PRETRAŽIVANJE / SEARCH
ŠTAMPANJE / PRINT
IZLAZ / EXIT

MEĐUNARODNO REGIONALNO SAVETOVANJE O ELEKTRODISTRIBUTIVNIM MREŽAMA

REGIONAL CONFERENCE AND EXHIBITION ON ELECTRICITY DISTRIBUTION

Crna Gora, Herceg Novi, 5 - 8. oktobar 2004. / ***Montenegro, Herceg Novi, October 5 - 8, 2004***

* *

COMPARISON OF SCADA COMMUNICATION PROTOCOLS WITH RESPECT TO AVAILABLE COMMUNICATION PATHS

A. Vučković, SRC Soft, Serbia and Montenegro
I. Vučković, SRC Soft, Serbia and Montenegro

INTRODUCTION

Rationalization and privatization in the global electrical distribution industry is forcing utilities to consider new ways to optimize their business from both a performance and cost perspective. Utilities are increasingly required to meet the performance criteria set by the regulators of these companies. This is making remote control and automation of their distribution networks a real necessity if they are to meet these requirements.

SCADA system is usually supplied to permit the monitoring and control of a geographically dispersed system or process. It relies on communication systems that can be intermittent. Many SCADA systems for high-integrity applications include capabilities for validating data transmissions, verifying and authenticating controls and identifying suspect data.

In view of this, different messaging protocols and formats are used in different industries and applications.

APPLICABLE STANDARDS

In order to explain difference between individual protocols we first have to define fields of application. There are two major fields: first is DCS (Distributed Control System), and second is SCADA (Supervisory Control And Data Acquisition). Depending on application, different protocols are chosen.

In the field of DCS, the "Bus" protocols (Modbus, FieldBus, ProfiBus, etc.) and a slew of proprietary protocols are prevalent. These are suitable for the requirements of DCS Input/Output (I/O) and intended to communicate with IED (Intelligent Electronic Devices). Main characteristics of these are simplicity, modest memory requirements, small number of data types and smaller frame.

In the field of SCADA systems, the most commonly used protocols are DNP3, IEC 60870-5-101, Modbus variants and proprietary protocols. Specific applications also have specific protocols designed to meet their needs. Telecontrol and telemetry are areas where system design is required. There is no single solution that is right for every situation.

Reasons for standardization

Nowadays the market is characterized by vendor specific hardware-oriented solutions. As a consequence there is a large number of protocols for communication, which generally lead to the problem that devices from different manufacturers and even devices from different generations from the same manufacturer cannot communicate with each other or only with disproportionate expenditure. Due to the increasing number of modern information systems, the increasing of data and the fact that the innovation cycles of hardware and software are constantly becoming shorter the number of incompatible protocols is expected to rise. A reduction of variety in a relatively small market is extremely beneficial for both vendors and users. Thus standardization is the key for the advancement of the connectivity and interoperability of systems. Through standardization both users and suppliers arrive at economically suitable, reliable solutions.

SCADA standards

Two main open architecture protocols are in use today. Of these two, 60870-5-101 has been heavily influenced by the European community, while DNP was largely influenced by North and South America, together with the African and Asian regions. Both of these protocols are specified, developed and controlled by regulatory committees to ensure they allow inter-operability between different implementor’s equipment. These regulatory groups are the DNP V3.00 User Group and International Electrotechnical Commission (IEC) 60870-5 Technical Committee 57 Working Group 03.

The IEEE Standard 1379 was published in 1998. It recommends the use of either DNP 3 or IEC 870-5-101 for remote terminal unit to intelligent electronic device messaging.

IEC 60870-5. IEC Technical Committee 57 (working group 03) has defined a standard for relatively simple, bit serial communication: IEC 60870-5. The standard is optimized for efficient and reliable transfer of process data and commands to and from geographically widespread systems over low-speed (up to 64 kbps) fixed and dial-up connections. It harmonizes with the OSI reference model through its Enhanced Performance Architecture (EPA) , which uses three layers from the full seven-layer OSI model.

The IEC 60870-5 communication standard consists of the IEC 60870-5 Protocol Standard series (with International Standard status) and the IEC 60870-5 Companion Standard series. The Companion Standard specifies the information services in a specific domain of activity, and specifies in detail the use of Protocol Standard parts for specific telecontrol tasks (e.g. IEC 60870-5-101 and 60870-5-103). The IEC 60870-5 Protocol Standard and Companion Standard series specify communication protocols optimized for telecontrol systems that require short response times in relatively low-speed networks.

The diagram below highlights the roles of each part in defining 60870-5, divided by ISO OSI reference model levels.

Table 1 - Documents standard series IEC 60870-5

Standard	Description
IEC 60870-5-1	Transmission frame formats
IEC 60870-5-2	Link transmission procedures
IEC 60870-5-3	General structure of application data
IEC 60870-5-4	Definition and coding of application inform. elements
IEC 60870-5-5	Basic application functions
IEC 60870-5-101	Companion Standard for Basic Telecontrol Tasks
IEC 60870-5-101 A1	Amendment 1 to IEC 60870-5-101 Extension of Time Tags
IEC 60870-5-101 A2	Amendment 2 to IEC 60870-5-101 Supplementary Definitions

Standard	Description
IEC 60870-5-102	Companion Standard for the Transmission of Integrated Totals in Electric Power Systems
IEC 60870-5-103	Companion Standard for the Informative Interface of Protection Equipment
IEC 60870-5-104	Network Access for IEC 60870-5-101 using Standard Transport Profiles

From these writers perspective, there appears to be much confusion in relation to IEC companion standards 60870-5-101 and 60870-5-103.

The 60870-5-101 Companion Standard for Basic Telecontrol Tasks defines a set of data types and services, as detailed in 60870-5-1 to 5, that are suitable for telecontrol systems e.g. a substation control system. These data types are generic and include data such as single and double binary point statuses and commands, counters, analogs and set-points.

The 60870-5-103 Companion Standard for the Informative Interface of Protection Equipment extends the set of data types and services by defining specific data types formats and communication behavior for distance protection, transformer differential protection and line differential protection. These data types can include combined digital and analog data like currents, voltages, fault indications and disturbance data. Therefore, 60870-5-103 companion standard is an extension, not a subset, of the 60870-5-101 standard and is designed for specific use in data interchange between protection equipment and a substation control system.

DNP3. While IEC 60870-5-101 is specifically an electric power-oriented protocol (with specific objects for things such as Transformer Tap Positions, etc), DNP3 is a more generic SCADA protocol. As such it has found acceptance in a wider set of industries, including oil & gas pipeline control systems and water & wastewater systems. DNP3 is often used for distribution SCADA because of its capability to make efficient use of multi-drop radio communication networks.

DNP, the Distributed Network Protocol, is an open, public and non-proprietary protocol based on existing open standards to work within a variety of networks. DNP Version 3.0 was originally designed based on three layers of the OSI seven-layer model: application layer, data link layer and physical layer. The application layer is object-based with objects provided for most generic data formats. The data link layer provides for several methods of retrieving data such as polling for classes and object variations. The physical layer defines a simple RS-232 or RS-485 interface and an Ethernet interface.

Harris, Distributed Automation Products, developed DNP. In November 1993, responsibility for defining further DNP specifications and ownership of the DNP specifications was turned over to the DNP Users Group, a group composed of utilities and vendors who are utilizing the protocol.

DNP was developed to achieve interoperability among systems in the electric utility, oil & gas, water/waste water and security industries. DNP can also be implemented in any SCADA system for communications between substation computers, RTUs (Remote Terminal Unit), IEDs and master stations; over serial or LAN-based systems. As DNP is based on the IEC 60870-5-101 requirements, it is suitable for application in the entire SCADA/EMS environment. This includes RTU to IED communications, master to remote communications, and even peer-to-peer instances and network applications.

Feature analysis

This chapter intention is to compare major features of described protocols.

Common features. Both DNP3 and IEC 60870-5-101 serve similar functions. They both:

- Reliably and efficiently transfer field data (including information about transitory events) to the master station
- Allow commands to be issued to the field with a very high degree of control security (verification and rejection of errors) by using the high-integrity select-before-operate command strategy
- Suit medium bandwidth communication channels (e.g. 9600-baud serial connections)

- Include good data link frame integrity checking
- Support application layer data object identification
- Include data validity checking flags
- Support the transmission of digital (on/off) and analog data (in integer or floating point formats), counters and digital and analog control commands or setpoints
- Support transfer of files, setting of docks, etc. IEC 60870-5-101 also supports some electric power specific objects related to transformers and substation protection devices.

The protocols support the transfer of "report-by-exception" (RBE) where only changes in field data are reported. RBE improves the efficiency with which data can be transferred under "normal" conditions. The protocols are also capable of transmitting data with millisecond resolution timestamps, allowing accurate identification of the sequence of actions in the field. These event-reporting capabilities are useful for accurate analysis of power system events.

Differences. Most of differences between DNP3 and IEC 60870-5-101 are related to frame format, addressing, and structure of message. We will emphasize only that which are related to optimization of communication channel usage:

- DNP only uses balanced link services. 60870-5-101 may use balanced or unbalanced services.
- The DNP addressing format supports peer-to-peer operation, the 101 format does not.
- DNP groups data into four classes. This may be used to prioritize event reporting. One class is for “static” data: current values of inputs; the other three are for “event” data: reporting changes. All four classes may be requested simultaneously. IEC groups data into two classes, and while not explicitly stated in the 60870-5-101 standard, one class is intended for “cyclic” data, and the other class is for all other data. Only one class or the other may be requested in a single poll. The device indicates in the link layer which class should be polled for next.
- DNP supports unsolicited reporting using a collision-avoidance mechanism for multi-drop systems. 60870-5-101 only permits unsolicited reporting on point-to-point links where collision is impossible.

NETWORK DESIGN

It is important to choose the protocol network topology which best supports the electricity utility’s needs. Points to consider are the communications medium, network topology and whether continuous polling or report by exception / unsolicited reporting is required.

Transmission types

Two types of transmission procedures are used in SCADA systems:

- Unbalanced transmission, in which a master station controls the data traffic by polling outstations sequentially. In this case the master station (master) is the primary station that initiates all message transfers while outstations are secondary stations (slaves) that may transmit only when they are polled.
- Balanced transmission, each station may initiate message transfers – events can be reported without polling by the master.

Network configurations

There are two prevailing network configurations commonly used in SCADA systems:

- multipoint (party-line), if the links from a central control station (controlling station) to several outstations (controlled stations) share a common physical channel (e.g. radio communication).
- multiple point-to-point, central control station communicates to outstations using separate physical channels (e.g. leased line, cellular communication)

PRETRAŽIVANJE / SEARCH
ŠTAMPANJE / PRINT
IZLAZ / EXIT

Finding the right solution

When choosing appropriate transmission type and network configuration, available communication media must be considered. In majority of electrical distribution networks, communication between central control station and outstations is feasible over radio link, and in less extent by leased line or fiber optic links. Depending on cellular provider coverage, cellular links may also be implemented

DNP3 supports an "unsolicited reporting" (balanced) mode where a field device can report events without being polled by the master. Unsolicited reporting can be very useful for a large electrical distribution network where (for example) pole-top reclosers can report activity on a shared radio bearer without being polled.

IEC 60870-5-101 also supports an "unsolicited" reporting mode, but only with a dedicated point-to-point communication channel - unlike the DNP3 model that can support unsolicited reporting on multi-drop communications channels.

Systems in practice. From our experience in design of SCADA systems for electrical distribution companies, the most popular type of communication between master (central) station and RTUs is radio communication. Some of reasons for that are:

- electrical distribution companies already have one or more radio channels, and, in most cases, one of them is dedicated for SCADA communication.
- price of purchase and installation of radio equipment necessary to establish communication with one RTU is comparable to costs of leased line for one year.
- events which are to be reported over SCADA communication are rear, with relatively small amount of data circulating in system, so there is no need for communication channel with large bandwidth.
- functioning of radio communication channel is self responsibility of electrical distribution company. Functioning of other communication channels depends on other companies (telephone company, cellular provider, ...)

If we decide to use radio communication, network topology is dictated by nature of radio link – multipoint (party-line).

Next to choose is type of transmission. Easier way is to choose unbalanced transmission – continuous polling. System with continuous polling functions work well with only a few RTUs connected. Problem arises with RTU number increase. Beyond certain number of RTUs, delay between two successive polls becomes impractical. Also, radio equipment is constantly in use, practically 24h a day (especially at master station), with work hours closing rapidly to MTBF value and increasing risk from damage. Practical question is: why to spend time for sending same data all day when RTU can initiate transmission only on event? Since such waste is not allowed on communication channel with limited bandwidth, logical choice is balanced transmission – report by exception.

Balanced transmission is described in IEC 60870-5-101, but only with point-to-point network where collision is impossible. As illustration, there is original text from IEC 60870-5-101 Companion standard for basic telecontrol tasks (Chapter 4.3. Link Layer):

If the links from a central control station (controlling station) to several outstations (controlled stations) share a common physical channel, then these links must be operated in an unbalanced mode to avoid possibility of more than one outstation attempting to transmit on the channel at the same time.

So, it is impossible to use IEC 60870-5-101 over radio link in practical way - only by exhaustive continuous polling. On the opposite, DNP3, with implemented collision-avoidance mechanism, provides means for realization of balanced transmission / unsolicited reporting in practice.

CONCLUSION

Our intention was to clarify application of communication protocols in practical terms, during realization of SCADA system. We described two mostly used protocols and compared major features concerning communication over radio link.

PRETRAŽIVANJE / SEARCH
ŠTAMPANJE / PRINT
IZLAZ / EXIT

Conclusion is that IEC 60870-5-101 is a choice when optical or hard-wired connection is used, DNP3 is more suitable for radio connection. In real system there are numerous reasons to choose one over another, but neither is good enough to cover every particular situation.

In order to solve particular problem, large number of manufacturers use their own proprietary protocols. Example for this is Motorola's MDLC protocol which is dedicated for communication over radio link and is very functional. Connection with equipment working with different protocol is then made using gateways. This is a common practice when equipment of different manufacturers needs to be connected. Considering this, there is no excuse for putting request for some special protocol when purchasing equipment for SCADA system (which became practice these days, so to say fashion). Requests which are crucial are concerning functionality, reliability, serviceability and implementation costs of system.

LIST OF REFERENCES

1. International Standards

Telecontrol equipment and systems – Part 5: Transmission Protocols:

Section 1 - Transmission Frame Format,

Section 2 - Link Transmission Procedures,

Section 3 - General Structure of Application Data,

Section 4 - Definition and Coding of Application Information Elements,

Section 5 - Basic Application Functions,

Section 101 - Basic Telecontrol Tasks,

Section 103 – Informative Interface of Protection Equipment,

International Electrotechnical Commission Publication, 1995.

2. "DNP3 Protocol – Users Guide", 2003, "Tavrida Electric"

3. O'Sullivan N, Mikli L, 2003, "DNP V3.00 and IEC 60870-5-101 Implementations in Intelligent Electrical Devices (IEDs)", "Technical papers of NU-LEC Industries - Schneider Electric company"

4. "Norwegian IEC 870-5-101 User Conventions, Approved version, Revision no. 2.0", 2000, "Statnett SF, Oslo, Norway"

5. West A, 2003, "SCADA Communication Protocols", "Power Transmission and Distribution", "aug 2003"