



## Selecting a Top-Class Communication Oriented RTU for Water SCADA Systems

Dan Ehrenreich, Motorola

### Overview

Implementation of reliably operating wireless SCADA systems requires the use of RTUs, which are adapted for optimized features including: Reliable data communications, peer-to-peer and peer-to-master links and data security. In addition, these solutions must support smart channel access monitoring, report by events, handle avalanches of messages, remote programming and configuration, remote diagnostics, air-time efficient detection and correction of digital errors, and more.

### Data Networking

RTUs are designed to perform local control functions (like a PLC). However modern communications based RTUs must also offer three more functions: Implementation of peer-to-peer (Store and Forward) communications in a wireless SCADA system and integration of multiple communications media.

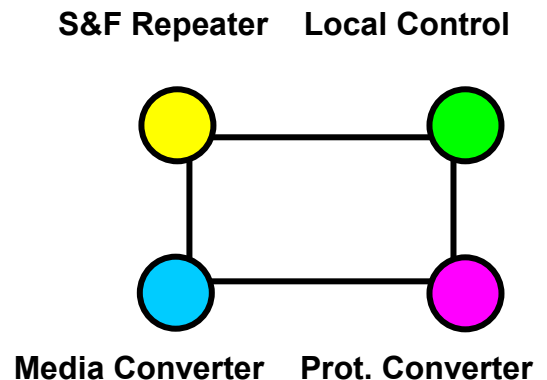
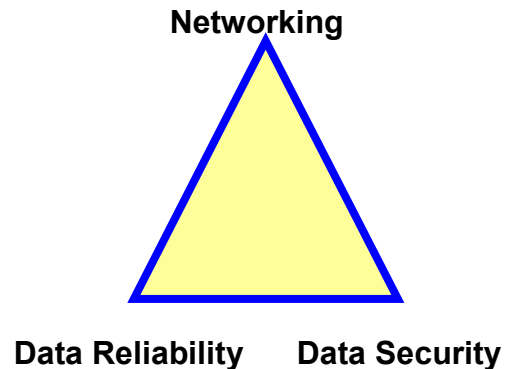
Each RTU may be required to act as a trans-coder (translating protocols) for 3<sup>rd</sup> party Intelligent Electronic Devices (IED) RTUs and PLCs made by other vendors, etc.

### Application Programming

Modern SCADA RTUs shall preferably utilize the seven-layer protocol defined by the International Standard Organization and its recommended Open Systems Interconnection (ISO/OSI) suite, where each layer is responsible for handling different functions associated with the SCADA process.

The SCADA application program (specify the functions RTU s shall perform), requires a set of media independent codes (protocol) that allow portability of the defined SCADA process to all RTUs in the system. In order to comply with this requirement, the program based in the "Application Layer" of the RTU must be completely isolated from the communications functionality and any changes in the network structure shall not affect the application.

**Note:** Only few of SCADA solution's vendors have the expertise to offer seven layers ISO/OSI based SCADA wireless communication, which comply with these features, while some are trying to provide it in various unsuccessful ways. Their usual approach is to adapt modem to a low tier protocol to perform these communication functions in a wireless network.





### **Communication Channel Loading**

Properly configured SCADA systems shall be tuned in a way that minimizes channel utilization/loading (air time usage). This is important in order to allow timely/immediate reporting of unusual events and to perform corrective actions without reducing response time for other RTUs, which are not involved in the specific event.

This can be achieved by properly filtering the data communicated via the channel. One must carefully define what status change or level of analog level change should be considered as critical, that requires immediate reporting to the control center.

Reporting by event is the optimal choice selected by the system architect, and this is to be combined with periodic health check (via polling) to verify system integrity. Using this method will statistically assure the most efficient updating the SCADA HMI's database

### **Data Communication Reliability and Security**

During recent years the industry has started to appreciate the need for secure SCADA communications. In order to reach this goal, the operator must trust the validity of indications and parameters seen on the screen and he needs to be sure that all issued commands are accurately and timely implemented at the remote sites.

SCADA systems must be absolutely immune to illegal intrusion attempts, such as recording and retransmitting of commands, modification of communicated SCADA-data, viruses, etc. These challenges can only be met with transmitting encrypted data and by providing a time based stamp attached to each message. Use of low tier PLCs and PLC protocols do not provide these capabilities. The risks of not being able to detect illegal intrusions might cause critical SCADA-operation related failures.

### **System Operating Reliability**

Our experience with implementing SCADA systems has shown that typical life-cycle cost of SCADA- related hardware (RTUs, field sensors, radio modems, antennas, etc.) is 120% - 180% of the initial procurement cost. Therefore the utilized hardware must be built with highly reliable components, tested over a wide operating temperature range -40 deg. C to 70 deg. C, up to 90% humidity conditions, pass rigorous environmental testing such as electrical surges, immunity to external electromagnetic interference, etc.

SCADA RTU modules are to be built with advanced technology components such as Surface Mounted Devices (SMD) and pass accelerated life test (ALT) procedures. To assure long term operating reliability it is not recommended to repair these modules but when needed replaced with new ones. This is important since imperfect repairs might cause unreliable operation and risk of SCADA related consequential damages.

### **Employing a Professional Integrator**

Integrators performing SCADA system architecture design must have in-house expertise in: SCADA hardware and software, and also have in-depth knowledge of the specific application requested by the customer.

The integration process including RTU installation and programming, installation of all communication components and related software must be accompanied by manufacturers support for software issues, warranty replacement, periodic upgrades, etc. This assures long term, reliable and high performance SCADA system operation.



## Highlights of Operating and Cost Benefits Achieved with Motorola ACE3600 RTUs

The following list of technical features clearly highlights the main leading edge capabilities of the ACE3600 Remote Terminals Units (RTUs) that are required to implement a high-quality Supervisory Control and Data Acquisition (SCADA) system solutions.

- ACE3600 RTUs perform reliable peer to peer (RTU-to-RTU) and peer to master communication, allowing extending the geographical coverage for those RTUs which do not have direct link with repeater and not with the Master Control Center (MCC).
- ACE RTUs perform Store and Forward (S&F) operation using a pair or single radio frequency. Prior the data is retransmitted it is verified for data integrity. If an error is detected it is corrected prior retransmission using a packet based retry mechanism.
- ACE3600 RTUs are truly optimal for wide area SCADA communication (hardware, software, protocol) and are ready to be upgraded with features required to assure secure communication, which help to assure system wide operating reliability.
- ACE3600 RTUs have built in capability to perform encapsulation or emulation of other vendors' data protocols, allowing the MCC communicating with a wide range of RTUs, PLCs and Intelligent Electronic Devices (IED) over the communication network.
- 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 implementation of time-based data analysis.
- ACE3600 RTUs have capability to link communication by connecting between 2 or more different wirelesses of physical media, providing geographical coverage via multiple media which can be optimally selected for the SCADA communication.
- ACE3600 RTUs have capability to communicate via digital or analog conventional or trunking networks; VHF, UHF, ASTRO Analog and Digital 800 MHz MAS radios in all bands, wireless IP, microwave, satellite, fiber-optic and telephone line modems, etc..
- ACE3600 RTUs have capability operate in polling by exception and reporting by event modes via a network combining multiple media. When simultaneous events/reports occur, these RTUs have a built-in capability to quickly and reliably clear that condition.
- ACE3600 based data communication data reliability is assured by checking data reliability for each communication segment, using retry mechanism for error elimination. Upon receipt of a correct message, it is reconfirmed to the sending site.
- ACE3600 RTUs seamlessly interface to a wide range of MCCs supplied by leading vendors worldwide. This can be done via RS-232 serial ports, Ethernet using TCP/IP, MODBUS, DNP 3.0, OPC and a range of other SCADA protocols.
- ACE3600 RTUs run the application program in a way which is separately defined from the data communication process. This allows "on-the-fly" modifying their application program or parameters, without interrupting the RTU operation.
- ACE3600 RTUs are designed to operate in an indoor or outdoor environment in extended temperature ranges, e.g. -40°C to +70°C, combined with non-condensing humidity 0-95%. An Accelerated Life test was performed to confirm this feature.
- The integrated power supply built into ACE3600RTUs utilize a high quality 13.8V temperature compensated battery charger, which assures reliable operation, optimal and efficient charging of the integrated Lead Acid battery and assure long battery life.