KTS Wireless Product Vision

Supervisory Control and Data Acquisition (SCADA) Applications using the Agility Radios

February 2014

Version 1.0

1.0 Introduction

Koos Technical Services, Inc (KTS) began the development of its family of software-defined radios in 2009. This collection of products carries the name ‘Agility’ because it was designed to be flexible. All of the following performance can be modified with the click of a mouse:

- Data rate (2.4 kb/s to 6.25 Mb/s)
- Transmit Power (0.01 to 5 Watts)
- Frequency bandwidth of up to 300 MHz
- Channel spacing as low as 1.25 kHz
- Media Access Control (Poll/Select or Device controlled)
- Modulation Scheme (2 FSK, QPSK, SOQPSK)
- FEC (Rate ½ Viterbi)
- Hub or Remote
- SCADA Protocol (Modbus, transparent, custom)
- Serial Port Configuration
- US or International Regulation compliance
- 9 – 24 VDC input

Two of the three members of the KTS Agility family of radios can be used for SCADA applications. The **Agility Telemetry Radio (ATR)** was designed for legacy applications but includes the capabilities to migrate to more modern applications including Ethernet support, higher data rates up to 64 kb/s and FIPS-140-2 security with equipment and management authentication. The **Agility White Space Radio (AWR)** supports even higher capacities up to 6.25 MB/s in 6-8 MHz channels in the 470-698 MHz TV bands. The AWR was the first FCC-approved TV Band Device (TVBD) that could operate in the unused TV bands. These UHF frequencies have much better propagation characteristics than the 900 MHz, 2.4 and 5.7 GHz unlicensed bands and provide more reliable service.

2.0 ATR Applications

The ATR is shown in Figure 2-1. It includes an Ethernet and serial (RS-232) user interfaces which can be used simultaneously. It has a screw-attached power connector to make in compliant with NEC classified hazardous locations such as petroleum processing sites. All connectors are locking and comply with this standard when the ATR is installed in a compliant enclosure at such sites.

The ATR accepts 9-24 VDC and consumes about 18 W of power. Two LEDs indicate power on or fault conditions as well as transmit/receive over-the air messages.

The ATR is installed at either the central site near the SCADA host or at remote sites connected to RTUs or PLCs. It can be configured to support either role. At the central site, the ATR’s Ethernet port can connect to the Host using, for example, the Modbus TCP port. A dedicated TCP port is used to exchange SCADA messages between the Host and ATR over an Ethernet connection. The Hub ATR’s Media Access Control (MAC) software can be configured to round-robin poll all the remote ATRs or allow the SCADA host to do all the polling (Device controlled). In most legacy SCADA protocols, the SCADA host controls polling. When Ethernet TCP/IP is used, the Hub ATR can take over polling.

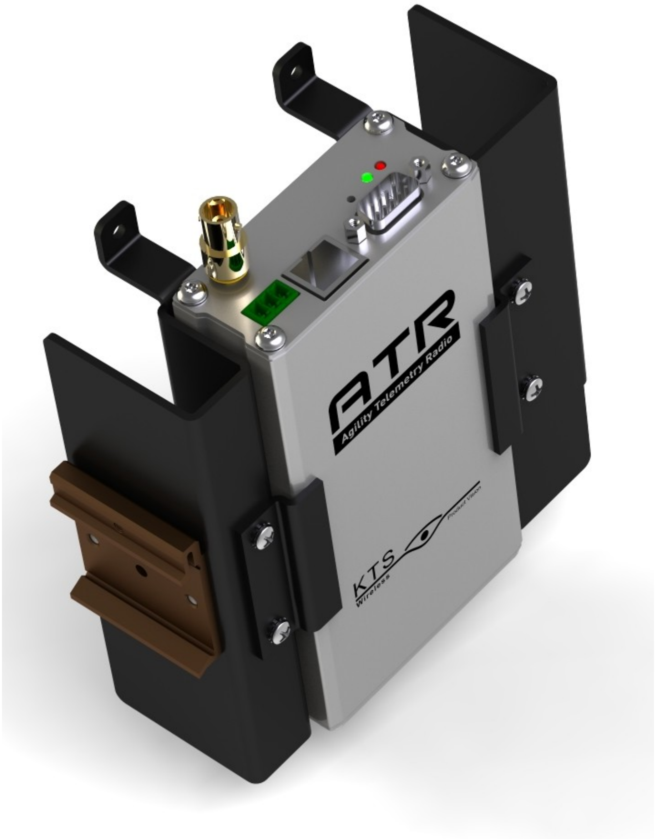


Figure 2-1: Agility Telemetry Radio (ATR) in an optional Wall/DIN Rail Mount

The remote ATRs are typically installed in a weatherproof enclosure with the PLC. This may be a water storage tank, water well site, wastewater lift station, oil or gas well or electrical substation. The ATRs Ethernet or Serial port can be used to connect to the PLC. The serial port can accept Modbus messages or any other protocol using transparent mode. This mode can be used for any serial protocol since message delineation is determined by activity and not message format. Message size and line idle times can be set to trigger forwarding over the air. If the PLC supports Ethernet, it can be directly connected to the ATRs Ethernet port. Both the ATR and the PLC are configured with IP addresses that allow direct connection to the SCADA host.

In some applications the PLC is not the only device requiring connectivity back the central site. An IP camera may be present that is triggered by motion detection, a contact closure or time of day. An Ethernet switch can be used to route this and the PLC to the ATRs Ethernet port. Or, the PLC can be connected via the serial port and the camera can use the Ethernet port.

Since the ATR support relatively narrowband channels from 6.25 to 100 kHz and data rates from 2.4 to 64 kb/s, video cameras must have two important features. First, video compression (H.264) must be used to compress along with lower frame rates (1-2 fps) and resolution (QVGA – 320 x 240) transmitted over the air. Many IP cameras can store the video in HD mode on an SD card in the unit so resolution is not lost. Second, video should be triggered by an event and not sent or recorded constantly. Many cameras include video analysis where motion within a portion of the frame can trigger recording and transmission. In addition, external motion detectors can be connected to the camera's alarm input terminals (typically one or two). Using these techniques and wider bandwidth channels (≥25 kHz) in certain frequency bands allow security cameras to be used at SCADA sites. The ATR will prioritize serial data over Ethernet traffic to make sure video traffic does not delay SCADA responses.

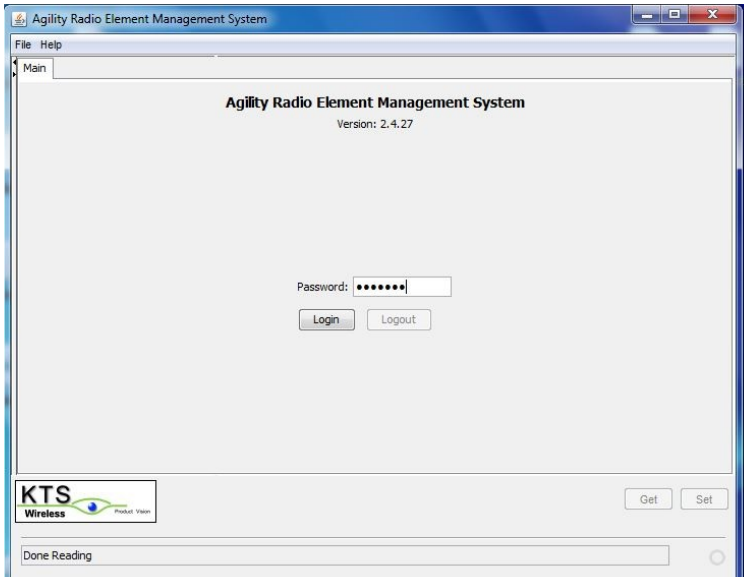
2.1 Security

Secure communications for critical infrastructure SCADA systems is no longer an option. The threat level is rising every day making wireless SCADA links vulnerable. This year KTS Wireless will release a comprehensive Security Framework that adds best of class security to networks deployed with its Agility family of radios. This framework is standards based using the EAP-TLS algorithm of IEEE 802.1x for Authentication and Authorization and the IEEE 802.11i-2004 standard for key management. Moreover, the framework is implemented using FIPS 140-2 validated cryptography.

Encryption can be applied using a pre-shared key (e.g., used with wireless routers) or along with device and management system authentication and authorization (AA). This AA option prevents network access from radios not on a ‘white list’ and local management of radios by unauthorized personnel.

2.2 Element Management System (EMS)

KTS provides PC-based software tools (free) to manage its family of Agility radios. The ATR and AWR EMS are slightly different due to the differences in management requirements imposed by the FCC and other regulatory agencies. However, they both have a similar ‘look and feel’. Both versions of the EMS can connect locally to a single radio or connect to a remote radio joined to a wireless network.
Figure 2.2-1(a) through (d) show four of the eight EMS screens for the ATR version. The Main screen prompts the Operator to enter a valid password. If the AA/Security Framework option is implemented for the network, the PC running the EMS software must have a certificate pre-installed. This certificate plus a valid password must present before management access is allowed. If no or the pre-shared key security is selected for the network only a valid password is required by the EMS.



Agility Radio Element Management System

Agility Radio Element Management System

Version: 2.4.27

Password: •••••••

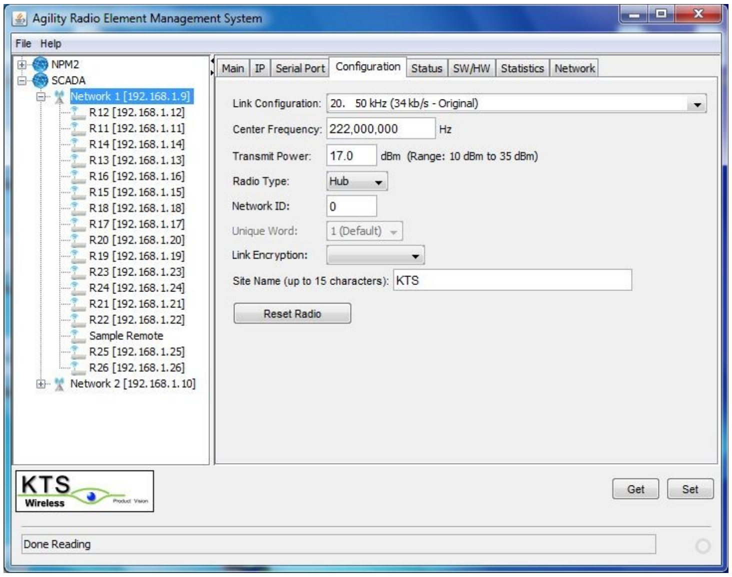
Done Reading

Figure 2.2-1(a): ATR EMS Main (Login) Screen

After login is complete, access to all other screens (tabs) on the EMS is available for monitoring status or performing configuration changes. The Configuration screen allows the operator to completely configure the ATR. Notice the top field, Link Configuration. A drop down menu provides a selection of over 20 link configurations which specify the data rate and channel bandwidth. For example, one selection is 12.5 kHz FCC Part 90 which supports 9.6 kb/s with a waveform that is compliant with FCC Part 90. This screen also provides fields for setting the operating frequency, transmit RF Power level and Radio Type (Hub and Remote). All KTS Agility radios can be configured as a Hub or Remote. Hub Radios will support a poll/select MAC for Ethernet traffic. A Network ID is used to prevent radios in networks with overlapping coverage and using the same frequency from joining with the wrong Hub. Link Encryption (Pre-shared key or AA) can also be configured.

A Statistics screen can be used to count transmit and received user and control packets over a defined timer interval in minutes. A cunt of message received with errors is also provided.

The Network screen is available when connected to a Hub radio. It displays all the remote ATRs that have automatically joined with the Hub (same frequency, Network ID and Encryption key). The receive signal strength (RSSI) of the last message and the radios IP address are displayed.



Link Configuration: 20. 50 kHz (34 kb/s - Original)

Center Frequency: 222,000,000 Hz

Transmit Power: 17.0 dBm (Range: 10 dBm to 35 dBm)

Radio Type: Hub

Network ID: 0

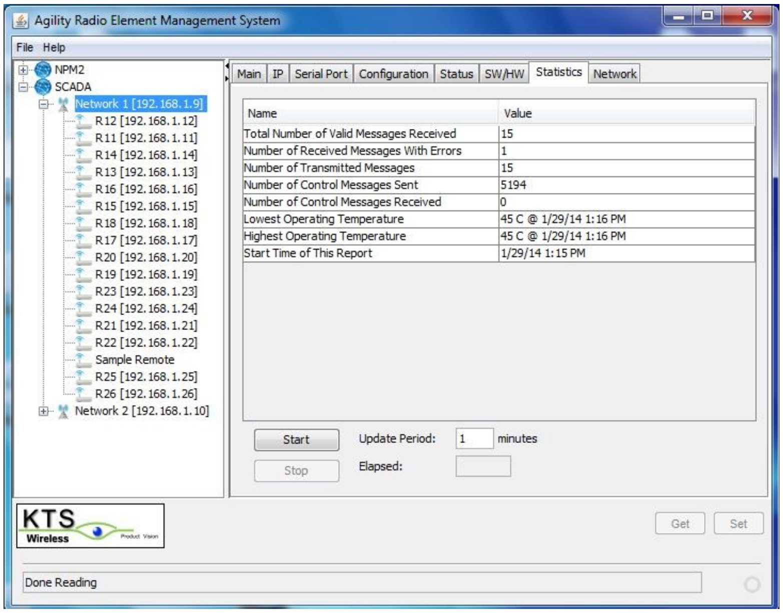
Unique Word: 1 (Default)

Link Encryption:

Site Name (up to 15 characters): KTS

Done Reading

Figure 2.2-1(b): ATR Configuration Screen



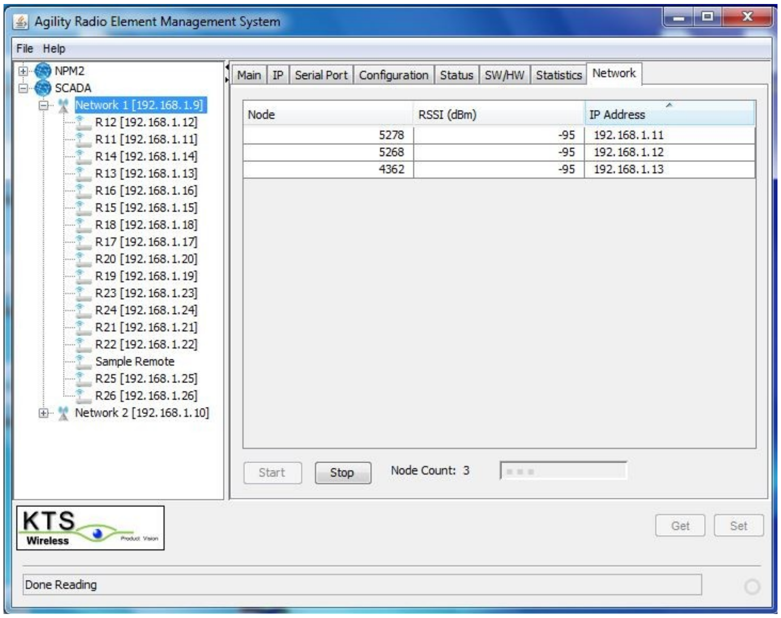
Name	Value
Total Number of Valid Messages Received	15
Number of Received Messages With Errors	1
Number of Transmitted Messages	15
Number of Control Messages Sent	5194
Number of Control Messages Received	0
Lowest Operating Temperature	45 C @ 1/29/14 1:16 PM
Highest Operating Temperature	45 C @ 1/29/14 1:16 PM
Start Time of This Report	1/29/14 1:15 PM

Update Period: 1 minutes

Elapsed:

Done Reading

Figure 2.2-1(c): Statistic Screen



- NPM2
- SCADA
  - Network 1 [192.168.1.9]
    - R12 [192.168.1.12]
    - R11 [192.168.1.11]
    - R14 [192.168.1.14]
    - R13 [192.168.1.13]
    - R16 [192.168.1.16]
    - R15 [192.168.1.15]
    - R18 [192.168.1.18]
    - R17 [192.168.1.17]
    - R20 [192.168.1.20]
    - R19 [192.168.1.19]
    - R23 [192.168.1.23]
    - R24 [192.168.1.24]
    - R21 [192.168.1.21]
    - R22 [192.168.1.22]
    - Sample Remote
    - R25 [192.168.1.25]
    - R26 [192.168.1.26]
  - Network 2 [192.168.1.10]

Node	RSSI (dBm)	IP Address
5278	-95	192.168.1.11
5268	-95	192.168.1.12
4362	-95	192.168.1.13

Node Count: 3

Done Reading

Figure 2.2-1(d): Network Screen

3.0 AWR Applications

The AWR is shown in Figure 3-1. This unit operates in 6-8 MHz bandwidth channels and supports data rates up to 6.25 Mb/s. It is mounted outdoors at the top of the mast near the antenna or at the bottom for easier access. It is provide in a complete kit with pole mount bracket, watertight Ethernet connector and PoE (Power over Ethernet) Power Supply. The Power Supply (also shown in Figure 3-1) is installed indoors near the user equipment and plugged into a standard 120 VAC outlet. A CAT 5e/6 Ethernet cable is run from the AWR on the antenna support pole to the power supply. This cable can be terminated on both ends using a standard RJ45 jack. The watertight Ethernet connector (provided) covers the standard jack (also provided) and screws into the AWR. The other end of the Ethernet cable connects to the Power RJ45 plug and the user equipment connects to the LAN plug (cable not provided).

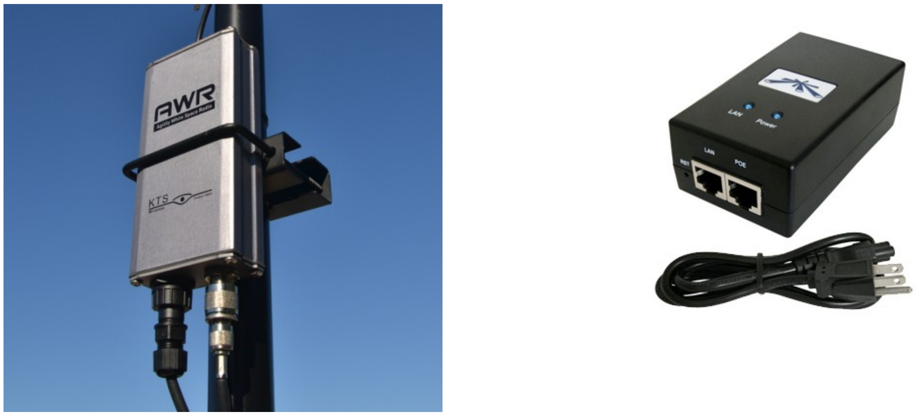


Figure 3-1: KTS Agility White Space Radio (AWR) and Power Supply

All white space approved radios must periodically connect to a Server that updates its available channel list. Several companies provide access to these Servers including Spectrum Bridge and Google. These servers, in turn, query the official FCC database to retrieve information on the location of all TV band incumbent users such as TV broadcast stations and facilities using wireless microphones. These users have priority access to certain channels and TVBD like the AWR must avoid interference with them. Even with these incumbents, a significant portion of the UHF band is available for TVBD usage. Figure 3-2 illustrates the varying amounts available around the continental US. Notice that more bandwidth is available outside the major cities and in rural areas. Few or no channels are available in Dallas, TX, Miami, FL, Southern California, San Francisco and the New York area. These areas are shown in black. The dark and light blue areas indicate areas with significant white space spectrum availability.

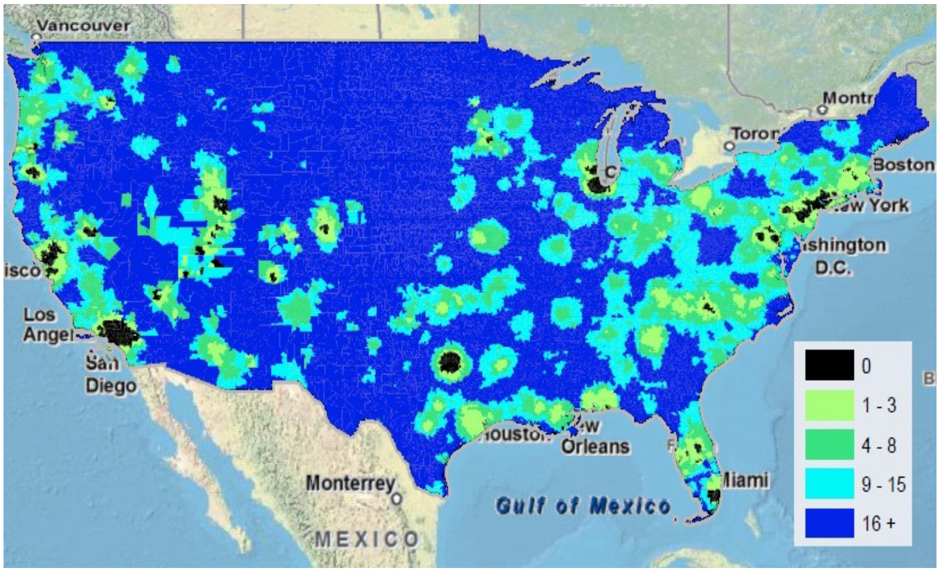


Figure 3-2: White Space Spectrum availability in the US

The AWR network consists of a Hub and multiple Remotes. The Hub is installed at a central location that must provide Internet access, at least periodically. The Hub AWR must be able to connect to the Server to get the currently available channel list at least once per day. It will stop operating if it is unable to connect for 48 hours.

The Hub radio also connects to the SCADA host via Ethernet. The AWR wireless network acts as a layer 2 learning bridge and connects the devices at the Remote sites to the LAN connected to the Hub AWR. The learning bridge feature prevents most of the non-SCADA traffic on the Hub LAN from going over the wireless network. Some broadcast and multicast traffic will be sent so care should be taken to limit this type of traffic on the Hub LAN. The Hub AWR will poll each Remote AWR in a round-robin fashion after it has transmitted all of its outbound messages. Each Remote AWR will transmit its queued outbound messages after receiving its individual poll message from the Hub. This polling takes place transparently to the SCADA equipment and provides efficient use of half-duplex the wireless channel.

The AWR has a unique feature referred to as Telemetry Plus. It’s often desirable to tradeoff throughput for range. A throughput of 3 or 6 Mb/s may not be needed. IF so, the AWR can be configured to reduce its throughput and achieve longer ranges. Table 3-1 shows the typical ranges for the various link configurations. For SCADA networks that can be adequately serviced with 200 kb/s of throughput, a significant range advantage can achieved. These configurations can be set using the AWR EMS.

Link Configuration	Typical Range (mi)
6.25 Mb/s - No FEC	up to 1
3.1 Mb/s - No FEC	1-2
3.1 Mb/s - 1/2 Rate FEC	2-3
1.5 Mb/s - 1/2 Rate FEC	3-4
768 kb/s - 1/2 Rate FEC	4-6
200 kb/s - 1/2 Rate FEC	7-10

Table 3-1: Typical Ranges for AWR Link Configurations

Current regulations for using the white space spectrum require that the frequency and maximum power be controlled by the database. The maximum antenna height is also regulated and different for hubs and remotes. In the US, the FCC limits the hub antenna height to 30 m above ground level (AGL) and the remotes to 10 m AGL. The precise geographic location of all the AWR sites must also be supplied to the EMS and be accurate within 50 m. The exact frequency is not determined by the database. Instead a list of available frequencies is supplied to the Hub AWR. The EMS allows the Installer to input preferences. For example, the available channel list may be 14, 18, 22, 30 and 45. The EMS allows the Installer to enter 3, preferred channel choices (first, second and third). If the Installer entered the choices shown below, Channel 30 would be used.

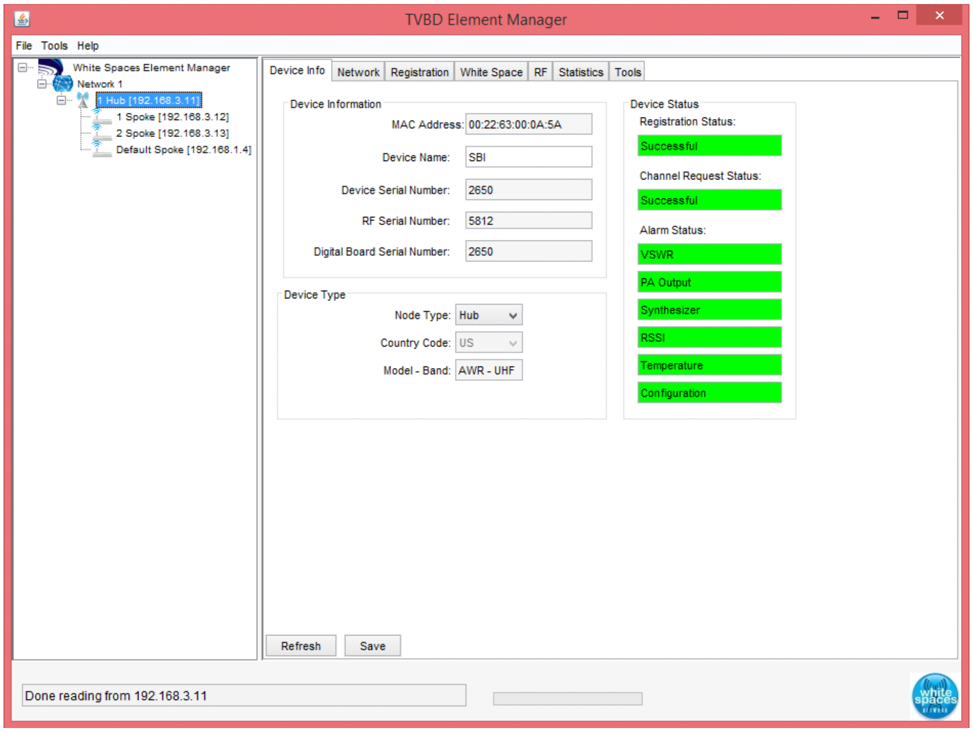
Choice 1: 15
Choice 2: 20
Choice 3: 30

Some Database Providers such as Spectrum Bridge, Inc. offer additional services that allow the AWR to select channels from the available list that are not in use by other white space networks in the same area. This may be a useful service to reduce the potential for interference. The basic database service doesn’t typically include any this ‘pick the best channel’ feature unless an additional fee is paid. The typical fee charged for the basic service (just the available channel list with no recommendations) is $50 per radio. This is a one-time charge and is included in the price of the KTS AWR for the Spectrum Bridge database.

3.1 AWR Element Management System (EMS)

As stated above, the EMS for the AWR differs slightly from the ATR version due to FCC regulations that prevent the Operator from selecting the transmit frequency and power level. These parameters are set by the FCC and vary with location.

Figure 3.1(a) – (d) show four of the seven available screens.



Device Information

MAC Address: 00:22:63:00:0A:5A

Device Name: SBI

Device Serial Number: 2650

RF Serial Number: 5812

Digital Board Serial Number: 2650

Device Type

Node Type: Hub

Country Code: US

Model - Band: AWR - UHF

Device Status

Registration Status: 🟩 Successful

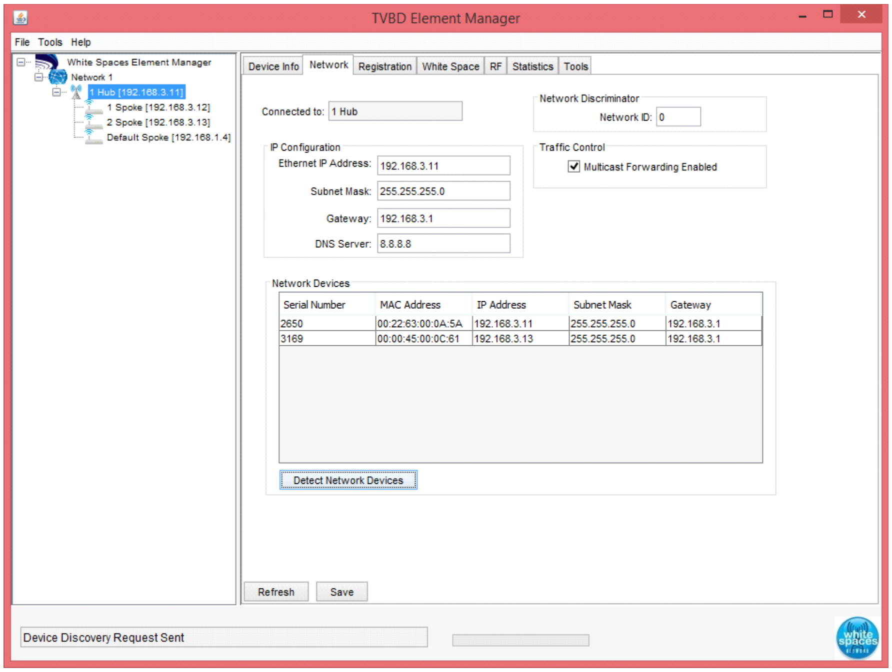
Channel Request Status: 🟩 Successful

Alarm Status:

- 🟩 VSWR
- 🟩 PA Output
- 🟩 Synthesizer
- 🟩 RSSI
- 🟩 Temperature
- 🟩 Configuration

Done reading from 192.168.3.11

Figure 3.1(a): Device Info Screen



Connected to: 1 Hub

Network Discriminator

Network ID: 0

IP Configuration

Ethernet IP Address: 192.168.3.11

Subnet Mask: 255.255.255.0

Gateway: 192.168.3.1

DNS Server: 8.8.8.8

Traffic Control

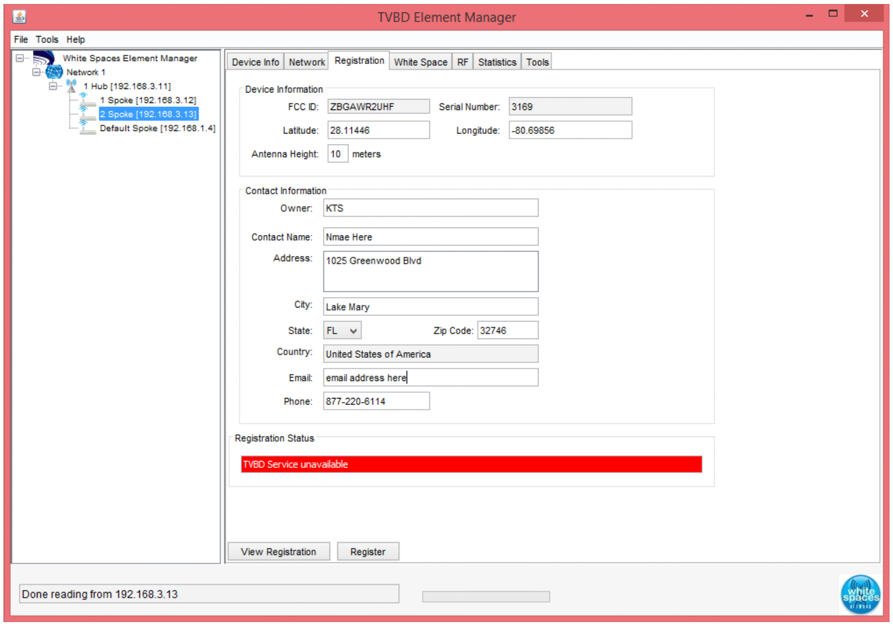
☑ Multicast Forwarding Enabled

Network Devices

Serial Number	MAC Address	IP Address	Subnet Mask	Gateway
2650	00:22:63:00:0A:5A	192.168.3.11	255.255.255.0	192.168.3.1
3169	00:00:45:00:0C:61	192.168.3.13	255.255.255.0	192.168.3.1

Device Discovery Request Sent

Figure 3.1(b): Network Screen



White Spaces Element Manager
Network 1
1 Hub [192.168.3.11]
1 Spoke [192.168.3.12]
2 Spoke [192.168.3.13]
Default Spoke [192.168.1.4]

Device Information

FCC ID: ZBGAWR2UHF Serial Number: 3169
Latitude: 28.11446 Longitude: -80.69856
Antenna Height: 10 meters

Contact Information

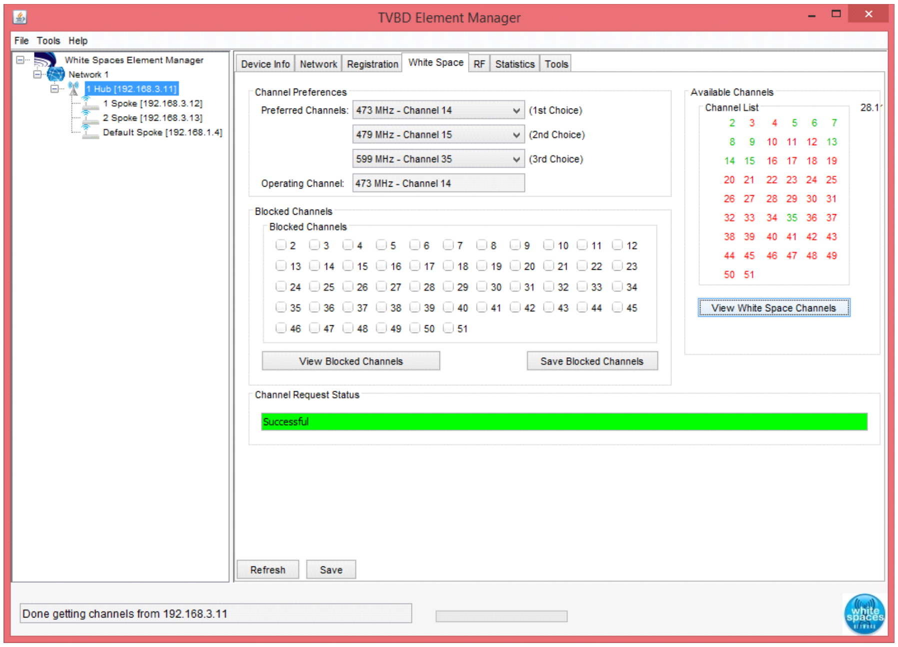
Owner: KTS
Contact Name: Nmae Here
Address: 1025 Greenwood Blvd
City: Lake Mary
State: FL Zip Code: 32746
Country: United States of America
Email: email address here
Phone: 877-220-6114

Registration Status

TVBD Service unavailable

Done reading from 192.168.3.13

Figure 3.1(c): Registration Screen



White Spaces Element Manager
Network 1
1 Hub [192.168.3.11]
1 Spoke [192.168.3.12]
2 Spoke [192.168.3.13]
Default Spoke [192.168.1.4]

Channel Preferences

Preferred Channels: 473 MHz - Channel 14 (1st Choice)
479 MHz - Channel 15 (2nd Choice)
599 MHz - Channel 35 (3rd Choice)
Operating Channel: 473 MHz - Channel 14

Blocked Channels

Blocked Channels

□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ 11	□ 12
□ 13	□ 14	□ 15	□ 16	□ 17	□ 18	□ 19	□ 20	□ 21	□ 22	□ 23
□ 24	□ 25	□ 26	□ 27	□ 28	□ 29	□ 30	□ 31	□ 32	□ 33	□ 34
□ 35	□ 36	□ 37	□ 38	□ 39	□ 40	□ 41	□ 42	□ 43	□ 44	□ 45
□ 46	□ 47	□ 48	□ 49	□ 50	□ 51					

Available Channels

Channel List 28.1

2	3	4	5	6	7
8	9	10	11	12	13
14	15	16	17	18	19
20	21	22	23	24	25
26	27	28	29	30	31
32	33	34	35	36	37
38	39	40	41	42	43
44	45	46	47	48	49
50	51				

Channel Request Status

Successful

Done getting channels from 192.168.3.11

Figure 3.1(d): White Space Screen

Figure 3.1(a) illustrates the status of a successfully registered Hub. This AWR Hub is connected to the Internet and has contacted the approved FCC database (via the Provider) and obtained the available channel list. Figure 3.1(d) shows this list (UHF channels 14, 15 and 35). Notice that the operator selected these channels in order of frequency with channel 14 being the first choice. The AWR Hub selected the first choice since it was on the available channel list.
Figure 3.1(b) shows the Network screen which can be used to obtain the assigned IP address of any AWR locally or remotely connected. Figure 3.1(c) shows the information required to

register a radio. The serial number and radio manufacturer's FCC ID must be supplied along with site installation specifics and user contact information.

The Hub AWR will contact the database at least once every 24 hours to get an updated list of available frequencies. If the currently used channel is no longer present on the list.

4.0 Summary

The KTS Agility family of commercial radios (ATR and AWR) provide powerful wireless solutions for any SCADA solution. They can be configured in the field to operate using different data rates/channel sizes and allow the user to tradeoff range for throughput. They support both serial and Ethernet interfaces making the migration from Legacy to IP-based traffic seamless.

A unique feature of the Agility radios is its programmable waveform usage. This allows the ATR, for example, to communicate with older radios that may no longer be in production. This emulation feature can be used by the customer to avoid a 'forklift cutover' to a newer radio. The ATR can be rolled-out slowly as budgets allow and operate in a compatible mode with older technology radios. Then, once the network is fully converted to the ATR months or years later, a simple click of a button on the EMS can change their operation to a more efficient modulation scheme, MAC layer and user interface (Ethernet).

The modulation type and MAC scheme are implemented in software in both Agility Radios and can be upgraded over time to comply with new regulations or provide more efficient use of the available spectrum. This makes them safe technology investments with many years of optimal performance.