



# Advanced RTUs Simplify and Enhance SCADA-Data Communications

Dan Ehrenreich, Motorola Inc.



## Overview

Supervisory Control and Data Acquisition (SCADA) solutions must provide reliable and timely communications, and have tested interfaces between a wide range of instrumentation and field sensors as well as SCADA HMI's. This means that to assure reliable SCADA-Data communications messages are sent between the control center and the Remote Terminal Unit (RTU), directly (point -to- point) or via one or more repeaters. They must be delivered error-free. When the SCADA engineer utilizes any type of wireless medium, the implementation requires more attention and expertise in order to achieve communication reliability. To achieve this important goal, engineering firms often suggest Radio Frequency (RF) path analysis. Measurement of the Signal-to-Noise (S/N) ratio and calculation of the Fade Margin provides indications on the expected communication quality and reliability. However, as explained in this paper, one must differentiate between mobile and transportable data communication vs. Fixed Data communication, where the RF engineer may consider unique solutions without spending time and money on actual point-to-point signal strength measurements.

## Communication Network Selection

When analyzing the actual SCADA-Data Communication performance for each option and its adaptability for a designated SCADA solution, the following considerations should apply:

- a. Transparent link vs. processing the data. Does the network offer absolute transparent communication between RTUs connected via the radio or does the radio process the data, such as performing error detection and correction, data routing, encryption, etc.?
- b. Private vs. Shared. Is the network defined as "private", where the loading is controlled by the network owner/operator or is the network a shared consumer channel resource (cellular or spread Spectrum), where no one can control nor predict the expected loading at any given moment?
- c. Preconfigured vs. Configurable Infrastructure. Does the network operation require installed infrastructure (data entry nodes, repeaters, computers, etc.) or is it a completely stand-alone operation, so that the data routing is controlled by the SCADA system/RTU protocol?
- d. Industrial Solution vs. Commercial Standard. Does the available radio meet industrial quality level/standards or only consumer level equipment available? Are the considered radios capable of operating in outdoor temperature and humidity conditions, electromagnetic interference, and were these tested to meet the most stringent industrial standards?
- e. Formal Type Approval/Certification. Were the selected radios certified to operate in the country where they are to be installed? In case the radio is installed within the RTU, was the complete assembly (with a dedicated model number) homologated for the country of the end user?

## Selecting Wireless SCADA-Data communication

Among the typical wireless media one can find licensed and non-licensed channels, dedicated/private or public networks, different communication methods, etc:

- a. Analog Conventional VHF and UHF Radio: These are narrow band (12.5 or 25 kHz bandwidth) voice radios that operate over licensed channels. Typically they provide transparent data communication at the rate of 1200 - 9600 b/s, utilizing DFM, FSK or DPSK modulation.
- b. Analog Trunking VHF, UHF, 800 MHz radio: These are narrow (12.5 kHz bandwidth) band voice type radios, connected with a central channel controller that operate over licensed channels. Typically they provide transparent data communication rates of 1200 b/s, utilizing DPSK method. Here it is important that one pays attention to the selected data protocol.
- c. Analog VHF, UHF, 900 MHz Multiple Address system (MAS) radio network: These are narrow band (12.5 kHz bandwidth) radios that are configured for dual (F1/F2) or single (F1) licensed channels

and may have an analog or RS-232 interface. Typically they provide transparent data communication at rates up to 9600 b/s and utilize DFM modulation method.

- d. Digital VHF, UHF, 800 MHz Integrated Voice and Data (IV&D) network: These are also narrow band (12.5 kHz bandwidth) radios operating over licensed channels that are integrated with the RTU using IP connectivity via RS-232 interface. They provide data communication rates up to 9600 b/s. Here the data delivery (network addressing) to each site is handled by the system.
- e. Digital broadband 900 MHz and 2400 MHz Spread Spectrum network: These radio modems typically operate over non-licensed channels and are integrated with the RTU using RS-232 serial port connection or IP connectivity via Ethernet or RS-232 interface. They provide data communication rates up to 512 k b/s.
- f. Digital broadband 900/240/3700/5700 MHz Spread Spectrum network: These radio modems operate over non-licensed channels and are integrated with the RTU using RS-232 serial port connection or IP connectivity via Ethernet. They can serve as an alternative to physical medium backbone and provide data communication up to 1 Mb/s.
- g. Digital broadband General Packet Radio Service (GPRS). These cellular commercial devices operate as 900/1800 MHz or 950/1900 MHz modems in parallel with the Global System for Mobile (GSM) communication network: This modem is usually external to the RTU and uses IP connectivity via RS-232. They provide 56 -114 kb/s data rates, however one must be aware that the data rate and its reliability depends on the actual (momentary) loading of the network.
- h. Digital and Analog Microwave network: These point-to-point radios require line of sight and operate over broadband GHz range licensed channels and are integrated with the RTU using RS-232 serial port. They can provide data communication rates up to 1 Mb/s.
- i. Digital Satellite Public/Commercial network: These broadband radios operate in GHz range licensed channels and are integrated with the RTU using RS-232 serial port. They can provide data communication rates up to 100 Mb/s.

### **Factors Influencing Data Reliability**

Upon analyzing the quality of the communication channel one can point out several factors which may affect the operating reliability of the system. Among the most visible factors are:

- a. Received Signal Level: This parameter influences the data reliability, since during low signal condition errors might not be corrected and cause system downtime. In other cases the effective data rate might slow down, as complete messages need to be retransmitted.
- b. RF Modem Modulation method: Selecting a suitable RF signal modulation method can be as important as selecting good quality hardware. For example, DPSK modulation results in slower data rate but delivers more reliable data communication than FSK or DFM.
- c. Radio Hardware Quality: In case of extreme operating temperature, outside of the normal operating range of the radio unit, the data recovery process might not be as accurate as required and therefore data errors may start appearing.
- d. Data Communication Protocol: Some SCADA protocols are more robust than others and under extreme conditions which might cause loss of data packets or interference(e.g., weather related lightning), the less robust protocols result in less reliable communication.

## Verifying Wireless Coverage

Upon obtaining information from the customer on the location of planned remote sites, the role of the RF engineer is to verify that appropriate RF coverage is provided. Such testing can be performed only after knowing several details of the planned solution:

- Operating frequency band: VHF/UHF/800 Mhz/900 Mhz/2400 MHz/3700 MHz... etc.
- Transmission Power of the radio
- Type of modulation: FSK/DPSK/DFM/ QPSK, etc.
- GPS coordinates of available repeaters, radio power, antenna height and gain, etc.
- GPS coordinates, type and effective height of the antenna in each remote location
- Required signal reception (dBm) to assure adequate error free RF communication
- Physical and natural signal barriers: hills, buildings, distances, and other known issues

## Fixed Data Communications

An important fact to take into consideration is that there is a major difference between handheld and mobile radios or cellular phones, which must allow good communication in every place and every corner of the street or in buildings vs. fixed installation. In order to achieve adequate communication in fixed installations, the RF engineer has many options to assure coverage, and this helps simplify and reduce the cost of the RF design. The following possibilities apply for fixed locations:

- Select the type (gain) of the antenna and if needed add a small tower for its installation
- Use of an off-the-shelf power type amplifier, suitable for the type of the radio utilized
- Move the location of the antenna (within few meters) if this helps to receive a stronger signal
- Use a better quality coaxial cable if the antenna has to be installed far way from the radio

Furthermore, using an RTU technology that implements all seven layers of the OSI/ISO-Seven layer stack and the Network Layer (no 3), results in the fact that each RTU may act as a Data Store & Forward (S&F) communicate node. This allows RTUs, which do not have effective line of sight with the repeater tower or with the Control Center tower to communicate through nearby RTUs and thereby establish communication with the control center. This solution can be repeated several times by communicating between and pair of RTUs and by that extends the coverage. In special cases, use of these advanced RTUs allows the integration of several media types into the same communication schemes. This allows a SCADA system to benefit from almost any combination of media (VHF, UHF, 900 MHz, 2400 MHz, etc.) which is optimal for the geographical area to be covered.

## Conclusions

Obvious conclusion of this white paper is that providing RF communication for Fixed Data sites is a much simpler task than certifying coverage for mobile and handheld radio users. Therefore, prior to investing in a costly RF path analysis (utilizing instrumentation for actual signal strength monitoring) radio engineers may use computer programs (i.e., [www.pathloss.com](http://www.pathloss.com)) that can estimate the signal strength and the fade margin for every segment of the network. In cases where a low signal is expected, they may consider communicating through other RTUs acting as S&F repeaters or add a minimal configuration RTUs, consider better antennas, boost the tower height, etc. Use of these methods helps to reduce the investment in a wireless system, and helps to justify use of advanced RTUs vs. PLC or low-tier RTUs which are unsuitable for wireless SCADA-data communications. All these alternatives are far less expensive than dispatching an expert team for testing, this will assist in expediting the SCADA project, reduce implementation cost and boost operating performance.

@@@@@@@@@



# Motorola ACE3600 RTUs Support High Performance SCADA-Data Communications

(Appendix to White paper)

- ACE3600 RTUs support a wide range of data communication media such as Analog and Digital Conventional and Trunking in the VHF/UHF/800 MHz, Multiple Address Systems in the VHF/UHF/900 MHz ranges, and variety of broadband radio networks, spread spectrum radios and more. Furthermore these RTUs are certified to operate over Motorola Canopy and ASTRO IV&D wireless IP networks, microwave, satellite, fiber-optic and telephone line modems, etc.
- ACE3600 RTUs operate with a range of Motorola and 3rd party radios and data modems operating over wireless and physical media, microwave, satellite, spread spectrum, power line carrier cellular networks. These units may interface via one of the 5 ports integrated to the ACE3600 CPU.
- ACE3600 RTUs run the application program separately from the data communication process. This solution supported by the Motorola Data Link Communication (MDLC) protocol allows “on-the-fly” modifying their application or parameters, without interrupting the RTU operation.
- ACE3600 RTUs feature transparent communication, while the data routing, error detection and correction, remote program uploading and downloading, remote diagnostics are supported with the MDLC seven layer (based on OSI/ISO based stack) protocol.
- ACE3600 RTUs perform reliable peer to peer (RTU-to-RTU) and RTU to master control center communication. This capability is supported by the MDLC Network layer allows extending the geographical coverage for those RTUs which do not have direct link with the control center.
- ACE3600 RTUs perform Store & Forward (S&F) operation using a single radio frequency. Prior the repeater retransmits the data it is verified for data integrity. If an error is detected, it is corrected prior retransmission using a unique MDLC protocol-based retry mechanism.
- ACE3600 RTUs are truly optimal for reliable and secure SCADA communication (hardware, software, protocol) and are ready to be upgraded with encryption (using preprogrammed keys), which help to assure system wide operating reliability and data security.
- ACE3600 RTUs have built in capability to perform data encapsulation or emulation of other vendors' data protocols, allowing the SCADA control center communicating with a wide range of RTUs, PLCs and Intelligent Electronic Devices (IED) using their native protocol.
- ACE3600 RTUs have built-in capability to send time stamped messages. They also allow performing over-the-network RTU clock synchronization simultaneously with normal operation. This feature allows implementing post-event analysis utilizing time-stamped reports.
- ACE3600 RTUs have capability to link between 2 or more different wireless physical media. This allows extending the geographical coverage via multiple nodes, while selecting the media which is the most optimal for SCADA-Data communication for each specific segment.
- ACE3600 RTUs have capability operating via the wireless network using cyclic polling, reporting by exception and reporting by event modes. When simultaneous events are reported to the control center, these RTUs have a built-in capability to quickly clear that (avalanche) condition.
- ACE3600 communication reliability is assured by checking the data integrity for each message and between S&F segments. Upon detecting an error, these RTUs resend only the missing packets and upon receipt of a complete/correct message, it is reconfirmed to the sending site.
- ACE3600 RTUs seamlessly interface with a wide range of SCADA Control centers units supplied by vendors worldwide. This can be done via RS-232 serial ports, Ethernet using MDLC, MODBUS, DNP 3.0 and OPC over TCP/IP, and a range of other SCADA protocols.

@@@@@@@@@

