Unitywater's Telemetry SCADA Radio Network Upgrade

Presented by **Raymond Lao**

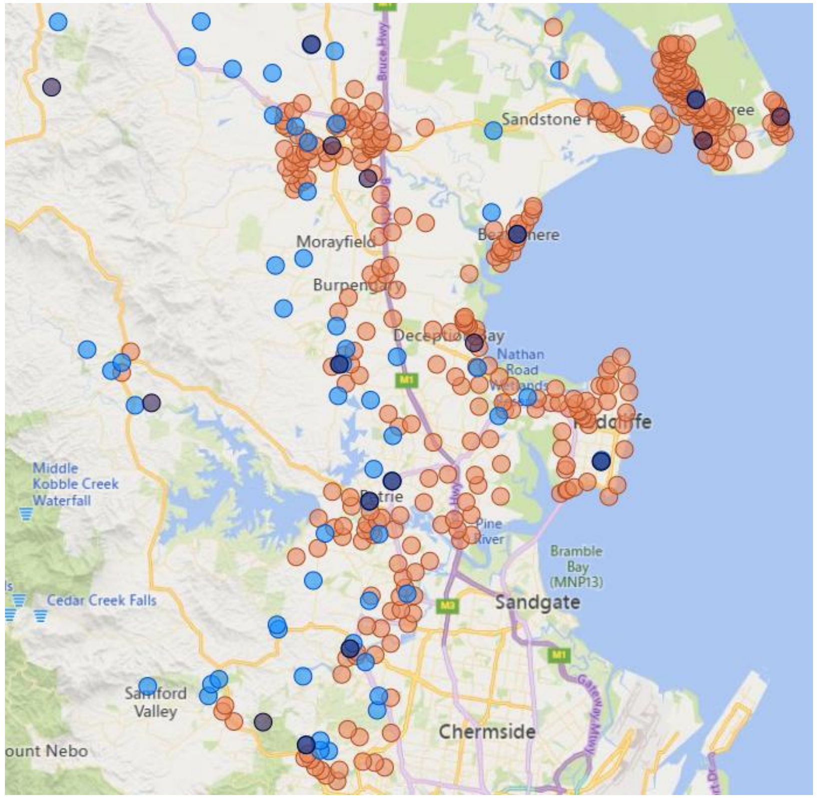
Lead OT Engineer (Networks) at **Unitywater**

Radio Telemetry at Unitywater

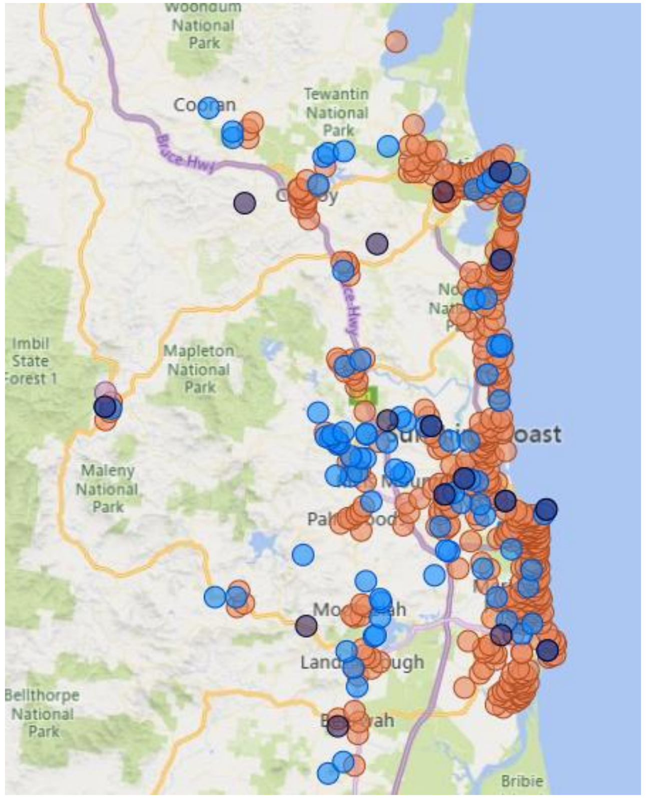
- Our telemetry SCADA monitors 1,000+ water and sewer sites, split across a North and South network (total 5,000 km^2 area).
- Each site is controlled by a **Remote Telemetry Unit** (RTU) that communicates back to SCADA.
- Radio is essential for providing reliable communication:
  - Between Control Room and RTUs
  - Between different RTUs for remote equipment control (such as filling a reservoir from a remote pump station)

Radio Telemetry at Unitywater

Southern Telemetry Network

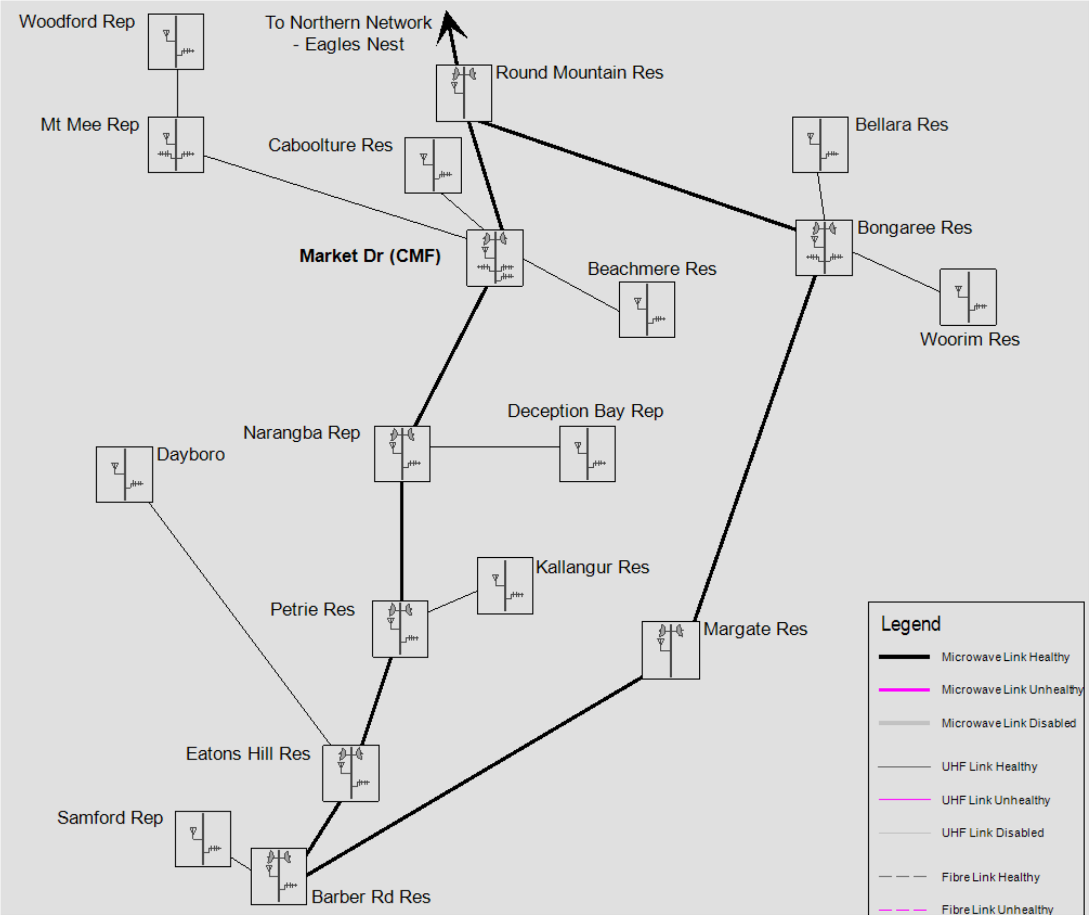


Northern Telemetry Network



Existing Radio Network

- Backhaul: **1Mbps** microwave ring linking our PTMP base stations.
- Fronthaul: Serial UHF analog PTMP radios (Trio E-Series) providing **9.6kbps data rate** across **12.5kHz bandwidth**.
- Midhaul: Some PTMP bases connect into main ring as spurs, utilizing UHF PTP serial link (Trio E-Series) operating at **19.2kbps** across **25kHz bandwidth**.



Why upgrade?

- Remote troubleshooting was not possible, meaning physical site visits were often needed.
- Trio E-Series radios were end-of-life and experiencing increasing rates of failure.
- Limited performance diagnostics, making investigation of radio signal issues difficult, especially in the uplink direction.
- Backbone ring network was on a flat IP subnet, limited control of network traffic

Why not migrate to cellular?

- LTE relies on an external provider, a single point of failure for which we have no oversight.
- Telecom providers not willing to provide suitable SLAs.
- As critical infrastructure, we need to maintain control of our network at all times.

Upgrade Tasks

Upgrading UHF radios from analog serial to digital Ethernet

Converting hybrid serial-Ethernet network to full Ethernet

Digital Ethernet Radios

- Upgrade project started with a market evaluation phase to decide new radio product.
- After evaluation and bench-testing of various products in the market, decision was made to adopt 4RF Aprisa SR+ radios.
- Final decision was primarily based on ease-of-use, diagnostic & fleet management capabilities.

Full Ethernet Network

- Existing radio network was hybrid Ethernet/serial:
  - Ethernet on microwave backhaul
  - Serial on all UHF radio links

- With digital Ethernet radios, a full Ethernet network was achievable, allowing better network throughput, accessibility and control through L3 routing.

- Segregate each base station to its own subnet, then introduce firewalls to address the increased cybersecurity risks of a full Ethernet network.

Full Ethernet Network

- A decision was made to not utilize NAT for standardizing individual site LAN networks to a common IP range.

- This meant a systematic IP schema was needed to allocate unique IP addresses to all network devices across our 1,000+ telemetry sites.

	Base Station ID	Site ID	RTU ID	Outstation Description	Physical Location	DNP3 Address	Router WAN IP Address	WAN Subnet Mask	Router LAN IP Address	Outstation IP Address
01	3	0	0	Monitor RTU - Base	Base Station	103	010.001.255.014	255.255.255.248	010.003.000.254	010.003.000.201
	3	0	1	Reserved	-	11000	-	-	-	-
	3	1	1	Site RTU 1 - Site 01	Remote	11001	010.003.000.001	255.255.255.000	010.003.001.254	010.003.001.001
	3	2	1	Site RTU 1 - Site 02	Remote	11002	010.003.000.002	255.255.255.000	010.003.002.254	010.003.002.001
	3	3	1	Site RTU 1 - Site 03	Remote	11003	010.003.000.003	255.255.255.000	010.003.003.254	010.003.003.001
	3	4	1	Site RTU 1 - Site 04	Remote	11004	010.003.000.004	255.255.255.000	010.003.004.254	010.003.004.001

Upgrade Outcomes

Rollout completed in two years

Significantly improved data speeds across telemetry network

Better control and monitoring of network traffic

Redundancy of radio and network equipment

Better diagnostics of RF signal quality

Rollout Schedule

- **Two years** needed to fully cutover all 1,000+ telemetry sites (950+ radios) on both North and South radio networks.

- Initial **pilot phase**: cut over one small-sized base station catchment on each North and South network to assess performance.

- After 6-month proving period, **wider rollout** commenced.

- Logistical challenges in keeping up pace of rollout while ensuring **minimal downtime** of telemetry network.

Telemetry Data Speeds

- Licensed channel bandwidth also upgraded from 12.5kHz to **25kHz**.

- Using **digital QAM**, the new radio network significantly outperforms the baseline 9.6kbps data rate of the old network.

- QAM algorithm dynamically adjusts RF speeds based off signal quality:
  - Sites with **strong** radio signal: 120kbps using 256QAM
  - Sites with **marginal** radio signal: 40-50kbps using 16QAM
  - Sites with **poor** radio signal: 20kbps using QPSK

Network Control & Monitoring

- Each base station PTMP network segmented into its own subnet, routed by **firewall routers** at each base station site.

- Firewalls **control** and **monitor** traffic to and from the base station network, improving cybersecurity and diagnostic capabilities.

- **OSPF** used to route traffic between base stations, better recovery times than ring protocols.

Network Redundancy

- **Hot standby** arrangements used at base stations for base radios, switches & firewalls.
- **LTE modem backup** implemented on spur base stations.
- **BGP routing** used to automatically fail over to LTE modem if PTP link to spur bases is lost.

RF Diagnostic Capabilities

- New radios allow monitoring of SNR and RSSI in both uplink and downlink directions via SNMP.
- A dedicated RTU was installed at each base station to poll all its remote radios and send aggregated data back to SCADA for trending.
- RTU ensures all downlink data from remotes and uplink data from base are mapped to the correct SCADA site.

Upgrade Challenges

Streamlining the upgrade rollout

Maintaining a hybrid network of old and new radios

Managing RF interference and cross-talk

Streamlining the Rollout

- Use of a temporary rack to keep old radio network online during cutover, minimizing downtime.

- A template configuration was applied to every remote radio.

- Each telemetry site on SCADA generates a **4RF configuration script** that loads onto each templated radio to apply site-specific settings:
  - Terminal details (radio name, address, etc)
  - Tx/Rx frequencies
  - IP address settings

Maintaining a Hybrid Network

- During the two-year rollout, the radio network will consist of old serial radios and new Ethernet radios.

- The flat network of the old radios needs to coexist alongside the new segregated network of the new radios.

- Introduce a temporary VLAN arrangement so that the two networks can operate simultaneously in a hybrid state.

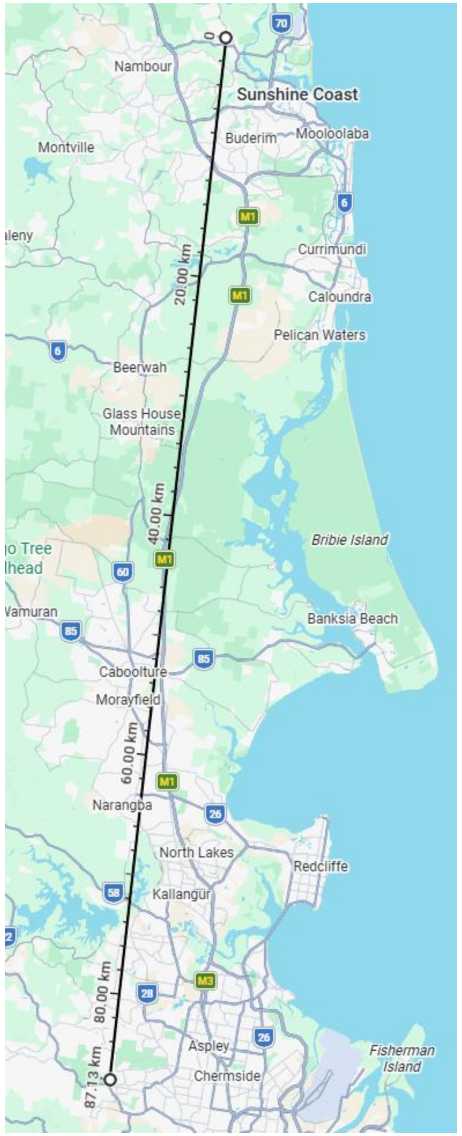
- Performance limitations: hybrid network takes up to three minutes to recover from a radio link going down.

RF Cross-Talk

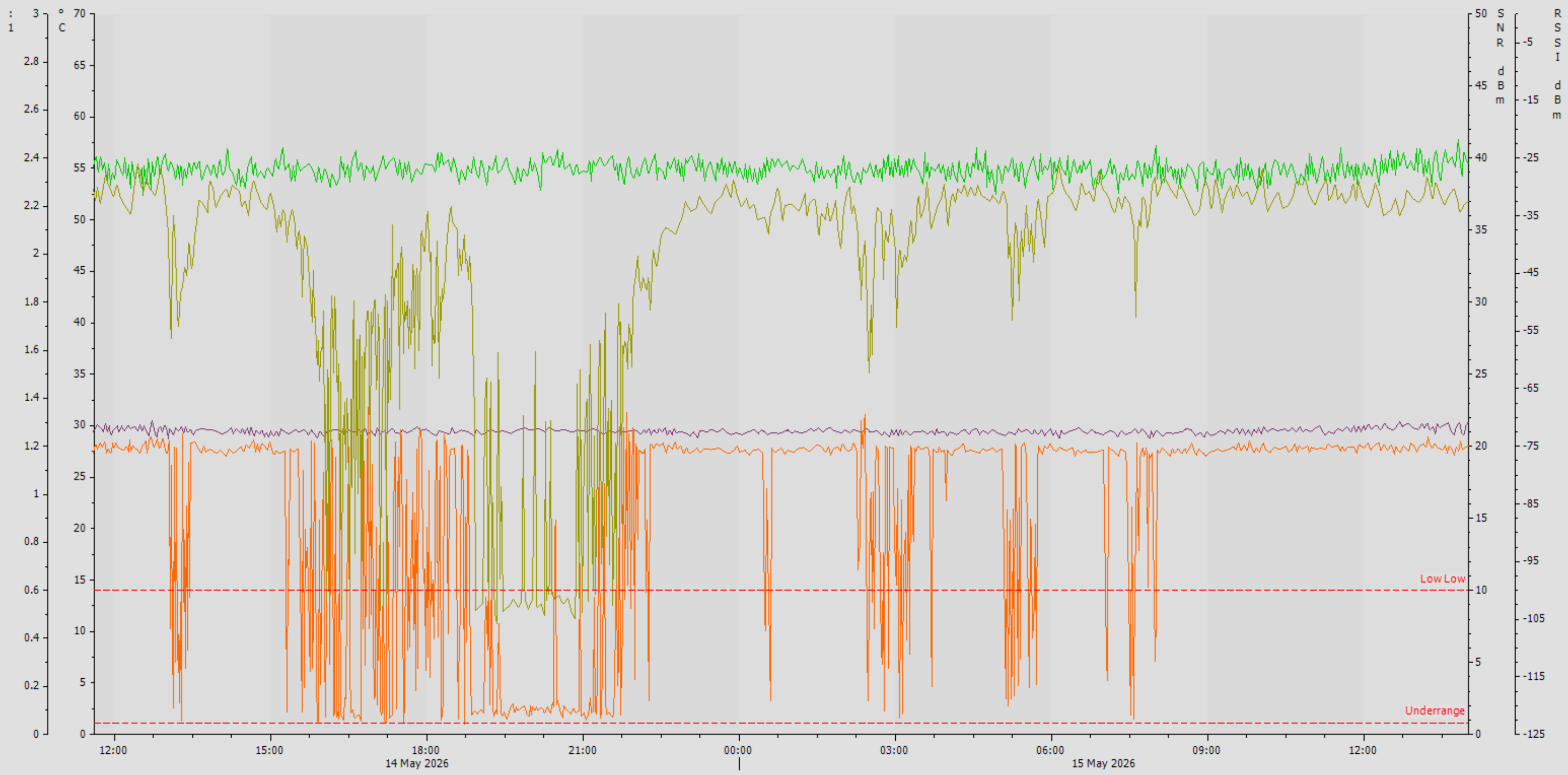
- Post-upgrade: mysterious uplink signal dropouts on all South telemetry remote sites talking to our Barber Road base station.
- Root cause: RF cross-talk with Bli Bli base station 87km away on our North network.
- Bli Bli is assigned the same frequency pair as Barber Road by ACMA.

RF Cross-Talk

- ACMA frequency reuse distance is 100km between base stations per RALI-FX16 specification.
- Due to crowding in 470-480MHz, ACMA issued us reused 25kHz assignments between our North and South bases that are separated by >90km.
- Despite very weak signal, Barber Rd remotes were still able to momentarily register to Bli Bli base on random occasions.



RF Cross-Talk



Trace	Type	Ruler Value	Axis
VSWR	Processed Historic	-	:1
Temperature	Processed Historic	-	ºC
Downlink RSSI	Processed Historic	-	RSSI dBm
Uplink RSSI	Processed Historic	-	RSSI dBm
Downlink SNR	Processed Historic	-	SNR dBm
Uplink SNR	Processed Historic	-	SNR dBm

RF Cross-Talk

- Different OTA encryptions did not eliminate cross-talk. Radios were registering on their own proprietary protocols.
- 4RF radios have a base station ID feature designed for allowing frequency reuse.
- Changing the base station ID on Barber Road base and its remotes resolved the cross-talk issues.

RF Interference

- SCADA communications to a reservoir site in Coolum started deteriorating shortly after the radio was upgraded.

- Replacing radio and antenna did not fix the issue but moving the antenna to a lower location provided improvement to signal.

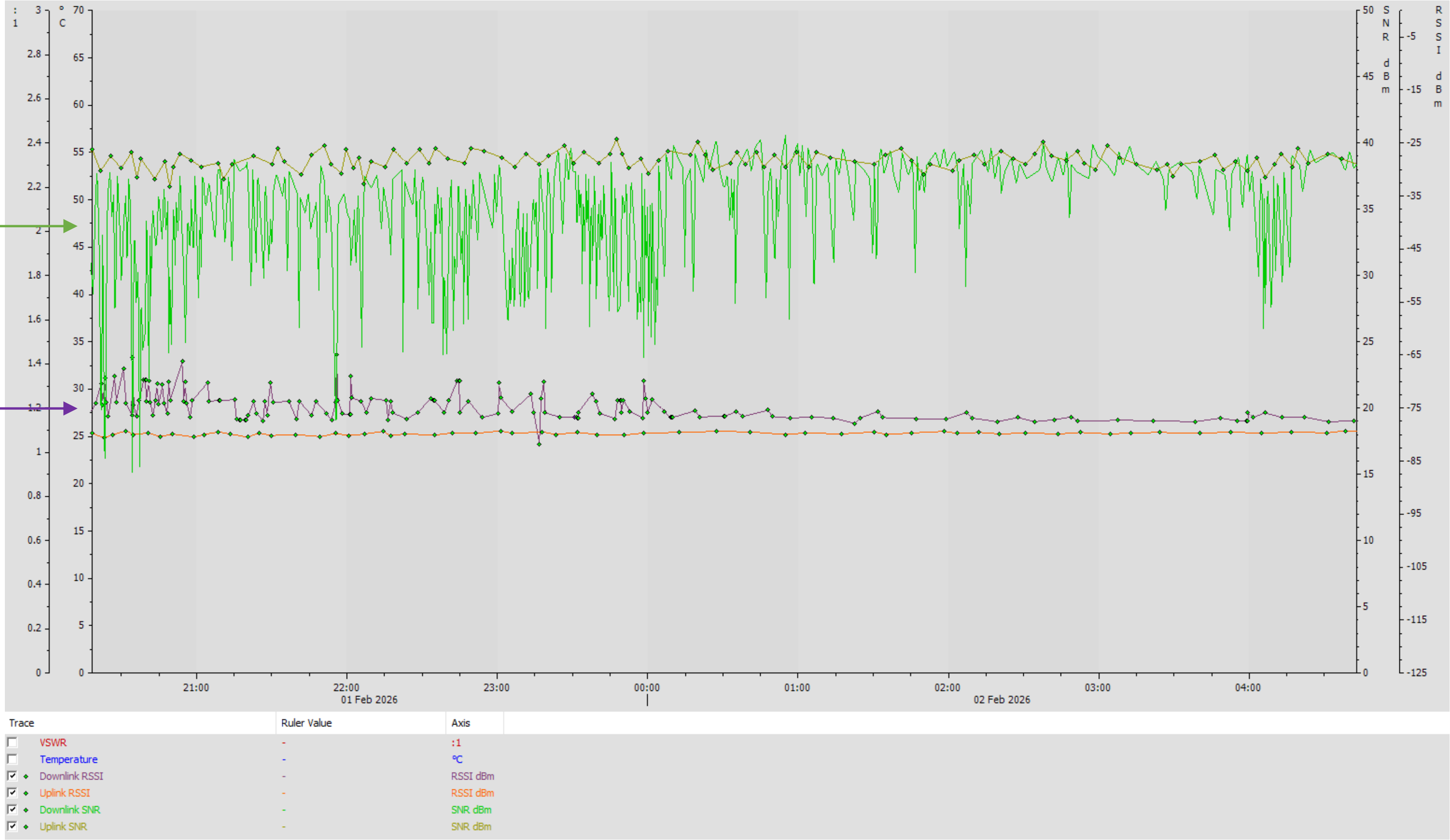
- SCADA trends showed the downlink RSSI getting stronger when the downlink SNR plummeted, indicating interference on downlink frequency.

ARCIA

RF Interference

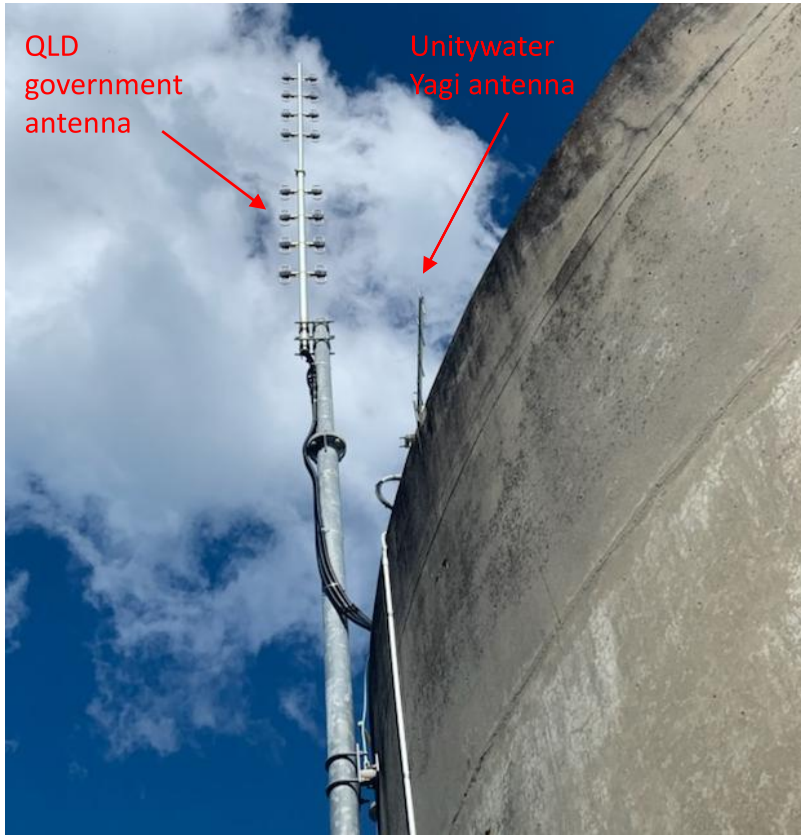
Poor SNR

Good RSSI



RF Interference

- External consultant (SAT) was engaged to investigate source of the interference.
- Source was identified to be a QLD Government collinear antenna transmitting at 420MHz, located next to our Yagi.
- QLD government licence became live a few months after our radio was upgraded.
- Fitting a duplexer onto our radio eliminated the interference effect



Lessons Learnt

Dealing with remote site interference

Impact of new equipment on existing UPS batteries

Staff training

Managing RF Interference

- Interfering signal from QLD government antenna was 420MHz, but licensed for up to **83W EIRP** on our reservoir site.

- 420MHz sits outside the frequency band of 450-520MHz of 4RF radio

- However, the high radiated power of their signal still caused major issues for us.

Centre Frequency	420.7875 MHz
Bandwidth	12.5 KHz
Frequency Range Start	420.78125 MHz
Frequency Range End	420.79375 MHz
Lat,Long (GDA94)	-26.54238°,153.091804°
Service	Land Mobile
Subservice	Land Mobile System - > 30MHz
Client Number	20029073
Coverage	Local
Transmitter or Receiver Details	
Device Type	T
Emission Designator	10K1F9W
System ID	3951489
Date Authorised	28 May 2026
Antenna	BA4040-67
Antenna Height (AGL)	10
Antenna Polarisation	V - Vertical linear
Antenna Multi Mode	N
Transmitter Power	86.9 W
Power Indicator	pY
Feeder Loss	5.4
EIRP	83 W
Mode	D
Class of Station	FB - Base station

Managing RF Interference

- The PTMP licence for our reservoir site only applies to the base station location that the reservoir site talks back to.
- Hence, no ACMA licensing protection at remote sites, so no recourse to remove interfering transmitters if they are ACMA-compliant.
- Interference at remote sites can only be reactively dealt with by installing our own protection (e.g. duplexers).
- SNR diagnostics from newer radios allow easier diagnosis of such issues, compared to our older radios which only measured RSSI.

UPS Batteries

- UPS batteries were not upgraded or replaced as part of radio upgrade.

- During Cyclone Alfred, widespread power loss occurred across Southeast QLD. Some base stations only lasted a few hours on battery power.

- Review and replacement of UPS batteries as part of radio upgrade design could have mitigated these issues during the cyclone.

Staff Training

- Newer radios proved more difficult for maintenance staff to learn due to:
  - Increased number of features on new radios
  - Reliance on IP addressing

- Older radios (and older electronics in general) relied on serial and/or USB for connection.

- Newer networking devices require IP addressing knowledge, major paradigm shift for older technicians.

Thanks for Listening!

- Questions?