Data Communications for Oil & Gas SCADA Systems

by: Dan Ehrenreich, Shlomo Liberman ***Motorola Inc.***

Automated monitoring and control of Oil and Gas systems is now increasingly being introduced by pipeline operators. Implementation of these modern systems helps achieve trouble free flow of oil or gas along the pipelines, monitoring pressure and flow, detecting leakage and fraud, reducing operating costs, and enhancing employee satisfaction. One of the most important building blocks of such systems is the communications network. Use of advanced communications protocols allows implementation of versatile networking features, remote diagnostics and remote up- and downloading of programs, parameters and databases. This process should be possible without interrupting the normal operation of the system.

Field installed Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs) provide the means for remote control of production equipment at remote sites. Among these are motor operated valves, oil and gas separation chambers, pressure reduction installations, scrapper location monitoring, cathodic protection monitoring, etc. Using advanced RTUs for these systems provide means for smart corrective responses, better utilization of personnel, cost savings, improved reliability, fewer unexpected problems, more reliable operation of the system and enhanced operator & investor satisfaction. When evaluating future investments in communications, investors and system operators often ask some very basic questions:

- Which *specific needs* are to be served, and which new *goals* are to be achieved?
- What are the *various alternative solutions,* and *w*hich one is the *best-in-class*?
- Will the system handle *critical / extreme events* in an optimal way?
- How much will *system upgrades cost,* and which are the *practical alternatives*?
- What *added value and benefits* are achievable with the selected system?
- What is the possible future *migration* path with this system?
- How will the system be able to cope with *future communications solutions*?

Selection of Communications Protocol

It is important to differentiate between radio/wireless (RF) and other media. While physical media such as wirelines and fiber-optics are less prone to interference, radio (RF) is subject to natural noises that may cause errors. Integration of a modern SCADA system requires use of a seven layer protocol that was designed according to the guidelines provided by the International Standards Organization (ISO) for Open Systems Interconnection (OSI). ISO/OSI type protocols separate the communications handling from the application functionality. By using a layered protocol approach in SCADA systems, the programmer does not need to deal with features such as; system diagnostics, networking, error detection, correction and message retry mechanisms.

There is no standard protocol for SCADA communications which is accepted worldwide. SCADA vendors offer numerous implementations of three layer and seven layer protocols. However, most of these protocols are incompatible with each other. Protocols used in SCADA systems such as the DNP 3.0, IEC 870-5-101/-5-103, and others implement <u>only three layers</u> of the ISO/OSI stack: Physical, Link, and Application. They leave out the <u>important</u> *Networking layer* function. Without this feature, the data network can not route messages via multiple nodes (between the RTUs and the Master Control Center), which limits the communications configuration to direct links or use of line-of-sight channels. In addition, due to lack of separation between the communication functionality and the SCADA system application program, the programming of the system is more complicated, costs more, and is less “open” for later upgrades.

Protocol Features

The use of seven layer protocols in radio frequency (RF) based system has been known for years but is still relatively unknown in Oil & Gas applications. It facilitates the design of advanced systems, in which the communications system is optimized for the specific application and type of medium. This allows a large number of RTUs to use a common infrastructure and share available RF channels. A seven-layer protocol over radio offers a grade of data reliability, similar or superior to that encountered when using wireline communications. The Motorola Data Link Communications (MDLC) protocol implement these features, and is well suited for SCADA and for integration of multiple types of communications media into a single network. The tasks of the ISO/OSI layers are shown in Figure 1.

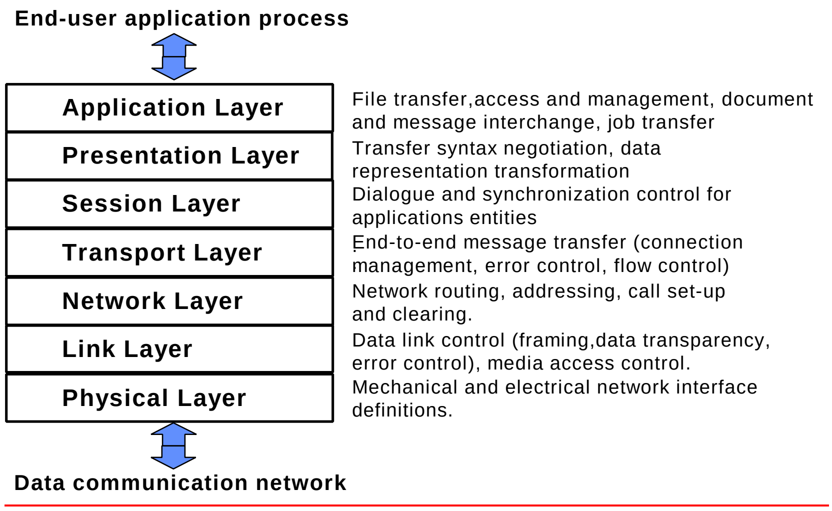


Figure 1. ISO/OSI Protocol Structure

The basic data reliability of the seven layer MDLC protocol is achieved within the Link Layer. In a radio environment, it is imperative that a powerful CRC-32 error detection code be appended to every transmitted frame. This error detection mechanism makes it virtually impossible for a frame containing a digital transmission error to go undetected by the receiving RTU. Upon reception of a message, every frame is checked for errors and a positive acknowledgment is sent to the transmitting RTU side. If an error is detected, no acknowledgment is issued, the damaged frame is discarded and the transmitting end RTU will automatically resend the related frame. This action is called a *link retry*. By comparison, three layer type protocols will resend either the entire transaction or the remainder portion of the message, starting from the frame in which an error was detected.

The *Network and Transport layers* provide the next level of end-to-end data integrity. The network layer is responsible for routing the information through selected RTUs in the system over one or more media. One of the roles of the network layer is to establish an alternate communications path between end points in case the primary data path becomes unusable.

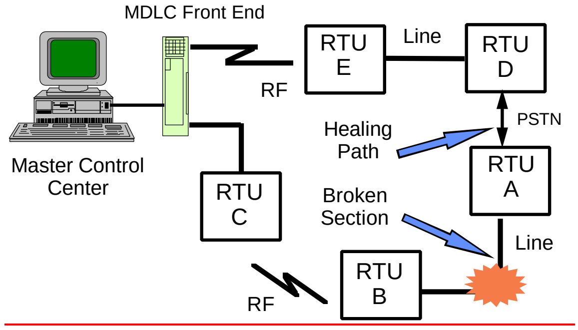


Figure 2. Communication Path Restoration

In Figure 2, the communication between RTU “A” and the MCC is established via RTU “B” and “C”, both of which act as communication nodes. Assume that the link between RTU “A” and RTU “B” fails. In order to restore the link between RTU “A” and the MCC, the Network Layer will automatically activate the PSTN line between RTU “A” and RTU “D. The result is, that a problem in the primary communication link (A to B) does not lead to total system failure.

The *transport layer’s* responsibility is to confirm end-to-end integrity of the information. If the receiving RTU detects a “gap” in the received frames, it will request the originating RTU to resend *only* the missing packets. This process is known as a *transport layer retry*. A full frame retry will occur only if most of the information is lost due to a major disruption in the network. The *Session layer* offers extra protection by synchronizing lenghty transactions. This is of major importance particularly when an interference causes an interruption in the middle of a transmission. Synchronization by the session layer allows the application to continue sending the message from the point where the communication was interrupted, without the need of resending the message from the beginning. This feature reduces response time and saves precious radio air time.

Performance comparison

Selecting the optimum data protocol for an RF network (whether Conventional or Trunked radio, Spread Spectrum radio, Multiple Address Systems - MAS, Satellite communications or Shared data networks), poses a problem for anyone who is not an expert in data communications. The considerations for selecting an appropriate communications medium and data protocol need to be properly explained, since selection of the communication protocol affects the overall performance of the system. The discussion that follows outlines the most critical and important considerations selected for the purpose of comparison among system concepts.

System throughput for lengthy messages

The ideal Oil and Gas SCADA protocol should have the capability to communicate using variable length messages, and its *effective throughput* should be unaffected by the message length. In the MDLC protocol, the number of frames sent during a single transmission can be programmed and, if an error occurs, only frames received in error will be re-transmitted. Other protocols commonly used in SCADA systems, such as DNP 3.0 and IEC 870-5-101, use a stop-and-wait mechanism in which the next frame is transmitted only if the previous frame was successfully received.

Calculation of channel loading

Selection of a specific Channel Access method obviously affects the “air time utilization” and the total channel loading. The channel access mechanism used by the link layer of the MDLC protocol provides very fast update of the database and the display at the SCADA central. Figure 3 shows the results of a simulation for a SCADA system using variable data rates. This chart addresses the common misconception voiced by some system designers who claim that a higher channel data rate always results in higher data throughput. The chart presents the average delay for the MDLC protocol transmitted via radio at various channel bit rates, compared to a polling scheme (such as used by some three layer protocols).

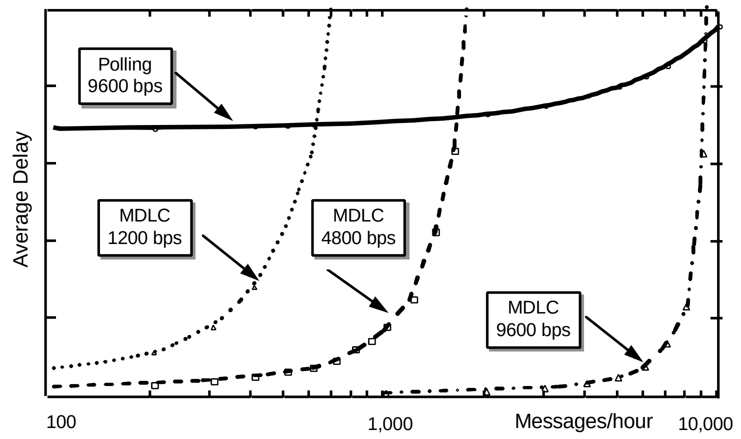


Figure 3. Polling vs. Contention-type Reporting

Protocol Interface

A main component in a SCADA System is the Master Control Center (MCC). It may consist of a single site computer or a multi-site networked control center. In an integrated system, RTUs are linked to the MCC via a single or multiple communications media and may also directly communicate with other RTUs over the same data network. The operating performance of a SCADA system depends on the communication capability and robustness of the data protocol. Some of the most important characteristics normally requested for a modern system are:

- Fast communication/priority for commands initiated by the *MCC* and alarms reported by RTUs
- Efficient handling of simultaneous reporting by many RTUs
- “Air-time-efficient” polling of all RTUs linked to the data network
- Provision for automatic back-up redundancy in the communication network

- Additional operating features such as:
  - ◊ Efficient integration of multiple media into a single network
  - ◊ Transmitting simultaneous messages to all or a selected group of RTUs.
  - ◊ Peer-to-peer links involving any pair of RTUs (using more than one media)
  - ◊ Providing 100 % communication coverage by using data Store & Forward (S&F) solutions and communications nodes connecting multiple media.
  - ◊ Efficient solutions for maintenance of RTUs over the communication channel

Connectivity

Independently of the selected MCC protocol, each MOSCAD RTU in the field may interface directly to a wide range of field sensors, typically using their specific protocol. In Figure 4, the MOSCAD RTU interfaces over the RS-485 multi-drop serial port to a set of smart sensors. From the communications perspective it must be noted that there is no direct logical link between the MCC and the sensors. The MCC talks only with the MODBUS Front End processor (FEP) and the sensors talk only with the MOSCAD CPU, which acts as a data concentrator for these sensors. Use of the MDLC communications protocol allows integration of additional services along with the SCADA system. For example, a SCADA system may integrate transmission of video image snapshots (slow-scan video) directly from the site to the control center. In case of an alarm this feature may serve for confirmation of the reported event. In this case, the control center supports both the SCADA application as well as reception of video images from remote sites.

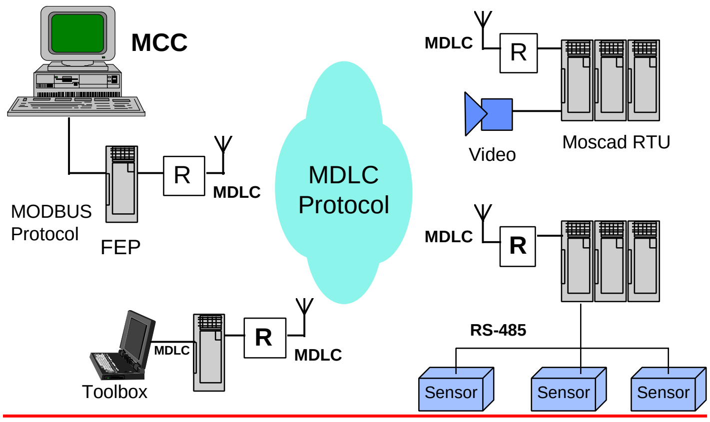


Figure 4. MODBUS Interface to a Wireless System

Integration of a system using multiple protocols

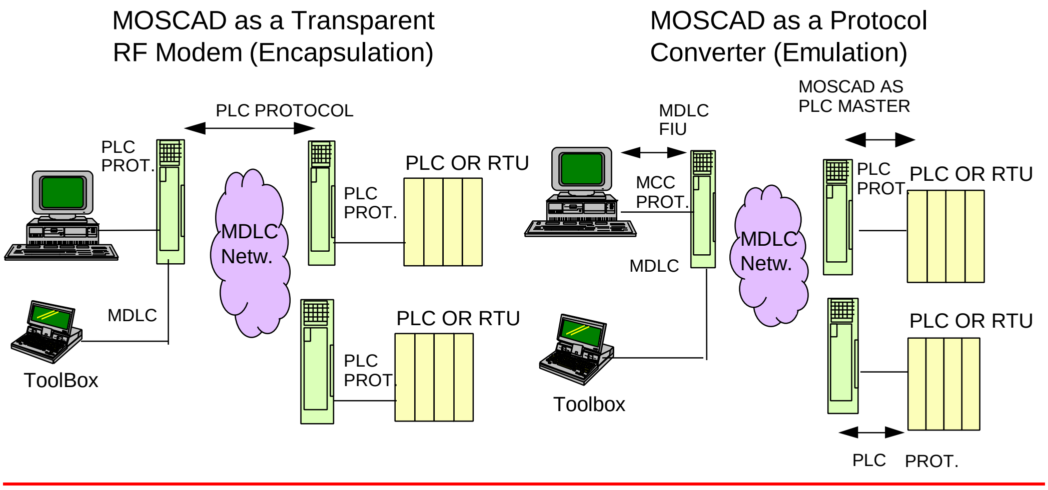
In an evolving SCADA system, there may be a need to connect several existing devices (sensors, PLCs) with new ones that were supplied by different vendors. It may be expected for these units to use different protocols. This requirement is very common in SCADA system upgrade, retrofit and expansion projects. There are a number of solutions that allow linking MCCs with RTUs and PLCs that use different communications protocols. Two valid concepts are: *protocol emulation and protocol encapsulation*. Both are acceptable and the selection depends primarily on the sensors used and on the preferred communications network.

Protocol encapsulation

In this case the MCC and the RTUs/PLCs are connected to a pair of smart RF Modems which encapsulate and de-capsulate the RTU/PLC and MCC protocols with the MDLC protocol serving as a cocoon (all encapsulated protocols must be of identical type). During transmission, the MDLC based RF network provides absolute data transparency to "its users" and does not interfere with the RTU/PLC/MCC message (monitoring, alarms, control, etc.) which the original protocol carries. An illustration of a network utilizing the encapsulation concept is shown in Figure 5a.

Protocol emulation

The configuration in Figure 5b also uses a pair of MDLC based smart RF Modems. The RF modem at the MCC site is acting as a Front End Processor (FEP) and communicates with the MCC using its native protocol. At the remote site, the PLCs/RTUs are polled by a second RF modem using the protocol of that RTU/PLC. In this case, the MCC and each RTU/PLC may use *different protocols.*



(a) (b)

Figure 5. Encapsulation vs. Emulation of Protocols

Summary

This paper summarizes the needs and benefits of advanced communications solutions for automating Oil and Gas infrastructures. The unique benefits of using a seven layer protocol are expressed in terms of more reliable SCADA system operation, the ability to integrate multiple media into one communication network, cost effective utilization of the available communications infrastructure, etc. The use of modern seven layer protocols such as MDLC results in many additional improvements including simpler programming resulting from the separation of the communication and the application functionality, simplified and less costly system upgrades, retrofits and expansions, and improved maintenance procedures. The integration of advanced communications protocols with radio based SCADA systems generates major operating benefits that more than justifies the investment.

Dan Ehrenreich *is Marketing Manager for SCADA Business Development at Motorola. He received his B.Sc. in Electronics Engineering in 1975, and joined Motorola in 1991. Dan may be contacted at email:* *b10002@email.mot.com* . *For more details refer to website* ***motorola.com/moscad*** *(no need for* ***http://www****)*

Shlomo Liberman *is Regional Distribution Manager in Asia-Pac for Motorola Data products. He received his M.Sc. in Electronics Engineering in 1974, and joined Motorola in 1978. Shlomo may be contacted at email:* *bcms87x@email.mot.com, tel (852) 2966-4368, fax (852)-2966-4388.*