

Modern RTUs and Advanced Protocols Enhance Operation of Oil & Gas SCADA Systems

Authors: Dan Ehrenreich b10002@email.mot.com
Shlomo Liberman bcms87x@email.mot.com



<http://www.motorola.com/moscad>

Abstract

Supervisory Control And Data Acquisition (SCADA) for monitoring of oil and gas systems is now increasingly implemented for pipelines. One of the most important building blocks in such operations is the communications network. ¹⁾ Widely used communications media in these systems are fiber-optic links, dial-up and leased telephone lines, analog Trunking radio systems ²⁾ and digital wireless networks. Modern communication systems allow sending messages from any remote site to any remote site in addition to the control center. Use of advanced communications protocols allows implementation of networking features, remote diagnostics and calibration (“over-the-air”), up- and downloading of programs, parameters, databases, etc. Motorola as a leading provider of data communications solutions introduced the MOSCAD system and the Motorola Data Link Communications (MDLC) protocol in order to provide reliable and advanced solutions for wide area SCADA systems while at the same time preserve OPEN PROTOCOL Standards interfaces

Introduction

Reliable operation of oil and gas pipelines requires reliable communications solutions. SCADA systems play an important role by providing the means for reliable fault detection and safe control of the entire infrastructure. Utilizing advanced Remote Terminal Units (RTUs) such as the Motorola MOSCAD facilitate timely and smart corrective responses, better utilization of personnel, fewer unanticipated problems, cost savings, and enhanced employee satisfaction. When evaluating investments in communications for a SCADA system, senior managers ask some very basic questions which recently put more focus on communications:

- Which operating *functions* need improvements?
- Which new system *goals* are to be achieved?
- What are the *best-in-class alternative solutions*?
- Will the system handle *extreme events* optimally?
- What *added benefits* are achievable with the system?
- What is the future *migration* path for this system?
- Will the system cope with *future communications*?
- Will the solution yield *Return-On-Investment (ROI)*?
- Which *vendor* can provide a long-lasting solution?

Communications Media and Protocols

SCADA system implementation starts with a clear definition of operation goals and definition of ultimate needs, which are expected to be required in the future. Selection of the proper communications media and the protocol are very important and must be taken into consideration already at the system design phase. While physical media such as wire-lines and fiber optics are less prone to interference, it is widely known that wireless media might be affected by natural noises and interference on the same channel. However, this media has many important advantages and operating benefits, which should be taken into consideration while designing a radio based SCADA system.

Integration of a reliable SCADA system requires use of a seven-layer data protocol such as MDLC that matches the guidelines provided by the International Standards Organization (ISO) for Open Systems Interconnection (OSI). Data protocols, which are structured according to the ISO/OSI suite, allow separate handling of communications functionalities from the application functionality related to the transmitted messages. By using such an approach, the system programmer does not need to deal with complex communications functions such as system diagnostics, network routing, error detection, message retry mechanisms, etc. These are taken care of by the protocol structure, and thanks to this, the system programmer has to worry only about the application program.

Systems, which utilize the MDLC communications protocol, are better prepared for future system expansion and for upgrading their operation with extended capabilities and improvements without losing any part of the investment spent on the original installation. Implementation of secured interface to an Internet protocol (IP) network, time synchronization over the communications network etc., may be added to a specific layer within the communications protocol, without affecting the application program.

Using the technology and system solutions described in this paper, Motorola has integrated hundreds of systems worldwide, containing tens of thousands of MOSCAD RTUs. In addition to Oil and Gas systems, these RTUs successfully operate in a wide range of other applications such as electricity Distribution Automation (DA), public safety and security, communications network monitoring water and waste-water and other SCADA systems.

It is a widely known fact, that as of today there is no SCADA communications protocol standard, which is accepted worldwide. In light of this situation, system providers use various types of de-facto accepted protocol implementations such as the DNP-3.0, IEC 60870-5-10x, and others. These protocols are derivatives of the TC-57 IEC workgroup and implement only three layers of the ISO/OSI stack: *Physical*, *Link*, and *Application* Layers. Figure 1 outlines the descriptions of the specific protocol layers of the seven-layer ISO/OSI suite.

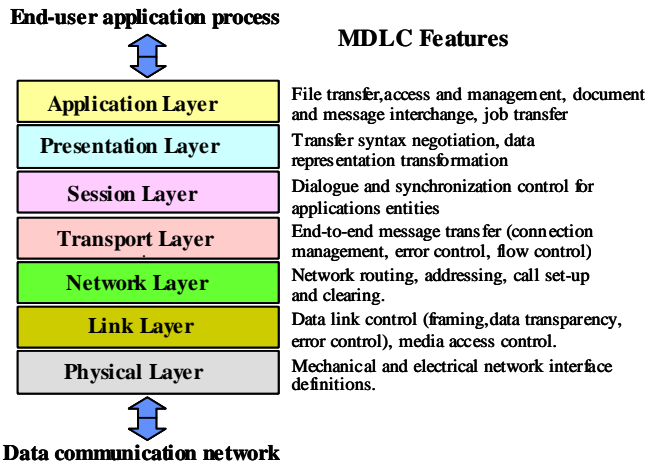


Figure 1 – ISO/OSI seven-layers of MDLC

Being three-layer type protocols, they leave out the important *Network layer* function (Layer 3). Without this feature, the data network cannot route messages between the RTUs and the control center in a flexible way, which limits the configuration to direct (point-to-point) links or use of line-of-sight wireless channels. Alternate routing can therefore not be automatic, and needs to be programmed for each specific system. In many SCADA systems, the availability of an automatic back-up communication link is mandatory, so lack of the networking feature is a severe limitation.

The basic data reliability is achieved within the *Link Layer*. This is imperative for wireless media, which require a powerful CRC-32 error detection code to be appended to every frame. This type of error detection mechanism makes it virtually impossible for a frame containing a digital transmission error to go undetected by the receiving RTU or even by the digital data repeater. Upon reception of a message, every frame is checked for errors. If no errors are detected, the frame is passed to the upper layers for further handling. The next level of data reliability is provided by the *Network* and *Transport Layers*, which are responsible for routing the information via selected RTUs in the system.

In the example shown in Figure 2, the communication between RTU “A” and the MCC is established via RTU “B” and “C” which both act as communication nodes. Assume now that the link between RTU “A” and RTU “B” fails. In order to restore the data flow between RTU “A” and the MCC, the *Network Layer* will activate the PSTN link between RTU “A” and RTU “D”, which acts as a node. The important benefit is that a data link problem (between sites A to B) does not result in total system failure.

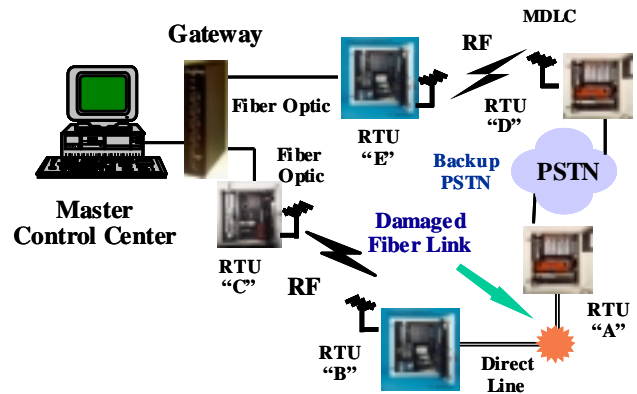


Figure 2 – Automatic Alternate Routing

Protocol Features

The mostly visible 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. The following list provides some important features normally required in a high performance SCADA system:

- Immediate transmission of control center commands and immediate attention to alarms reported by RTUs.
- Efficient handling of “avalanche of messages” received at the MCC; i.e. simultaneous reports from multiple RTUs (due to the same or related event).
- Built-in protocol solution for automatic back-up links in the system to provide network redundancy.
- “Air-time-efficient” communications to/from all RTUs linked to the data network.
- Efficient integration of multiple communications media (radio, lines) into a complete network.
- Transmitting simultaneous messages to a group of RTUs, e.g. for Emergency Shut Down (ESD) operation.
- Peer-to-peer communications; involving multiple RTU sites (using the same or different media).
- Coverage extension created by Store & Forward (S&F) repeaters and nodes connecting multiple media.
- Solutions for remote maintenance of RTUs over the network eliminate trips by helicopter or terrain vehicle.

Integration of IEDs Using Multiple Protocols

In a new or upgraded integrated SCADA system, there may be a need to connect new Intelligent Electronic Devices (IEDs) to the RTU such as sensors and PLCs, side-by-side with existing ones. Consequently, it may be expected for these units to use different data protocols. To perform this connection there are a number of solutions that allow linking the SCADA control center to IEDs and sensors, which use different communications protocols. To carry out this integration, there are two basic concepts:

- *Protocol emulation*
- *Protocol encapsulation*

Both solutions are acceptable and the selection depends primarily on the data flow (communications) in the network between the RTU and the control center.

Protocol encapsulation; In this case the control center and the PLCs are connected to a pair of smart MDLC protocol based RF Modems. These encapsulate and de-capsulate the messages between the PLC and control center protocol while the seven-layer protocol serves as a “wrapping” cocoon. During message transmission, the data network provides absolute data transparency to "its users" and does not interfere with the transmitted message (monitoring points, alarms, control, etc.), which the originating protocol carries. The advantage of this solution is, that any data protocol can be transmitted over the network and that the implementation requires no detailed knowledge of the message content sent via the originating protocol. The network protocol, makes sure that data integrity is guaranteed. An illustration of a network utilizing the encapsulation concept is shown in *Figure 3*.

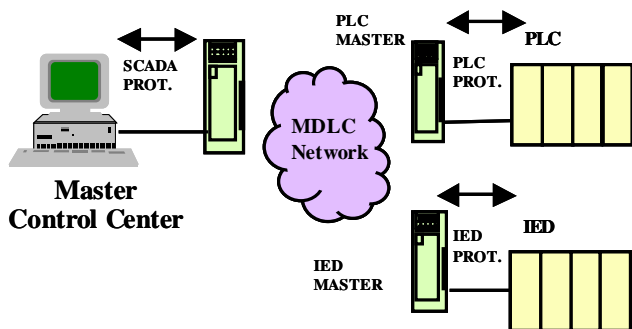


Figure 3 – Protocol Encapsulation

Protocol Emulation; The configuration in *Figure 4* also uses a pair of MDLC protocol based RF Modems. In this case, these RTUs perform protocol translation (*emulation*), to assure reliable passage of the transmitted data over the network. At the remote site, the IEDs/PLCs are polled by a second RF modem using the protocol of that IED/PLC. In this case, the control center and each IED/PLC may use *different data protocols*. This feature itself provides great benefits to the system operator, as it allows connecting all existing and future units into a fully integrated system. *Emulation* is preferable when the originating protocol is unsuitable for over-the-air transmission, e.g. by requiring frequent and fast polling responses, such as MODBUS or other common PLC protocols. If such a protocol is used in *Encapsulation mode*, the channel would be overloaded.

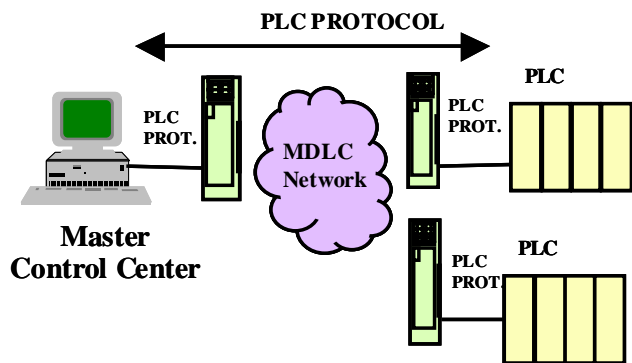


Figure 4 – Protocol Emulation

Open System Connectivity

In a typical system, not all RTUs use the same media across the network since the same communications backbone may not be available. In addition, 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.

Figure 5 shows how the MDLC seven layer protocol is utilized to provide OPEN connectivity between a range of control centers, RTUs and PLCs supplied by multiple vendors and integration of these multiple protocols into a complete SCADA system.

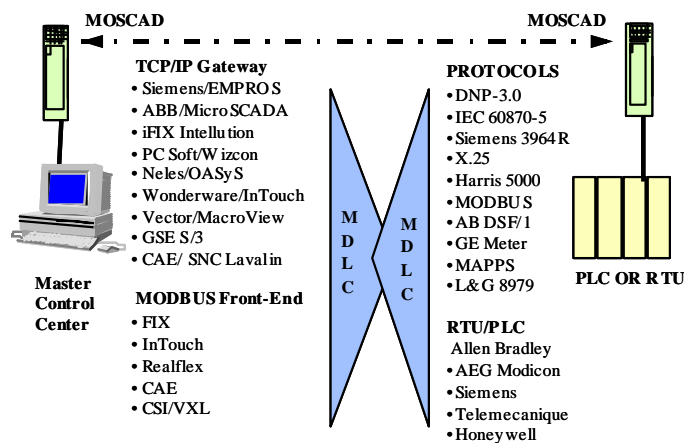


Figure 5 - Open System Connectivity

Wide Area Network (WAN) Connection

Operation of modern SCADA systems is based on reliable wide area communications. This means that remotely controlled sites must be able to communicate with the control center either directly or via communications nodes. It is also required that remote sites can be linked to the network using a wide range of communication media, including; lines, telephone network, microwave, satellite, fiber optics, narrow band analog or digital wireless network, or any combination of these.

In order to assure cost effective system design, it is preferable that each RTU will have the capability to act as a communications node or a Store and Forward (S&F) repeater, serving other field RTUs, which do not have direct communication with the control center.

In order to implement such a feature, it is required that the selected communication protocol is based on the seven layers ISO/OSI protocol suite, such as the MDLC protocol, which was specifically adapted for radio media. Use of an advanced seven-layer communications protocol allows integration of additional services side-by-side with the SCADA system.

Figure 6 shows a simplified system, in which RTUs act as communication nodes and repeaters.

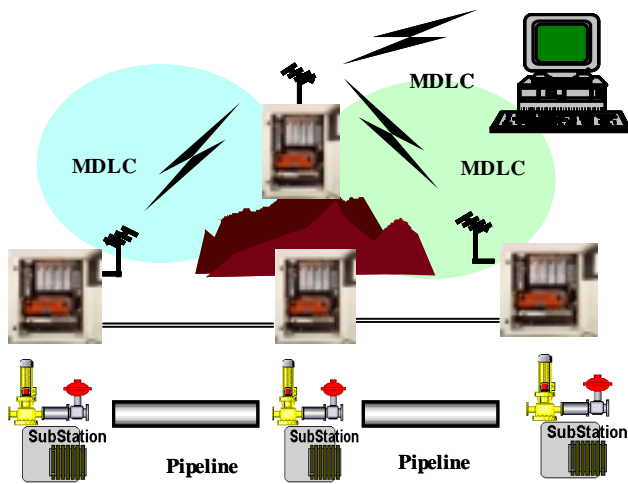


Figure 6 – RTU as Store & Forward Data Repeater

The RTU, which serves as an S&F repeater, actually tests the message content and verifies if it is directed to that site or it is required to retransmit the message to another RTU. This can be performed thanks to the availability of the *Network Layer*, which is part of the data protocol.

Another desirable protocol feature is that upon reception of the message from the source RTU, the MDLC protocol performs data integrity testing, using a CRC-32 error detection code, which is embedded in the seven-layer protocol. Only those data packets, which are detected with errors, will be retransmitted upon request issued by the S&F repeater or the final destination RTU. Upon reception of the correct packets, these are being re-inserted into their original time slot, and transmitted to the next destination site, which will again test the integrity of the received packets. Once the complete message is received by the destination site (RTU or MCC), it will issue an end-to-end confirmation, a function of the *Transport Layer* Direct IP Connection

Pipeline engineers who plan new installations nowadays pay more attention to modern communications. The reason is that in order to assure safe pipeline operation as well as to perform computerized control by a SCADA system, pipelines are now monitored at many more points and subsystems. RTUs, installed along the pipeline are designed to perform pressure and flow measurements, cathodic protection equipment monitoring, leakage detection, valve control, scraper station monitoring, gas pressure reduction and compressor station monitoring and also *Custody Transfer* calculations.

While in the past, these RTUs primarily used microwave and satellite communications, today the recently installed pipelines include a fiber optic link, installed alongside the metal pipe. Having this type of high performance media available for pipeline control allows implementation of high-speed data networks, using Internet protocol (IP) connectivity directly at the RTU level. See *Figure 7* for a system concept involving IP connected RTUs.

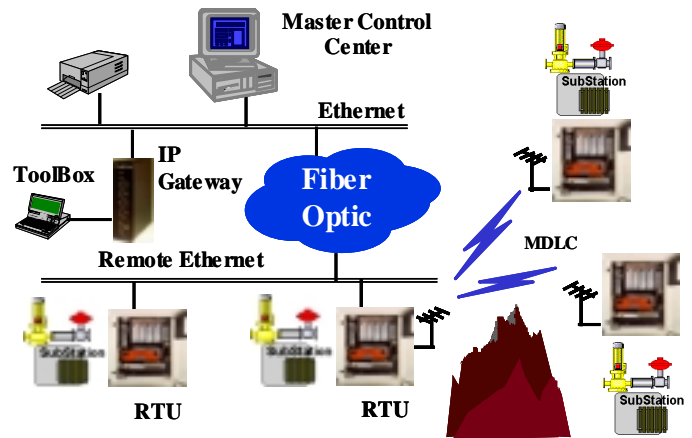


Figure 7- SCADA over IP

SCADA System Maintenance

In order to rely on the operation of the entire infrastructure, reliable SCADA communications must be assured. However, from time to time there may be a need to verify whether the message received from a specific site indeed reflects the true condition at the site, or is the result of a malfunction of the RTU.

In such cases, it is highly desirable, that an embedded diagnostics feature will be in place. This allows monitoring operation of specific hardware or software functions at the remote site, and when a problem occurs, log the relevant information in a Diagnostics Data Logger, which is an integral part of the RTU. Having this feature in place, allows speedy analysis of almost any problem, which happens at the remote site and helps the operator to make a decision on how to react and to fix the detected problem.

When a SCADA system is being expanded, upgraded, or modified, it may be required to update the application program running at the remote sites via the communications link. Since oil and gas installations are often spread out over remote and vast areas, a high tier SCADA system must include a set of remote maintenance functions such as:

- *Remote download of updated application programs* to RTUs via the network and MDLC protocol. This is required in order to upgrade or modify the operation at remote sites and save costly traveling time.
- *Remote download of operating parameters* to RTUs via the network. This is required in order to optimize the operation at remote sites.
- *Remote calibration* process for analog measurement ports. This feature is required to eliminate the need of frequent traveling of maintenance people to sites just for the purpose of analog port calibration.
- *Remote time synchronization* of sites down to a resolution of 2 msec. This feature is required in order to analyze specific events along the pipeline network (specifically detects which of the events occurred first).

Innovative Communications-Based Functions

Transmission of video image stills: Reliable operation of a remote infrastructure often requires having an alternate way of verifying the reported event, in addition to what was reported via the SCADA system, to avoid false sensor alarms to cause costly maintenance trips. One solution can be the use of image stills, which can be transmitted from the remote site to the control center. As seen in *Figure 8*, a video camera is directed to the supervised remote equipment or installation. Once an event, which requires attention is recorded by the RTU, the camera is turned on to capture a still picture. In order to allow sending this picture to the control center, the typically very large data image file (5-25 Mbytes) is being adjusted to lower resolution, and compressed to a smaller file. The outcome of this process is a manageable file size of 5-15 Kbytes, which can be transmitted over a narrowband wireless or line media in a matter of 3-30 seconds (depending on the channel quality).

In addition, the operator can request the MOSCAD RTU to capture a specified set of still pictures (up to five consecutive stills) and have these transmitted to the control center. This will create a short slow-scan image sequence and assist the operator in his decision making process.

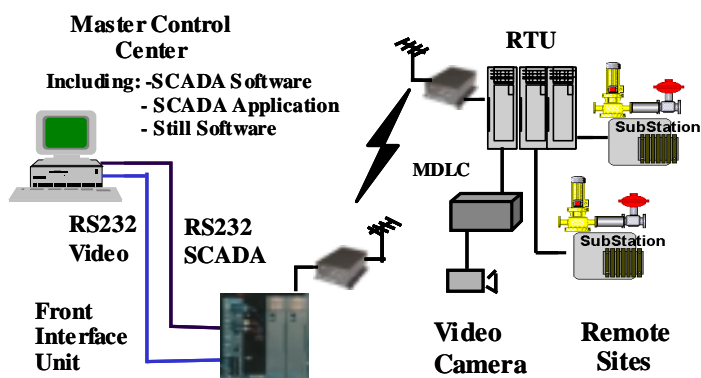


Figure 8.- SCADA Plus Video Image Stills

The connection to the control center is done via two serial ports, one for SCADA type messages and one for the image stills received by the wireless modem.

Instant Pager Notification: Maintenance people spend most of their time in the field, and communicate with their office via wireless media. In case an emergency takes place or any event that requires their immediate attention, they typically are being notified via a pager and asked to call their head office for further instructions. Today, when most communications networks are digital, it is possible to link these field teams directly to the SCADA network. As shown in *Figure 9*, the message transmitted between a specific RTU and the SCADA control center, is being directly sent to the pager transmitter. Once the message is transmitted over the paging system, the maintenance person will instantly see the message. For example: “Station 52 shows high pressure” which is identical to the message that appears on the SCADA operator’s screen. This will allow the service person to respond immediately, without contacting the operations center for further instructions.

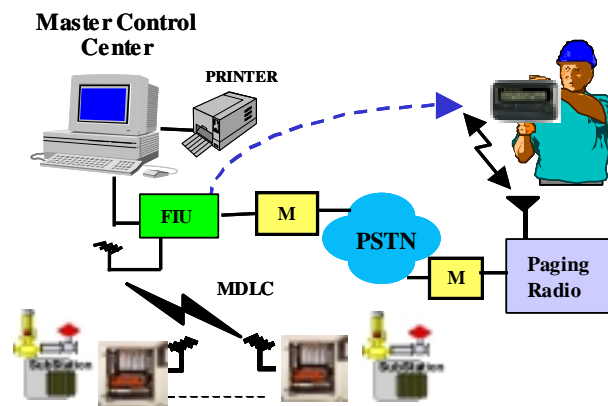


Figure 9 – SCADA with Paging Interface

The paging operation can be provided by a private system, if such is owned by the company, or it can take advantage of a public paging operator. Most paging operators provide computer dial-up or leased-line access to their system.

Enhanced System Operation

Modern SCADA systems can provide innovative solutions which otherwise could not be implemented. Among these are: implementation of closed loop control along pipelines, smart decisions made locally by the RTU software, etc.⁷⁾ A modern RTU can make decisions based on the following:

- Its own application program
- Locally monitored analog and status conditions
- Parameters downloaded from the control center
- Intervention from the control center
- Imported data from other RTUs in the network

In our case, the MOSCAD RTU can be programmed to make local decisions based also on status conditions and analog levels imported from other RTUs. This type of Peer-to-Peer communication is possible if the system is implementing a seven-layer type communications protocol, like the MDLC, which includes the *Network Layer*.

Summary and Conclusions

Use of a high quality and advanced data protocol such as the Motorola MDLC protocol, allows implementation of unique functions such as system diagnostics, remote calibration, smart RTU decisions based on imported data (from another RTU), update of programs via the network, download of new operating parameters, interface to paging and transmission of video still images.

Use of the MDLC protocol in a wide area SCADA system as described in this paper, results in simplified programming, less costly system upgrades, retrofits and expansions, and improved maintenance procedures. The integration of advanced communications protocols and existing OPEN PROTOCOL interfaces with wireless SCADA systems generate major operating and cost benefits, which more than justify the investment.