

University of Southern Queensland  
Faculty of Health, Engineering and Sciences

**Automatic Circuit Recloser (ACR) Communications  
Using P25 RMU (Radio Modem Unit)**

A dissertation submitted by

**Hung Hoang**

in fulfilment of the requirements of

**ENG4111 and 4112 Research Project**

towards the degree of

**Bachelor of Engineering (Electrical & Electronics)**

**Submitted October 2016**

## **Abstract**

The current Ergon Energy telecommunications in the field for remote smart grid operations to its Automatic Circuit Reclosers (ACRs) uses public carriers such as Telstra mobile data services and Immarsat BGN network (Satellite).

The operational cost of using Immarsat BGN network is very costly (\$8 per Megabyte) so there is financial incentive to investigate the use of the P25 Radio Modem Unit (RMU) to provide communications to ACR using existing the Ergon Energy P25 Radio Network.

This project aims to assess the capabilities of the P25 devices in the context of Ergon Energy's operational requirements through both research and practical experimentation. The results will be used to identify and quantify (where possible) potential issues and make recommendations about any implementation.

The main aim is to use P25 RMUs over the Ergon Energy P25 Radio Network for communications to ACRs by benchmarking against the existing NextG modems in use. Communications must be implemented for two serial ports on the ACR, one for SCADA and the other for engineering configuration access.

The data and packet formats of the P25 communications protocol for both the SCADA DNP3 and engineering access connections have been documented. The operational requirements of the ACR SCADA and Remote Engineering connections have been identified. Following this a testbed was established and used to evaluate performance across a range of parameters. These were compared to the identified requirements.

The P25 RMU testbed assessed performance against the benchmarks established for the existing NextG modem application used on ACR. The P25 RMU worked with limitations which are to be outlined in the report on findings and hence recommendations to further improve the performance.

**University of Southern Queensland**

**Faculty of Health, Engineering and Sciences**

**ENG4111/ENG4112 Research Project**

## **Limitations of Use**

The Council of the University of Southern Queensland, its Faculty of Health, Engineering & Sciences, and the staff of the University of Southern Queensland, do not accept any responsibility for the truth, accuracy or completeness of material contained within or associated with this dissertation.

Persons using all or any part of this material do so at their own risk, and not at the risk of the Council of the University of Southern Queensland, its Faculty of Health, Engineering & Sciences or the staff of the University of Southern Queensland.

This dissertation reports an educational exercise and has no purpose or validity beyond this exercise. The sole purpose of the course pair entitled “Research Project” is to contribute to the overall education within the student’s chosen degree program. This document, the associated hardware, software, drawings, and other material set out in the associated appendices should not be used for any other purpose: if they are so used, it is entirely at the risk of the user.

**University of Southern Queensland**

**Faculty of Health, Engineering and Sciences**

**ENG4111/ENG4112 Research Project**

## **Certification of Dissertation**

I certify that the ideas, designs and experimental work, results, analyses and conclusions set out in this dissertation are entirely my own effort, except where otherwise indicated and acknowledged.

I further certify that the work is original and has not been previously submitted for assessment in any other course or institution, except where specifically stated.

Hung Hoang

0018847370

# Acknowledgements

The author would like to acknowledge the support received throughout the course of the project. My sincere appreciations are offered to the following people:

## **Mrs. Catherine Hills (USQ)**

For her assistance and guidance throughout the project, the flexible supports on already busy schedule, the real world experiences and knowledge proving to be invaluable and her enthusiasm on the industry base topic.

## **Mr. Glen Firth (Ergon Energy Corporation)**

For conceiving the project topic, the engineering support and the guidance provided.

## **Mr. Greg Borger (Ergon Energy Corporation)**

For supplied resources and shared knowledge on the Project 25.

## **Mr. Ian McNalty (Ergon Energy Corporation)**

For supplied resources to Project 25 asset information.

## **Mr. James Lowes (Ergon Energy Corporation)**

For the supports and allowed access to the running config of the P25 network for monitoring and testings.

## **Mr. Trevor Gilliland (Ergon Energy Corporation)**

For providing valuable expertise in SCADA master station, configuration and providing time for assistance.

## **My Family**

Much appreciation to my wife and kids for their patience with me in time and supports throughout my project works.

# Table of Contents

<b>ABSTRACT.....</b>	<b>II</b>
<b>LIMITATIONS OF USE.....</b>	<b>III</b>
<b>CERTIFICATION OF DISSERTATION .....</b>	<b>IV</b>
<b>ACKNOWLEDGEMENTS .....</b>	<b>V</b>
<b>TABLE OF CONTENTS.....</b>	<b>VI</b>
<b>LIST OF TABLES .....</b>	<b>X</b>
<b>LIST OF FIGURES.....</b>	<b>XI</b>
<b>GLOSSARY.....</b>	<b>XII</b>
<b>1.0 INTRODUCTION .....</b>	<b>1</b>
1.1 SUMMARY OF PROJECT.....	1
1.2 AIM OF PROJECT .....	1
1.3 PROJECT BACKGROUND .....	2
1.4 THE NEED FOR THE PROJECT.....	4
1.5 PROJECT OBJECTIVES.....	5
1.6 CHAPTER SUMMARY .....	6
<b>2.0 LITERATURE AND BACKGROUND.....</b>	<b>8</b>
2.1 CHAPTER OVERVIEW .....	8
2.2 RELEVANT STANDARDS .....	8
2.2.1 <i>P25 Standards</i> .....	8
2.2.2 <i>P25 Digital Modulation Two – Phase Plan</i> .....	10
2.2.3 <i>Common Air Interface</i> .....	11
2.2.4 <i>Data Encryption Standard</i> .....	13
2.2.5 <i>IEC 61870.5 and DNP3</i> .....	13
2.2.6 <i>DNP3 over TCP/IP</i> .....	14
2.2.7 <i>AS 61850.1</i> .....	14
2.2.8 <i>AS 61508.3</i> .....	15
2.3 SAFETY ESSENTIALS TO LEGISLATIVE AND REGULATORY .....	15
2.4 THE TESTING OF SAFETY RELATED EQUIPMENT AS LEGISLATIVE REQUIREMENTS .....	16
2.5 CHAPTER SUMMARY .....	16
<b>3.0 PROJECT METHODOLOGY .....</b>	<b>17</b>
3.1 P25 NETWORK REQUIREMENTS .....	17
3.1.1 <i>P25 Digital Modulation</i> .....	17
3.1.2 <i>Key Components of P25 System and RMU</i> .....	18

3.1.2.1	KEY COMPONENTS OF AN ERGON ENERGY P25 LAND MOBILE BASE SITE.....	22
3.1.2.1.1	<i>The Receiver Multi-Coupler .....</i>	23
3.1.2.1.2	<i>The Transmitter Multi-Coupler .....</i>	24
3.1.2.1.3	<i>The Diplexer.....</i>	25
3.1.2.1.4	<i>VSWR Alarm Monitor Base Antenna .....</i>	25
3.1.2.1.5	<i>RF Feeder of the P25 Base .....</i>	26
3.1.2.1.6	<i>Base Antenna .....</i>	26
3.1.2.1.7	<i>Lightning Protection of the P25 Base .....</i>	27
3.1.2.1.8	<i>Base Transceivers TB8100 .....</i>	28
3.1.2.1.9	<i>Channel Controller (P25CCe) and Base Station Controller .....</i>	29
3.1.2.2	P25 RMU KEY COMPONENTS .....	29
3.1.2.2.1	<i>Key Features of P25 RMU .....</i>	31
3.1.2.2.2	<i>The RMU in P25 Network Context.....</i>	31
3.1.2.2.3	<i>P25 RMU Front Panel Interfaces .....</i>	32
3.1.3	<i>Capabilities and limitations of P25 network and RMU .....</i>	33
3.2	ASSESS THE LOCATION OF EXISTING ACRs TO THE P25 NETWORK COVERAGE .....	36
3.2.1	<i>ACRs locations.....</i>	37
3.2.2	<i>Potential ACRs with P25 coverage .....</i>	38
3.3	P25 COMMUNICATIONS PROTOCOL .....	39
3.3.1	<i>Carrying DNP3 over a TCP/IP network.....</i>	40
3.3.2	<i>Remote Engineering Access .....</i>	41
3.4	ERGON ENERGY ACR OPERATION REQUIREMENTS .....	42
3.4.1	<i>Capabilities for reliable operations .....</i>	42
<b>4.0</b>	<b>P25 RMU ASYNCHRONOUS V.24 SERVICE.....</b>	<b>43</b>
4.1	P25 RMU SERVICE SPECIFICATION.....	43
4.2	P25 RMU INTERFACE SPECIFICATION.....	44
4.3	P25 RMU CAI SECURITY SPECIFICATION.....	45
4.4	P25 RMU SERVICE PERFORMANCE .....	45
4.5	P25 RMU SERVICE PERFORMANCE LEVELS .....	46
4.5.1	<i>Service Performance Severity Level Definitions.....</i>	46
4.6	P25 RMU SERVICE ACTIVATION .....	48
4.7	P25 RMU SERVICE RESTORATION.....	49
4.8	P25 RMU SERVICE CHANGE OF MANAGEMENT .....	49
<b>5.0</b>	<b>PROJECT TASKS.....</b>	<b>51</b>
5.1	P25 RMU TESTBED INSTALLATION .....	51
5.2	P25 RMU CONFIGURATION .....	54
5.2.1	<i>IP address allocation for a P25 RMU.....</i>	54
5.2.2	<i>NLR Database Configuration.....</i>	54

5.2.3	<i>P25 RMU Database Configuration</i> .....	56
5.3	P25 RMU OPERATION .....	60
5.3.1	<i>P25 RMU LED indicators</i> .....	61
5.3.2	<i>P25 RMU Troubleshooting</i> .....	67
<b>6.0</b>	<b>P25 RMU OPERATION ASSUMPTIONS</b> .....	<b>70</b>
6.1	P25 CAI UPLINK AND DOWNLINK LESS THAN 1% BIT ERROR RATE .....	70
6.2	P25 RMU TCP IS USED AS NETWORK TRANSPORT LAYER AND OPERATE AS TCP SERVER.....	70
6.3	P25 RMU HARDWARE FLOW CONTROL APPLICATION.....	71
6.4	P25 RMU SCADA GIVEN A HIGHER PRIORITY THAN VOICE .....	71
6.5	VOICE AND SCADA GIVEN PRIORITY TO PRE-EMPTIVE GPS OR WSOS.....	72
6.6	UN-DEDICATED DATA CHANNEL USED .....	72
<b>7.0</b>	<b>P25 RMU TESTS AND FINDINGS</b> .....	<b>74</b>
7.1	P25 RMU RS232 SCADA DNP3 TESTING AND FINDINGS .....	74
7.1.1	<i>DNP3 data fragmentation</i> .....	76
7.1.2	<i>Communications Failed alarm</i> .....	77
7.1.3	<i>P25 Channel control Issue</i> .....	79
7.1.4	<i>P25 RMU locked onto a weak adjacent Land Mobile Base</i> .....	80
7.2	P25 RMU RS232 ENGINEERING ACCESS (WSOS) TESTING .....	80
7.3	P25 RMU RF DYNAMICALLY SELECT .....	91
<b>8.0</b>	<b>RECOMMENDATIONS</b> .....	<b>93</b>
8.1	P25 RMU TCP RE-ESTABLISHMENT REQUIREMENT .....	93
8.2	P25 RMU TCP MAXIMUM SEGMENT SIZE AND RECONNECT TIMER .....	93
8.3	P25 RMU TCP PACKET SIZE IN WSOS .....	94
8.4	P25 RMU DNP3 DATA LINK AND APPLICATION LAYER CONFIRMATIONS .....	94
8.4.1	<i>DNP3 Data Link Layer Frame Confirmations</i> .....	94
8.4.2	<i>DNP3 Application Layer confirmations and timeouts</i> .....	95
8.5	P25 RMU ACR FILE TRANSFERS.....	95
8.5.1	<i>ACR File transfer during Off-peak</i> .....	95
8.5.2	<i>ACR File transfer block size</i> .....	96
8.6	P25 RMU TCP TIMESTAMP OPTION.....	96
8.7	UNIT CALL PRIORITY .....	96
8.8	VOICE AND DATA TRAFFIC HANG TIME .....	97
8.9	ACTIVITY THRESHOLD .....	97
8.10	GPS UPDATE.....	98
8.11	SCADA MASTER STATION POLL FREQUENCY.....	98
8.12	P25 RMU RESTRICTED TO ONE LAND MOBILE BASE.....	98
8.13	INCREASE P25 NETWORK CAPACITY.....	99

<b>9.0 CONCLUSIONS .....</b>	<b>101</b>
<b>LIST OF REFERENCES.....</b>	<b>104</b>
<b>APPENDIX A: PROJECT SPECIFICATION.....</b>	<b>106</b>
<b>APPENDIX B: ERGON ENERGY P25 LAND BASE MOBILE COMMUNICATIONS SCHEMATIC DIAGRAM .....</b>	<b>108</b>
<b>APPENDIX C: P25 SA2C-8QA RECEIVER MULTI-COUPLER .....</b>	<b>109</b>
<b>APPENDIX D: P25 TRANSMITTER MULTI-COUPLER PEI TM2-6-P6-04.....</b>	<b>110</b>
<b>APPENDIX E: P25 BANDPASS DUPLEXER 2XA12-3 .....</b>	<b>114</b>
<b>APPENDIX F: VSWR ALARM BASE ANTENNA MONITOR PAAP .....</b>	<b>115</b>
<b>APPENDIX G: PROJECT RISK.....</b>	<b>116</b>

# List of Tables

TABLE 1: P25 RMU RSSI LEDs MEASURING STATE DEFINITION .....	35
TABLE 2: FEATURES AND CAPABILITIES SUPPORTED BY TIA/EIA-232 .....	40
TABLE 3: P25 RMU V.24/RS232 INTERFACE 1 AND 2 PORT SETTINGS .....	44
TABLE 4: P25 ASYNCHRONOUS V.24 SERVICE PERFORMANCE .....	45
TABLE 5: P25 RMU SERVICE AVAILABILITY .....	47
TABLE 6: P25 RMU SERVICE ACTIVATION.....	48
TABLE 7: P25 RMU SERVICE RESTORATION .....	49
TABLE 8: P25 RMU SERVICE CHANGE OF MANAGEMENT .....	50
TABLE 9: NETWORK LOCATION REGISTER CONFIGURATION PROCEDURES .....	54
TABLE 10: P25 RMU CONFIGURATION SETTINGS PROCEDURES.....	56
TABLE 11: P25 RMU LED1, LED2 & LED3 ILLUMINATION SEQUENCES.....	62
TABLE 12: P25 RMU SYSTEM ERROR CODES .....	66
TABLE 13: P25 RMU TROUBLESHOOTING AND REMEDIES .....	67
TABLE 14: TESTBED ACR REMOTE ENGINEERING ACCESS VIA WSOS FEATURES.....	83
TABLE 15: P25 RMU DETAILED RISK TABLE.....	116

# List of Figures

FIGURE 1: ACR COMMUNICATIONS USING NEXTG MODEM.....	3
FIGURE 2: ACR COMMUNICATIONS USING M2M SATELLITE TERMINAL.....	3
FIGURE 3: ACR COMMUNICATIONS USING P25 RMU (RADIO MODEM UNIT) .....	4
FIGURE 4: BASIC BLOCK DIAGRAM OF P25 TRANSCEIVER (ADAPTED FROM DANIEL ELECTRONICS LTD, 2007).....	11
FIGURE 5: P25 STANDARD PHASE 1 AND PHASE 2 COMMON AIR INTERFACE (CAI) CHARACTERISTIC (ADAPTED FROM MOTOROLA INC, 2009).....	12
FIGURE 6: ACM VHF HIGH BAND PLAN (AIRWAVE SOLUTIONS P25 RACK TRAINING, 2012).....	19
FIGURE 7: EXAMPLE OF ERGON ENERGY P25 PHYSICAL ARCHITECTURE.....	20
FIGURE 8: ERGON ENERGY P25 LOGICAL ARCHITECTURE.....	21
FIGURE 9: ERGON ENERGY P25 TX/RX MULTI-COUPLER EXPECTED RF LEVELS WITH 150kHz CHANNEL SPACING (BASED ON ERGON ENERGY P25 SPECIFICATIONS DOCUMENTS) .....	23
FIGURE 10: P25 BASE ANTENNA BA80-41-DIN RADIATION PATTERNS (ADAPTED FROM BIRD TECHNOLOGIES GROUP TX RX SYSTEMS, VHF OMNIDIRECTIONAL DIPOLE ARRAYS)).....	27
FIGURE 11: P25 RMU ES1105-V RADIO MODEM UNIT .....	30
FIGURE 12: P25 RMU SYSTEM COMPONENT CONTEXT OF PACKET DATA SERVICE CONNECTIVITY .....	32
FIGURE 13: RMU PHYSICAL PORT CONNECTION .....	33
FIGURE 14: AUTOMATIC CIRCUIT RECLOSER POSITIONS ON THE MAP .....	38
FIGURE 15: ERGON ENERGY P25 NETWORK COVERAGE .....	38
FIGURE 16: DNP3.0 OVER TCP/IP PROTOCOL STACK (DNP3 IEC 60870.5) .....	41
FIGURE 17: ASYNCHRONOUS V.24 SPECIFICATION.....	44
FIGURE 18: P25 RMU TESTBED SCHEMATIC DIAGRAM .....	53
FIGURE 19: P25 RMU FRONT PANEL LEDs AND BUTTON.....	60
FIGURE 20: WIRESHARK CAPTURED OF DATA FRAGMENTED FROM REMOTE DEVICE VIA P25 RMU .....	76
FIGURE 21: WIRESHARK CAPTURED OF HOURLY TCP RETRANSMISSION.....	78
FIGURE 22: EVENT LIST OF TEST ACR COMMUNICATIONS FAILED.....	78
FIGURE 23: TEST RMU_ACR EXPIRE DURATION 3600 SECONDS. ....	79
FIGURE 24: SERIAL-IP RS232 COM PORT EMULATOR CONFIGURATION.....	81
FIGURE 25: WSOS COMMUNICATIONS CONFIGURATION. ....	82
FIGURE 26: WSOS ENGINEERING ACCESS CONNECTED. ....	82

# Glossary

<b>Acronym</b>	<b>Description</b>
ACR	Automatic Circuit Recloser
APCO	Association of Public Safety Communications Official
APCO P25	APCO Project 25 digital conventional and trunked radio standard
BS	Base Station
BSC	Base Station Controller
CAI	Common Air Interface
DB	Data Base
Downlink	The direction from the FNE to a mobile unit
DSN	Data Service Node
FNE	Fixed Network Equipment, typically BSC
GPS/GIS	Global Positioning System/Graphical Information System
ICMP	Internet Control Message Protocol – message generated in response to errors in IP operations for diagnostic or control.
IP	Internet Protocol
LOC	Location Operation Control
LSC	Location Service Centre
MR, MS	Mobile Radio, Mobile Station – used the same as SU.
MSS	Maximum Segment Size
NLR	Network Location Register
OCN	Ergon Energy Operational Control Network
P25	Project 25 See APCO P25

P25CC	P25 Channel Controller
PDU	Protocol Data Unit
PSTNG	PSTN Gateway(interface to Public Switch Telephone Network)
RCB	RMU Control Board
RCI	Remote Control Interface
RF	Radio Frequency
RFSS	RF Subsystem
RNC	RFSS Network Controller
RMU	Radio Modem Unit
RSSI	Received Signal Strength Indicator
RX	Receive or Receiver
SCADA	Supervisory Control and Data Acquisition
SU	Subscriber Unit – used as equivalent of terminal, portable or radio
TCP	Transmission Control Protocol
TIA	Telecommunications Industry Association
Transceiver	Transmitter/Receiver Capable
TX	Transmit or Transmitter
Uplink	Uplink – the direction from a mobile unit to the FNE
USB	Universal Serial Bus
WSOS	Windows Switchgear Operating System (a software package that allows the remote control and monitoring of pole mounted Automatic Circuit Recloser)

# **1.0 Introduction**

## **1.1 Summary of Project**

Ergon Energy is one of the electricity suppliers or distributor entities in Queensland. The state's regulatory framework provides strong financial incentives to improve power quality and availability. Current initiatives such as ACR and Switching Equipment Application Strategy are accelerating the need for greatly improved telecommunications in the field for remote smart grid operations. This has led to the use of public carriers such as Telstra mobile data services and Immarsat BGN satellite network.

The operational cost of using Immarsat BGN satellite network is very costly (\$8 per Megabyte) so there is financial incentive to utilise Ergon Energy Communications network where-ever possible. A P25 Radio Modem Unit (RMU) is investigated to be used on ACR communications using existing Ergon Energy P25 Radio Network.

## **1.2 Aim of Project**

The main aim is to use Radio Modem Units (RMUs) over Ergon Energy P25 Radio Network for communications to Automatic Circuit Reclosers (ACRs). A RMU provides two local serial connections to an Automatic Circuit Recloser, one using DNP3 for access by Supervisory Control and Data Acquisition (SCADA) from the master station, and the second serial is for engineering access (raw RS232) for the remote management of the ACR such as configuration settings and firmware upgrade using WSOS (Windows Software Operating System).

A previous attempt has been made to utilise the P25 system which was unsuccessful and so was discontinued. The use of the low frequency P25 network

remains an attractive alternative to NextG and especially Satellite connections. This project aims to assess the capabilities of the P25 devices in the context of Ergon Energy's operational requirements through both research and practical experimentation. The results will be used to identify and quantify where possible potential issues and make recommendations about the suitability or otherwise of the equipment.

### **1.3 Project Background**

Ergon Energy's current arrangement for accessing its Automatic Circuit Recloser(s) is either using a NextG Modem or a Satellite Terminal. The operational expenditures for satellite terminal can be costly and NextG coverage is limited mostly near the highways and densely populated areas. Ergon Energy's P25 network using the Hi-Band VHF (165 - 170 MHz) possesses better coverage over the NextG (900 MHz) as Radio Frequencies (RF) propagates further at lower frequencies. The main attraction of using the P25 RMU is no ongoing operational cost compared to using third party networks such as BGAN M2M for satellite and Telstra for NextG modem.

Blocks diagram Figure 1 shows typical NextG, an M2M Satellite Terminal in Figure 2 and P25 RMU communications to ACR on Figure 3.

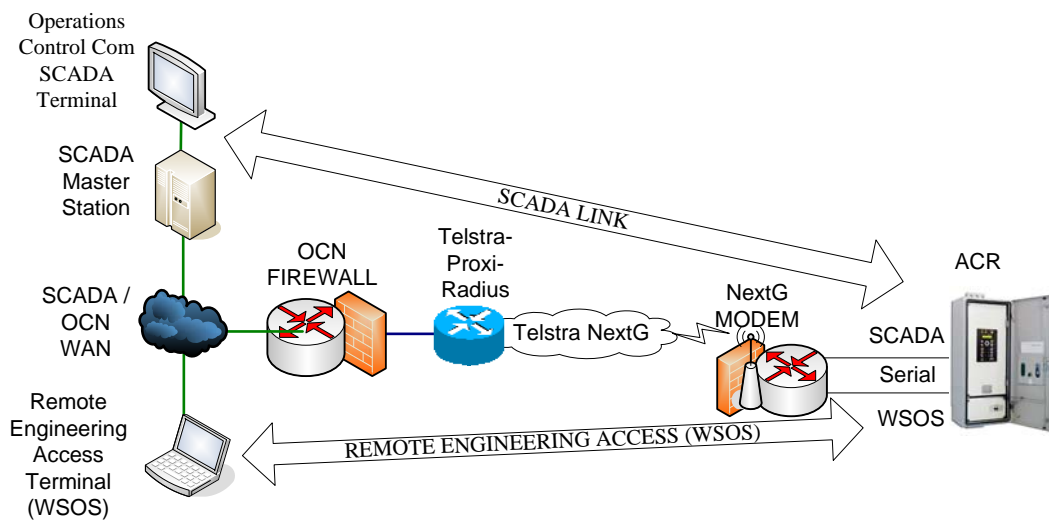


Figure 1: ACR Communications Using NextG MODEM

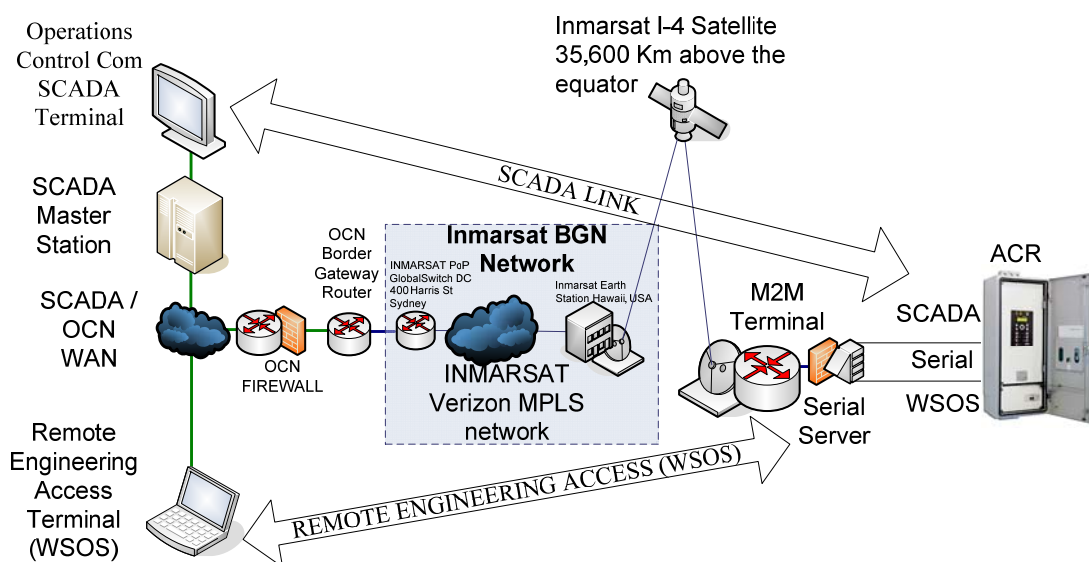


Figure 2: ACR Communications Using M2M Satellite Terminal

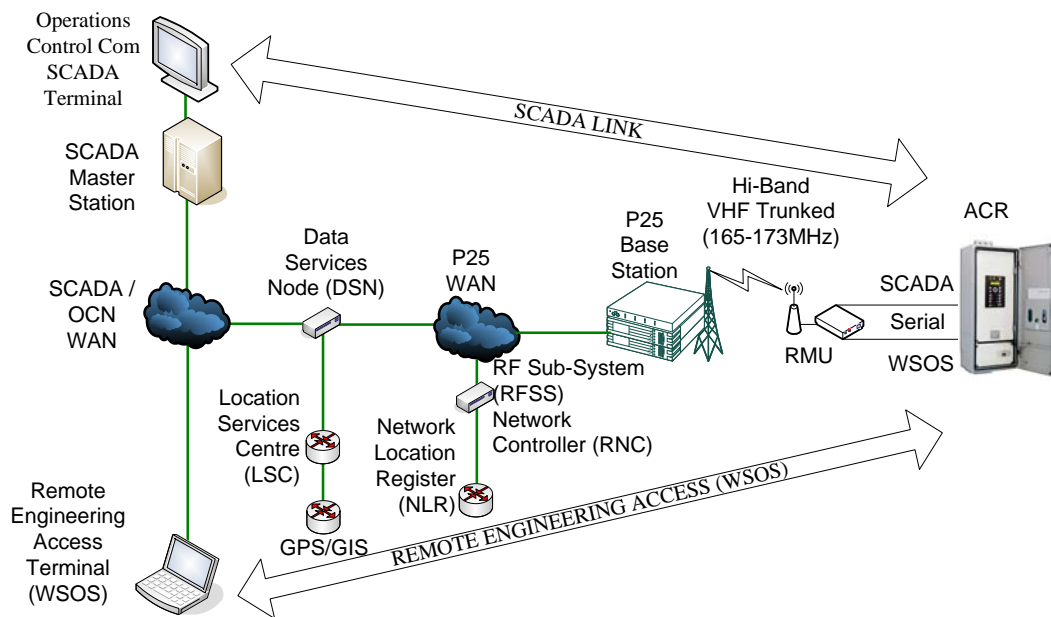


Figure 3: ACR Communications Using P25 RMU (Radio Modem Unit)

## 1.4 The Need for the Project

Ergon Energy currently has 608 Automatic Circuit Recloser (ACRs) that are equipped with remote communications control and engineering access, 168 of which communications to the Control Centres using Satellite Terminals and the remaining using Telstra NextG network. These ACRs are connected to a communication infrastructure enabling connectivity for SCADA and remote engineering access for configuration.

The data plan using NextG modems is 1 Gigabyte for \$15 per month with Telstra and with 440 (and growing) devices the access cost is \$79,200 annually. Satellite access is \$8 per Megabyte so operating cost becomes very expensive for 168 (increasing) terminals.

Equipment or establishment cost for a P25 RMU, the Auria Wireless ES1105-V RMU is cost a little more compared to a NextG modem (Cybertec 2255) but much cheaper compared to a Satellite Terminal (M2M Sabre Ranger BGAN M2M

Terminal), with no ongoing operating cost using Ergon Energy existing P25 network.

Once successfully tested P25 RMU will provides an alternative choice on future ACR Installation projects and possible fault replacement for existing ACR in the field.

## **1.5 Project Objectives**

The ultimate goal is to ensure the P25 RMU (Auria Wireless ES1105-V) provide reliable communications to Automatic Circuit Recloser using the existing Ergon Energy P25 network as the communications path. It is expected that the project will:

1. Identify all components required for the Auria Wireless ES1105-V RMU to operate as remote communications device which complies with both the Ergon Energy P25 network and the Nulec (ACR) equipment. These includes antenna type, RF surge arrester type, coaxial cable and connectors, power consumption that the Nulec is capable of providing with appropriate circuit breaker protection to be used and serial cables or adapters for RS232 interfaces between P25 RMU and ACR's serial communications ports.
2. Development of a configuration process to enable the P25 RMU accessing the Ergon Energy P25 network. This includes the registration process on the NLR (Network Location Register) necessary to access the P25 network, allocate IP addresses in IPAM (IP Address Management) to enable RS232 communications for SCADA DNP3.0 between ACR and SCADA Master Station and Engineering Configuration Access between ACR and PC terminal using WSOS for Nulec. A configuration template as

a result is to be developed for Auria Wireless ES1105-V RMU (P25 RMU) configuration or initial setup work.

3. Ensure reliable communications as the operational requirements of ACR's SCADA and Remote Engineering are met. This is done by testing the Auria Wireless ES1105-V RMU to ensure:

- a. The P25 RMU dynamically selects or locks onto a better signal strength P25 radio site. This is to ensure the P25 RMU hunts properly.
- b. When the P25 RMU successfully affiliates and registers with a P25 radio site, the data connection should be reliable in terms of link RF margin. That is the thresholds set for affiliation or registration needs to be appropriate.
- c. The P25 RMU serial 1, DNP3 SCADA communications to the SCADA master station must be reliable.
- d. With regards to capacity and reliability of Remote Engineering Access, the P25 RMU serial 2 must be capable of file downloads and uploads.

## **1.6 Chapter Summary**

This chapter has provided an overview of the research project to be undertaken. By introducing the potential of the P25 RMU to provide communications to ACR equipment in the Ergon Energy electricity network, it has been shown that a continual focus on distribution network service provider's operational and the potential of delivering an effective alternative to the use of external service

providers which could provide Ergon Energy with additional choice for future ACR install projects and lower operation cost with existing assets on fault replacement.

## **2.0 Literature and Background**

### **2.1 Chapter Overview**

To have the understanding of the Project 25 (P25) standards and the requirements needed to enable a P25 RMU such as the Auria Wireless ES1105-V to be successfully implemented as a remote communications device on ACR using Ergon Energy P25 network, a literature review has been looked into on the following:

- Relevant Standards
- Legislation requirements of safety related systems

### **2.2 Relevant Standards**

The propose P25 RMU functions on ACR to provide physical interface DNP3 (RS232), Remote Engineering Access (Raw RS232) and P25 radio link back to master station. To ensure a P25 RMU meets legislation compliance (Electricity Act, 1994) and communications standards it is a must to benchmark against relevant standards.

#### **2.2.1 P25 Standards**

Ergon Energy P25 network and all its communications apparatus are operating under the strict rules governed by products licencing. Electromagnetic Frequency

(EMF) emission from a base radio transmitter for example is governed by ACMA licence applied for a particular licence at a site. Furthermore P25 formal standards built had been conducted by the Mobile and Personal Private Radio Standards Committee (TIA TR-8) of the Telecommunications Industry Association's (TIA) Standards and Technology Department. TIA is a voluntary industry standards development for telecommunications products and is credited by American National Standards Institute (ANSI).

Ergon Energy P25 network is chosen for it had been developed based upon a family of public safety communications standards for which the requirements have been defined by state, local and national government users (Source, P25 Document Suit, p1).

Project 25 constitutes the public safety community's overall strategy had been developing a digital modulation solution and achieved Federation Communications Commission (FCC) by North America spectrum efficiency mandates aiming for migration to narrowband channel spacing in the VHF and UHF bands, which calling for eventually four-to-one reduction in spacing 25 kHz bandwidth (BW) to 6.25 kHz BW per voice channel.

Project 25 FCC's mandates with a two-phase plan (Source, P25 Document Suit, p1):

- Phase 1 defines the required technologies to provide channel reduction from 25 kHz to 12.5 kHz bandwidth. Phase 1 refers to P25 requirements and standards for a digital common air interface (CAI) based upon frequency division multiple access (FDMA) using a 12.5 kHz bandwidth channel. Ergon Energy P25 network using Phase 1 a 12.5 kHz channel size due to licencing availability in high VHF band.
- Phase 2 defines a further 50 percent reduction in channel size to 6.25 kHz. Phase 2 refers to P25 requirements and standards for a digital common air interface (CAI) based on time division multiple access (TDMA) using a 6.25 kHz equivalent channel, two slots in a 12.5 kHz

channel. To achieve the same coverage distance as in Phase 1 system the number of bases would have to be doubled as TDMA has limitation due to the time delay between remote unit and base station.

### **2.2.2 P25 Digital Modulation Two – Phase Plan**

P25 Phase 1 technology with channel reduction from 25 kHz to 12.5 kHz and refer to section 2.2.1 the standards digital CAI base upon FDMA. Ergon Energy P25 network has been based upon Phase 1, a 12.5 kHz channel size due to licencing availability and cost effectiveness due to spectrum availability in Hi-VHF Mobile Trunking Band. Phase 2 P25 digital CAI based on time division multiple access (TDMA) using a 6.25 kHz equivalent channel with two slots in a 12.5 kHz channel which further improved bandwidth efficiency. The use of Phase 2 technology Ergon Energy would have to doubles the number of Mobile Base Station sites to achieve the same coverage in phase 1 FDMA is not restricted with time delay limitation.

A basic block diagram of a typical P25 transceiver represents in Figure 4 that separates into three sections. The A/D or D/A plus Speech Coder/Decoder area, digitise voice using Improved Multi-Band Excitation (IMBE™) method called vocoder. The IMBE™ vocoder produces speech characteristics at 4400 bits per seconds. Channel Coding / Decoding section deploy error correction techniques to overcome noise and fading. These including Hamming codes, Golay codes, Reed-Solom on codes, Primitive BCH and shorten cyclic codes (P25 Training Guide). Modulating / Demodulating and Filtering using a type of differential Quadrature Phase Shift Keying called C4FM where each symbol shifted in phase by 45 degrees from the previous symbol.

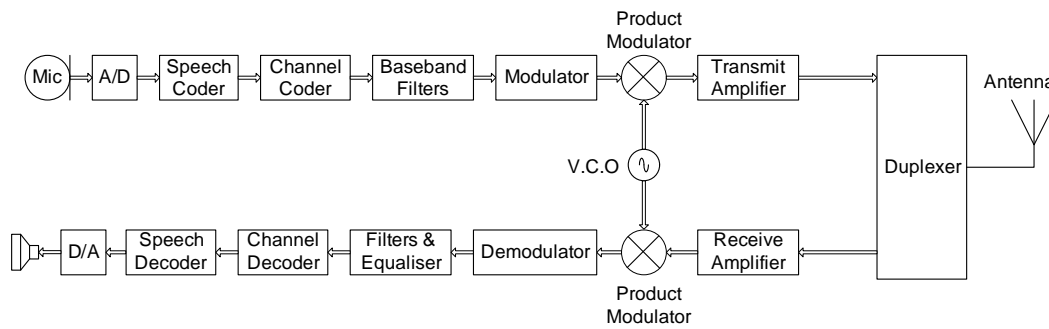


Figure 4: Basic Block Diagram of P25 Transceiver (Adapted from Daniel Electronics LTD, 2007)

P25 channels are capable of carrying voice or data at 9600 bits per second and protected by forward error correction to improve RF conditions and operating range. P25 employs over-the-air rekeying (OTAR) features, Advance Encryption Standards (AES) algorithm, and Data Encryption Standards (DES-OFB) algorithm to achieve secure transmissions.

### 2.2.3 Common Air Interface

The Common Air Interface (CAI) of the P25 uses the frequency division multiple access (FDMA) techniques with dual modulations. The first defines the digital modulation used in the 12.5 kHz voice channel bandwidth. The second defines the FM modulation used in 25 kHz and 12.5 kHz bandwidth on subscriber units. The general P25 CAI mandatory standard based on *Project 25 Common Air Interface Operational Description for Conventional Channels*, ANSI/TIA-102.BAAD-A (Feb 2010). The guidance mandatory to meet the optional Phase 1 P25 FMDA Trunked Digital standard is based on *Project 25 Trunking Procedures*, TIA-102.AABD-A (Dec 2008) (Source, P25 Document Suit, p11).

CAI allows wireless communications both voice and data directly between P25 subscriber units and fixed base station and P25 mobile to P25 mobile via fixed base station. In the case of P25 RMU application the packet data bearer services

as standard which enables data to be communicated to or from the data network via RFSS connectivity.

The most widely utilised P25 interface is the CAI in the suite of P25 standard interfaces. Figure 5 summarised the operation features of P25 Phase 1 and Phase 2 standards.

Common Air Interface		
Attributes	Phase 1 FDMA	Phase 2 TDMA
Vocoder	Full-rate vocoder	Enhanced half-rate vocoder
Channel bandwidth	12.5 KHz FDMA	12.5 KHz TDMA (6.25e)
Modulation	C4FM	H-CPM / H-DQPSK
Encryption	AES	AES
Voice channel data rate	9.6 kbps	12 kbps
Control channel data rate	9.6 kbps	9.6 kbps

Figure 5: P25 Standard Phase 1 and Phase 2 Common Air Interface (CAI) Characteristic (Adapted from Motorola Inc,2009)

#### **2.2.4 Data Encryption Standard**

Ergon Energy P25 network employed Advanced Encryption Standard (AES) a provision featuring Security Threats, Confidential, Integrity, Authentication and Key Management base on *Project 25 Security Services Overview*, ANSI/TIA-102.AAAB-A. The confidentiality and authenticity of data is maintained while in transit between the service and the end point. Encryption type used is AES256 and Authentication applied is SHA-1 or equivalent.

#### **2.2.5 IEC 61870.5 and DNP3**

Generally speaking International Electrotechnical Commission (IEC) 60870.5 and DNP3 protocol are the same. IEC 60870.5 has been defined primarily for the telecommunications of electrical system and control information which includes general data type that could be used in any SCADA application. The use of IEC 60870 has been mainly confined to the electricity industry.

The DNP3 protocol had been developed in North America by Harris Controls Division, Distributed Automation Products in early 1990's and released to the industry based DNP3 Users Group in November 1993.

DNP3 (Distributed Network Protocol Version 3.0) is a telecommunications standard, defines communications between Master Stations, Remote Telemetry Units (RTUs) and other Intelligent Electronic Devices (IEDs) such as Automatic Circuit Reclosers (ACRs). The significant feature of DNP3 protocol is has widely adapted by large number of equipment manufacturers for it is an open protocol standard.

Both DNP3 and IEC 60870.5 were created specifically for SCADA applications. These involved acquisition and sending of control commands between physically separate devices. Data transmission designed to transmit relatively small packets

of data in a reliable manner with the message involved arriving in a deterministic sequence.

#### **2.2.6 DNP3 over TCP/IP**

The concept of a SCADA system is the presence of communications systems that link together one or more master devices with a number of slave devices. The scale of distances and the nature of the data conveyed had dominated the technologies used to carry the communications. The systems used such as analog data radio links. The data rate varied from 2400 to 9600 baud where the physical layer (OSI) specified using RS232C serial asynchronous communications. As the requirements of communications had become more intensive SCADA protocols of DNP3 and IEC60870-5-101 has been evolved to the carrying DNP3 over a network environment, which involves encapsulation of data frames from the DNP3 data link layer within the transport layer frames of the Internet Protocol.

#### **2.2.7 AS 61850.1**

The Australian Standard, AS61850.1 dictates the operational safety of safety-related programmable equipment in relation to Remote Engineering Access, such as ACR proposed in this project. The standard describes the operational safety management, the validation processes over the life of equipment requirements.

The standard outlines procedures that shall be engaged for effective functional safety which include:

- remote engineering access for configuration management of safety related equipment

### **2.2.8 AS 61508.3**

In relation to programming of Remote Terminal Unit (RTU) such as ACRs, the Australian Standard AS61508.3 stipulates software requirements for safety operation of programmable safety-related apparatus. In the operational requirements of ACR Remote Engineering Access will provide detail review of this standard will help as a guide to develop acceptable methods on software used for the remote management of ACR.

## **2.3 Safety Essentials to Legislative and Regulatory**

In Queensland, the legislative essentials for the testing of safety-related equipment to be manage in the determination of the limitations during commissioning and operational works with remote engineering access configuration tasks. The following Legislation has been observed:

- Workplace Health and Safety Act, 2011.
- Electricity Act, 1994.
- Electricity Regulation, 2006.

## **2.4 The testing of safety related equipment as legislative requirements**

A Electricity Supplier as a service provider have the duty of care to protect its electricity network to safeguard connection and supply to its customers and must obey with directives defined as per National Electricity Rules (Electricity Act, 1994).

To comply utilities have practical design experience to understand the defects of the targeted equipment to establish maintenance programs accounted to act in accordance with the legislation requirement. The above legislation compliances do not provide the frequency or the instruction on how to test of equipment.

## **2.5 Chapter Summary**

The literature has identified some initial requirements for RMU remote engineering access for ACR configuration, management via Windows Switchgear Operating System (WSOS) and RMU SCADA control using DNP 3.0 from a SCADA Master Station via P25 network.

## **3.0 Project Methodology**

The proposed methodology considers the objectives outlined section 1.5.

### **3.1 P25 Network Requirements**

To enable a P25 RMU such as the Auria Wireless ES1105-V to be successfully implemented as a remote communications device in ACR using Ergon Energy P25 network, the understanding of the P25 network operation requirements the following areas are considered:

- Digital Modulation Two – Phase Plan
- Key Components of P25 System and RMU
- Capabilities and limitations of P25 network and RMU

#### **3.1.1 P25 Digital Modulation**

Ergon Energy P25 network has been based on Phase 1 (refer section 2.2.1.2) with operation frequency availability in High VHF Mobile Trunking Band using Common Air Interface (CAI). The P25 channels are capable of carrying voice or data at 9600 bits per second and protected by forward error correction to improve RF conditions and operating range. The confidentiality and authenticity of data is maintained while in transit between the service and the end point. Ergon Energy P25 network employs Encryption type AES256 and Authentication technique SHA-1 or equivalent.

### **3.1.2 Key Components of P25 System and RMU**

Ergon Energy P25 network is based upon APCO Project 25 Phase 1 Digital Trunked Radio technology. Refer to Figure 6 inside the red circle shows the P25 operating frequencies in the High VHF Trunked Band (165 – 173 MHz), with Mobile Base Station receive high (BR) and transmit low (BT).



Figure 6: ACM VHF High Band Plan (Airwave Solutions P25 Rack Training, 2012)

An example of Ergon Energy P25 Physical Architecture and the Logical Architecture with P25 RMU are represented in in Figure 7 and 8 respectively. Data path for the ACR's SCADA and REA (Remote Engineering Access) shows in green using the P25 RMU. The P25 RMU connects to a Land Mobile base transceiver via CAI over the air and to the P25 Channel Controller (P25CC). The Base Station Controller (BSC) embedded in the P25CC determines where the packet is to be sent which sends data packet to the Data Service Node (DSN) for data or to the RF Sub-System Network Controller (RNC) for voice. The BSC sends the P25 RMU's received data packet to the Data Service Node (DSN) and the DSN transfer the packet to the SCADA master station (RDAS) via the Data Network Interface on Ergon Energy Operational Control Network (OCN) WAN. The data packet sends out from the SCADA master station to the ACR is in the reverse order of the above described process.

Ergon Energy P25 network is primarily designed to transport voice traffics and therefore Voice takes precedence over P25 RMU's data.

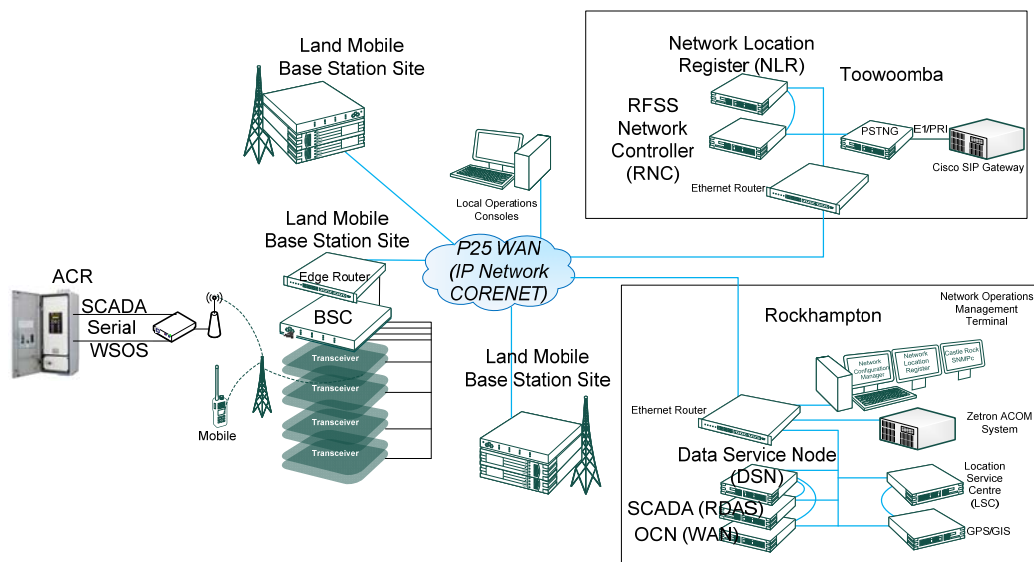


Figure 7: Example of Ergon Energy P25 Physical Architecture

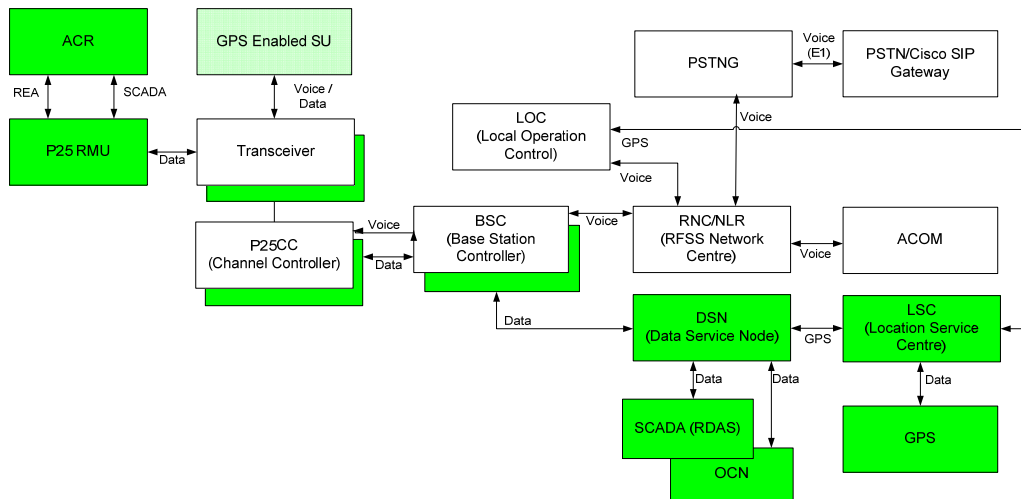


Figure 8: Ergon Energy P25 Logical Architecture

The Ergon Energy P25 network radio interface points to its P25 mobiles and P25 RMUs are at the base station sites. The Land Mobile base station standard operations using single antenna to achieve:

- One control channel for P25 operations and three voice or data channels (1 + 3), expandable to (1 + 5).
- ACMA limitation to 'down link' direction is 83W EIRP (Equivalent Isotropic Radiated Power).
- 5% BER (Bit Error Rate) Threshold of -119dBm into the Receive Multi-Coupler (PEI SA2C-8QAN-DP).

### **3.1.2.1 Key components of an Ergon Energy P25 Land Mobile Base Site**

It can be seen from the schematic diagram Appendix B, a typical Land Mobile Base Station Site consists of the following essential components being used that also represented as shown on Figure 9:

1. Receiver Multi-Coupler (RxMC) – PEI (Polar Electronics Industries PTY LTP) SA2C-8QAN-DP.
2. Transmitter Multi-Coupler (TxMC) – PEI TM2-6-P6-04.
3. Diplexer (148 – 174 MHz) – PEI 2x4AI2-3.
4. VSWR Monitor – PEI PAAP.
5. Diplexer (148 – 174 MHz) – PEI 2x4AI2-3.
6. Base Transceiver - TAIT TB8115.
7. Channel Controller (P25CCe) and Base Station Controller (BSC).

The current P25 RF Multi-Coupling to the Land Mobile Base is capable of 4 VHF channels with future expansion to 6 channels, as shown in Figure 9. The system has the specifications of 4.5dB insertion loss with the diplexer included. TX to TX isolation is 75dB, TX to RX is 80dB and TX noise suppression is 100dB. RX gain is 1dB with +/- 0.5 dB, RX to RX isolation is 20dB. TX input VSWR is 1.2:1 and RX output VSWR is 1.5:1. 150 kHz channel spacing with 4.6 MHz TX to RX spacing uses a single antenna.

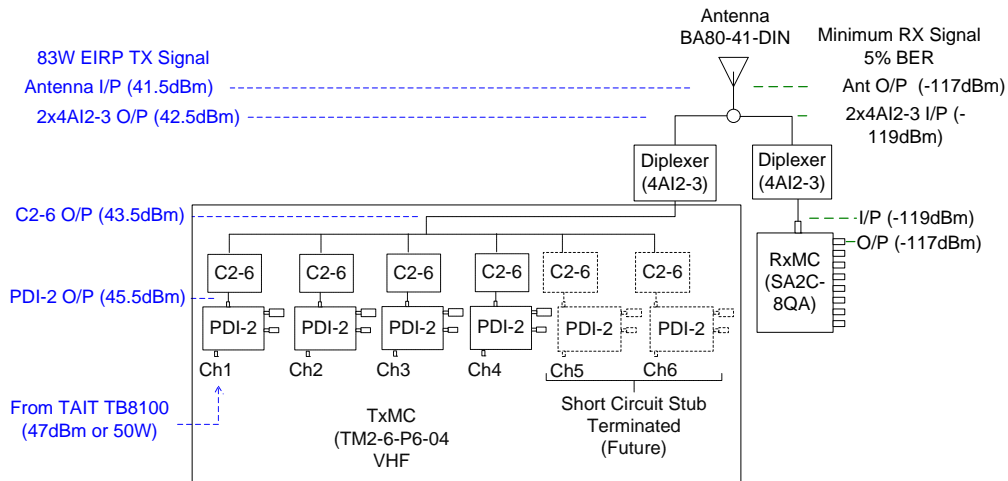


Figure 9: Ergon Energy P25 TX/RX Multi-Coupler Expected RF Levels with 150kHz Channel Spacing  
(Based on Ergon Energy P25 Specifications Documents)

### 3.1.2.1.1 The Receiver Multi-Coupler

Ergon Energy P25 is using a PEI SA2C-8QA which is a 19" panel mount with 1 rack unit (RU) high for its VHF high-band receiver multi-coupler (Figure 9 also Appendix C). The input RF signal is amplified and splits 8 ways to the output ports of the receiver multi-coupler (RxMC). Each of the output port then connects to TAIT TB8100 Receiver 1 to 4 respectively. This way the all the transceivers receive all the channel signals from the antenna. Channel specific filtering occurs at the transceiver's RF and IF (intermediate frequency) receive filters.

The receiver multi-coupler has two low noise amplifiers incorporated using hybrid dividers on the input and outputs to service the output signals. If one of the amplifiers failed the second amplifier continue to provide the signal required.

This allows the system to continue operate at a lower level until full service is restored. The current sense monitor circuit is used to monitor the current drawn by the active devices in the RF amplifier path. When one or both of the amplifiers operating outside the pre-set limits then alarm is set through an alarm relay output. Ergon Energy uses Sensor Probe to monitor this alarm output.

#### **3.1.2.1.2 The Transmitter Multi-Coupler**

As can be seen in Figure 9, the Transmitter Multi-Coupling TM2-6-P6-04 is made up of  $\frac{1}{4}$  wavelength tuned cavity resonators, RF isolators and cabling harness to achieve a single output at to the diplexer. A 50W RF C4FM signal transmits from the TAIT TB8100 power amplifier feeds to the dual stage isolator (PDI-2). The PDI-2 protects the power amplifier from RF reflection due to an impulse of high VSWR condition. This can damage the amplifier if the amplifier happens to be transmitting at the time of the VSWR incident. The isolator significantly reduces unwanted signals from adjacent channels, and from the antenna that may enter the front end of the power amplifier which can creates unwanted intermodulation products that may be re-transmitted. The signal continues onto the cavity resonator (C2-6) for band-pass channel filtering, since the presence of the isolator, its ferromagnetic properties has the effect of increasing unwanted wide-band emissions. The cavity resonator band-pass filtering response allows all the cavity resonators cabling together in a 'star' connector combine all channels into one RF feeder output refer Appendix B.

The cable harness connected to future channel 5 and 6 are terminated with low impedance coaxial stubs which allow the combiner to function as if the cavity resonators are presence. The transmit multi-coupler is a passive device.

The Transmitter Multi-Coupling TM2-6-P6-04 physical specifications refer Appendix D.

### **3.1.2.1.3 The Diplexer**

The diplexer is a passive device that performs frequency domain multiplexing. That is, two ports are multiplexed onto a third port. The scenario shown in Figure 9, the diplexer is best described as a duplexer that allows bidirectional communication over a single feeder. This way only a single antenna has been used for simultaneously transmit and receive operation.

The diplexer is a band-pass diplexer which means that at the same time it's performs the duplex function, the device provides further band-pass filtering in both transmit and receive directions. The wideband transmitter noise and unwanted transmitter intermodulation products are further attenuated in the transmit direction. In the receive direction the band-pass response provides useful receiver pre-selector filter which attenuates unwanted signals and interference entering the receiver multi-coupler.

The RF diplexer 2x4AI2-3 physically is 4RU high to be mounted on 19" rack refer Appendix E which comprises four (3x4 inch) band-pass  $\frac{1}{4}$  wavelength cavity resonators in each diplexer module.

### **3.1.2.1.4 VSWR Alarm Monitor Base Antenna**

The VSWR monitor PEI PAAP provides continuous monitoring both the transmitter and the antenna. The device raises an alarm if the forward power falls below a set level or if the antenna VSWR goes high. Ergon Energy P25 network uses a Sensor Probe manage the alarm contact output at every Land Mobil Base Site. The alarm signal stays set until a reset is applied on the front of the panel. The alarm device is mounted on a 1RU high 19" unit as can be seen in Appendix F.

#### **3.1.2.1.5 RF Feeder of the P25 Base**

RF cables used on P25 panel are 'Heliax' foam-dielectric FSJ1-50. From the P25 Panel to the RF gland plate FSJ4-50 is used for its flexibility. The RF feed to the antenna from the gland plate LDF4-50 cable is used. These foam dielectric RF cables processed most effective RF shielding, durability and flexibility for their corrugated solid copper outer conductor construction.

RF cables termination on P25 equipment using N-type or BNC connector types.

#### **3.1.2.1.6 Base Antenna**

The antenna used on P25 base is RFI BA80-41-DIN. This omnidirectional arrays with stacked dipoles characteristics which provides wide bandwidth covering from 136- 174 MHz with 6dBd or 8.1dBi. The antenna covers 38 MHz bandwidth with less than 1.5:1 VSWR (14dB), vertical beamwidth is 18°, horizontal beamwidth is Omni +/- 0.5dB, 50Ω input impedance and capable of 750 watts maximum power. Antenna radiation patterns for BA80-41-DIN shows in Figure 10.

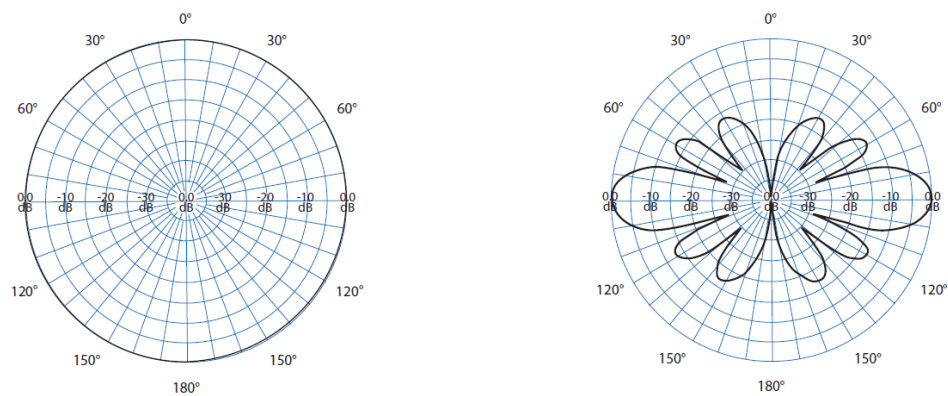


Figure 10: P25 Base Antenna BA80-41-DIN Radiation Patterns (Adapted from BIRD TECHNOLOGIES GROUP TX RX SYSTEMS, VHF Omnidirectional Dipole Arrays))

### **3.1.2.1.7 Lightning Protection of the P25 Base**

The base antenna is earthed at the bottom of the support pole section, to the tower earth conductor. The LDF4-50 RF feeder is earthed at the base of the antenna, the transition point from vertical to horizontal on cable tray at the radio tower base and at the gland plate prior to building entrance. The LDF4-50 is terminated onto to a bulk-head inline surge protection device (RFI VHF50HD) mounted on the gland plate which also earthed to sink all the surge energy from lightning strikes.

### **3.1.2.1.8 Base Transceivers TB8100**

The TB8100 Dual Base Transceivers are housed in a 4RU 19" rack mount to provide two VHF High Band channels operation. The standard Ergon Energy P25 base site configuration has two TB8100 units which capable of four channels operation and room available for a 3rd TB8100 unit on additional 5th and 6th channel as required in the future. Each transceiver is cabled to a dedicated channel card in the associated P25 Channel Control (P25CCe) unit.

Each of the transceiver connected to its respective P25CCe channel card by using a nine core data cable. On this cable the transmit direction from the P25CCe channel to the transceiver is the over-the-air 'downlink' and the receive direction is the over-the-air 'uplink' in the form of a raised-cosine filter 4-level PAM signal. In the transmit direction, the 4-level PAM modulates from the transceiver's VCO to produce the compatible P25 C4FM (4-FSK) modulated RF carrier. In the receive direction, the C4FM RF signal is demodulated by the transceiver's FM demodulator to produce the desired 4-level PAM signal. These functions are carries out in the transceiver units.

Each of the 4RU 19" rack mount TB8100 unit accommodates two transceivers, two power amplifiers and a power supply unit. The power amplifiers boost the RF transmit signal to 50W. The power supply unit accepts -48VDC input to provide the internal DC power rails as required by the transceivers, amplifiers and fan units. The power supply unit also provides a +12VDC output which is used to power associated P25 equipment. This equipment includes the VSWR Power Alarm Monitor, Rx Multi-Coupler and P25CCe units. The no.1 TB8100 provides the main power supply and the no.2 TB8100 provides the backup power supply for reliability operation. When a TB8100 failed the Land Base Mobile operates as a P25 '1+1' Trunk instead of the normal '1+3'.

The TB8100 unit module summary alarms are captured by the P25CCe units using the Transceiver to channel card data cable. Ergon Energy monitored the TB8100 using SNMP client setup on the Sensor Probe at each Land Mobile Base site. The TB8100 'Service Kit' software application is used for remote configuration and management of the TB8100 units which accessed by the

transceiver's separate Ethernet port using the IP address for the Transceiver using Cisco 2911 router that also resides in the P25 panel.

#### **3.1.2.1.9 Channel Controller (P25CCe) and Base Station Controller**

The P25CCe is a rack mounted (1RU high) device located at each base station that provides a fully compliant APCO P25 digital air interface implementing full forward error correction and channel control as specified by the APCO P25 Standard.

Each P25CCe can interface with up to four individual base stations to provide digital trunked control operation with voice and data traffic capability. Two P25CCe units are used in Ergon Energy P25 network at each site to provide physical redundancy and allow support for up to eight digital radio channels.

The P25CCe includes a high performance embedded processor to provide the Base Station Controller application. The embedded BSC in each P25CCe, the Ergon Energy P25 Phase 1 is setup with high availability implementation of the BSC. This consists of Active and Standby embedded processors co-located in the P25CC at each site in an individual chassis. The Standby P25CCe will automatically take over data call processing upon the Active P25CCe processor fail.

#### **3.1.2.2 P25 RMU Key Components**

The P25 Radio Modem Unit (RMU) proposing is an ES1105-V RMU (RMU) made by Auria to be used to provide communications to ACR as shown in Figure 3. The P25 RMU is to provide wireless communications to ACR with both Remote Engineering Access and SCADA control using RS-232C ports. A mobile VHF

antenna (RFI CD28) would typically mounted on a Hockey Stick (RFI HS72) with a short 1.5m RF feeder coaxial RG58 connect to a lightning arrester on the controller box. An RFI bulk-head IS-B5OLU-C1 or equivalent can be used for lightning protection. RF connectors are male N-type at the surge arrestor and male TNC on the antenna port of RMU. The RMU uses less than an Ampere at 12V DC which the Nulec (ACR) power supply is sufficient.



Figure 11: P25 RMU ES1105-V Radio Modem Unit

The RMU integrates a Nexus XR25 transceiver and an RMU Control Board within a rouged aluminium casing as can be seen in Figure 11.

#### **3.1.2.2.1 Key Features of P25 RMU**

The RMU features are as follows:

- Support for Trunked P25 operation with Sub Network Dependent Convergence Protocol (SNDTCP) packet data.
- Integrated TCP/IP protocol stack.
- Integrated Nexus XR25 radio transceiver.
- 2 x RS-232C serial ports.
- 10/100M Ethernet.
- USB 2.0.
- 12V DC operation.
- 10W transmit power option.
- Sensitivity RSSI as low as -119dBm.
- IP-67 rated aluminium enclosure.

#### **3.1.2.2.2 The RMU in P25 Network Context**

The position of the RMU can be illustrated in the context of a P25 Radio Frequency Sub-System (RFSS) as shown in Figure 12. The RMU interfaces directly to the ACR's SCADA and Remote Engineering Access (WSOS) via RS232. The RMU communicate to the P25 RFSS fixed network equipment via the common air interface (CAI).

The Data Service Node (DSN) also located within the P25 network is used as a gateway between the P25 RFSS and external applications such SCADA Master Station, Remote Engineering Access (WSOS) or GPS.

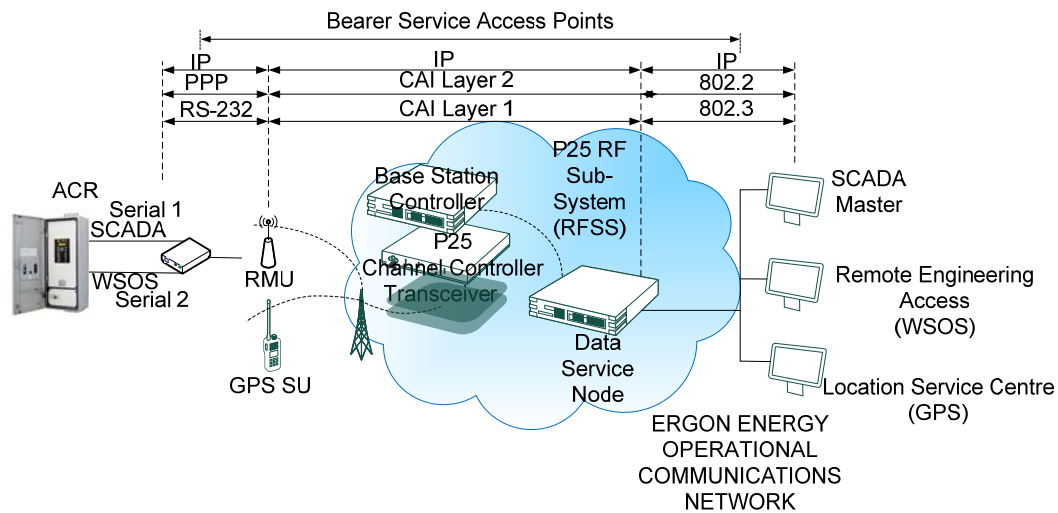


Figure 12: P25 RMU System Component Context of Packet Data Service Connectivity

### 3.1.2.2.3 P25 RMU Front Panel Interfaces

The RMU physical interfaces and port allocations can be seen in Figure 13 are as follows:

- Auxiliary Test Interface – for factory compliance testing purposes.
- RS232 Port 1 – Allocated for ACR SCADA DNP 3.0 connection.
- RS232 Port 2 – Designated for Remote Engineering Access (WSOS).
- Ethernet Port – For connection to remote terminal (not use on Ergon Energy ACR).
- Power – 12V DC input connection.
- Antenna – Uses a TNC connector to connect to antenna (VHF).
- LED indicators – For indicating RMU state, status, data port connectivity and RSSI in tri-colour.
- USB – Universal serial bus port used for RMU firmware updates, programming and debug.
- Button – Uses to enter or exit Standby and RSSI Measuring modes which indication via the LED.

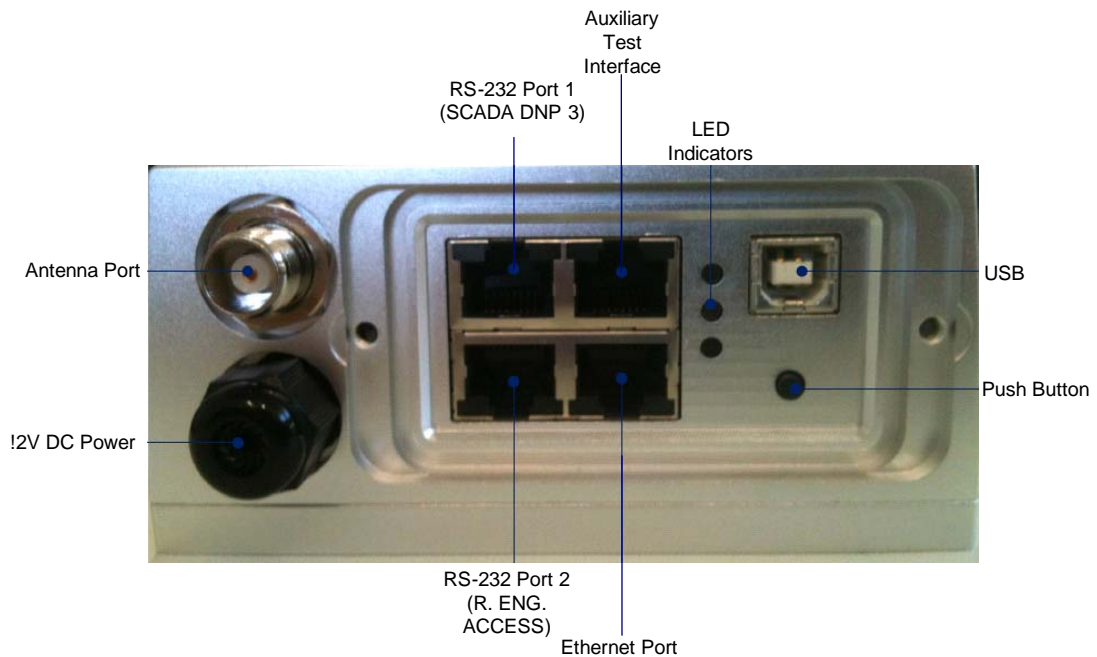


Figure 13: RMU Physical Port Connection

### 3.1.3 Capabilities and limitations of P25 network and RMU

The Ergon Energy P25 network is based on APCO P25 Phase 1 standards for a digital common air interface (CAI). This is based upon frequency division multiple access (FDMA) using a 12.5 kHz channel. The operating frequencies are in the High VHF Trunked Band (165 – 175 MHz). Ergon Energy power distribution grids are providing electricity over large areas to most regions in the state of Queensland. For this reason Ergon Energy P25 Land Mobile Base sites are strategically located throughout the state to provide coverage primarily for voice communications to its mobile fleet during fault and maintenance works. As RF groundwave propagates further at lower frequencies hence VHF has been used for Ergon Energy P25 network.

Apart from providing voice communications to its vehicles fleet, Ergon Energy P25 network also obtaining GPS/GIS information of every mobile radio with its Location Service Centre (LSC) from the P25 Data Service Node (DSN). This mobile unit tracking feature is used for the management of mobiles on the P25 network

and also can be used for locating a mobile unit in vehicle during emergency situation. For this reason it makes perfect sense to utilise the existing DSN on the P25 network to transport both ACRs SCADA DNP 3.0 over P25 network to SCADA Master Station and remote engineering access management to ACRs for remote configuration using WSOS.

The capabilities and limit of the P25 network to pass ACR's DNP 3.0 and Remote Engineering Access traffics using P25 RMU is greatly depends upon the channels available at its Land Mobile Base site's using CAI:

- At a base site one channel dedicating for P25 control function and three channels available for Mobile voice or RMU data (fixed) traffics (1+3). There is room available for additional two channels by just adding a TB8100 unit as hardware to make the Network as 1 + 5 (ACMA licences are secured).
- P25 network is primarily designed to carry voice traffics hence RMUs' data traffics takes lower priority. A P25 channel will only pass RMUs' data traffics through its CAI when it is idle without voice traffic. The P25 channel CAI will drops its RMUs' traffics when a voice mobile unit requires connection onto the P25 network at a base site when all other channels are occupied.
- Setup for testing RMUs' traffics, each P25 channel could accommodates up to five P25 RMUs' traffics to pass through its CAI at a time. Up to fifteen RMUs can be connected to a P25 base site via CAI for any instance.
- It is required that the performance of all RF channels to be configured and checked to ensure that low Bit Error Rate (BER) of less than 1% on both uplink and downlink directions. One technique that RF performance can be measured by generating P25 1011 test tone and measure the BER on the receiving side. Both P25CC and RMU support the generation and

calculation of BER and are the absolute reference for BER measurements. Procedures on how to use the necessary test modes can be found in the user documentation of Ergon Energy relevant products manual.

- The base receive RSSI is rated to a level of -119dBm and the P25 RMU sensitivity is similar, which will set the coverage distance a P25 RMU can be from a base. However it would be wised to benchmark the current NextG modem for consistency operation RF RSSI level which has been aimed for minimum of -91dBm that also can be estimated using path loss calculation or using software such as 'Radio Mobile'. The P25 RMU also comes with LED(s) indicator to aid the determination of RF RSSI level during operation refer Table 1.

Table 1: P25 RMU RSSI LEDs Measuring State definition

<b>RSSI (dBm)</b>	<b>LED 1 Colour</b>	<b>LED 2 Colour</b>	<b>LED 3 Colour</b>
>-60	Green	Green	Green
-60 to -64	Off	Green	Green
-65 to -69	Off	Off	Green
-70 to -74	Blue	Blue	Blue
-75 to -78	Off	Blue	Blue
-79 to -83	Off	Off	Blue
-84 to -87	White	White	White
-88 to -91	Off	White	White
-92 to -96	Off	Off	White
-97 to -101	Orange	Orange	Orange

-102 to -106	Off	Orange	Orange
-107 to -110	Off	Off	Orange
-111 to -114	Red	Red	Red
-115 to -119	Off	Red	Red
< -119	Off	Off	Red

The P25 RMU will only enter to RSSI measuring state from the Modem State only with a short press on the button at front panel to activate or to deactivate. LED1, LED2 or LED3 illuminating sequence flashes on 900ms and off 100ms.

### **3.2 Assess the location of existing ACRs to the P25 network coverage**

Ergon Energy current has twenty one thousand one hundred and five ACRs on its electricity network state wide and only a third of which has been equipped with communications for supervisory control and data acquisition and remote engineering access. It is best to present the P25 network coverage that could potentially provide communications to existing ACRs on the Ergon Energy Electricity network using Google Earth.

### 3.2.1 ACRs locations

Figure 14 shown the location of ACRs on the map using Google Earth, each 'grey square' is represents the ACR with red or light red lines represents the electricity grid that using ACRs.



Figure 14: Automatic Circuit Recloser positions on the map

### 3.2.2 Potential ACRs with P25 coverage

The Ergon Energy P25 network coverage for the whole state of Queensland as displayed in Figure 15. Relating two Figures 14 and 15, the P25 network coverage covers significant amount of ACRs on the electricity grid to provide the potential communications using P25 RMUs.

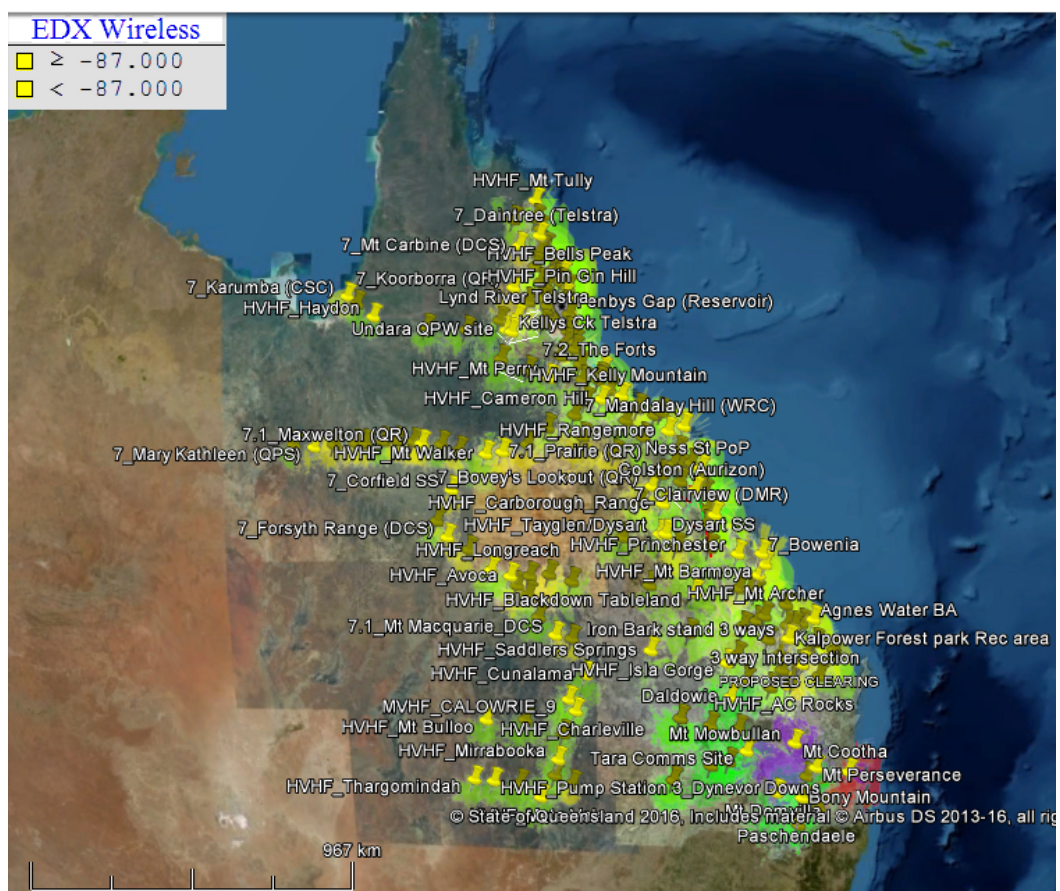


Figure 15: Ergon Energy P25 Network Coverage

### **3.3 P25 Communications Protocol**

The P25 RMU can be served as a P25 digital radio in a P25 digital radio system (Ergon Energy P25 system) that supports circuit and packet data bearer services as standard. The P25 radio system serves multiple packets protocols, including TCP/IP, X.25 (Packet Switched WAN), and SNA (System Network Architecture). To keep the complexity of a P25 radio system to a minimum while supporting such a variety requirement, it is suggested that the radio support a single standard packet protocol interface. The Ergon Energy P25 radio system uses IP for standard packet protocol that allows other packet to be served via encapsulation within IP.

As previously shows in Figure 12, the packet data standard between a P25 RMU and a Fixed Network Equipment (FNE) interface, a TCP/IP standard packet network (interface between DSN and SCADA Master). Only packets of information abide to this network protocol will accept for transport across the radio network, with all attached data peripheral devices being established by standard IP network identities. Error control and correction is the responsibility of the mobile and fixed stations. Standard IP network applications to a P25 radio via a PPP (Point to Point Protocol) or SLIP (Serial Line Internet Protocol) is transparent.

P25 RMU intended communications on ACR using RS232 DNP3 (SCADA) encapsulate IP and RS232 raw (WSOS) also uses IP encapsulation.

The information in Table 2 outlines TIA/EIA-232 parameter data representative of the P25 RMU implementation of the standard TIA/EIA-232-E on the Physical Layer interface (OSI layer1).

Table 2: Features and Capabilities Supported by TIA/EIA-232

Parameter	Typical Value	Option
Signal Voltage	-12V to +12V	5V systems (short range)
Data Rate	9.6 kbps	Up to 115.2kbps
Data Transport	Serial binary data	
Data Construction	5 to 9 wires	
Device Access	Single Transmit/Receive	Multipoint Receive (Star)
Power Configuration	Each Host Self Powered	
Critical parameters	Number of output lines Type of interface driver IC Output line state	
Standard	TIA/EIA-232-E	

### 3.3.1 Carrying DNP3 over a TCP/IP network

Figure 16 shows the idea of transporting DNP3.0 over a network involves encapsulation of the data frames from the DNP3.0 data link within the transport

layer frames of the Internet Protocol suit and allowing that protocol stack to deliver the DNP3.0 data link layer frames to the destination location in place of the original DNP3.0 physical layer. A P25 RMU RS232 DNP3.0 encapsulated over IP shares the same approach.

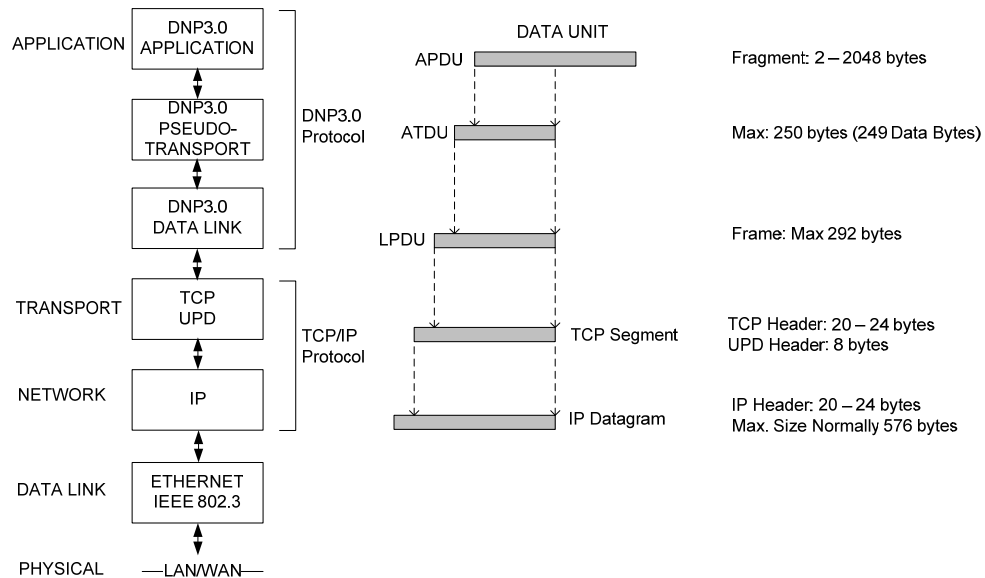


Figure 16: DNP3.0 over TCP/IP Protocol Stack (DNP3 IEC 60870.5)

### 3.3.2 Remote Engineering Access

Remote engineering access using WSOS via RS232 over IP encapsulation employed the same process as per DNP3.0 but the protocol will be raw RS232.

### **3.4 Ergon Energy ACR operation requirements**

This is the baseline capabilities for reliable operation which includes:

- e. The P25 RMU dynamically selects or locks onto a better signal strength P25 radio site. This is to ensure the P25 RMU hunts properly.
- f. When the P25 RMU successfully affiliates and registers with a P25 radio site, the data connection should be reliable in terms of link RF margin. That is the thresholds set for affiliation or registration needs to be appropriate.
- g. The P25 RMU serial 1, DNP3 SCADA communications to the SCADA master station must be reliable.
- h. With regards to capacity and reliability of Remote Engineering Access, the P25 RMU serial 2 must be capable of file downloads and uploads.

#### **3.4.1 Capabilities for reliable operations**

Operational requirement for capabilities and reliability operation will be benchmarking NEXTG modem application figure for testing.

## **4.0 P25 RMU Asynchronous V.24 Service**

The following section describes the communications application associated with P25 RMU Asynchronous V.24 Service use on ACR. This is to give a general view of service specification, technical specifications and capabilities of the P25 Asynchronous V.24 Service.

The P25 RMU Asynchronous V.24 Service provides asynchronous serial communication link to typically two serial ports on each ACR for SCADA DNP3.0 and Engineering Access, located within P25 coverage areas across the Ergon Energy operational service areas. The service provides the Engineering Access port on the ACR as a virtual port within Ergon Energy's Operational Network defined by an IPv4 address and a TCP port as raw TCP socket. This enables remote communications via serial port (TCP) over IP for configuration of ACR using WSOS application. The service also provides a TCP/IP adaptation layer to DNP3.0 frames communications on the SCADA port of the ACR and presents as a DNP3.0 over TCP access point within the Ergon Energy's Operational Network. This facilitates communications with a SCADA Master Station's TCP over IP front end processor. The Engineering Access service has its own unique IP address and so is the SCADA DNP3.0 service.

### **4.1 P25 RMU Service Specification**

Figure 17 has been simplified from Figure 12 of RMU in P25 network context shows the asynchronous V.24 services can be provided using P25 Digital Trunked Radio network as Access Network technologies between two service endpoints (OCN and P25 RMU).

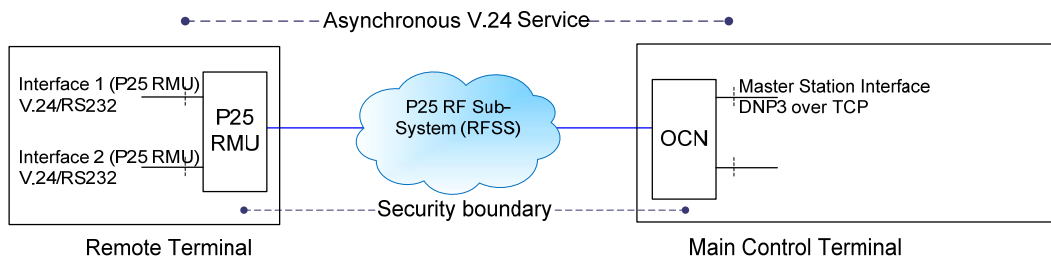


Figure 17: Asynchronous V.24 Specification

The P25 RMU in Figure 17 provides interfaces for connectivity onto ACR at a remote location and appropriate to Access Network (P25). OCN provides a secured and controlled entry point to the Master Station or the Remote Engineering Access interface.

## 4.2 P25 RMU Interface specification

The P25 RMU asynchronous V.24/RS232 interface 1 and 2 port settings specifications are as shown in Table 3.

Table 3: P25 RMU V.24/RS232 Interface 1 and 2 Port Settings

Port Settings	Interface 1	Interface 2
Baud Rate	9600	19200
Data Bits	8	8
Stop Bits	1	1

Parity	None	None
Flow Control	None	None

### 4.3 P25 RMU CAI Security Specification

The P25 RMU uses CAI with P25 standard authentication and encryption to provide the security and authenticity of data during transit between the service end points. They are:

- AES256 encryption
- SHA-1 authentication

### 4.4 P25 RMU Service Performance

The P25 Asynchronous V.24 service performance parameters between the Remote Terminal and the Main Control Terminal on Figure 17 are outlined as shown in Table 4.

Table 4: P25 Asynchronous V.24 Service Performance

Performance Metric	Values
Throughput	Minimum of 6.4 kbps half duplex
Packet Loss Rate	Maximum of 1%

Latency	Maximum of 1600 milliseconds round-trip
Jitter	Maximum of 500 milliseconds

## 4.5 P25 RMU Service Performance Levels

The P25 Asynchronous V.24 service performance levels shows on Table 5 including some metrics Target Service Levels.

### 4.5.1 Service Performance Severity Level Definitions

Service performance severity levels are designed to categorise incidents as follows:

- **Severity Level 1** – error rate that or loss of service that renders the service unavailable for a continuous 8 hours.
- **Severity Level 2** – link traffic degradation in which service still usable but impaired or partial loss of a service element.
- **Severity Level 3** – any non-service affecting alarms resulted from abnormalities in transmission performance.

Table 5: P25 RMU Service Availability

Service Availability Metric and Measurement Methodology	
Metric Definition	The Availability of each Service to be measured on per service basis. The availability of a Service defines the communications link via V.24 between the P25 RMU interface and the OCN interface is accessible to the customer, and able to pass traffic across the network, as measured at the Measurement Point specified below. The Service is said to be unavailable when Ergon Energy Operational Support System service agent reports an average round-trip time greater than 1600 milliseconds or a packet loss rate higher than 5% ICMP echo requests of 100 byte length (payload) sent every 1 second for 10 seconds (corresponds to a data rate approximation of 800 bps).
Measure Period	24 hours, 7 days a week and every day of the year.
Target Service Level	99%
Measurement Point	Measured from within the Ergon Energy Operation Control Network
Calculation	$\text{Actual Availability} = \left[ \frac{\text{Actual Hours Available} + \text{Excusable Downtime}}{\text{Available Hours}} \right] \times 100$ <p>Where:</p> <p><b>Actual Hours Available</b> means that the time duration within the Available Hours that the actual Service actually available.</p> <p><b>Excusable Downtime</b> means the aggregate time within the Available Hours that the Service is not available due to:</p> <ul style="list-style-type: none"> <li>Any Scheduled Down,</li> <li>Any other excusable event under the Customer contract.</li> </ul> <p><b>Available Hours</b> means 24 hours, 7 days a week continuous all year round.</p>
Period of Calculation	Calculated on a calendar monthly basis.
Frequency of Measurement	A service response measurement is taken once every 2 hours.
Data Source	Measurement Using Ergon Energy's Operation Support System.
Measurement	Ergon Energy Network Operations Centre.

Responsibility	
Report Frequency	Monthly (Report to be provided within 10 Business Days of every month).
Reporting Requirements	Reports to be provided in soft copy of all relevant support data to verify the Service Level calculations and made available in acceptable format.

## 4.6 P25 RMU Service Activation

Table 6 outlines the target service activation level for P25 RMU.

Table 6: P25 RMU Service Activation

Service Activation	
Measure Period	24 hours, 7 days a week and every day of the year.
Target Service Level	It is recommended that one Service activation per business day and a maximum of 5 service activations per week.
Measurement Point	Measured from within the Ergon Energy Network Operation Control at the service request time.
Measurement Responsibility	Ergon Energy Network Operations Centre.
Report Frequency	Monthly (Report to be provided within 10 Business Days of every month).
Reporting Requirements	Reports to be provided in soft copy of all relevant support data to verify the Service Level calculations and made available in acceptable format.

## 4.7 P25 RMU Service Restoration

Table 7 outlines the target service restoration level for P25 RMU.

Table 7: P25 RMU Service Restoration

Service Restoration	
Measure Period	24 hours, 7 days a week and every day of the year.
Target Service Level	It is recommended that one Service activation per business day and a maximum of 5 service activations per week.
Measurement Point	Measure the incident reported time.
Measurement Responsibility	Ergon Energy Network Operations Centre.
Report Frequency	Monthly (Report to be provided within 10 Business Days of every month).
Reporting Requirements	Reports to be provided in soft copy of all relevant support data to verify the Service Level calculations and made available in acceptable format.

## 4.8 P25 RMU Service Change of Management

Table 8 outlines P25 RMU Service Change of Management such firmware upgrade etc.

Table 8: P25 RMU Service Change of Management

Service Change of Management	
Metric Definition	Measures successful completion of operational change activities.  Successful completion means that the process does not introduce unforeseen problems subsequent to implementation of the change and has been completed.
Schedule Hours	N/A
Minimum Service Level	95% of changes successfully completed in accordance with scheduled change window.
Target Service Level	98% of changes successfully completed in accordance with scheduled change window.
Calculation	$\text{Successful Changes} / \text{Total Changes} \times 100\%$ .
Period of Calculation	Measured on each change.
Frequency of Measurement	Monthly.
Data Source	Change Management tracking data base and related records.
Measurement Responsibility	Ergon Energy Network Operations Centre.
Report Frequency	Monthly (Report to be provided within 10 Business Days of every month).
Reporting Requirements	Reports to be provided in soft copy of all relevant support data to verify the Service Level calculations and made available in acceptable format.

## 5.0 Project Tasks

A testbed to be installed and configured to test P25 communications link via V.24 asynchronous RS232 over IP connections both SCADA DNP3.0 and WSOS remote engineering applications.

### 5.1 P25 RMU Testbed installation

Installation of the testbed according to the schematic diagram in Figure 18 involves the following steps:

- Mount or set up P25 RMU ES1105-V unit on a secured bench.
- Mount ACR TEST BOX.
- Attach DB25- RJ45 (P8) RS232 cable for SCADA DNP3.0 between PORT 1 of P25 RMU and PORT 8 of ACR.
- Attach DB25- RJ45 (P9) RS232 cable for WSOS between PORT 2 of P25 RMU and PORT 9 of ACR.
- Install RF Surge Arrestor (IS-B50LU-C1).
- Attach earthing cables to P25 RMU, ACR TEST BOX and appropriately earth RF surge arrestor.
- Attach the RF cable between RF PORT of P25 RMU and RF surge arrestor input (TNC – N-TYPE connector end).
- Install RFI-CD28 VHF whip antenna and attach to RF Surge Arrestor.

- Setup power supply for 12V DC output and connect DC power cable using 1A Fuse to P25 RMU DC input.
- Power up ARC TEST BOX by plug onto GPO and turn switch to on.

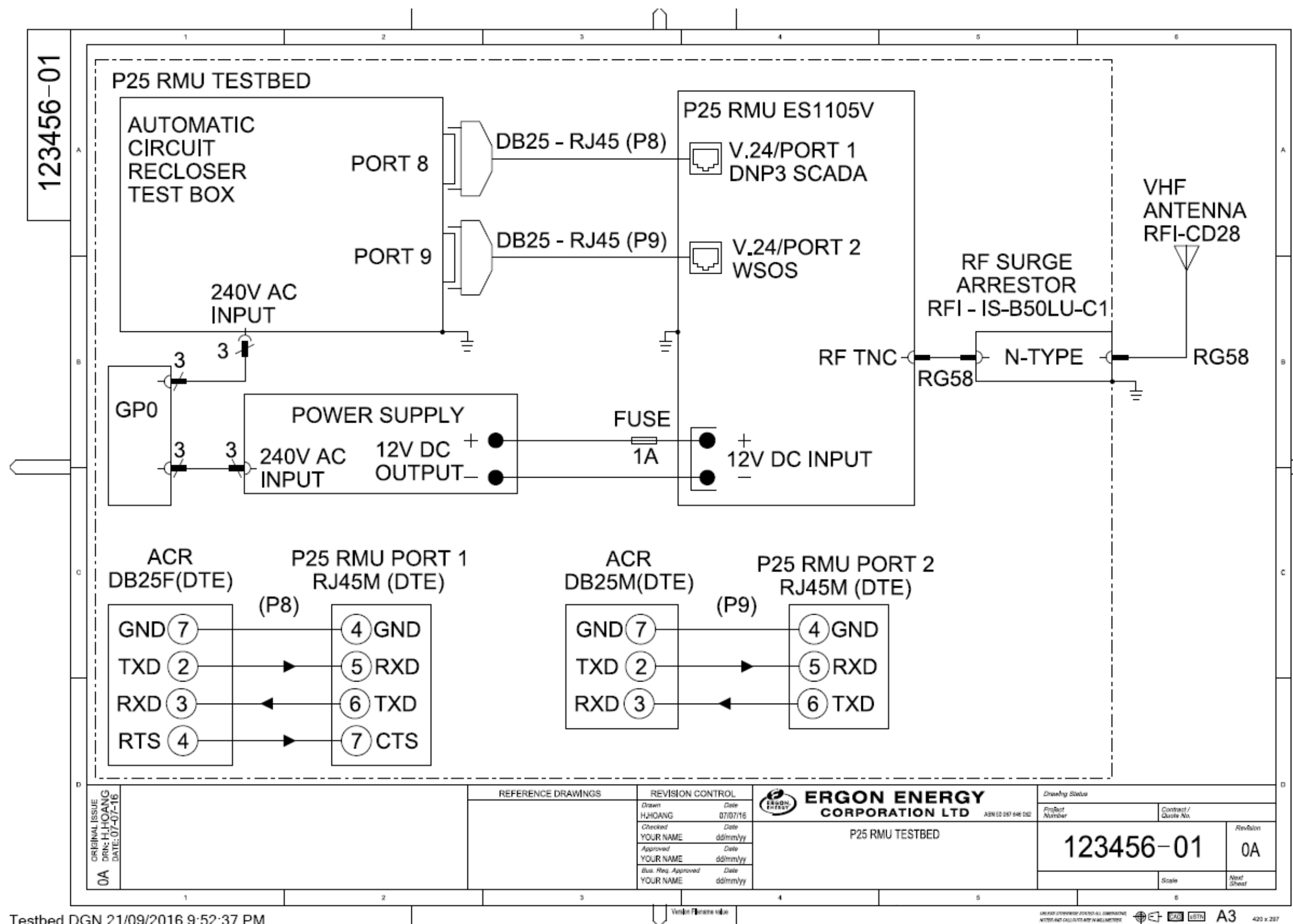


Figure 18: P25 RMU TESTBED SCHEMATIC DIAGRAM

## 5.2 P25 RMU Configuration

The configuration of the P25 RMU involves using the following steps for operation on the P25 Trunked radio network. Both the P25 RMU data base and NLR must be set up to enable operation on the network.

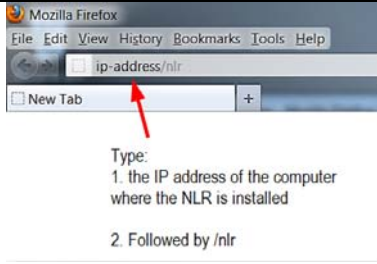
### 5.2.1 IP address allocation for a P25 RMU


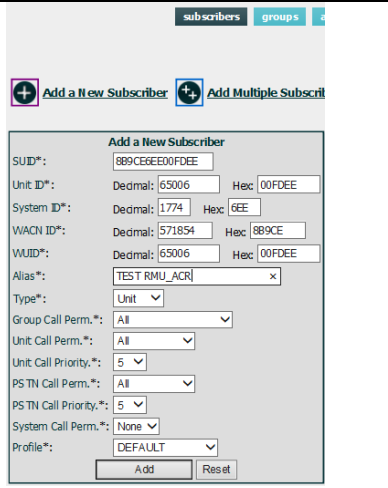
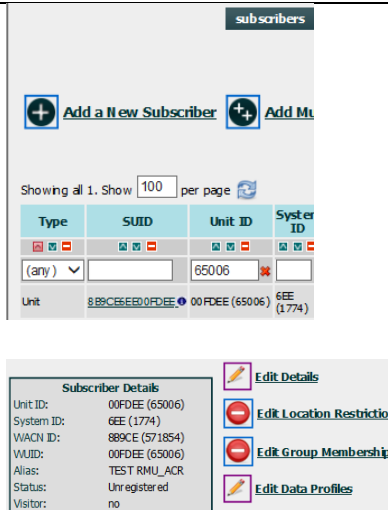
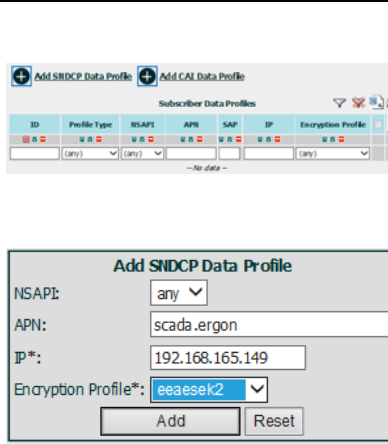
Subnets and IP addresses are to be uniquely assigned for SCADA DNP3.0 and remote engineering access WSOS.

### 5.2.2 NLR Database Configuration

The Network Location Register (NLR) contains the unit identification of every subscriber unit (SU) on the network. Therefore the P25 RMU subscriber unit identification assigned must be configured on the NLR to allow its connection onto the P25 network. This has been outlined in Table 9.

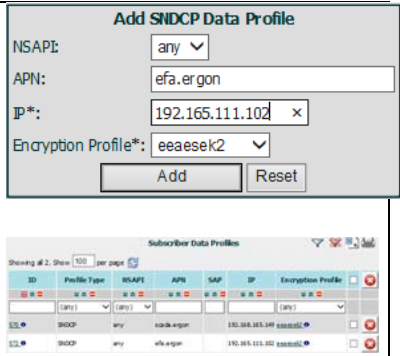
Table 9: Network Location Register Configuration Procedures

<p>1. Enter NLR IP address in Web browser example: <a href="http://192.168.78.15/nlr/">(http://192.168.78.15/nlr/)</a></p>	
--	--

<p>2. Enter Username and Password</p>	
<p>3. To add new subscriber unit, select 'Add a New Subscriber' tab then enter the unit ID and Alias as follows:</p> <ul style="list-style-type: none"> <li>• Fill in 'Unit ID' (65006)</li> <li>• Fill in 'Alias' (TEST RMU_ACR)</li> </ul> <p>Then select 'Add' tab to save new subscriber.</p>	
<p>4. Setup data profiles for subscriber unit by:</p> <ul style="list-style-type: none"> <li>• Search for just created RMU by entering the number in Unit ID window (65006).</li> <li>• Double clicked on the SUID result found for 65006 (8B9CE6EE00FDEE).</li> <li>• Edit data profiles for RMU by select 'Edit Data Profiles' tab.</li> </ul>	
<p>5. Configure SNDCP Data Profile for subscriber unit by:</p> <ul style="list-style-type: none"> <li>• Select 'Add SNDCP Data Profile' tab.</li> <li>• Enter SCADA profile and select 'Add' tab: <ul style="list-style-type: none"> <li>- NSAP (any)</li> <li>- APN (scada.ergon)</li> <li>- IP (unique IP address)</li> </ul> </li> </ul>	

- Encryption Profile (eeassek2)
- Input Remote Eng. Access profile and select 'Add' tab:
  - NSAP (any)
  - APN (efa.ergon)
  - IP (unique IP address)
  - Encryption Profile (eeassek2)

The results showed on Subscriber Data Profiles when added successful.



The screenshot shows the 'Add SMDCP Data Profile' window with the following fields: NSAPI: any, APN: efa.ergon, IP\*: 192.165.111.102, and Encryption Profile\*: eeassek2. Below the window is a table titled 'Subscriber Data Profiles' showing the added profile.

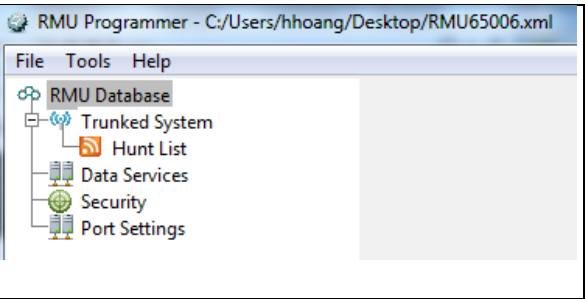
ID	Profile Type	NSAPI	APN	SAP	IP	Encryption Profile
10	GROUP	any	efa.ergon		192.165.111.102	eeassek2
11	GROUP	any	efa.ergon		192.165.111.102	eeassek2

5.2.3 P25 RMU Database Configuration

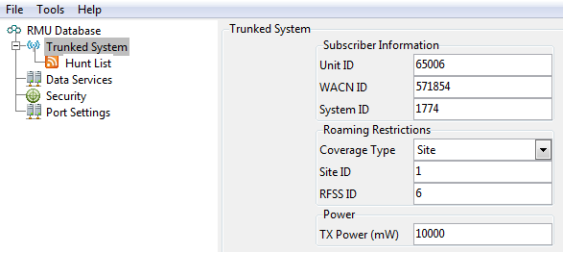
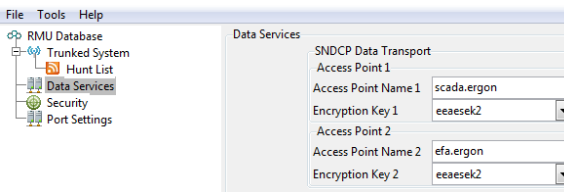

Similar to the NLR the P25 RMU must be configured with the correct unit identification to enable the subscriber unit (SU) to operate on the network. Table 10 describes the configuration settings for P25 RMU using 'RMU Programmer' software.

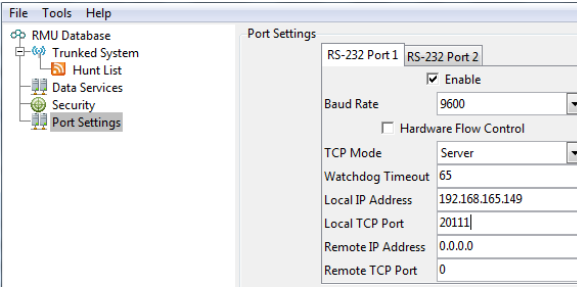
Table 10: P25 RMU Configuration settings procedures

1. Execute the RMU Programmer



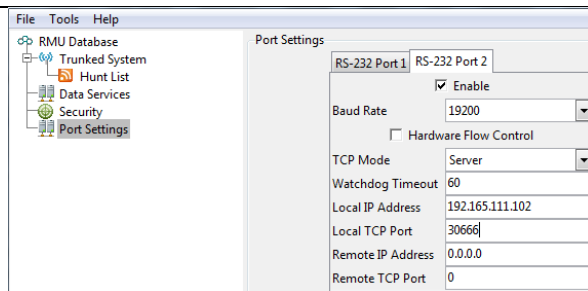
The screenshot shows the 'RMU Programmer' window with a menu bar (File, Tools, Help) and a tree view on the left containing: RMU Database, Trunked System, Hunt List, Data Services, Security, and Port Settings.

<p>2. Edit by select 'Trunked System' and set:</p> <ul style="list-style-type: none"> <li>Unit ID (65006)</li> <li>WACN ID (57154)</li> <li>System ID (1774)</li> <li>Coverage Type (Site)</li> <li>Site ID (1) – site the SU connects to</li> <li>RFSS ID (6)</li> </ul>	
<p>2. Configure SMDCP Data Transport by select 'Data Service' and edit as follows:</p> <p>➤ Access Point 1:</p> <ul style="list-style-type: none"> <li>Access Point Name 1 (scada.ergon)</li> <li>Encryption Key (eeaesek2)</li> </ul> <p>➤ Access Point 2:</p> <ul style="list-style-type: none"> <li>Access Point Name 2 (efa.ergon)</li> <li>Encryption Key (eeaesek2)</li> </ul>	
<p>3. Configure security settings by select 'Security' tab then check Enable Encryption and edit each section as follows:</p> <p>➤ Select 'Add' in 'Keyset List' and enter each</p>	

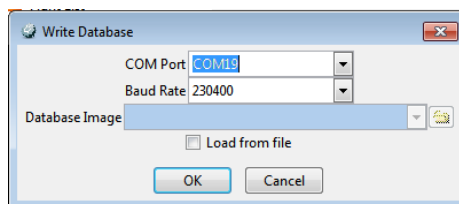
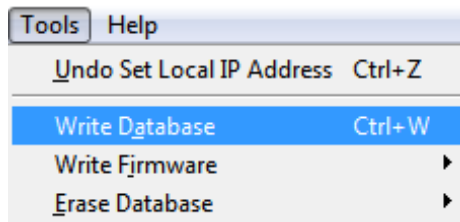
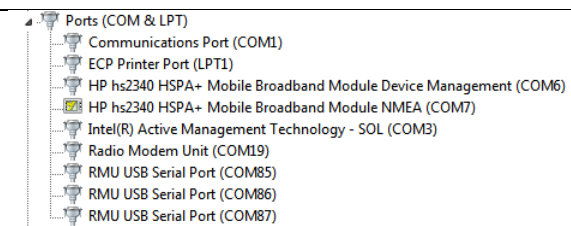
<p>field as below:</p> <ul style="list-style-type: none"> <li>• Keyset Name (eeaesek2)</li> <li>• Keyset ID (2)</li> <li>• Key Type (TEK)</li> <li>• Algorithm ID (AES)</li> </ul> <p>➤ Select 'Add' in 'Key List' and enter each field as describes:</p> <ul style="list-style-type: none"> <li>• Key Name (eeaesek2)</li> <li>• Key ID (2)</li> <li>• Key Type (TEK)</li> <li>• Algorithm ID (AES)</li> <li>• Keyset ID (2)</li> <li>• SLN (2)</li> <li>• Key Material (pre-generated obtained from secret server)</li> </ul>	
<p>4. Configure RS232 port settings by select 'Port Settings' tab then edit each section as follows:</p> <p>➤ In RS-232 Port 1 input as follows:</p> <ul style="list-style-type: none"> <li>• Enable (checked)</li> <li>• Baud Rate (9600)</li> <li>• TCP Mode (Server)</li> <li>• Watchdog Timeout (65)</li> <li>• Local IP Address</li> </ul>	

(192...)

- Local TCP Port (20...)
- In RS-232 Port 2 input as describes:
- Enable (checked)
  - Baud Rate (19200)
  - TCP Mode (Server)
  - Watchdog Timeout (65)
  - Local IP Address (192...)
  - Local TCP Port (30...)



5. Program the P25 RMU by establish communications to RMU via USB port with installed Radio Modem Unit (COM19) driver, go to 'Tool' then select 'Write Database' and select 'OK' tab to write the database configuration to the radio.



### 5.3 P25 RMU Operation

Upon the successful of database configuration the P25 RMU is ready to operate on the P25 Trunked network.

The button on the front of the P25 RMU in Figure 19 can be used to toggle in and out of the RSSI Measuring state when a short press is applied. This can be used as a tool to perform a basic check of the RSSI level by field staffs. The signal strength received at the antenna is reflected by the LEDs on the front panel using a colour base encoding scheme as previously described in Table 1 of section 3.1.3 when in the RSSI Measuring state. When the button at front panel has been pressed for greater than 5 seconds the P25 RMU toggled in and out Standby state. On Standby state the P25 RMU is de-registered from the P25 Trunked Network.

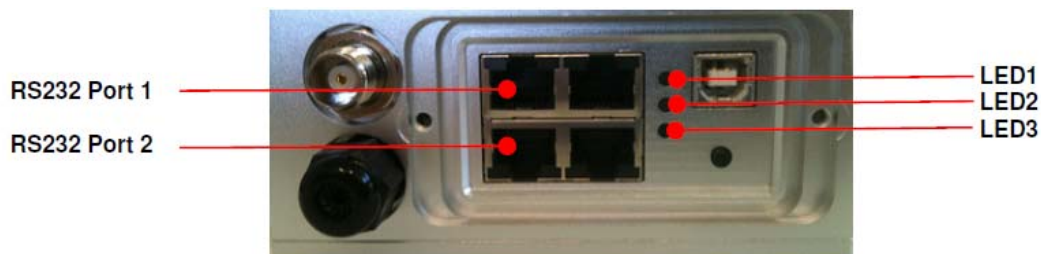


Figure 19: P25 RMU Front Panel LEDs and button

The three LEDs on the front panel are used to indicate the operation state of the device using illumination sequences to reflect the P25 RMU operational state of the XR25 receiver and also the activity on the RS232 data ports.

### 5.3.1 P25 RMU LED indicators

LED1 indicates P25 RMU's overall operational state describes in Table 11 and LED2 & LED3 provide additional sub-states aiding diagnosis of faults.

In general, solid red indicates error and solid green means non-error states, flashing red indicating transient states of possible error condition. A heartbeat green means a stable error free condition. Short duration of solid blue indicates a transmission of data on associated communication device and a short fixed duration of green indicates a reception of data.

Illumination durations are proportional to the amount of data transferred over the serial ports and it depends on the baud rate configured for these ports. For 25 communications illumination durations are fixed to 200ms.

To indicate the P25 RMU is in a controlled state a single LED is flashing. When all three LEDs are flashing this would indicate the P25 RMU is in uncontrolled state. An exception when the P25 RMU is in RSSI reassuring state when the button on the front panel is momentarily pressed, all three LEDs are used to reflect the RSSI in dBm value as per Table 1.

The following table specifies the illuminations sequences of P25 RMU LED1, LED2 and LED3 for different states of operations.

When the P25 RMU is in the Initialising State, LED1 flashes RED 250ms (on) and off for 250ms. LED2 indicates the status of the RMU control board (RCB), while LED3 reflects the status of the XR25 transceiver.

In the Modem State, LED1 is used to show the current state of the P25 RMU. In the Establishing phase LED2 is used to reflect the P25 control channel hunting state, and LED3 is used to indicate the registration state. When the P25 RMU is in Established State, LED2 and LED3 revert to showing the state of their respective remote serial ports.

When the P25 RMU is in the operating Programming State LED1 will flashing Blue 250ms and off 250ms with LED2 will also indicating the programming state which flashing Blue during transmitting data and Green when receiving data.

Table 11: P25 RMU LED1, LED2 & LED3 Illumination Sequences

LED1 Illumination Sequence	LED2 Illumination Sequence	LED3 Illumination Sequence	P25 State	Description
Flashing Red (250ms on & off)	Flashing Red (250ms on & off)	Off	Initialising: RCB loading	Starting RMU Control Board and loading the database.
Flashing Red (250ms on & off)	Solid Green	Flashing Red (250ms on & off)	Initialising: XR25 starting	Power applied to XR25 and waiting for Remote Control Interface protocol negotiation.
Flashing Red (250ms on & off)	Solid Green	Flashing Green (250ms on & off)	Initialising: XR25 Database Verification	RCI protocol negotiation is successfully completed. RCB is waiting for status of database.
Flashing Red (250ms on & off)	Solid Green	Solid Green	Initialising: XR25 started	Database confirmed valid and RCI protocol negotiation is successfully completed.
Flashing Green (250ms on & off)	Flashing Red (250ms on & off)	Off	Modem: Establishing – idle	XR25 is hunting for a P25 channel.

LED1 Illumination Sequence	LED2 Illumination Sequence	LED3 Illumination Sequence	P25 State	Description
Flashing Green (250ms on & off)	Flashing Green (250ms on & off)	Off	Modem: Establishing – hunting	XR25 is hunting for a P25 control channel.
Flashing Green (250ms on & off)	Solid Green	Flashing Red (250ms on & off)	Modem: Establishing – checking	XR25 is validating a P25 control channel found.
Flashing Green (250ms on & off)	Solid Green	Flashing Green (250ms on & off)	Modem: Establishing – registering	XR25 has validated the P25 control channel and is registering attempt.
Heart Beat Green (50ms on, off, on then off 850mms)	Solid Green	Solid Green	Modem: Established	XR25 has successfully registered on to the P25 Network.
Heart Beat Green (50ms on, off, on then off 850mms)	Off	Off	Modem: Established - unused	The remote serial port is not in used.
Heart Beat Green (50ms on, off, on then off	Flashing Red (250ms on & off)	Off	Modem: Established - configuring	The remote serial port is establishing a packet data context with the network.

LED1 Illumination Sequence	LED2 Illumination Sequence	LED3 Illumination Sequence	P25 State	Description
850mms)				
Heart Beat Green (50ms on, off, on then off 850mms)	Slow Flashing Green (1s on & 3s off)	Off	Modem: Established - listening	The remote serial port has established a packet data context and is listing for a socket connection.
Solid Blue (200ms on)	Heart Beat Green (50ms on, off, on then off 850mms)  - Solid Green  For RX data on serial port, duration depends on baud rate configured.  Solid Blue for TX data on serial port duration is proportional to the	Off	Modem: Established - active	The remote serial port has established a socket connection and may transfer data.

LED1 Illumination Sequence	LED2 Illumination Sequence	LED3 Illumination Sequence	P25 State	Description
	configured baud rate.			
Flashing Blue (250ms on & off)	Flashing Blue (250ms) or Green (250ms)	Off	Programming: Data transfer	The P25 RMU is transferring the programming data file.
Very Slow Flashing Blue (1s on & 4s off)	Off	Off	Standby: RCB is in standby state	P25 RMU in standby status, to exit press and hold the button on the front panel for more than 5s.
Solid Red	Flashing Red (250ms on & off)	Flashing Red (250ms on & off)	Error	P25 RMU in error state when internal error detected.

When the P25 RMU running in error this is signifies by LED1 illuminate Solid Red with LED2 indicates the Group ID error and LED3 indicates the Error Code. LED2 and LED3 are both flash a particular number of times to reflect the error condition, with a distinct off sequence before repeating. By viewing the LEDs on the front panel of the P25 RMU the technician could count the number of flashes on LED2 and LED3 to diagnose the cause of the problem. The possible errors are described in Table 12. The System error is grouped according to their hardware module and the subsystem.

Table 12: P25 RMU System Error Codes

Group	Error	Error		
ID bit	Code	Description	Subsystem	Module
0	0	Initialising Timeout	Application	RCB
0	1	Programming Timeout		
0	2	Modem Controller Start Failure		
0	3	Modem Controller Stop Failure		
0	4	RCI Link Failure		
2	0	Delay rite Fail	Database	
2	1	Hardware Failure		
2	2	Incomplete Block		
2	3	Expired Block		
2	4	Block Corruption		

Group ID bit	Error Code	Error Description	Subsystem	Module
2	5	Page Corruption		
2	6	Catalogue Failure		
10	0	Database Invalid	Database	XR25

### 5.3.2 P25 RMU Troubleshooting

The symptoms, possible causes and suggested corrective actions may serve as a basic guidance during P25 RMU installation work is shown in Table 13.

Table 13: P25 RMU troubleshooting and remedies

Symptoms	Probable Cause	Suggested Action
No Activity on LEDs	Power Supply	Check power supply polarity, voltage and current ratings against specifications
Device stays in Establishing-idle or hunting state	Cannot detect P25 control channel	Check antenna connection. Check P25 system configuration parameters in P25 RMU database. Check control channel operational using P25 voice radio.

Device enters Establishing – registering state but fails to register with P25 network	Wrong P25 RMU database or NLR configuration not aligned.	Check RMU database configuration parameters. Check NLR subscriber settings.
Device transitions from an Established state to Establishing – hunting during normal operation.	Poor receive signal quality.	Check RMU RSSI level when the device is in Established – registered state. Check RF cable, connectors and antenna connection.
Remote Serial Ports stays in Established – configuring state.	Not able to establish SMDCP packet data connection with the Data Service Node.	Check RMU database SMDCP packet data configuration parameters. Check DSN is operational and correctly configured. Check NLR subscriber data profile settings.
External application cannot establish TCP connection to Remote Serial Port.	Not registered with trunk network or no SMDCP packet data connections established. Mismatch addresses between RMU database and external application element.	Ensure that the RMU has established connection with P25 network and check the related Remote Serial Port indicating Established – listening via LEDs on the front panel. Check RMU TCP/IP settings matched those being used on the ACR.
Reset upon connecting to PC via USB interface.	RMU device drivers have not been installed on PC.	Ensure RMU programmer and related comms ports drivers are installed on PC.
Device entered error State with RCB Application Initialisation timeout with error indicates (Group 0, Error 0).	Internal Hardware Failed.	Return to supplier for service.
Device entered error State	USB communication failed	Check USB cable

with RCB Application Programming Timeout with error indicates (Group 0, Error 1).	during programming.	connection from PC to RMU.
Device entered error State with RCB Application Modem Controller Start Failure with error indicates (Group 0, Error 2).	Internal hardware fault.	Return to supplier for service.
Device entered error State with RCB Application Modem Controller Stop Failure with error indicates (Group 0, Error 3).	Device failed to de-register with P25 Trunked Network when go into Standby Mode.	P25 network will drop the device after a timeout period – No action required.
Device entered error State with RCB Application RCI Link Failure with error indicates (Group 0, Error 4).	Internal hardware fault.	Return to supplier for service.
Device entered error State with RCB Database with error indicates (Group 2, Error 0-6).	No internal database had been configured.	Using RMU programmer – load RMU database configuration.
Device entered error State with XR25 Database with Database Invalid on error indicates (Group 10, Error 0).	No internal database had been configured.	Using RMU programmer – load RMU database configuration.

## **6.0 P25 RMU Operation Assumptions**

A testbed set up to be operated with the Ergon Energy P25 Trunk Network with the assumptions detailed in the following sections.

### **6.1 P25 CAI uplink and downlink less than 1% Bit Error Rate**

It has been assumed that RF performance on all P25 channels the P25 RMU to operate on are less than 1% Bit Error Rate (BER) typically for both CAI uplink and downlink directions. The data throughput over the air would reduce significantly in poor RF link path or link conditions as a result from dropped packets. This will increase the chance of TCP connection failures between the SCADA master station and client or dropped session during remote engineering access via WSOS between PC and ACR configuration settings.

The RF performance can be measured by putting the P25 RMU in RSSI Measuring State or alternatively measured by generating the P25 1011 test tone and measure the BER on the receiving side.

### **6.2 P25 RMU TCP is used as Network Transport Layer and operate as TCP Server**

The P25 RMU asynchronous RS232 ports data transactions with devices such as ACR are assumed via an established TCP socket connection from a SCADA Master or WSOS application. This is because the P25 RMU only supports forwarding data to the RS232 ports which has been delivered to it via a TCP socket connection from a client application. Data received via other transport layer protocols such

as UDP will not be forwarded to device attached to the P25 RMU's serial data ports.

The P25 RMU does not support configuration as a TCP Client. It is therefore assumed that the P25 RMU will be configured as a TCP Server for TCP connections with external client such as a SCADA Master or WSOS application.

### **6.3 P25 RMU Hardware Flow Control application**

The P25 RMU employs fixed internal buffering capacity and will drop data received on the serial RS232 ports if these buffers are full. For this reason the P25 RMU uses RTS/CTS hardware flow control on its serial ports input signalling to prevent flooding the input buffers from devices it is connected to. It is assumed that a stop and wait protocol is applied over the serial port with a maximum transmit message size of 2048 octets when hardware flow control is disabled.

If the P25 RMU connected to devices with transmit packets larger than 2048 octets in a single or multiple consecutive messages with no stop and wait flow control mechanism employed between messages, hardware flow have to be used.

### **6.4 P25 RMU SCADA given a higher priority than Voice**

If a P25 base site is busy and the P25 RMU SCADA data has been queued for a channel then a channel will be allocated before any other unit requesting a channel for voice, GPS updates or WSOS access. If the data SCADA data is not of higher priority than any other request then the queuing time would become excessive which can lead to failed DNP3.0 operations. Therefore it is assumed

that the SCADA traffic is more important than voice if the target is to ensure key actions and time constraints tied with those actions are met. For example the time constraints associated with SCADA Master successfully polled the remote ACR and requesting a class 0 report update.

## **6.5 Voice and SCADA given priority to pre-emptive GPS or WSOS**

It is assumed that that all voice will be given the higher priority than that of GPS location updates or remote engineering access via WSOS. That is if voice has been in the queued for a channel to a busied P25 base site then voice will be allocated a channel before any subscriber unit trying to perform a GPS update or remote engineering access using WSOS. This is a solution to manage excessive site load rather than delay or denying voice subscribers registration.

To ensure that all voices and SCADA traffic to be pre-emptive, it is assumed that the pre-emptive priority level is set. That is if there are no free traffic channels and the request subscriber unit has a higher priority than existing traffic then the request will be allocated over an existing traffic channel for voice or data. As the radio system operating in a half-duplex scenario which make it impossible to provide a guarantee of bandwidth available to service data or voice whilst the network has a provisioned for a pre-emptive priority level. Due to subscriber units continuing to transmit once started, the network cannot interrupt to reassign an existing channel to traffic that it knows is more essential.

## **6.6 Un-dedicated data channel used**

It is assumed that the P25 network will operate using shared voice or data channels which do not use solely for transporting data traffics. This is because

using a channel to carry voice or data traffic achieves better overall channel utilisation. If a channel is dedicated solely for data then it may improve data service at the expense of voice.

## 7.0 P25 RMU Tests and Findings

The following section outlines the P25 RMU testbed test operations and findings with the Ergon Energy P25 Trunk Network.

### 7.1 P25 RMU RS232 SCADA DNP3 Testing and Findings

In simple term in the following steps describe the communications sequences the master station communicates with the remote device (ACR) via DNP3.0. This will help for interpreting Wireshark captures at the time when there is an issue with the data transmission. Note 0 is the master station id and 60011 is the remote device id using on testbed:

1. The master station polls the remote device (ACR) via 'Reset of Remote Link' in a TCP with DNP3 encapsulated message to check if the communications link to the ACR is up (0 to 60011, len5, Reset of Remote Link). This polling process (ping) will repeat at random with longer delay with the nth time and after the 5<sup>th</sup> time the master station raises a 'Communications Failed Alarm' if no acknowledgement received from the remote device. The polling process will start again after ten minutes.
2. When an acknowledgement received from the remote device (60011 to 0, len5, ACK) and only after a 'Communications Failed Alarm' or first turned on, the master station will write 'Time and Date' to the remote device. Once successful the master station will write 'Internal Indications' to the remote device and waits for the response from the remote device.
3. Once a communications link to the remote device has been established, that is when an a response received from the remote device (60011 to 0, Response) the master station will request a class 0 status report from the remote device (0 to 60011, Read, Class 0). Once all the information has

been successfully updated the master station will pole the remote device again in every ten minutes using the 'Reset of Remote Link' to ensure the communications link is still up. A class 0 update on a remote device is only done once in every 24 hours if the communications link is up for the entire period.

If the data transfer process had been interrupted during the class 0 update the master station will repeat the transmission packet and registers a 'Communications Failed Alarm' after five attempts at random with nth delay time. After a 'Communications Failed' event the master station will try to re-establish communications to the remote device after ten minutes using 'Reset of Remote Link'.

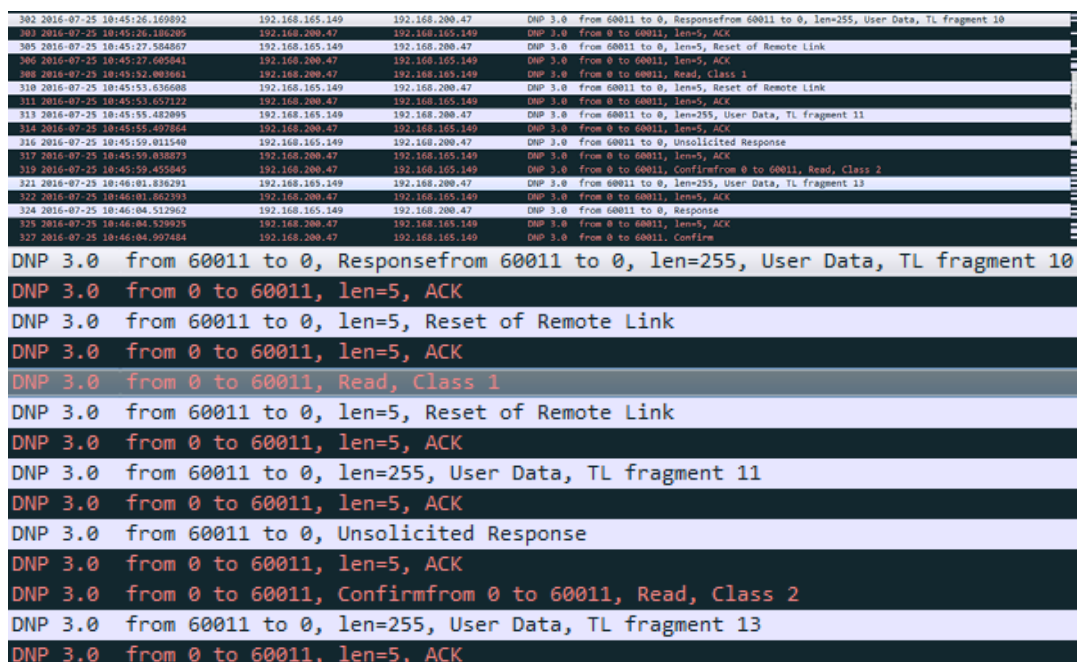
Note: The master station performs steps 1 to 3 when the remote device first switched on and only performs the same operations after a 'Communications Failed Alarm' had been raised. The rest of the time the master station will be in listening mode to monitor any 'Unsolicited Response' from the remote device. That is when an event happened on the remote device such as a 'Trip' event an 'Unsolicited Response' will be sent to the master station and the master station will perform 'Reset of Remote Link' on step 1, acknowledge and write time & date on step 2 and followed by class 0 update on step 3. The master station will clear the 'Communications Failed Alarm' in the system whenever a 'Reset of Remote Link' is acknowledged had been received from the affected remote device.

The following test performance results of the testbed had been found that may potentially determine the key outcome to use P25 RMU to provide communications to ACR on the network.

### 7.1.1 DNP3 data fragmentation

The screen captured of the Wireshark captures with DNP3.0 filtered shown in Figure 20 displayed the data package has been fragmented from the remote device (60011). This issue can be seen on line 302, line 313 and line 321 in Figure 19 which would had caused by the RMU serial input buffer overflowed.

As the testbed with its ACR test box is benchmarked against the NextG modem application, the fragment size was set at 2048. And the P25 network components had been set or optimised for TCP maximum segment size (MSS) of 536 octets to achieve maximum data throughput. The buffer overflow condition can be minimised by set the SCADA master station and the ACR fragment size to 536 octets.



No.	Time	Source	Destination	Protocol
302	2016-07-25 10:45:26.169892	192.168.165.149	192.168.200.47	DNP 3.0 from 60011 to 0, Responsefrom 60011 to 0, len=255, User Data, TL fragment 10
303	2016-07-25 10:45:26.186295	192.168.200.47	192.168.165.149	DNP 3.0 from 0 to 60011, len=5, ACK
305	2016-07-25 10:45:27.584867	192.168.165.149	192.168.200.47	DNP 3.0 from 60011 to 0, len=5, Reset of Remote Link
306	2016-07-25 10:45:27.605941	192.168.200.47	192.168.165.149	DNP 3.0 from 0 to 60011, len=5, ACK
308	2016-07-25 10:45:52.093681	192.168.200.47	192.168.165.149	DNP 3.0 from 0 to 60011, Read, Class 1
310	2016-07-25 10:45:53.636688	192.168.165.149	192.168.200.47	DNP 3.0 from 60011 to 0, len=5, Reset of Remote Link
312	2016-07-25 10:45:53.837272	192.168.200.47	192.168.165.149	DNP 3.0 from 0 to 60011, len=5, ACK
313	2016-07-25 10:45:55.482995	192.168.165.149	192.168.200.47	DNP 3.0 from 60011 to 0, len=255, User Data, TL fragment 11
314	2016-07-25 10:45:55.497864	192.168.200.47	192.168.165.149	DNP 3.0 from 0 to 60011, len=5, ACK
316	2016-07-25 10:45:59.011540	192.168.165.149	192.168.200.47	DNP 3.0 from 60011 to 0, Unsolicited Response
317	2016-07-25 10:45:59.030873	192.168.200.47	192.168.165.149	DNP 3.0 from 0 to 60011, len=5, ACK
319	2016-07-25 10:45:59.455045	192.168.200.47	192.168.165.149	DNP 3.0 from 0 to 60011, Confirmfrom 0 to 60011, Read, Class 2
321	2016-07-25 10:46:01.636291	192.168.165.149	192.168.200.47	DNP 3.0 from 60011 to 0, len=255, User Data, TL fragment 13
322	2016-07-25 10:46:03.832993	192.168.200.47	192.168.165.149	DNP 3.0 from 0 to 60011, len=5, ACK
324	2016-07-25 10:46:04.512962	192.168.165.149	192.168.200.47	DNP 3.0 from 60011 to 0, Response
325	2016-07-25 10:46:04.520925	192.168.200.47	192.168.165.149	DNP 3.0 from 0 to 60011, len=5, ACK
327	2016-07-25 10:46:04.997484	192.168.200.47	192.168.165.149	DNP 3.0 from 0 to 60011, Confirm

Protocol	Details
DNP 3.0	from 60011 to 0, Responsefrom 60011 to 0, len=255, User Data, TL fragment 10
DNP 3.0	from 0 to 60011, len=5, ACK
DNP 3.0	from 60011 to 0, len=5, Reset of Remote Link
DNP 3.0	from 0 to 60011, len=5, ACK
DNP 3.0	from 0 to 60011, Read, Class 1
DNP 3.0	from 60011 to 0, len=5, Reset of Remote Link
DNP 3.0	from 0 to 60011, len=5, ACK
DNP 3.0	from 60011 to 0, len=255, User Data, TL fragment 11
DNP 3.0	from 0 to 60011, len=5, ACK
DNP 3.0	from 60011 to 0, Unsolicited Response
DNP 3.0	from 0 to 60011, len=5, ACK
DNP 3.0	from 0 to 60011, Confirmfrom 0 to 60011, Read, Class 2
DNP 3.0	from 60011 to 0, len=255, User Data, TL fragment 13
DNP 3.0	from 0 to 60011, len=5, ACK

Figure 20: Wireshark captured of data fragmented from remote device via P25 RMU

### **7.1.2 Communications Failed alarm**

It had been consistent on all of the Wireshark captures and on SCADA master station alarms records for the ACR under test that a 'Communications Failed' alarm occurred at the same time on hourly basis. This was identified on the NLR (P25 network location register) that Subscriber Unit (SU) registration duration is 3600 seconds and needed to be re-registered once expired. This is a feature that Ergon Energy P25 Network uses to manage its mobile Subscriber Units (SU) when moving to different regions on the P25 Network. The Wireshark captured on Figure 21, TEST ACR on SCADA Event historical alarm database on Figure 22 and NRL registration Expire duration for TEST RMU\_ACR on Figure 23.

The hourly communications link failure of a P25 RMU would greatly affected the severity level 2 of performance which outlined on section 4.5. Hence will make the P25 RMU unattractive alternative to provide communications for ACRs. To overcome the hourly registration which had caused most of the communications dropped outs, the P25 Network will required smarts written into the NLR and the RNC operation software that can identified the P25 RMU as fixed SU(s) and do not have the requirement of the mobile SU(s). It is also can be suggested that a pre-set list of IDs allocated on the NLR to be used for P25 RMU(s) without expired time function.

On the current P25 Network with the NLR and the RNC (RFSS Network Controller) are inter-related and the RNC controls the registration process and it does not have a dedicated setting for single SU. The registration duration is a global setting which affects every Subscriber Units on the network. It is not a simple fix to make the registration duration on the P25 network available for editing as the change must be made at system operation software level. Currently Auria-Wireless does not a service/maintenance contract with Ergon Energy to do software changes.

15	2016-07-25 12:45:09.272041	192.168.200.47	192.168.165.149	DNP 3.0	from 0 to 60011, len=5, Reset of Remote Link
16	2016-07-25 12:45:10.562040	192.168.165.149	192.168.200.47	DNP 3.0	from 60011 to 0, len=5, ACK
17	2016-07-25 12:45:10.759057	192.168.200.47	192.168.165.149	TCP	62670 → dnp [ACK] Seq=41 Ack=41 Win=64957 Len=0
18	2016-07-25 12:45:13.640461	192.168.165.149	192.168.200.47	TCP	dnp → 62670 [RST, ACK] Seq=41 Ack=41 Win=2144 Len=0
19	2016-07-25 12:45:15.736241	192.168.200.47	192.168.165.149	TCP	50699 → dnp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
20	2016-07-25 12:45:18.745973	192.168.200.47	192.168.165.149	TCP	[TCP Retransmission] 50699 → dnp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
21	2016-07-25 12:45:20.830955	192.168.165.149	192.168.200.47	TCP	dnp → 50699 [SYN, ACK] Seq=0 Ack=1 Win=2144 Len=0 MSS=536
22	2016-07-25 12:45:20.830976	192.168.200.47	192.168.165.149	TCP	50699 → dnp [ACK] Seq=1 Ack=1 Win=65392 Len=0
23	2016-07-25 12:45:23.512084	192.168.165.149	192.168.200.47	TCP	dnp → 50699 [RST, ACK] Seq=1 Ack=1 Win=2144 Len=0
24	2016-07-25 12:45:25.610852	192.168.200.47	192.168.165.149	TCP	50710 → dnp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
25	2016-07-25 12:45:26.055255	192.168.165.149	192.168.200.47	TCP	dnp → 50710 [SYN, ACK] Seq=0 Ack=1 Win=2144 Len=0 MSS=536
26	2016-07-25 12:45:26.055273	192.168.200.47	192.168.165.149	TCP	50710 → dnp [ACK] Seq=1 Ack=1 Win=65392 Len=0
27	2016-07-25 12:54:46.866365	192.168.200.47	192.168.165.149	DNP 3.0	from 0 to 60011, Write, Time and Date
28	2016-07-25 12:54:48.192389	192.168.200.47	192.168.165.149	TCP	[TCP Retransmission] 50710 → dnp [PSH, ACK] Seq=1 Ack=1 Win=65392 Len=25
29	2016-07-25 12:54:50.844310	192.168.200.47	192.168.165.149	TCP	[TCP Retransmission] 50710 → dnp [PSH, ACK] Seq=1 Ack=1 Win=65392 Len=25
30	2016-07-25 12:54:56.132484	192.168.200.47	192.168.165.149	TCP	[TCP Retransmission] 50710 → dnp [PSH, ACK] Seq=1 Ack=1 Win=65392 Len=25
31	2016-07-25 12:55:06.693468	192.168.200.47	192.168.165.149	TCP	[TCP Retransmission] 50710 → dnp [PSH, ACK] Seq=1 Ack=1 Win=65392 Len=25
32	2016-07-25 12:55:27.815192	192.168.200.47	192.168.165.149	TCP	[TCP Retransmission] 50710 → dnp [PSH, ACK] Seq=1 Ack=1 Win=65392 Len=65
33	2016-07-25 12:56:10.058794	192.168.200.47	192.168.165.149	TCP	50710 → dnp [RST, ACK] Seq=66 Ack=1 Win=0 Len=0
34	2016-07-25 12:56:12.150337	192.168.200.47	192.168.165.149	TCP	51421 → dnp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
35	2016-07-25 12:56:12.872258	192.168.165.149	192.168.200.47	TCP	dnp → 51421 [SYN, ACK] Seq=0 Ack=1 Win=2144 Len=0 MSS=536
75	2016-07-25 13:46:38.683258	192.168.165.149	192.168.200.47	DNP 3.0	from 60011 to 0, len=5, ACK
76	2016-07-25 13:46:38.900750	192.168.200.47	192.168.165.149	TCP	51421 → dnp [ACK] Seq=139 Ack=381 Win=65012 Len=0
77	2016-07-25 13:46:42.559167	192.168.165.149	192.168.200.47	TCP	dnp → 51421 [RST, ACK] Seq=381 Ack=139 Win=2144 Len=0
78	2016-07-25 13:46:44.658041	192.168.200.47	192.168.165.149	TCP	55920 → dnp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
79	2016-07-25 13:46:47.667629	192.168.200.47	192.168.165.149	TCP	[TCP Retransmission] 55920 → dnp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
80	2016-07-25 13:46:49.747213	192.168.165.149	192.168.200.47	TCP	dnp → 55920 [SYN, ACK] Seq=0 Ack=1 Win=2144 Len=0 MSS=536
81	2016-07-25 13:46:49.747227	192.168.200.47	192.168.165.149	TCP	55920 → dnp [RST] Seq=1 Win=0 Len=0
82	2016-07-25 13:46:51.771367	192.168.200.47	192.168.165.149	TCP	55927 → dnp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
83	2016-07-25 13:46:53.888380	192.168.165.149	192.168.200.47	TCP	dnp → 55927 [SYN, ACK] Seq=0 Ack=1 Win=2144 Len=0 MSS=536
84	2016-07-25 13:46:53.888403	192.168.200.47	192.168.165.149	TCP	55927 → dnp [ACK] Seq=1 Ack=1 Win=65392 Len=0
85	2016-07-25 13:56:13.947309	192.168.200.47	192.168.165.149	DNP 3.0	from 0 to 60011, Write, Time and Date
86	2016-07-25 13:56:20.311884	192.168.200.47	192.168.165.149	TCP	[TCP Retransmission] 55927 → dnp [PSH, ACK] Seq=1 Ack=1 Win=65392 Len=25
87	2016-07-25 13:56:33.041209	192.168.200.47	192.168.165.149	TCP	[TCP Retransmission] 55927 → dnp [PSH, ACK] Seq=1 Ack=1 Win=65392 Len=25
88	2016-07-25 13:56:58.484097	192.168.200.47	192.168.165.149	TCP	[TCP Retransmission] 55927 → dnp [PSH, ACK] Seq=1 Ack=1 Win=65392 Len=65
89	2016-07-25 13:57:49.369782	192.168.200.47	192.168.165.149	TCP	[TCP Retransmission] 55927 → dnp [PSH, ACK] Seq=1 Ack=1 Win=65392 Len=65
90	2016-07-25 13:58:49.381376	192.168.200.47	192.168.165.149	TCP	[TCP Retransmission] 55927 → dnp [PSH, ACK] Seq=1 Ack=1 Win=65392 Len=65
91	2016-07-25 13:59:49.392780	192.168.200.47	192.168.165.149	TCP	55927 → dnp [RST, ACK] Seq=66 Ack=1 Win=0 Len=0
92	2016-07-25 13:59:51.484349	192.168.200.47	192.168.165.149	TCP	56767 → dnp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
93	2016-07-25 13:59:51.923019	192.168.165.149	192.168.200.47	TCP	dnp → 56767 [SYN, ACK] Seq=0 Ack=1 Win=2144 Len=0 MSS=536

Figure 21: Wireshark captured of hourly TCP Retransmission

Event List			
TEST ACR			
26/Jul/2016 13:59:51	TEST ACR	ACR TST1/Comms Failed Alm	OFF
26/Jul/2016 13:46:49	TEST ACR	ACR TST1/Comms Failed Alm	ON
26/Jul/2016 12:56:12	TEST ACR	ACR TST1/Comms Failed Alm	OFF
26/Jul/2016 12:45:13	TEST ACR	ACR TST1/Comms Failed Alm	ON
26/Jul/2016 11:54:42	TEST ACR	ACR TST1/Comms Failed Alm	OFF
26/Jul/2016 11:46:28	TEST ACR	ACR TST1/Comms Failed Alm	ON
26/Jul/2016 10:44:22	TEST ACR	ACR TST1/Comms Failed Alm	OFF
26/Jul/2016 10:43:59	TEST ACR	ACR TST1/Comms Failed Alm	ON

Figure 22: Event List of TEST ACR communications failed.


Alias	Status	Visitor	Location	Location Alias	Expires
  	  	  	  	  	  
<input type="text"/>	(any) 	<input type="radio"/> y <input type="radio"/> n	<input type="text"/>	(any) 	<input type="text"/>
TEST RMU_ACR	Registered	no	00001.06.6EE.8B9CE.p25dr	Gabbinbar 	3600

Figure 23: TEST RMU\_ACR Expire duration 3600 seconds.

### 7.1.3 P25 Channel control Issue

The P25 Channel Control at Gabbinbar P25 base station found to be not working as it should. After the testbed P25 RMU registered on the NLR via Gabbinbar, the BSC at Gabbinbar had been accessed via web browser using <https://acuity/> to monitor testbed traffic. With the testbed P25 RMU occupied a P25 Channel by using a continuous ping (192.168.165.149) to P25 RMU from the PC, the P25 RMU occupied data was dropped traffic channel when a P25 Voice radio (SU) keyed or pressed to talk (PTT) while two available P25 traffic channels were indicated in idle mode. It was expected that the P25 Voice takes precedence over data (P25 RMU) traffic, however data traffic (P25 RMU) should not be dropped when unoccupied channels were idle. That is, one of the free P25 channels should have taken up the P25 Voice traffic when it was keyed and allow the P25 RMU to stay connected. This test was repeated on numerous times and the problem kept repeating.

It is suggested that the problem may have caused by a glitch on the BSC running software or firmware that may requires updated. This is issue had been raised with Auria-Wireless to confirm if this is an isolated case at Gabbinbar P25 Base station and rectify where necessary.

#### **7.1.4 P25 RMU locked onto a weak adjacent Land Mobile Base**

As standard requirement the P25 radio network had been purposely designed with some overlaps to provide reliable coverage and depended where the P25 RMU situated on the network. If the P25 RMU on the border line of the adjacent base when the local P25 Land Mobile Base channels are fully occupied, the RMU had locked onto a marginally adjacent P25 base and stayed registered to the weak (overlapped) base until the registration period expired. Of course this can caused the communications failed alarm raised due too many retries a result from high noise on a weak RF signal or poor signal to noise ratio conditions. This issue can be overcome by allowing the P25 RMU access to a local P25 base with good RSSI level only and restricting from all other land mobile bases on the P25 network.

The above finding supported by the evidence experienced during testings of the P25 RMU testbed with higher frequency of communications failed alarms raised on SCADA master station when the RMU had been locked onto Mount Perseverance where the RSSI levels between -97 to -101 dBm refer section 7.3 for RMU location.

## **7.2 P25 RMU RS232 Engineering Access (WSOS) testing**

The P25 RMU RS232 serial port 2 had been used to test the testbed ACR Engineering Access using WSOS (Windows Switchgear Operating System). One of the methods to communicate with the ACR was by using RS232 Direct connection. This is achieved by the used of COM Port data emulator software which emulates a device connected through a serial RS232 (COM) over TCP/IP Ethernet port. The Serial-IP is COM Port redirector software that had been used for the testing of the testbed WSOS. An example of Serial-IP of COM Port 2 as shown on Figure 24 had been set up to redirect serial over TCP/IP for communication with the testbed ACR.

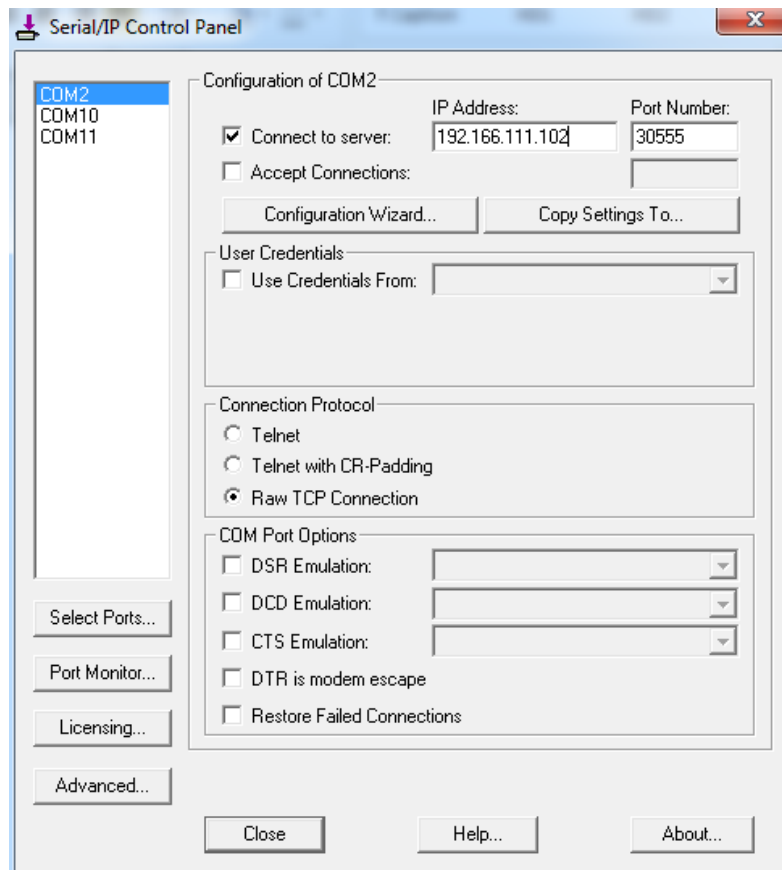



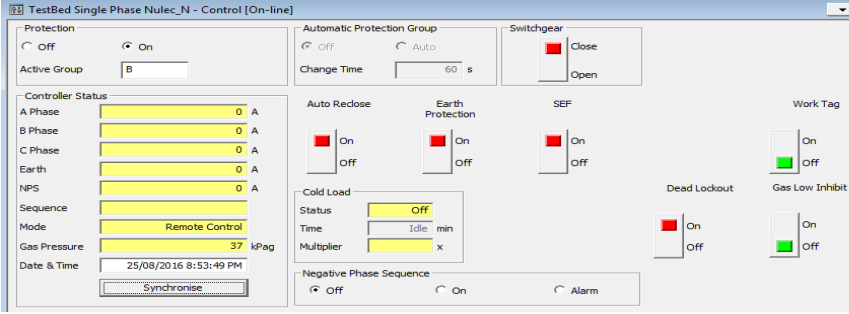

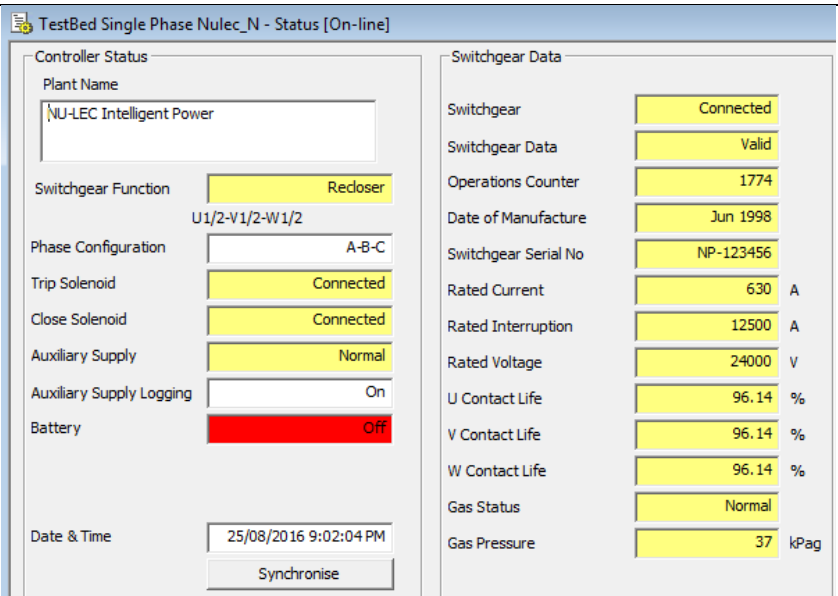
Figure 24: Serial-IP RS232 COM Port Emulator configuration.

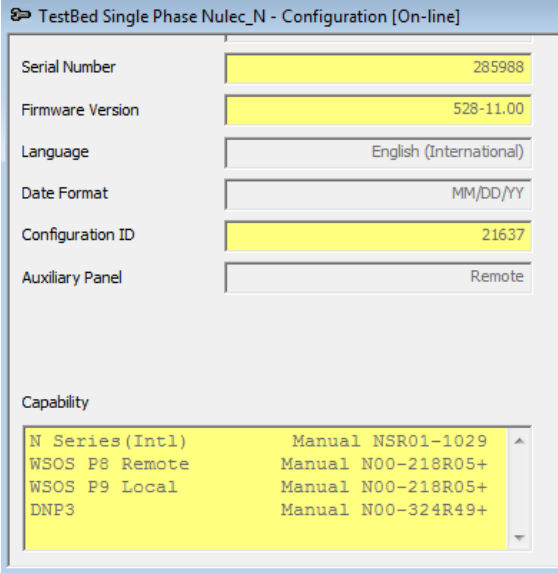
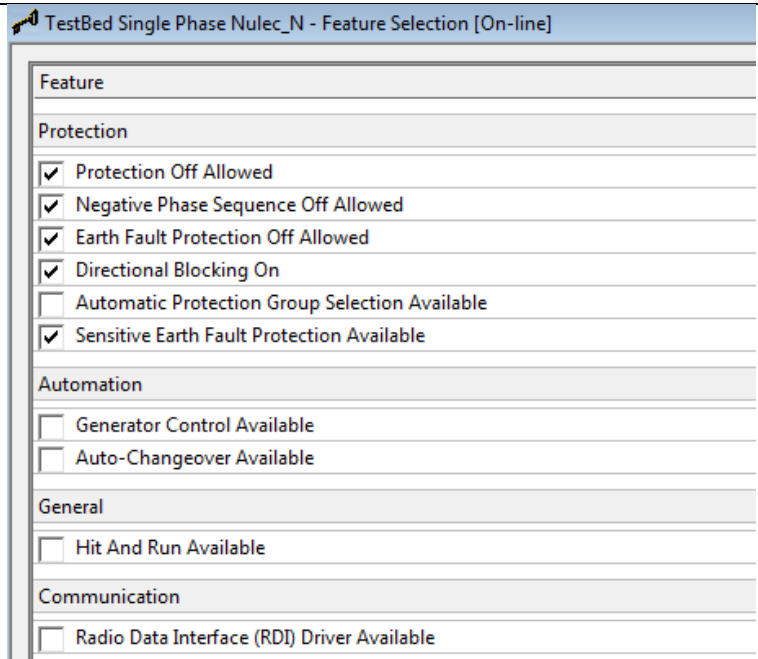
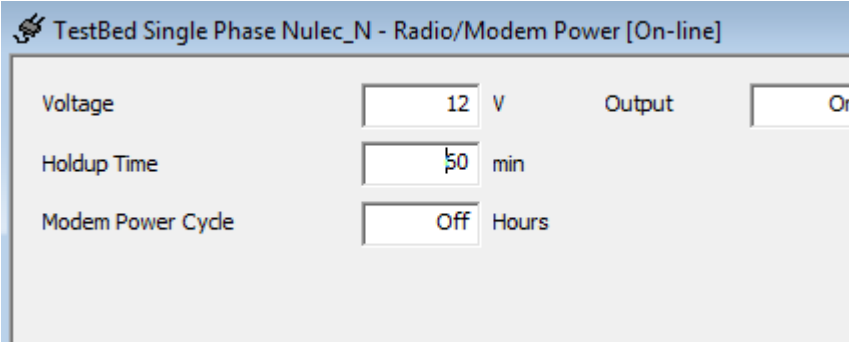
Communications with ACR using WSOS setup is as shown on Figure 25 and the successful WSOS connection to testbed as can be seen on Figure 26.

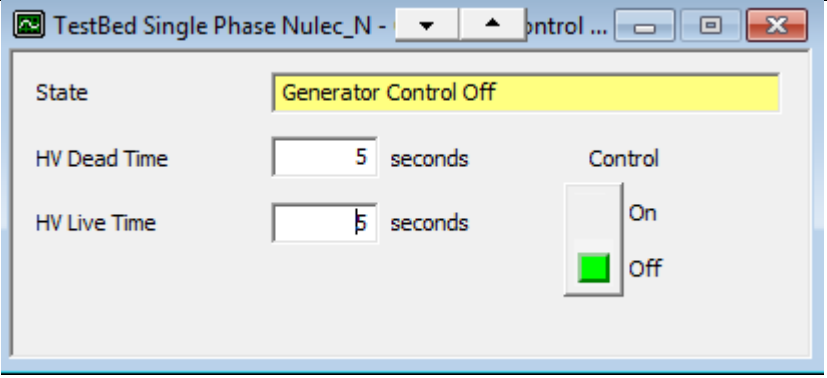
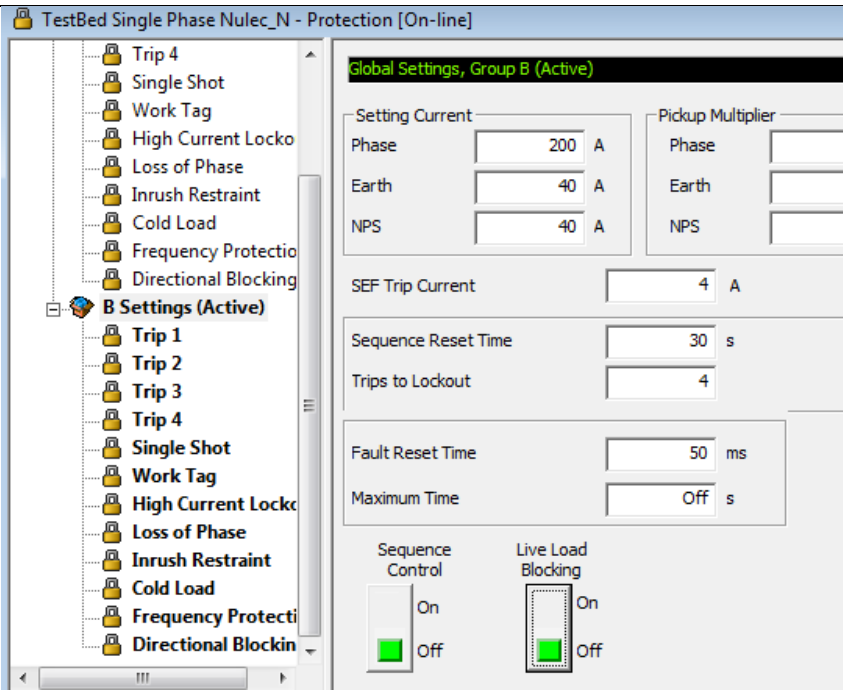
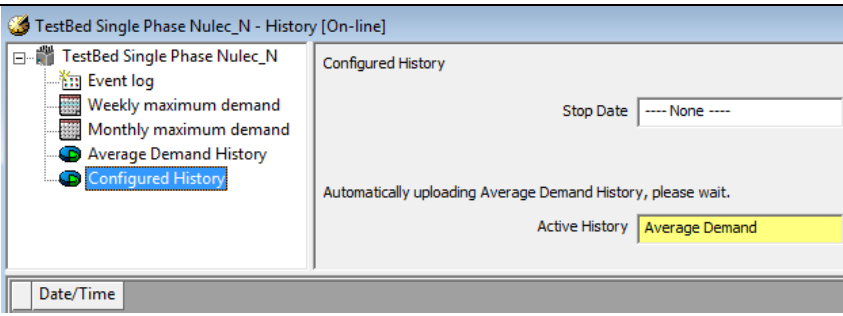



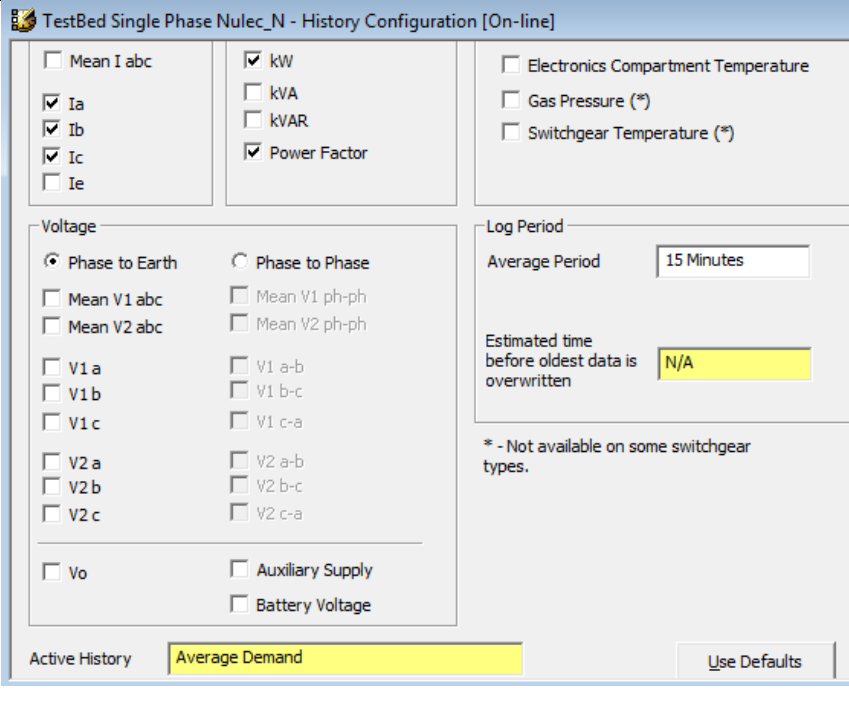

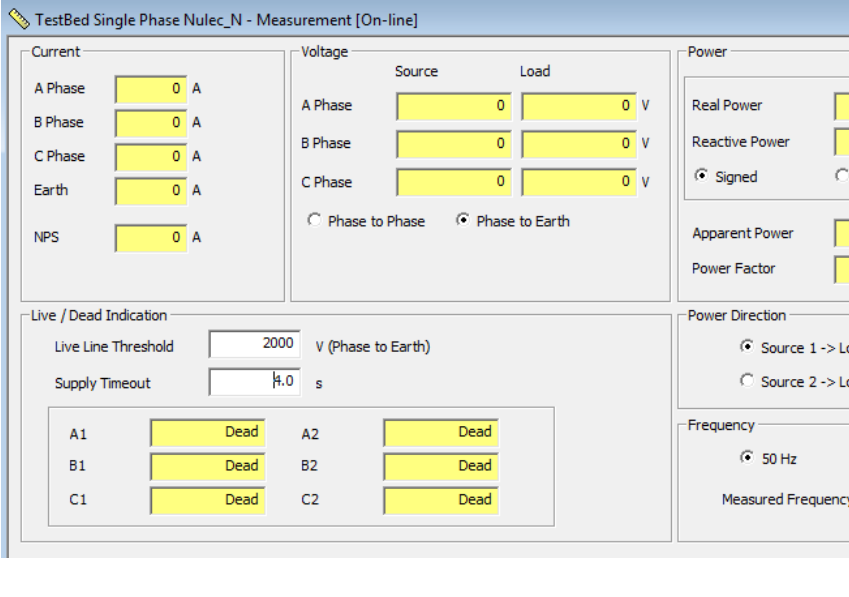

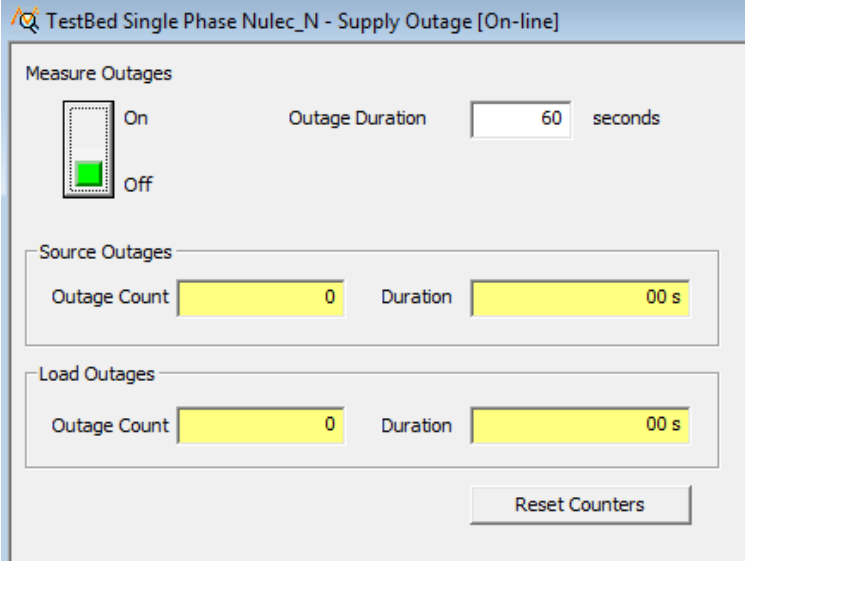
The Engineering Access on the testbed performance had been tested on all of the functions that are available on the ACR using WSOS. The tests results are tabulate for presentation purposes as shown in Table 14 with each functional setting and respective screen capture:





Table 14: Testbed ACR remote engineering access via WSOS features.

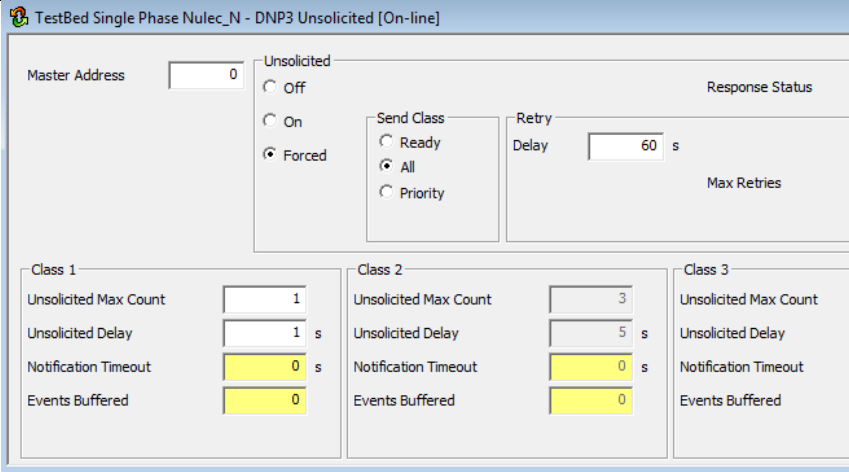
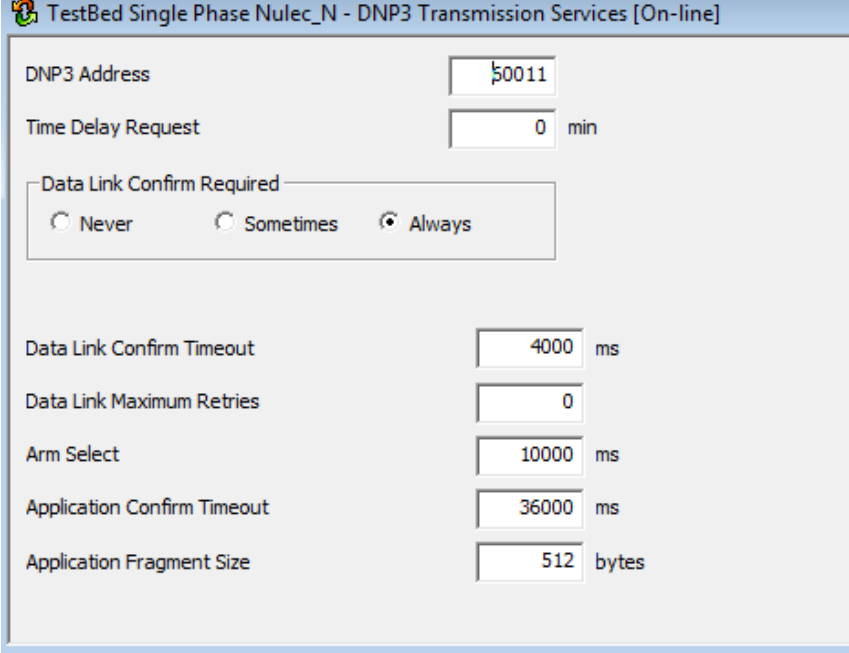
Functions	Screen Captured of function displayed Windows
 <b>Control</b>  ACR's Controls had been proved to be successful.	 <p>The screenshot shows the 'Control' window for 'TestBed Single Phase Nulec_N'. It includes sections for Protection (On/Off), Automatic Protection Group (Auto/Off), Switchgear (Close/Open), Controller Status (A, B, C Phases, Earth, NPS, Sequence, Mode, Gas Pressure, Date &amp; Time), Auto Reclose (On/Off), Earth Protection (On/Off), SEP (On/Off), Work Tag (On/Off), Dead Lockout (On/Off), Gas Low Inhibit (On/Off), Cold Load (Status, Time, Multiplier), and Negative Phase Sequence (On/Off/Alarm).</p>
 <b>Status</b>  Remote access to ACR's Status worked.	 <p>The screenshot shows the 'Status' window for 'TestBed Single Phase Nulec_N'. It includes sections for Controller Status (Plant Name: NU-LEC Intelligent Power, Switchgear Function: Redcloser, U1/2-V1/2-W1/2, Phase Configuration: A-B-C, Trip Solenoid: Connected, Close Solenoid: Connected, Auxiliary Supply: Normal, Auxiliary Supply Logging: On, Battery: Off, Date &amp; Time: 25/08/2016 9:02:04 PM) and Switchgear Data (Switchgear: Connected, Switchgear Data: Valid, Operations Counter: 1774, Date of Manufacture: Jun 1998, Switchgear Serial No: NP-123456, Rated Current: 630 A, Rated Interruption: 12500 A, Rated Voltage: 24000 V, U Contact Life: 96.14 %, V Contact Life: 96.14 %, W Contact Life: 96.14 %, Gas Status: Normal, Gas Pressure: 37 kPag).</p>

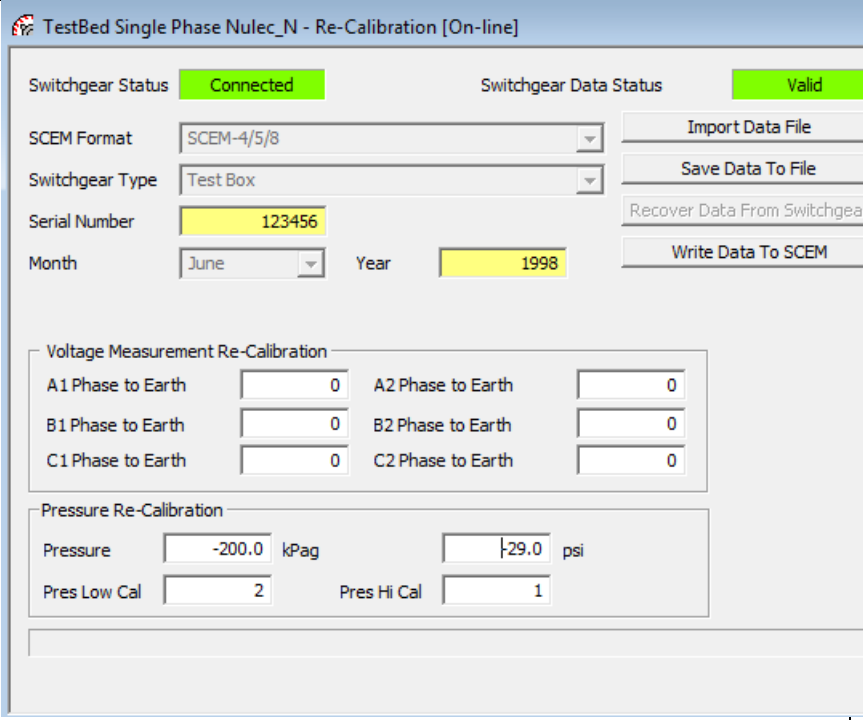

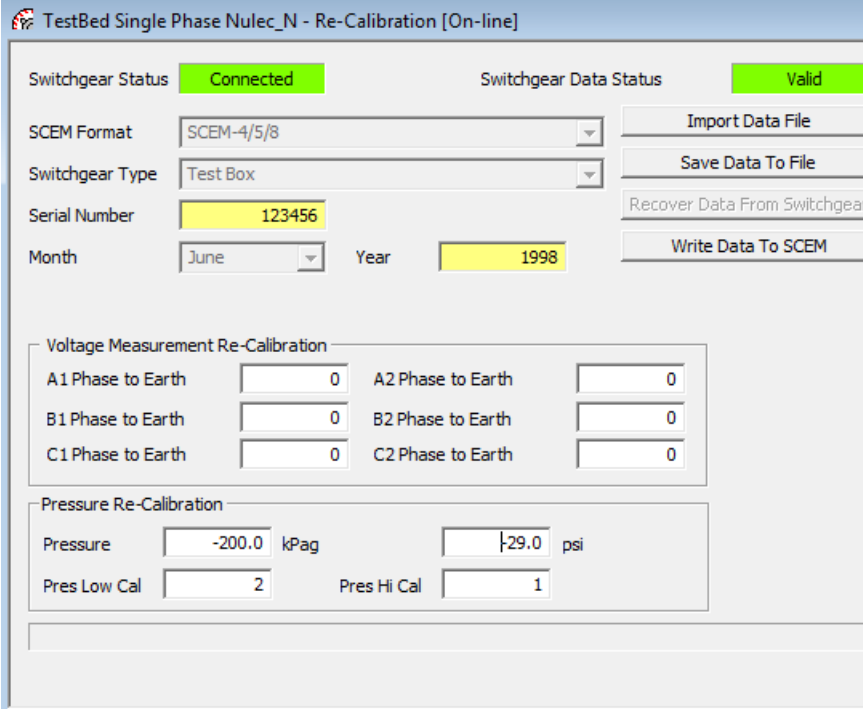
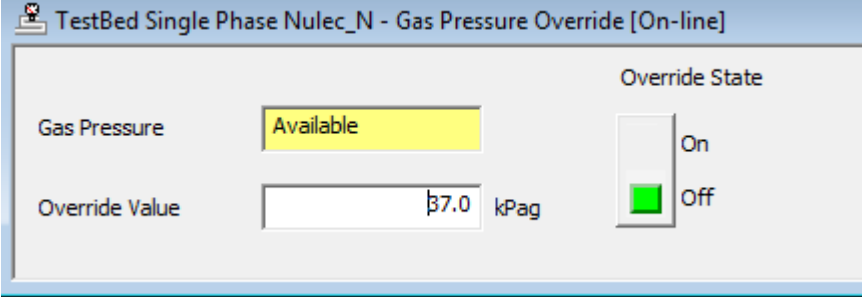
<p>Configuration of the testbed ACR had been successful accessed remotely.</p>	
<p>Configuration Feature Selection of testbed ACR had been successful accessed remotely.</p>	
<p>The Radio/Modem power management remote controlled worked.</p>	

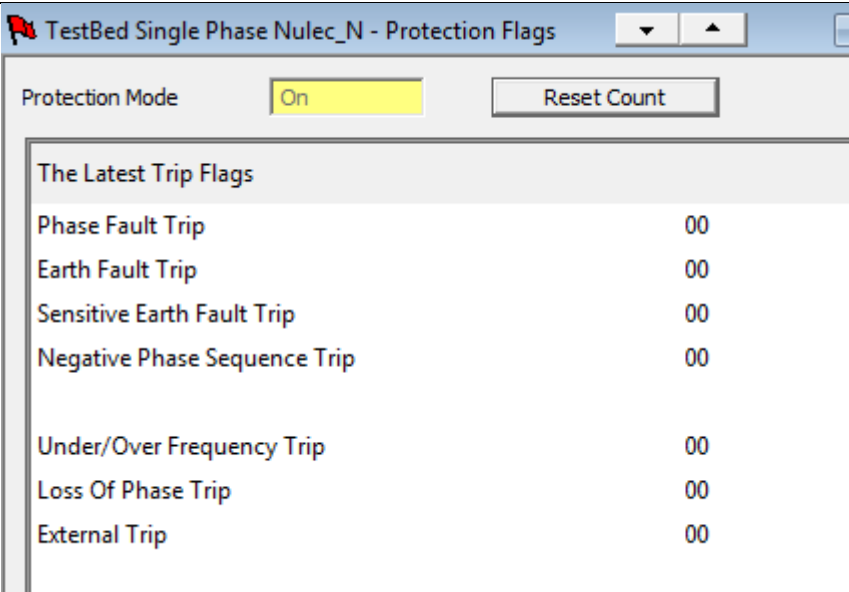
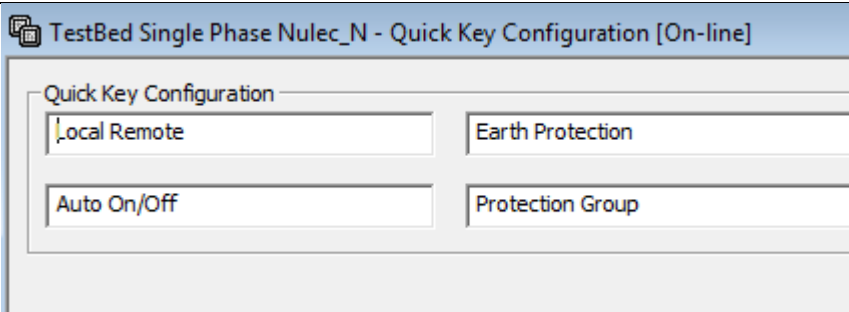
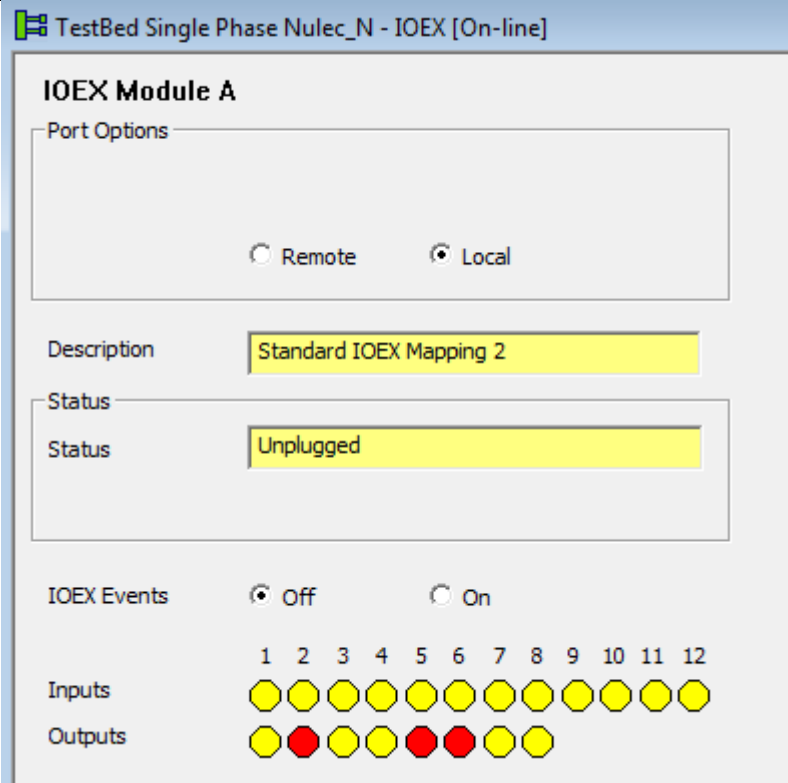
<p>Generator Control of testbed ACR was accessible.</p>	
<p><b>Protection</b></p> <p>The remote control of all Protection settings of the testbed ACR had been proved to be successful.</p>	
<p><b>History</b></p> <p>History Display features had been successful accessed.</p>	

<p> <b>History</b></p> <p>Configuration History was proved to be successfully accessed remotely.</p>	
<p> <b>Measurement</b></p> <p>Measurement of the ACR's live parameters can be accessed fine.</p>	
<p> <b>Supply Outage</b></p> <p>Provide access to the ACR's power quality 'Supply Outage' had proved to be working.</p>	

<p> <b>Communications</b></p> <p>Remote accessed to the ACR's WSOS Direct setting had shown to be working.</p>	<p> <b>TestBed Single Phase Nulec_N - Direct [On-line]</b></p> <p>Baud Rate <input type="text" value="19200"/> Baud Rate Selection</p> <p>Mode <input type="radio"/> Local <input checked="" type="radio"/> Remote</p> <p><input type="checkbox"/> Available <input checked="" type="checkbox"/> Not Available</p>
<p>Remote accessed to testbed ACR's DNP3 Comms Configuration had shown to be working.</p>	<p> <b>TestBed Single Phase Nulec_N - DNP3 Communications Configuration [On-line]</b></p> <p>Switchgear Port <input type="text" value="P8 RS-232"/> First Character <input type="text" value="5"/></p> <p>Communications Status <b>Running</b> Last Character <input type="text" value="F"/></p> <p>Pre Transmission <input type="text" value="10"/> ms First Character Repeat <input type="text" value="1"/></p> <p>Post Transmission <input type="text" value="0"/> ms Collision Avoidance <input type="text" value="100"/></p> <p>Baud Rate <input type="text" value="9600"/> Transmission Delay <input type="text" value="1"/></p> <p>Dialling <input checked="" type="radio"/> Disabled <input type="radio"/> Enabled</p> <p>Dialup Phone Number <input type="text"/></p> <p>CTS <input checked="" type="radio"/> Ignore <input type="radio"/> Don't Ignore</p> <p>Preamble <input type="checkbox"/> Enabled Carrier Detect <input checked="" type="checkbox"/> Ignore</p>
<p>DNP3 Points Configuration had been tested and working.</p>	<p> <b>TestBed Single Phase Nulec_N - DNP3 Point Configuration [On-line]</b></p> <p>Phase Current</p> <p>Default Deadband <input type="text" value="500"/> A</p> <p>High Alarm <input type="text" value="999"/> A</p> <p>Low Alarm <input type="text" value="0"/> A</p> <p>Phase Voltage</p> <p>Default Deadband <input type="text" value="600"/> V</p> <p>High Alarm <input type="text" value="38000"/> V</p> <p>Low Alarm <input type="text" value="0"/> V</p> <p>Analog Size <input checked="" type="radio"/> 16 bit <input type="radio"/> 32 bit</p> <p>Analog Alarm <input checked="" type="radio"/> Off <input type="radio"/> Binary <input type="radio"/> Both</p> <p>Earth Current</p> <p>Default Deadband <input type="text" value="500"/> A</p> <p>High Alarm <input type="text" value="999"/> A</p> <p>Low Alarm <input type="text" value="0"/> A</p> <p>System Power</p> <p>Default Deadband <input type="text" value="250"/> W</p> <p>High Alarm <input type="text" value="54000"/> W</p> <p>Low Alarm <input type="text" value="0"/> W</p> <p>NPS Current</p> <p>Default Deadband <input type="text" value="500"/> A</p> <p>High Alarm <input type="text" value="999"/> A</p> <p>Low Alarm <input type="text" value="0"/> A</p> <p>Binary Time <input checked="" type="checkbox"/> On <input type="checkbox"/> Off</p> <p>Binary Outputs Status Reporting <input checked="" type="checkbox"/> On <input type="checkbox"/> Off</p> <p>Analog Time <input checked="" type="checkbox"/> On <input type="checkbox"/> Off</p> <p>Analog Flag <input type="checkbox"/> On <input checked="" type="checkbox"/> Off</p> <p>Point Mapping <input type="text" value="N Series PTCC Test Box"/> <input type="button" value="Configure M..."/></p>

<p>DNP3</p> <p>Unsolicited</p> <p>had been</p> <p>tested and</p> <p>working.</p>	 <p>The screenshot shows the configuration window for 'TestBed Single Phase Nulec_N - DNP3 Unsolicited [On-line]'. It includes a 'Master Address' field set to 0. The 'Unsolicited' section has radio buttons for 'Off', 'On', and 'Forced' (which is selected). There is a 'Send Class' section with radio buttons for 'Ready', 'All' (selected), and 'Priority'. A 'Retry' section shows a 'Delay' of 60 s and a 'Max Retries' field. Below these are three class-specific sections: 'Class 1', 'Class 2', and 'Class 3'. Each class section contains fields for 'Unsolicited Max Count', 'Unsolicited Delay', 'Notification Timeout', and 'Events Buffered'. For Class 1, the values are 1, 1 s, 0 s, and 0 respectively. For Class 2, the values are 3, 5 s, 0 s, and 0. For Class 3, the values are 3, 5 s, 0 s, and 0.</p>
<p>DNP3</p> <p>Transmission</p> <p>Services had</p> <p>been tested</p> <p>successful.</p>	 <p>The screenshot shows the configuration window for 'TestBed Single Phase Nulec_N - DNP3 Transmission Services [On-line]'. It includes a 'DNP3 Address' field set to 50011. A 'Time Delay Request' field is set to 0 min. The 'Data Link Confirm Required' section has radio buttons for 'Never', 'Sometimes', and 'Always' (which is selected). Below this are several fields for timeouts and retries: 'Data Link Confirm Timeout' (4000 ms), 'Data Link Maximum Retries' (0), 'Arm Select' (10000 ms), 'Application Confirm Timeout' (36000 ms), and 'Application Fragment Size' (512 bytes).</p>

<p>DNP3</p> <p>Transmission Services had been tested successful.</p>	
<p> <b>Maintenance</b></p> <p>Remote accessed to testbed ACR's Calibration was successful.</p>	
<p>Remote accessed to ACR's Gas Pressure Override had been</p>	


successful.	
<p>Remote accessed Testbed ACR's Protection Flags had been successful.</p>	
<p>Quick Key Configuration remote access had been successful.</p>	
<p>IOEX remote access also had been successful.</p>	

The communications failed that had been experienced on the P25 RMU port 1 by DNP3 SCADA with hourly forced re-registration found on section 7.1.2 also replicate on port 2 for WSOS engineering access.

There was clear evidence that communications failed due to overflow condition with WSOS direct COM2 that set too high (baud rate of 19200) this is due to packet size limitation on P25 network. With WSOS direct comms baud rate manually reduced to 300 on the testbed remote comms link had been operated consistent.

### **7.3 P25 RMU RF dynamically select**

The testbed setup was located on 477 South Street and geometrically it is closest to Gabbinbar P25 Base compared to Mount Perseverance and Mount Domville P25 Base. The test was to ensure that the P25 RMU hunts properly where it is expected to select the best signal out of the all numerous of signals presented.

The RSSI level to Gabbinbar, Mount Domville and Mount perseverance were measured by programming each the base operating frequencies onto the P25 RMU individually. Another approach to make the P25 RMU locks onto the preferred Land Mobile Base site by configuring location restrictions the Net Work Register (NLR) settings. This can be done by logging into the NLR, searched the appropriate subscriber unit select 'SUID 

Once the P25 registered onto a particular P25 base the RSSI level was recorded. The RSSI level can be measured by pressing the toggled switch at the front of the P25 RMU panel as described on section 3.1.3.

The RSSI level of the testbed P25 RMU when locked onto Gabbinbar was measured -70 to -74 dBm, to Mount Perseverance was -97 to -101 dBm and to Mount Domville was measured -88 to -91 dBm.

On earlier tests the testbed had been occasionally locked onto Mount Domville P25 Base Station or sometimes Mt Perseverance. After resetting of the BSC at Gabbinbar, Mount Domville and Mount Perseverance the P25 RMU had

consistently locked or registered onto Gabbinbar P25 Base Station every time when the unit was switched on. This had proved that the P25 RMU RF dynamic selection of the highest RF signal level and hunt properly as expected.

## **8.0 Recommendations**

The following recommendations are based on the P25 network and TCP requirements to ensure that the P25 RMU can be used as an alternative to a Cybertec NextG modem or M2M SabreRanger satellite modem on ACR.

### **8.1 P25 RMU TCP re-establishment requirement**

TCP connection failures with the P25 RMU are certain in situations where the P25 RMU cannot access to a traffic channel for an extended period due to heavy voice traffic, or due to power supply or hardware failure. It is recommended that the SCADA Master station should automatically attempt to re-establish the connection to minimise the loss of critical data.

Due to the nature of TCP communications there is the chance that after a P25 communication failure the SCADA Master station will be unaware of that the TCP connections with the P25 RMU are down. It is therefore recommended that the DNP3 TCP keep a live timer on the Master station set to an interval less than 3 hours as the P25 RMU will reset the connection after 4 hours.

### **8.2 P25 RMU TCP maximum segment size and reconnect timer**

To achieve maximum throughput, the Ergon Energy P25 network components are optimised for TCP maximum segment size (MSS) of 536 octets. This is the default size configured in the P25 RMU database and therefore should be negotiated by default during establishment connection between itself and the TCP client application. It is recommended that the TCP maximum segment size

should be set at 536 octets on both the SCADA Master station and the remote device (ACR).

Sufficient time should be given for clients to establish connection over the P25 network. Re-attempting connection establishment too early will introduce unnecessary loading on the P25 traffic channel and could restrict other data subscribers of the bandwidth on the channel. It is therefore suggested that the TCP clients should not retry connection establishment attempts at a rate faster than once every 30 seconds.

### **8.3 P25 RMU TCP packet size in WSOS**

Unnecessary loading on the P25 data channel can be avoided by combining multiple requests into a single message. It is therefore recommended that the WSOS communications TCP packet size to be set to 'Long' as shown in Figure 24.

### **8.4 P25 RMU DNP3 Data Link and Application Layer Confirmations**

The following recommendations apply to the DNP3 communications data link and application layer confirmations requirement.

#### **8.4.1 DNP3 Data Link Layer Frame Confirmations**

The reliability mechanisms such as acknowledge and retries are already being applied at the P25 CAI layer and TCP transport layer, therefore it is unnecessary to have DNP3 Link layer frame confirmations and it is recommended that the

SCADA Master station and remote stations (ACRs) to be configured with Data Link Layer confirmations disabled.

#### **8.4.2 DNP3 Application Layer confirmations and timeouts**

There should be sufficient time allowed for retries to complete at the TCP layer before retrying at the DNP3 Application Layer. If the timeout values are too short, the result may be premature retries which would introduce unnecessary loading on the P25 channel data traffic. It is therefore recommended that the DNP3 Application Layer Request timeouts should be set at a value of 30 seconds or more.

Critical data such as unsolicited responses should be confirmed at the DNP3 application layer and retries using timeout of no less than 30 seconds and retry count of greater than 3. It is suggested that the DNP3 Application Layer confirmations should be enabled for critical data.

### **8.5 P25 RMU ACR File transfers**

The following recommendations relate to file transfer applications on ACRs.

#### **8.5.1 ACR File transfer during Off-peak**

During large data transfers the site traffic will be placed under heavy load and there is a chance of interruption due to higher priority voice services. It is

therefore suggested that executing files transfers from the ACR via P25 RMU using WSOS application should be done during off-peak times.

### **8.5.2 ACR File transfer block size**

As previously mentioned the P25 network components are optimised with an MSS of 536 octets. Using a block size of 512 octets will avoid TCP or P25 CAI fragmentation and reduce the request-response latency through the P25 network. It is recommended that the file transfers from the P25 RMU use a block size of 512 octets or less.

## **8.6 P25 RMU TCP Timestamp Option**

Improvement of data throughput by reducing the number of TCP retransmissions is possible by enabling TCP timestamps which improve the accuracy and frequency of Round Trip Time (RTT) calculations in the TCP client. It is therefore recommended that TCP Timestamp option should be enabled on both SCADA Master Station and PCs running WSOS. The command is:

`“netsh int tcp set global timestamps=enabled”`

## **8.7 Unit Call Priority**

Any change on the priority on Unit/Group/PSTN calls through the NLR interface will have an effect on other voices and data services. It is recommended that all groups' priority should be set at a value of 5 in the NLR.

## **8.8 Voice and Data Traffic Hang Time**

The hang time is a mechanism that helps to guarantee that a channel is available for a group between each unit's transmissions. A voice hang time on a full traffic loaded system can lead to occupied but unused channels traffic. It is therefore recommended that hang time of all groups should set to zero in the NLR.

Due to the property of data channels there must be a hang time for send or receive applications. The 5 seconds hang time provides a compromise between keeping the channel open long enough to ensure that any application response of the data packet already has a channel ready and does not required to re-page the unit but short enough so that unused but occupied channels data traffic do not tie up these critical resources. It is therefore recommended that the hang time of data channels should be set to 5 seconds in the DSN.

## **8.9 Activity Threshold**

On the P25 base station the CAI is a full-duplex traffic channel, while the subscriber unit (SU) is half-duplex. There are time durations where a channel can be utilised by other units during a data transaction between a SU and the application server. This had has led to the allocation of multiple subscriber units to a traffic channel. This may result in units of different data types such as GPS, SCADA and WSOS all using the same channel. The activity threshold value will be determined the maximum number of data units can share a traffic channel. That is, a data unit request access will be given an existing traffic channel if the activity threshold value has not reached.

It is recommended that the activity threshold value of 3 should be set which is a compromise between ensuring enough subscriber units to share the channel such that they do not impact on each other excessively but is suitable to achieve a reasonable throughput.

## **8.10 GPS Update**

To prevent unnecessary loading on the traffic channel it is recommended that the periodic trigger for Tier2 GPS updates on subscriber unit no greater than once a minute.

## **8.11 SCADA master station Poll Frequency**

To reduce loading on the system traffic channel it is recommended that the SCADA master station polling frequency to be set to no greater than once an hour. Enabling faster updates will take up traffic channels which would increase the chance of communication failures during peak period due to voice calls having the priority over data traffic. The hourly polling frequency could overcome the communications failure found in section 7.1.2 caused by the RNC forced every subscriber units on the system to register hourly. That is, only if the SCADA master station polls the remote device just after the subscriber unit re-registration onto the P25 network period.

To ensure that all P25 RMUs on the network are re-registering at about the same time so they can expire at the same time after 3600 seconds, the ACR 12V DC supply to the P25 RMU can be programmed to recycle at 24:00 Hour.

## **8.12 P25 RMU Restricted to one Land Mobile Base**

To setup new device off the shelf such as the P25 RMU it had been always good practice to have a standard configuration template (file) for simplicity, especially for repetitive programming works over multiple units. Due to the possibility of

different people configuring the P25 RMU, the template reduces the chance of human errors for new programmers. It is recommended that the configuration template should contain all the operating frequencies of all Land Mobile Bases on the P25 network as well as any parameters requiring editing (as typically described on Table 10 of section 5.2.3).

The quality of data throughput on the P25 RMU is highly dependent on the quality or the good RF signal strength (RSSI) over the radio link path. On a weak signal strength, data packets will cause retries (re-sends) due errors introduced by noise. The chance of 'communications failed alarm' being raised is high when the retries were unsuccessful. During the fully loaded traffic channel or peak period traffic on the preferred P25 base, the P25 RMU will be locked and registered onto the weak overlapped P25 base and it will stays registered until 3600 seconds have expired, when the adjacent base traffic channel is available. This will result in a 'communication failed alarm' if the weak overlapped is too low due to too many retried packet.

To ensure that the P25 RMU will not lock or register onto a low RF signal on adjacent P25 base, the P25 RMU can restricted to other adjacent P25 bases and only enabled the preferred Land Mobile Base using the NLR configuration setting. This will prevent the unnecessary loading of channel traffic on adjacent P25 bases with high error data packets due to low RF signal quality.

The control of the subscriber unit registration onto Land Mobile Base(s) on the P25 network via the NLR is the preferred choice to manage devices on the network especially a great tool during faults trouble shooting.

### **8.13 Increase P25 Network Capacity**

The current P25 network capacity is restricted at the Land Mobile Base site where the system is working as the 1+3 operations. The ACMA licences are already secured and all other required hardware already available. To increase a

P25 Land Mobile Base site capacity to 1 + 5, the additional of a TB8100 Base Transceivers, a couple of C2-6 and PDI-2 as shown in Figure 8 for the cost of equivalent to three satellite modems is worth looking into.

With the two additional traffic channels it is recommended that two channels should be optimised for data traffic only. This will mean that Auria will be required to do configuration change to the P25 network. At the same time a request could be made to make the registration expired period on the NLR to be configurable to overcome the hourly 'communications failed' alarm raise in the SCADA master station.

## 9.0 Conclusions

It is to be noted that the tests performed were based on the testbed using a single P25 RMU with an ACR Test Box. Communications via the Remote Engineering Access with testing performed of all configuration settings on ACR via WSOS had proved to be working reliably when communications rate was set at 300 baud.

There were three major issues found on the SCADA port that had caused communications failed alarms raised on the SCADA master station, two that can be rectified via configuration settings that are currently available and one that will require global changes on the P25 system operations at the software level as follows.

1. Data fragmentation – as a result of bench marking the NextG communications application it had been found that the TCP maximum segment size on the ACR Test Box was set at 2048 octets and the P25 components are optimised at 536 octets. Setting the ACR Test Box to 512 octets had rectified the issue.
2. Communications link failed on weak RF signal – the P25 RMU had locked onto an adjacent P25 base when all of the traffic channels on the designated local base were fully occupied. Under a weak RF signal or bad signal to noise ratio conditions, the high rate of data retransmissions resulted in a ‘communications failed’ alarm raised on the SCADA master station. Under this condition the P25 RMU had taken up valuable P25 traffic resources with no actual benefits. When a P25 RMU is registered onto the P25 network, the system will maintain communications to the RMU via the same base until the 3600 seconds registration time expired. To prevent the P25 RMU from locking onto an adjacent P25 base it is recommended that the RMU to be restricted from all other bases on the network and allow communications to a predesignated base only.

3. Communications link failed on an hourly basis – it had been found that the ACR test port on the SCADA master station for the testbed had ‘Communications Failed’ alarm raised on an hourly basis. Investigations found that the NLR (P25 network location register) had a registration period of 3600 seconds on every Subscriber Units (SU) and needed to be re-registered once expired. This is a feature that Ergon Energy P25 Network uses to manage its mobile Subscriber Units (SU) when moving to different regions on the P25 Network.

To overcome the hourly registration which had caused most of the communications dropped outs, the P25 Network will required additional settings to be written into the NLR and the RNC operation software, to differentiate between static and mobile subscriber unit. It is also suggested that a pre-set list of IDs allocated on the NLR to be used for P25 RMU(s) without expired time function.

On the current P25 Network, the NLR and the RNC (RFSS Network Controller) are inter-related and the RNC controls the registration process and it does not have a dedicated setting for single SU. The registration duration is a global setting which affects every Subscriber Unit on the network. It is not a simple fix to make the registration duration on the P25 network available for editing as the change must be made at system operation software level. Currently Auria-Wireless does not a service/maintenance contract with Ergon Energy to do software changes.

Due to limited data traffic channel available on the P25 network it is recommended that P25 RMU to be used at ACR sites with only satellite communications available. It is recommended that up to three P25 RMU subscriber units are used for each P25 traffic channel. That is, up to nine RMU to be connected to a 1+3 Land Mobile Base site.

It is the preferred choice if the P25 RMU registration period can be changed on the NLR. However, the P25 RMU can be used on the current P25 network with special alarm monitor delay taken in consideration when a P25 RMU is used on an ACR. That is, if ‘Communications Failed’ on a device stays up for more than say two hours then the alarm display can show an active on the ‘CNOc Alarms

Panel'. This will stop the alarms flooding caused by hourly forced registration of the P25 RMU. It is to be noted that the SCADA master station cleared the 'Communications Failed' alarm when communications link had been restored (following a successful 'Reset of Remote Link' from a remote device).

As previously mentioned the tests had been performed using a single P25 RMU unit with acceptable outcomes. Further tests with using multiple RMUs sharing the same data traffic channel application will be required prior to rolling out the ACR communications strategy using P25 RMU. This will just be a confirmation test for proof of concept which will be set up and run over a week.

Based on the research and testing undertaken using the Auria Wireless ES1105-V, P25 RMU had shown that it is operationally stabled. Due to its cost saving advantage with no network access cost, the P25 RMU would make a very attractive alternative compared to the use of M2M satellite modem which has network access cost of \$8 per Megabyte of data. That is, the saving cost on network access alone for one satellite modem with an estimated figure of 300 Megabyte/month would be \$28,800 annually.

A document has been prepared for Ergon Energy summarising the project risk in using the P25 RMU. It is included in Appendix G to aid Ergon Energy Operational Managers as a tool for evaluating whether to use the P25 RMU.

## List of references

Project 25 Documents & Standards, 2010, *Public Safety Communications Research*, viewed 18 November 2015

[http://www.qsl.net/kb9mwr/projects/dv/apco25/P25\\_Standards.pdf](http://www.qsl.net/kb9mwr/projects/dv/apco25/P25_Standards.pdf)

Daniel Electronics, TG-001 P25 Radio Systems, *P25 Radio Systems Training Guide*, viewed 17 November 2015, P25 Interface Standards (page 17).

Daniel Electronics, TG-001 P25 Radio Systems, *P25 Radio Systems Training Guide*, viewed 17 November 2015, P25 Interface Standards (page 5).

[http://www.dvsinc.com/papers/p25\\_training\\_guide.pdf](http://www.dvsinc.com/papers/p25_training_guide.pdf)

Motorola Inc, 2009 (WHITE PAPER, Project 25 Standard)

Electronic Industries Alliance (TIA Document, P25 Data Overview TIA-102-BEEA-A)

Electronic Industries Alliance (TIA Standard, P25 Packet Data TIA-102-BAEB-A)

AIRWAVE, *Airwave Solutions P25 Rack Training*, August 2012 (page 3).

TIA Standard, TIA-102.BACF 2009. *Project 25 Inter-RF Subsystem Interface (ISSI) Messages and Procedures for Packet Data Services*.

Practical DNP3, *IEC 60870.5 & Modern SCADA Communication Systems*.

Bird Technologies Group TX RX SYSTEMS, *BA Series VHF Omnidirectional Dipole Arrays 136 – 174 MHz*, viewed 18 November 2015.

[http://btgmotorola.securespsites.com/Shared%20Documents/US39223-6\\_ba-series\\_vhf.pdf](http://btgmotorola.securespsites.com/Shared%20Documents/US39223-6_ba-series_vhf.pdf)

Electricity Act, Queensland, 1994, viewed on 25 October 2014.

< <https://www.legislation.qld.gov.au/LEGISLTN/CURRENT/E/ElectricA94.pdf> >

National Electricity Rules, Version 65, viewed on 25 October 2014.

< <http://www.aemc.gov.au/Energy-Rules/National-electricity-rules/Current-Rules> >

Australian Standard, AS61508.1 Second edition 2011. *Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1: General requirements*, viewed 24 February 2016.

Australian Standard, AS61508.3, Second edition 2011. *Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 3: Software requirements*, viewed 25 January 2016.

<<https://www.legislation.qld.gov.au/LEGISLTN/CURRENT/E/ElectricR06.pdf>>

# **Appendix A: Project Specification**

## **Topic:**

Automatic Circuit Recloser (ACR) Communications Using P25 RMU (Radio Modem Unit)

## **Supervisor:**

Catherine Hills

## **Project Aim:**

The purpose of this project is to evaluate the suitability of the P25 Radio Modem Unit (RMU) over Ergon Energy P25 Radio Network for communications to Automatic Circuit Reclosers (ACRs). The RMUs provide two local serial connections, one for DNP3 access by Supervisory Control and Data Acquisition (SCADA) systems, and the second for engineering access for remote management of Automatic Circuit Recloser (ACR) settings.

A previous attempt has been made to utilise the P25 system which was unsuccessful and so was discontinued. The use of the low frequency P25 network remains an attractive alternative to NextG and Satellite connections. This project aims to assess the capabilities of the P25 devices in the context of Ergon Energy's operational requirements through both research and practical experimentation. The results will be used to identify and quantify where possible potential issues and make recommendations about the suitability or otherwise of the equipment.

## **Programme:**

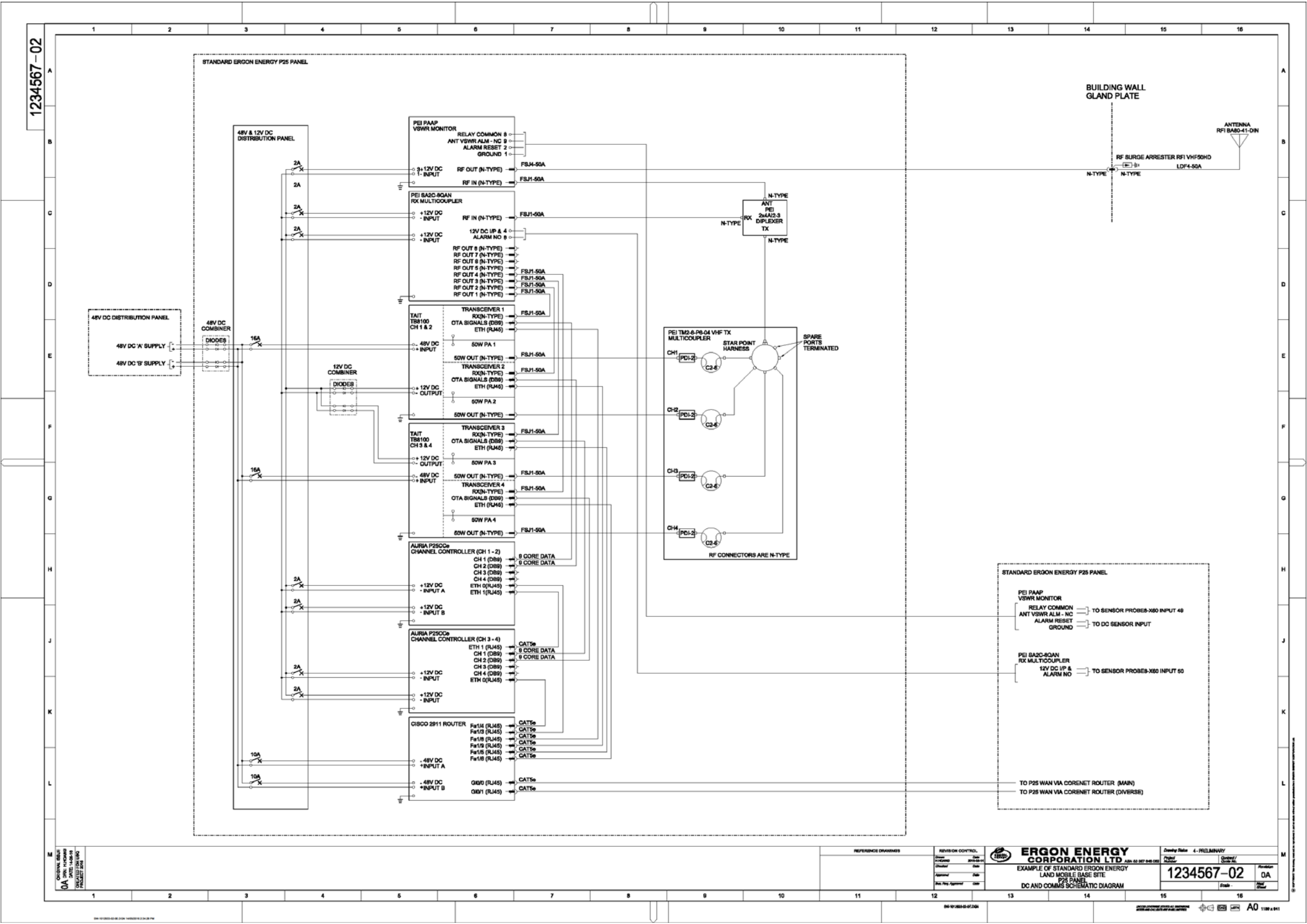
1. Research the key components, capabilities and coverage of the Ergon Energy P25 network. This will include encoding, modulation and filtering options as well as any particular capabilities or limitations of the hardware in use, the Auria wireless ES1105-V RMU.
2. Assess the location of existing ACRs to the P25 network coverage.

3. Research the data and packet formats of the P25 communications protocol for both the DNP3 and engineering access connections.
4. Investigate the operational requirements of the ACR SCADA and Remote Engineering connections. Identify baseline capabilities for reliable operation. Summarise these in criteria format for use in evaluation phase.
5. Setup and configure a test bed of equipment. This includes set up of P25 RMU and Nulec Test Box (ACR) as remote device, Test Port on SCADA master and using WSOS (Nulec configuration tool) to communicate to the remote device.
6. Measure the performance of the test bed under a range of parameters and assess results against the criteria developed in item 4, above.
7. Using these results and earlier research, complete a risk analysis covering the installation and use of a P25 network.
8. Document the results and recommendations in a format useful for Ergon Energy as a decision making tool.

As time permits:

9. Create a spread sheet tool that will use the baseline capabilities identified in item 4, along with network requirements, to help complete calculations and analysis of the network based on the parameters entered in by the network designer.

Appendix B: Ergon Energy P25 Land Base Mobile Communications Schematic Diagram



## Appendix C: P25 SA2C-8QA Receiver Multi-Coupler



### Model SA2C-8QA Rx Multicoupler 148~174 MHz



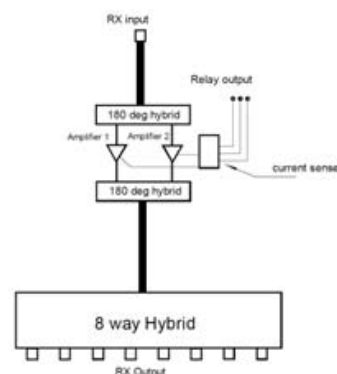
#### Product overview

The SA2C-8QA is High Band VHF Receive Multicoupler which incorporates a pair of amplifiers configured as a low noise parallel amplifier using hybrid dividers on the input and outputs which then feeds the 8 way hybrid. The advantage of this type of unit is superior intermodulation performance when compared to single device amplifiers and device failure redundancy. In the advent of one amplifier failing the second amplifier will continue to provide signal coverage. This allows the system to continue to function albeit at a lower level until service is implemented.

#### Specifications:

Frequency range:	148~174 MHz
Gain	3 dB nominal *
Maximum input no damage	+16 dBm
IP3	+33 dBm
Output to Output Isolation	20 dB min
Output port VSWR	< 1.5:1
Power requirements	+11 ~ 18 VDC @ 180 mA
Noise figure	3.7 dB
Alarm outputs	Dry relay contacts
Input connector	N female
Output connector	BNC female
Size	482.6 x 44.3 x 215mm (w x h x d)
Weight	4.0 kg

\*Various Gain levels can be ordered to suit customer requirements



#### POLAR ELECTRONIC INDUSTRIES PTY LTD

##### Communication Engineers

9 – 15 Friars Road, Moorabbin, Victoria, 3189, Australia.

Phone: +61 3 9555 2500, Fax: +61 3 9555 1515

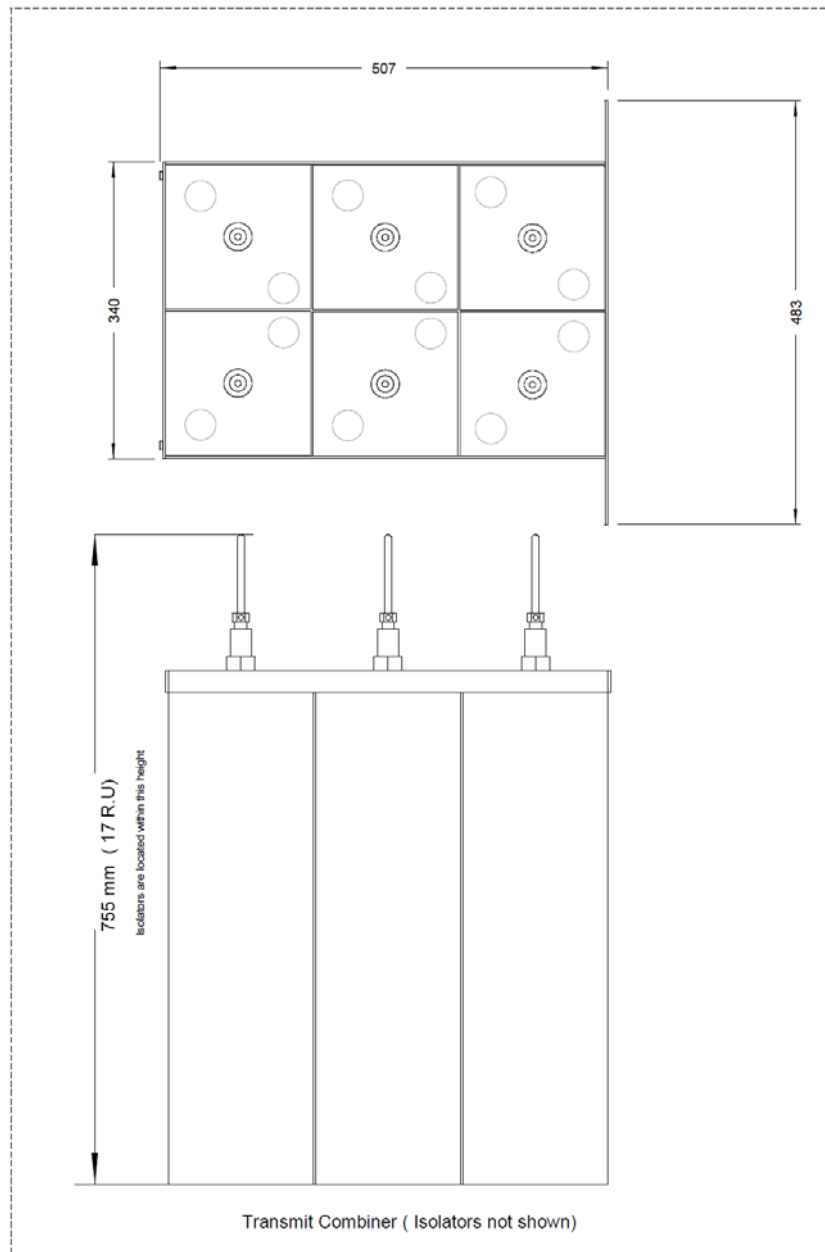
E-mail: [polar@polarelec.com.au](mailto:polar@polarelec.com.au) Web site: [www.polarelec.com.au](http://www.polarelec.com.au)

Quality  
Endorsed  
Company  
ISO 9001:2008  
Lic: QEC 1789  
SAI Global



## Appendix D: P25 Transmitter Multi-Coupler PEI TM2-6-P6-04

Polar Electronic Industries Pty Ltd





## MODEL C2-6

### FEATURES

#### Type 'C'

This range of highly selective quarter wave co-axial resonators will improve the RF selectivity of receivers and reduce the transmission of harmonics and spurious radiation from transmitters. The physically larger cavity resonators provide greater selectivity because of their higher 'Q'. A graph illustrating the selectivity increase afforded by larger resonators is shown.

#### Electrical Data:

A table of performance of the bandpass cavity filters is included for reference. All combinations have a minimum power capability of 150 watts, a temperature range of -10°C to +60°C, and a VSWR at resonance of 1.3/1 or better.

#### Operating Mode:

The standard range of resonators are 1/4 lambda re-entrant mode resonators, except for models with suffix 'X' which are 3/4 lambda.

#### Coupling:

Loops are factory preset to 1 dB insertion loss but may be varied from 0.5 dB to 2 dB insertion loss, if required. Note that selectivity will vary with a change of coupling.

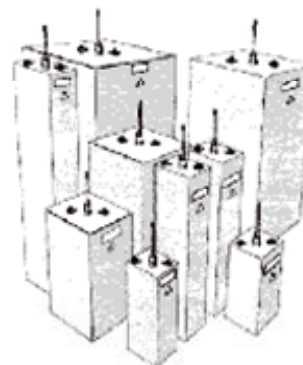
#### Stability:

Positive locking of the cavity to the tuned frequency, and the careful selection of materials and finishes ensures long term stability.

### CONSTRUCTION

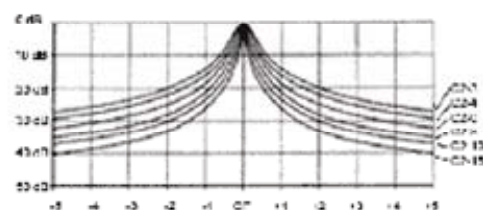
The cavity outer conductor is aluminium with a fully welded heavy aluminium top plate, the inner conductor is silver plated brass and copper, and the tuning rod is invar. Tuning is smooth with minimum backlash. The connectors are 'N' type female mounted on adjustable coupling loop carrier plates. The finish is grey enamel paint over chromate passivated aluminium body.

### NOTES

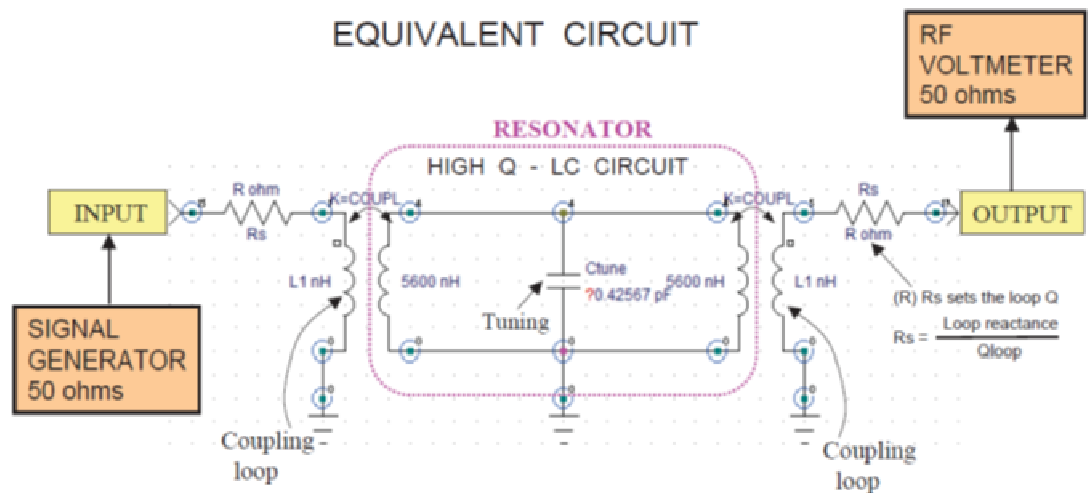


MODEL NO	C2-6
FREQUENCY BAND	148 - 174 MHz
ATTENUATION	25dB (@ +1%)
ATTENUATION	29dB (@ +2%)
ATTENUATION	32dB (@ +3%)
PASSBAND	1dB (loss)
WIDTH	164 mm
DEPTH	164 mm
HEIGHT	758 mm
WEIGHT	3.5kg

Brackets for wall or rack mounting may be supplied with all models of cavity resonators as an optional extra.



## BANDPASS CAVITIES EQUIVALENT CIRCUIT



- ❑ THE QUARTER WAVELENGTH RESONATOR IS MODELED WITH A HIGH Q - LC CIRCUIT
- ❑ TYPICAL RESONATOR  $Q_u$  VALUES: 2100 for 4 in. Cavity, > 5000 for a 6 in. cavity



## MODEL PDI-2

### FEATURES

Where there are two or more transmitters in close proximity or transmitters are combined on to one antenna an isolator will suppress intermodulation products by isolating the power amplifier of the transmitter to which it is connected from the reflected energy of other transmitters.

The 50 ohm matching provided by an isolator allows a transmitter to be tuned even with a cavity between the isolator and the antenna.

### CONSTRUCTION

High quality components contained in a black anodized machined solid aluminum housing with ample heat dissipation provided.

The units have integrated ceramic dummy loads of adequate power handling capacity.

### NOTES

All models of isolators have a temperature range of -10°C to +60°C, and a VSWR of 1.25:1.

Available in a high power rating version to special order.

Power ratings to 350 watts are available.

MODEL NO	PDI-2
FREQUENCY RANGE	148 - 174 MHz
BANDWIDTH	2 MHz
VSWR	1.25:1
INSERTION LOSS	1.4 db
ISOLATOR TYPE	DUAL
ISOLATION	50dB (typical)
TEMP. RANGE	-10°C to +60°C
POWER	100 Watts (max)
TERMINATION	'N' FEMALE
WIDTH	150 mm
DEPTH	28 mm
HEIGHT	80 mm
WEIGHT	0.7kg



**POLAR ELECTRONIC INDUSTRIES PTY LTD**

COMMUNICATIONS ENGINEERS

ACN : 005 545 291 ABN : 74 711 768 638

9 - 15 FRIARS RD MOORABBIN 3189 VICTORIA AUSTRALIA

T : + 61 3 9555 2500 F : + 61 3 9555 1515 TF : 1800 33 5633 (Australia only)

E : [polar@polarelec.com.au](mailto:polar@polarelec.com.au) W : <http://www.polarelec.com.au>



ISO 9001:2015 CERTIFIED

## Appendix E: P25 Bandpass Duplexer 2xAl2-3



DUPLEXER - BANDPASS

BANDPASS DUPLEXER "AI"

148 - 174 MHz

### MODEL 2x4AI2-3

#### FEATURES

The electrical feature of the bandpass duplexer is its ability to pass the wanted frequencies and to reject all unwanted frequencies, thus providing protection from nearby transmitters.

Its higher protection against receiver desensitization makes it suitable for use at congested urban sites.

#### CONSTRUCTION

Constructed from aluminium with all joints along the current path fully welded.

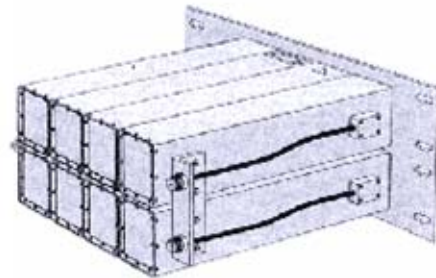
The cavities are tuned to resonance with a capacitive tuning element thus allowing a maximum resonator depth of 460mm. This allows a highly selective duplexer to be mounted in the minimum of rack space.

This model comprises four (4) "3x4 inch" bandpass cavities in each duplexer branch.

The robust mechanical construction ensures excellent mechanical stability and trouble free operation.

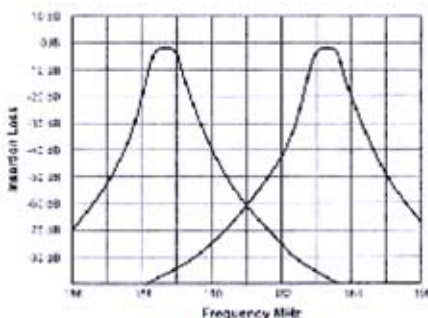
#### NOTES

All duplexers are factory tuned to customer specified frequencies, but may be field retuned.



MODEL 2x4AI2-3

MODEL NO	2x4AI2-3
FREQUENCY RANGE	148 - 174 MHz
IMPEDANCE	50 ohms
VSWR	1.3:1(max)
INSERTION LOSS	2 db
ISOLATION	80 dB (min) @ Tx Freq
ISOLATION	80 dB (min) @ Rx Freq
Tx-Rx SEPARATION	4.6 MHz (min)
TEMP. RANGE	-30°C to +60°C
CONFIGURATION	BANDPASS
FIELD TUNEABLE	YES
PRE-SET/TUNED	YES
POWER	100 Watts (input)
TERMINATION	1" FEMALE
CONNECTORS - INPUT	1" FEMALE
CONNECTORS - OUTPUT	1" FEMALE
WIDTH	483 mm
DEPTH	460 mm
HEIGHT	220 mm
WEIGHT	11kg
MOUNTING (POSITION)	19" 5 RACK UNIT
FINISH	GREY ENAMEL



Typical Response Curve



**POLAR ELECTRONIC INDUSTRIES PTY LTD**

COMMUNICATIONS ENGINEERS

ACN : 005 545 201 ABN : 74 711 768 636

9-15 FRIARS RD MOORABBIN 3189 VICTORIA AUSTRALIA

T : +61 3 9555 2500 F : +61 3 9555 1515 TF : 1800 33 5633 (Australia only)

E : [polar@polarelec.com.au](mailto:polar@polarelec.com.au) W : <http://www.polarelec.com.au>



# Appendix F: VSWR Alarm Base Antenna Monitor

## PAAP



### VSWR Power Monitor

35 to 960 MHz

#### Model PAAP

Model PAAP is a VSWR and power monitor alarm unit that provides for the continuous monitoring of a transmitter and an antenna and will signal an alarm condition if the transmitter forward power falls below a pre-programmed level, or if the antenna VSWR goes high.

A high VSWR or low power condition will cause separate red LEDs to light on the front panel of the unit and individual relays to latch.

The alarm signals will stay set until reset at the front panel or by an active low on the remote reset line.

The unit has application in monitoring the status of a remotely sited transmitter and antenna, especially in telemetry situations.



The alarm unit is housed in an enclosure mounted on a 1 RU 19" rack panel. Adjustments for Low Power trip levels and VSWR trip levels are available on the top panel of the unit.

The front panel has a reset switch, and four LEDs, one red LED will indicate transmitter power low, the second red LED will show antenna VSWR high and a amber LED shows that the transmitter is keyed.

The fourth green LED indicates power on.

The unit is powered from 13.8VDC.

Transmitter power outputs from 1 watt to 500 watts may be monitored with this unit.

Please specify the transmitter power output and frequency band when ordering and the PAAP will be adjusted to suit

The PAAP comprises the following sections.

- A ratio detector for detecting antenna VSWR.

- An adjustable voltage reference for setting the low power trip level.

- A voltage comparator for comparing the Tx power level to the low power trip level.

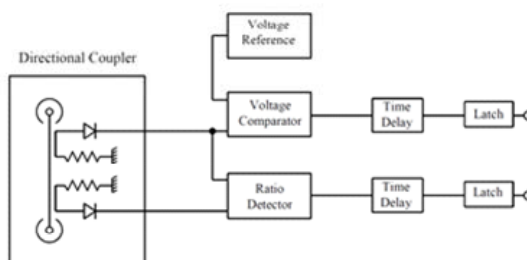
- A time delay circuit to ensure the Tx power stabilizes before monitoring begins.

- Two latching relay circuits for holding the alarm circuits on.

- A dual directional coupler for sensing VSWR and forward power levels.

*Note: Although the PAAP is able to detect when a small amount of power is applied to it's directional coupler, a total failure of the transmitter cannot be detected unless the Tx keyed signal is present. For this reason the Tx keyed signal must be supplied. (Active low or active high accepted).*

An illustration and function block diagram is shown below.



Page F12

#### POLAR ELECTRONIC INDUSTRIES PTY LTD

Communication Engineers

9 - 15 Friars Road, Moorabbin, Victoria, 3189, Australia.

Phone: +61 3 9555 2500, Fax: +61 3 9555 1515

E-mail: [polar@polarelec.com.au](mailto:polar@polarelec.com.au)

Web site: [www.polarelec.com.au](http://www.polarelec.com.au)



## Appendix G: Project Risk

The following risk analysis covering the installation of the P25 RMU to be used on the P25 network.

### Technology Acceptance Risk

The use of P25 RMU for efficiency will need to be well understood by the management of Telco and Communications Network Operations Centre (CNOC) supervisors. In its simplest form it offers the cost efficient alternative to the satellite ACR communications strategy and it is to be agreed by all parties when brought into operations.

The key operational risks revolve around the use of the P25 RMU on the P25 network as an alternative to satellite communications to ACR strategy are as outlined on table 15. Risk mitigation has been compared to existing satellite communications strategy as it is the targeted replacement.

Table 15: P25 RMU Detailed Risk Table.

Risk	Likelihood	Potential Impact	Mitigation
<b>Design time</b>			
Time associated with radio path coverage check on ACR location is higher than 1 hour.	LOW	LOW	Using software such as radio mobile or T-path to do RF path check can be very straight forward.
P25 RMU configuration cost is higher than that of configuring a satellite solution.	LOW	LOW	The time allocated to do a satellite modem configuration setup is adequate to do a P25 RMU.
SCADA page configuration time for P25 RMU is higher than that of a satellite ACR.	LOW	LOW	SCADA designing work will be the same as doing a satellite ACR setup.

Risk	Likelihood	Potential Impact	Mitigation
<b>Construction time</b>			
General installation time on ACR using the P25 RMU is higher than that of a satellite solution.	LOW	LOW	Equipment requirement is similar using a NextG modem on ACR, with less equipment count than a using satellite modem.
<b>Commissioning time</b>			
Commissioning time both CNOC and SCADA with using the P25 RMU is higher than that of a satellite solution.	MEDIUM	MEDIUM	The impact of voice traffic on the day plays the major part on the commission time as voice takes precedence over data traffic on P25 network.
<b>Equipment Cost</b>			
The cost of the Auria Wireless P25 RMU is higher than that of using the M2M SabreRanger Terminal.	LOW	LOW	The current cost to procure equipment necessary for a satellite setup is twice the cost of a single P25 RMU.
<b>P25 RMU on ACR Project Delivery</b>			
P25 RMU on ACR takes longer to construct than estimated.	LOW	LOW	Focussed project team engaged to manage and deliver the project.
Resource Availability, construction resources	LOW	LOW	Workshop team responsibility.
Equipment Availability	LOW	LOW	Equipment procurement for design and configuration prior to a construction scope
Weather Delay	MEDIUM	LOW	Project planning to accommodate

Risk	Likelihood	Potential Impact	Mitigation
Project Creep – stakeholder project expectations increase and the deliverable requirements are extended.	MEDIUM	MEDIUM	Project scope is well defined and any changes to business requirements are to be reflected in and agreed and modified scope.
<b>Technology</b>			
<p>There is a risk that the technology deployed will become obsolete</p> <ul style="list-style-type: none"> <li>- in terms of the equipment invested in to support the products / services</li> </ul>	LOW – MEDIUM	MEDIUM	Auria Wireless is the only vendor that P25 RMU can be sourced from.
There is a risk that the P25 network cannot support more up to three P25 RMU data traffic on a channel.	LOW	MEDIUM	Equipment to be used is Utility Grade and will support the business applications.
<b>Operational</b>			
There is a risk that the CNOC cannot configure the alarm monitoring system to activate a 'Communications Failed' alarm delay requirement to overcome the hourly registration on P25 network.	MEDIUM	MEDIUM	CNOC supervisors and SCADA group to be consulted and once operational requirements are met the P25 RMU application can proceed.