



How Can SCADA Systems Optimally Operate Over GPRS Networks?

Prepared by: Alex Wainapel, Dan Ehrenreich, Motorola

SCADA solutions are mandatory for upgrading the operating reliability of industrial and utility installations by providing remote control. The commercially available GPRS (2.5G level) wireless networks are not optimal for performance-critical SCADA applications. However, when Motorola ACE3600 RTUs are operating over GPRS using the MDLC protocol, this combined solution allows establishment of a more reliably operating and versatile SCADA system. This paper outlines the technical considerations and main operating and cost benefits achieved with Motorola SCADA solutions operating over GPRS-based communication.

When designing a Supervisory Control and Data Acquisition (SCADA) system based on wireless communication between field-installed Remote Terminal Units (RTUs) and SCADA Master Control Center (MCC), system architects must take into consideration the unique characteristics of the selected network as applicable for the considered system.

Some widely used wireless media for SCADA are: private wireless networks (analog or digital), dedicated wireless Multiple Address Systems (MAS), specialized public digital radio networks such as TETRA, iDEN or ASTRO (APCO-25), Broadband Networks and public cellular services such as the Global System for Mobile communications (GSM) and its General Packet Radio Service (GPRS) providing Internet Protocol (IP) service.

GPRS Communication Overview

The GPRS is a packet data switched technology, using the same infrastructure as the GSM network. The intention for developing the GPRS technology was to provide broadband access "on the move", similar to the wireline Internet service which uses circuit switched ISDN, ADSL, or coaxial cables. Over GPRS, network resources are instantly available when data (message) actually needs to be transmitted across the wireless media. The transmitted data is divided into packets prior to being sent via the wireless modem. Common data applications over GPRS include file transfer pictures, video, Voice over IP, and the ability to remotely access and control industrial installations as described in this article. The GPRS network offers data rates up to of 150 kbps, depending on network availability, channel coding scheme, and data terminal capability. This increase in data transmit rates with respect to GSM (circuit switching method) is achieved by using more than one timeslot of the TDMA frame, however each operator can assign one or more time slots.

GSM/GPRS networks operate in four RF bands: 850/1900 MHz (USA and Latin America) and 900/1800 MHz (Europe, Asia, Middle East, and Latin America). GPRS modems manufactured today, like the Motorola g-24, operate in all four ranges (quad-band).

IP Based Communications for SCADA

With the advent and growing popularity of wired and wireless IP networking, SCADA systems also migrated to the universal IP highway. The benefits provided by implementing IP based solutions are truly significant;

- (a) larger and more efficiently utilized bandwidth;
- (b) standard IP protocols and network applications family;
- (c) improvement of networking and interoperability.



GPRS Communications for SCADA

The GPRS service offered worldwide is attractive for SCADA systems as network operators charge only for the volume of data (IP packets) and not for the connection time as in a circuit switch connection (GSM). In a SCADA system it is required to create a sort of private IP based link between the SCADA control center and the RTUs,. All sites shall ideally have their own pre-assigned Static/Fixed IP address.

However due to the shortage of IP addresses and the IP address space (4-bytes as per IPv2 standard) GSM/GPRS operators are reluctant to allocate a pre-assigned (Fixed) IP address to each RTU. One possible solution is that data communications over GPRS can be achieved by using Dynamic IP addresses which are assigned "on demand" to subscribers for a short session (minutes).

Typically a master SCADA site is allocated a Fixed IP address, and all RTUs have temporary IP Addresses (Dynamic IPs) that are usually dropped after a pre-defined timeout. This operating mode allows the subscriber (RTU) to initiate a session with the SCADA control center but not vice-versa. Once the session is complete or the connection fails, the allocated IP address is released and returned to the common Network Address Translation (NAT) server, holding the available IP addresses. When polling of an RTU is required by the SCADA control center, a solution to obtain and maintain a Dynamic IP Address for each RTU can be achieved by using an RTU-initiated periodic contention message (keep-alive signal).

SCADA systems based on GPRS communication technology may work fairly well, however this solution can be applied only for simple and non time-critical applications. The method described above is not suitable for demanding SCADA applications, as RTUs cannot be frequently polled. This method also does not allow RTU-to-RTU communication. Under the classification of "demanding" or critical SCADA applications we find:

- real-time SCADA system designed for mission-critical systems
- near-real time operating SCADA applications
- SCADA applications serving Electrical Utilities that need system wide synchronization down to msec resolution and transmission of time-stamped messages.
- large SCADA systems with many RTUs, where RTU networking is required.
- wide geographical area SCADA systems that operate over hybrid (multiple media) networks and/or over several GPRS networks
- complex SCADA networks where the requirements call for back-up links, high availability of the communications, and/or operating redundancy.

Traditionally, SCADA applications for real-time or near-real time applications demand suitable networking and reliable solutions characterized by:

- (a) closed secure networks
- (b) point-to-point or high speed point to-multipoint
- (c) non-blocking medium
- (d) short time latency
- (e) synchronized network.

There are some drawbacks in the IP/Ethernet SCADA systems world such as stochastic network (unpredictable latencies) and network vulnerability. These disadvantages can be resolved by using networking solutions that are designed and optimized for SCADA over GPRS. In order to assure adequate operation, SCADA systems serving critical applications must utilize highly reliable communications and shall have at least the following important features:



- communication networks should support immediate availability and be ready for on-demand sessions in both directions between the RTUs and the SCADA control center.
- RTUs should be easily and instantly accessible from the SCADA control center or from another RTU connected to the system.
- to maintain data reliability, lengthy messages, and file transfers reliably; end-to-end acknowledgment within the protocol layers and not just via the application.
- the system must be able to limit the time validity of communicated messages. If a message can not be delivered within a predefined time slot, it shall be canceled with indication on non-delivery to the sending device.
- wireless networks serving SCADA should be secure in order to eliminate illegal access by hackers, electronic abuse attacks, and injection of harmful viruses.
- the system must allow remote diagnostics download & upload of applications and the flexibility to use alternate routing when the main link/network fails.
- use advanced communications protocols suitable for operation over fading radio links, by using advanced error detection (such CRC 32 bit) and error correction schemes (selective ARQ) which are efficient for SCADA.

Naturally, not all GPRS based communications are identical. Simple SCADA devices like standard RTUs or standard PLCs can communicate over GPRS networks using advanced-type GPRS modems with embedded IP stack and having a PC based server. The network in this case is similar to a fixed server-to-mobile cellular subscriber communication rather than being optimized for SCADA.

When a SCADA system uses a public GSM/GPRS network, users should set realistic expectations and remember that there is a compromise between cost and performance, since the operating parameters relating to data traffic are affected by the following factors:

- Network loading might be uncontrollable and unpredictable with a tendency to sudden increase during emergencies (weather conditions, earthquake, terror event, etc.).
- Re-establishing a disconnected IP link might take up to 10 seconds, depending on network loading. This delay might create a problem for time-critical SCADA applications.
- Overloaded networks often cause messages to get lost but this is not confirmed to the sender. These events might in turn trigger additional traffic and result in even more delays due to resending of messages, errors or poorly performing SCADA system.
- While operators are doing their best to ensure good Quality-of-Service (QoS), the GPRS remains a public network and is not a fault-proof system. It might crash due to overload and the service to parts of the network/areas can be interrupted for an extended period.
- In principle SCADA users on GPRS have no priority over regular cell phone subscribers. In some instances depending on the revenue scheme of the operator, other data users (video, news download, game players, etc.) may even be given a higher priority than SCADA users.

Motorola Communications SCADA solutions for GPRS

The optimal choice for all wireless SCADA systems is to use the Motorola ACE3600 RTU with the Motorola Data Link Communication (MDLC) protocol, which helps to ensure optimal system characteristic and reliable wireless SCADA communications.

In systems where it is essential to use the GPRS network where no other solution is available, the customer or system architect must carefully select the most suitable SCADA communication protocol for his application. The GPRS protocol stack allows network operators to implement an IP-based core architecture for data applications.



Simple GPRS modems have limitations, as they can not transfer DNP-3 or MODBUS protocols. In order to accommodate these SCADA protocols, RTUs must be interfaced to a more advanced type of GPRS modem using standard IP communications over serial link and Point to Point Protocol (PPP). The ACE3600 RTU with its MDLC protocol provides an advanced, flexible and effective solution for GPRS communication, and the implementation of the ACE36000 protocol stack for GPRS strictly adheres with standard UDP/IP/PPP stack as defined for SCADA protocols over IP networks.

Fig. 1 below illustrates on the left-hand side the Open Systems Interconnection (OSI) / International Standards Organization (ISO) protocol layers of the Motorola MDLC protocol which runs in MOSCAD, MOSCAD-L, MOSCAD-M and ACE3600 RTUs. On the right-hand side the integrated protocol stack is shown, combining the lower level GPRS stack and including the GPRS physical layer and the IP layers. As illustrated, the implementation of Motorola RTUs is using the GPRS modem in transparent mode.

All communication related MDLC layers remain intact while operating over the GPRS Physical and IP levels. This solution allows retaining a reliable operating communication link to appear as a completely transparent link in the MDLC network.

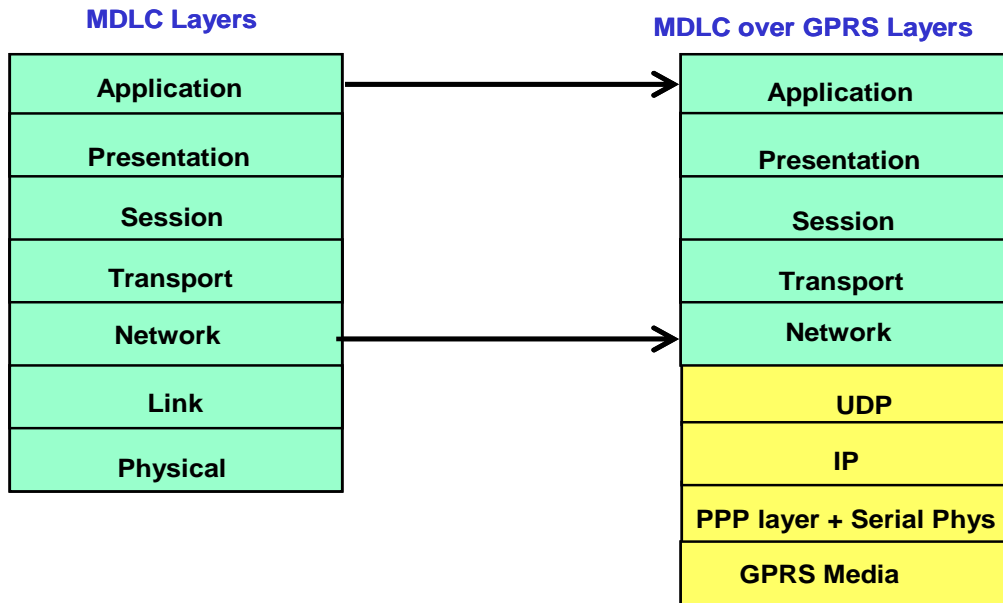


Figure 1 MDLC protocol Stack over GPRS

The proposed ACE3600 RTU based solution over GPRS is significantly different from GPRS networks operating with MODBUS or DF/1. These protocols have only three layers: Physical, Link, and Application. When PLC devices or simple RTUs are connected to the GPRS modem, it necessitates configuring the modem for non-transparent mode and use the full GPRS IP stack. Consequently, the performance of SCADA systems built with PLCs remains limited to the functionality supported by the PLC, such as:

- polling only for data collection by the SCADA master
- local programming and configuration
- limited capability to correct errors (beyond those handled by the GPRS modem)
- use of a single type communication media



Operating Benefits Achieved with MDLC Protocol over GPRS

Motorola ACE3600 RTUs utilize the communication principles defined by the seven-layer OSI/ISO protocol, where each layer is responsible for handling different functions associated with the SCADA process. The following list of technical features clearly highlights the capabilities of ACE3600 RTUs, specifically when operating over GPRS networks or any other IP based media:

- Motorola RTUs have the capacity to perform reliable RTU-to-RTU, RTU-to-SCADA control center, and control center-to-RTU network communications. This is important when upgrading the SCADA system performance by implementing advanced processes.
- Motorola RTUs may be programmed to operate with a wide range of GPRS modems including simple and complex systems. This is achieved by built-in capabilities to optimally configure the GPRS modem operation.
- Motorola RTUs have a built-in capacity to perform encapsulation or emulation of other devices' data protocol, allowing communication with a wide range of RTUs and PLCs. This is important for implementing a mixed system using devices from multiple vendors.
- Motorola RTUs have the capacity to connect between two or more wireless or physical media and route the data through an alternate medium when the main media fails. This is important for providing system reliability even when the main network fails.
- Motorola RTUs have the capacity to be re-programmed by the download of a new application program, configured, and diagnosed. This is all done remotely via the network which helps reduce the cost of system commissioning and maintenance.
- ACE3600 RTUs may perform multiple session operations, meaning that functions such as hardware diagnostics, report-by-event, new program download, etc. are done without interruptions while the normal SCADA operation is running.
- When comparing ACE3600 with PLC programming capabilities it should be noted that ACE3600 RTU is very powerful in handling indexed tables (two-dimensional arrays), while most PLCs work only with vectors (one-dimensional array).

Summary and Conclusions

For large utility systems, mission critical, and time applications, SCADA system architects should consider using optimized and robust communication media. These solutions are available with dedicated wireless networks which can be configured to provide high network availability and channel allocation priority for the SCADA system. Obviously in such cases, the use of a public GPRS network (the same infrastructure used by consumers for video, pictures, download, etc.) as a main communication backbone for the SCADA system should be avoided.

In some cases where the data reliability performance and communication delays are not a critical issue (for example: weather data, meter reading, water levels, etc.) it is possible to use the GPRS network. However even in these cases, the Motorola ACE3600 RTU solution is preferable over the public GSM/GPRS network in order to improve the SCADA system's operating reliability and to provide a reasonable, optimal, cost effective and flexible SCADA solution.

@ @ @ @ @ @ @ @ @ @

For more information on Motorola MOSCAD, ACE3600 and MDLC protocol based SCADA solutions contact: alex.wainapel@motorola.com or dan.ehrenreich@motorola.com