MOSCAD TECHNICAL NOTES

COMPARISON OF THE MDLC AND HDLC PROTOCOLS

The MOTOROLA MDLC protocol implements all seven communications layers of the Open System Interconnection (OSI) model. The recommendations of the OSI model are, of course, of a general nature and must be adapted to the type and media of the communications.

The MDLC protocol is designed for optimal operation in SCADA systems which use a variety of communications media such as radio, trunked radio, lines, etc. (which constitute the physical layer of the protocol).The HDLC protocol, however, **does not implements fully even two layers** of the OSI model, namely the link layer and part of the physical layer.The link layer of the MDLC protocol may be compared to the HDLC protocol, but before performing such a comparison, the following particulars must be emphasized:

1. The MDLC protocol is designed to operate in communications networks, that is, systems that incorporate connections between a large number of radio systems and line systems. The protocol enables communications between all sites in the system, including communications for diagnostics purposes, to any system site from any system or external site.

2. As opposed to the MDLC, the HDLC protocol is designed to support communications on a single channel between a control center and RTUs.

3. Among others, the following features are incorporated in the MDLC protocol's layers:

   a. Data authentication (To be implemented)

   b. Data encryption (To be implemented)

   c. Data compression (To be implemented)

d. The capability of efficiently sending short packets with low overhead as well as large quantities of data, for example, for program downloading.

e. The capability of maintaining a practically unlimited number of logical channels per each site, over one or more physical channels.

The link layer of the MDLC protocol incorporates all the benefits of the HDLC protocol as well as a number of additional features which constitute a significant advantage.

* The FLAG (frame synchronization) that appears at the beginning and at the end of every frame is identical to that of the HDLC protocol.

* The address to which the frame is directed appears at the beginning of the frame as in the HDLC. The MDLC supports up to 65,000 addresses. The unit receiving the MDLC protocol detects four different addresses:

  a. The site's specific address.
  b. The base system address (for broadcasting purposes).
  c. A dynamic address that enables automatic routing of data in the networks to the control center that is operational at that given time.
  d. A spare address (for future use).

* The CRC at the end of MDLC frame is of 32-bit length in accordance with CCITT recommendations and gives very good protection against errors. The CRC in most HDLC systems is of 16-bit length only. To get the feeling of the strength of 32-bit CRC formula versus 16-bit here are both formulas:

32-bit: - $X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^{8} + X^{7} + X^{5} + X^{4} + X^{2} + X^{1} + 1$

16-bit: - $X^{16} + X^{12} + X^{5} + 1$

* The frame numbering mechanism of the HDLC assumes that a unit receives data from only one unit, usually the control center, at any given time.

  In radio systems or in multi-drop line systems, which are widely used in SCADA systems, every unit that accesses the communications channel transmits to more than one unit in the course of a single transmission. Therefore, every unit may receive data from more than one unit before it has the possibility to respond with an acknowledgment message. The MDLC is provided with a frame-numbering and acknowledgment mechanism design especially to handle and solve this problem.

* The HDLC protocol comprises one address - the address of the unit to which the transmission is directed. The MDLC protocol, which supports communications between any two units on the channel or in the network, contains, at the link protocol level, also the address of the transmitting unit. The use of two addresses in the link layer, provides higher flexibility at the channel level such as network support, support of several control centers on the channel or in the network, etc.

* The MDLC protocol provides sophisticated broadcast communication that allows formation of an unlimited number of site-groups according to various categories. Broadcast commands can then be sent to each such group separately. This MDLC feature, supported by the higher protocol levels, is based on the link layer's capability to respond to four different addresses. It can therefore be viewed as a Multi-link layer.

Table 1. MDLC-HDLC Comparison

FEATURE	MDLC	HDLC	BENEFIT
Full seven layer OSI	Yes	No, only two layers (physical and link)	No additional programming effort to implement full OSI
Adapted for RF or multi-drop configuration	Yes	No	Efficient for SCADA in radio/multi-drop environments
Point-to-multi-point support	Yes	No	Ability to communicate from any site (RTU or control center) in the network to any site
Data encryption	Yes	No	Secure data transmission
Data authentication	Yes	No	Encrypted data is keyed and validated so retransmission cannot cause false alarms
Data compression	Yes	No	Efficient data transmission
Full download/upload capability	Yes	Yes	Allow full remote reconfiguration
Remote diagnostics	Yes	No	Full hardware/software diagnostics at any point in system
Remote retrieval of error logs	Yes	No	Full documentation of errors at RTU
CRC	32 bit	16 bit	Better error detection
Multiple addressing	Yes, 4	No	Supports broadcast and multiple masters
Dynamic broadcasting	Yes	No	Transmission hierarchies can be dynamically changed

LEGEND:

(shaded) To be implemented

APPENDIX

COMMUNICATION AND PROTOCOL

The RTU supports a variety of communication media and data rates:

- On conventional radio (Direct FM modulation) up to 4800 bps.
- On trunked radio up to 2400 bps.
- On wire-line, depending on its quality, up to 2400 bps.
- Via the RS-232 and RS-485 communication ports, up to 9600 bps.

* The RTU is capable of communication with the hierarchy(s) above it (RTU-to-control center), with hierarchy(s) parallel to it (RTU-to-RTU) and with hierarchy(s) under it (another RTU). The RTU is also capable of relaying messages through it to other RTUs (Store and Forward).

* The RTU can relay messages between line and radio and vice versa.

* The RTU with its protocol is capable of downloading/uploading: databases, parameters, events and application programs. The protocol is of high efficiency, by being able to transfer only the necessary information, target functions and parameters downward and by being able to transfer only selectable information like alarms, exceptions and selectable "important data" upward.

* The RTU contains a circuit to monitor activity on the radio or line communications channel. This prevents the RTU from transmitting during a busy period. Transmission is inhibited until the channel is clear.

The RTU operates on all radio frequencies: VHF 136-174 MHz, UHF 402-430 and 450-470 MHz, 900 MHz band, 800/900 MHz trunking and microwave.

The RTU can alarm locally or activate an alternative communication means if communication on any of its assigned channels (e.g., communication to the control center) is lost.

Information is transmitted in the form of variable-length digital words. Advanced security techniques are employed to provide protection against false messages.