



PROJECT PROFILE

Microwave Private Network

Sweetwater Authority

Client background

Sweetwater Authority (SWA) provides water treatment and distribution to 200,000 people in a service area that covers 32 square miles near San Diego, California. It is a publicly owned water agency governed by an elected Board of Directors. Since 1977 Sweetwater Authority has provided its customers their water services and has sourced water from three primary sources: freshwater ground wells, the Sweetwater Reservoirs, and San Diego Formation wells which provide brackish groundwater. Enterprise Automation has provided automation and integration services for Sweetwater Authority since 2005.

Project background

Sweetwater Authority's SCADA system monitors and controls remote assets from Hydro stations and reservoirs to booster sites and treatment plants. With so many resources spread out over a large geographical area, SWA required telemetry to communicate between all sites. As data grew, and more devices sought to communicate, older radio-based networks and landlines couldn't provide enough bandwidth. In addition, Sweetwater Authority planned for an Emergency Operations Center which had full SCADA control in case they ever had to abandon their primary control center. In order to securely future proof their system, SWA constructed their own private microwave network ring.

EA solution

EA was tasked with network design of the microwave system. EA engineers also updated the many PLC communications programs that were installed at the remote sites so they could be compatible with an updated communication system and updated the IP address of every device on the SCADA network to comply with the new subnet and VLAN standards. Engineers did additional testing to ensure the added networking components such as switches and firewalls would all work as intended with the new PLC programming and that startup and cutover would be quick and painless. EA simulated the entire network infrastructure within the Irvine office.

Project Manager



Jeff
Benson

Project Technical Lead



Alex
Coker

Key Insights:

- Radio network simulation was critical for in house testing
- Cyber security optimization through rugged routers allowed additional network segregation

Key Technologies:

- Cisco Networking Equipment
- MOXA Industrial Firewalls
- Palo Alto Firewalls