabolic antennae
- Point to Multipoint (PMP)
  - One sector controller and many subscribers
    - Requires more robust hardware
  - Utilizes a combination of parabolic and sector antennae



Types of Antennas

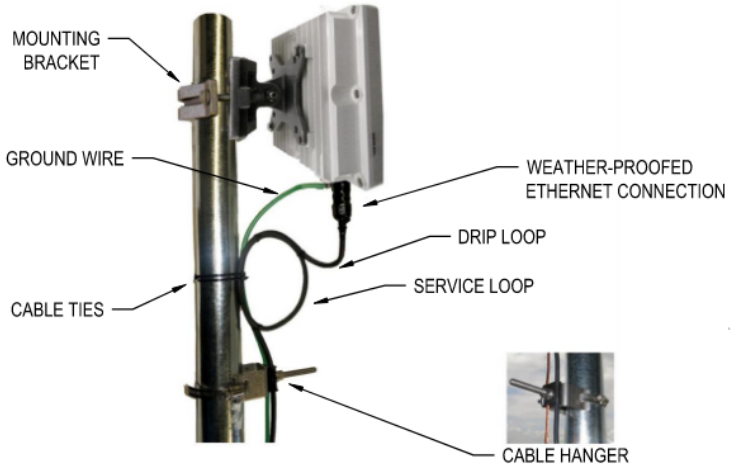
- Parabolic Antenna
  - Point to Point
  - Tight beam (typically ~3°)



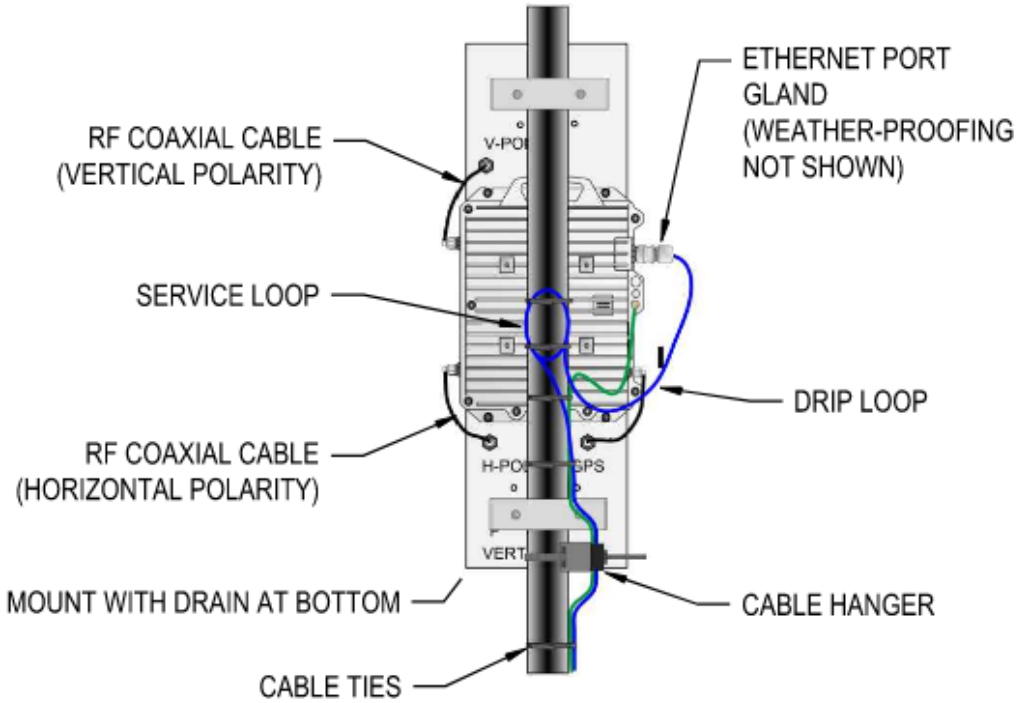
REDLINE ELLIPSE RADIO WITH PARABOLIC ANTENNA (REAR VIEW)

Types of Antennas (Continued)

- Integrated and Sectoral Antennas
  - Point to Point and Point to Multipoint
  - Wider beam (up to ~120°)



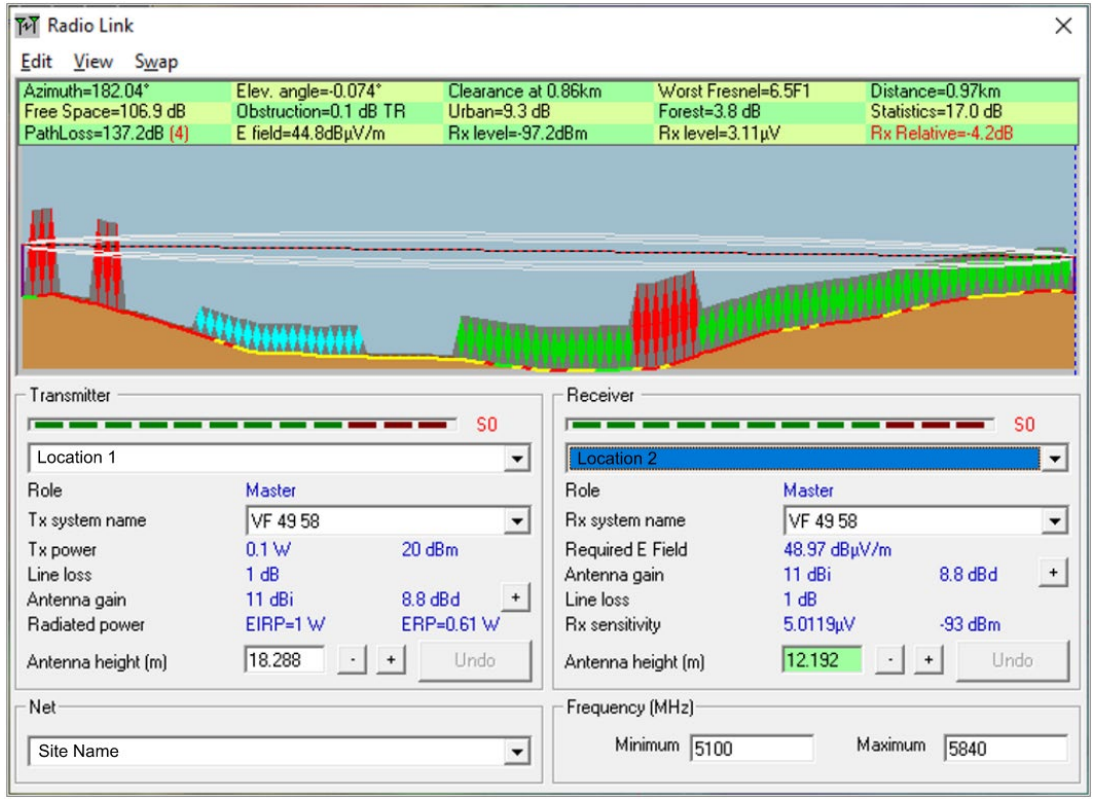
REDLINE ELTE INTEGRATED RADIO/ANTENNA (SIDE VIEW)



REDLINE ELLIPSE RADIO WITH SECTORAL ANTENNA (REAR VIEW)

Radio Path Analysis

- Perform feasibility analysis for each radio link
  - Radio heights
  - Radio locations
  - EIRP (Equivalent Isotropic Radiate Power)
    - Cannot exceed a set level for a given area to avoid interference with other users (set by FCC)
- GIS data can be utilized to identify radio locations and elevations
- Field testing still required



Case Study #1 – Overview

- Two geographically separate SCADA systems
- Needed engineering access to SCADA systems from an alternate location
- Provides remote operations center during state of emergency
- Fiber not an option
  - No existing right of way established
  - Cost prohibitive to run fiber

For illustrative purposes – Does not represent actual case study

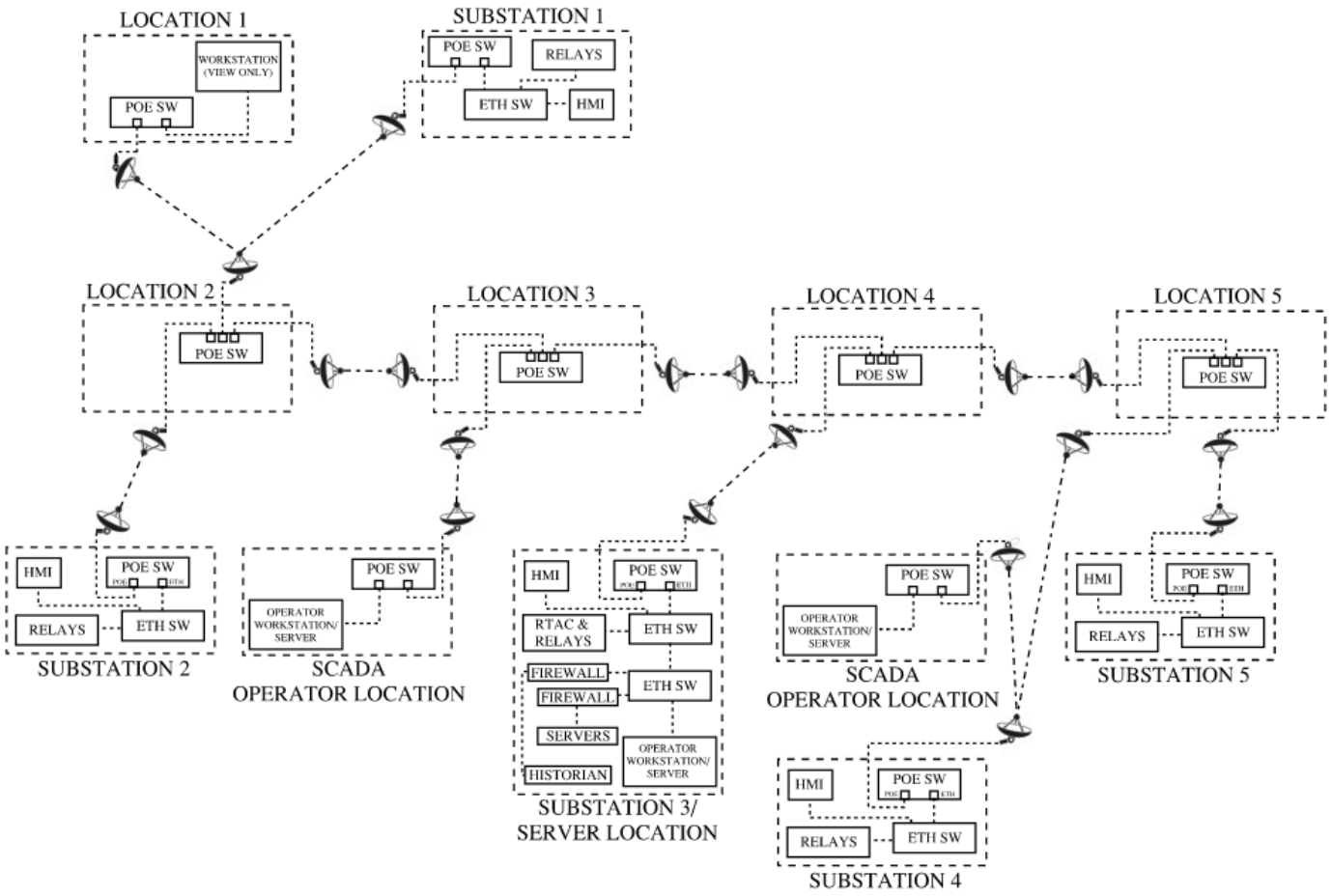
Case Study #1 – Solution

- 100ft pole at each location to allow direct line of sight above tree line
- Point to Point radio communications
- DNP3 Protocol

Case Study #2 – Overview

- Required substation level SCADA communications
- Difficult, rocky terrain
  - Very difficult/expensive to trench/bore for underground fiber
- Historical/tourist sites
  - Unable to run fiber overhead due to aesthetic requirements
- Heavily wooded
  - Significant differences in seasonal foliage

Case Study #2 – Solution

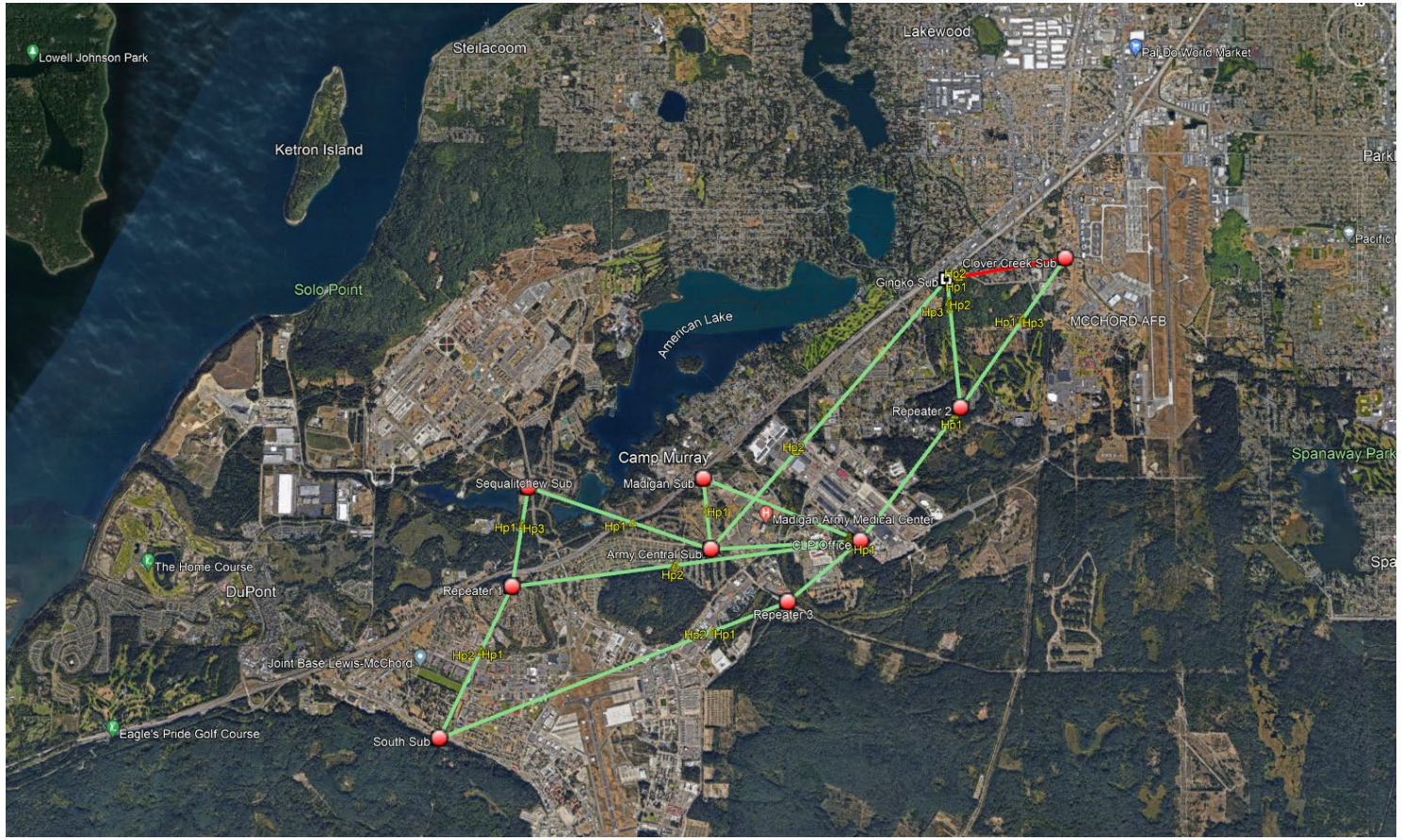


- 12 radio locations
  - Mixture of PTP and PMP communications
- DNP3 Protocol
- Utilized building infrastructure along with new poles for radio placement

Case Study #3 – Overview

- Several existing substations/locations to be added to new SCADA system
- Location in PNW covering large geographical area
  - Very tall and dense evergreen vegetation
- Difficult terrain
- Divided by major highway
- Lots of existing radio communications using free spectrum in the area
  - LTE cell network providers
  - Intermittent radar sites

Case Study #3 – Solution



- Multiple PTP links using multiple frequencies
  - Per device monitoring
- Mixture of all three types of radios based on backhaul link requirements, distance and terrain
- 105’-145’ wood and composite poles at each substation
- Utilized repeaters to allow for connectivity over hills with heavy 100’ evergreen vegetation
- Field testing was crucial

Case Study #4 – Overview

- Large, remote area with poor reliability
  - Only 3 linemen available to cover
  - Contractually obligated to 2-hour response time
- Wanted to implement FLISR system to improve reliability
- Minimal capital funds available
  - Key intent was to reduce O&M expenses

Case Study #4 – Solution

- Utilized radio communications to communicate with new overhead reclosers with 651R relays
  - Radios mounted directly to each recloser pole
- Sector antenna and controller at main substation
  - Single center frequency
  - Low bandwidth but fast and reliable
- RTAC is main controller for fault location, isolation and system reconfiguration (FLISR)
  - SEL Fast Message Protocol
  - Interfaces with cell modem to alert crews to faults and provide system statuses

Summary

- Know your application
- Perform cost analysis
- Field testing during design
- Choose correct radio and antenna type and configuration
- Consider construction constraints for your site
- Practice good cyber hygiene
- Lessons learned in case studies