Using DNP3 & IEC 60870-5 Communication Protocols In the Oil & Gas Industry

Provided by:
Triangle MicroWorks, Inc.
Raleigh, North Carolina
Phone 919-870-5101 • Fax 919-870-6692
www.TriangleMicroWorks.com

1 Industry Standards

DNP was originally created by Westronic, Inc. (now GE Harris) in 1990. In 1993, the "DNP 3.0 Basic 4" protocol specification document set was released into the public domain. Ownership of the protocol was given over to the newly formed DNP Users Group in October of that year. Since that time, the protocol has gained worldwide acceptance, including the formation of Users Group Chapters in China, Latin America, and Australia.

In January 1995, the DNP Technical Committee was formed to review enhancements and to recommend them for approval by the Users Group. One of the most important tasks of this body was to publish the "DNP Subset Definitions" document, which establishes standards for scaled-up or scaled-down implementations of DNP3.

DNP3 is an open, intelligent, robust, and efficient modern SCADA protocol. It can

- request and respond with multiple data types in single messages,
- segment messages into multiple frames to ensure excellent error detection and recovery,
- include only changed data in response messages,
- assign priorities to data items and request data items periodically based on their priority,
- respond without request (unsolicited),
- support time synchronization and a standard time format,
- allow multiple masters and peer-to-peer operations,
- allow user definable objects and file transfer.

IEC 60870-5 has many of the same features of DNP3 with the exception that it was created by the International Electrotechnical Commission (IEC). The IEC was founded in 1906 and is the world organization that prepares and publishes international standards for all electrical, electronic, and related technologies. The IEC was founded due to a resolution passed at the International Electrical Congress held in St. Louis (USA) in 1904. The membership consists of more than 50 participating countries, including all the world's major trading nations and a growing number of industrializing countries.

After becoming a member of the IEC, each National Committee agrees to open access and balanced representation from all private and public electrotechnical interests in its country. The whole organization of the IEC is designed to ensure that the National Committees play a leading part in all decision-making

instances of the Commission. This enables the widest degree of consensus on standardization work to be reached at an international level. It is up to the National Committees to align their policies accordingly at the national level.

2 DNP3 and IEC 60870-5 vs. Modbus

ModBus was developed in the process-control industry. It typically permits access to the inputs and outputs on a Programmable Logic Controller. It has the data types of "coils" (digital outputs), "status" (digital inputs), "Holding Registers" (analog outputs) and "Input Registers" (analog inputs). Each input or output has a unique identifier number, and these are broken up into special ranges (e.g. Holding Registers have addresses 40001 to 49999). Modbus treats all data as a "present value". It reads values from ranges of inputs (and outputs) by issuing a single request to read each range or type, and can write to outputs. Standard ModBus has no concept of events (transitory indications) or time. Any data that is not collected by reading it is lost when it is overwritten by new field data.

Because ModBus supports the concept of reading back the value of an output, many ModBus devices only implement "output" type data. All inputs are read and addressed as if they were outputs.

Many ModBus device manufacturers add custom extensions to their devices to extend the functionality beyond that provided by standard ModBus. This and the common use of outputs as inputs sometimes makes it quite difficult to make even simple ModBus devices inter-operate. Modbus has no independent technical committee to ensure interoperability and create standards for new functionality.

The advantage of ModBus is its simplicity for small devices and the very large range of devices that have some sort of ModBus interface.

DNP3 and IEC 60870-5 have basically the same functionality. The following compares the above issues to DNP3:

DNP3 was developed for use in Electrical Utility SCADA. It permits a device to report digital inputs, counter inputs and analog inputs; and to receive digital and analog controls. It explicitly allows for common electric utility functions such as pulsed pairs of outputs for circuit breaker trip/close control.

DNP3 supports reporting of data quality information, and the reporting of field events (changes of state of digital, counter and analog input data). It supports high-security 2-pass controls. DNP3 permits multiple types of data to be encapsulated in a single message to improve efficiency. To further improve efficiency it permits a method of operation where only changes are reported, reducing communication bandwidth usage. DNP3 permits events to be time-tagged so that the sequence of events occurring in the field can be accurately identified.

DNP3 is highly standardized, with relatively high compatibility and inter-operability between devices from different manufacturers. Both DNP3 and IEC 60870-5 have independent Technical committees that are working to ensure interoperability and create standards for new functionality.

3 Cost Savings Demonstrated in Electrical Utility Industry

The DNP3 and IEC 60870-5 industry standards have proven to save money in the Electric Utility industry over the last few years. The ability to rely on the assistance of Technical Committees and Working Groups have allowed the Utility Vendors the ability to promote the features they require in their products while still allowing robust communication protocols that will interoperate between equipment from different vendors. This high level of conformance enables any DNP3 or IEC 60870-5 equipment to be "plug and play" compatible directly into a SCADA system.

This method also assists large and small companies with their growing development budgets. It is much easier and safer to implement a product that is considered a worldwide standard instead of requiring an in-house staff to continually update a collection of proprietary protocols.

4 Oil & Gas companies and vendors currently using DNP3 and/or IEC 60870-5

There are already many companies in the Oil & Gas industry using DNP3 and IEC 60870-5. We have seen a growing interest in these companies for switching to standard protocols and believe that the use of DNP3 and IEC 60870-5 will continue to grow over the next decade.

Oil & Gas companies that are currently benefiting from DNP3 and/or IEC 60870-5 are as follows:

Illinois Power

JCS "Mazeikiu Nafta"

Kaist

Louisville Gas and Electric

Origin TA

Prosoft Technology, Inc.

Saudi Aramco

Siemens Advanced Engineering

Standard Automation

Teletrol, C.A.

Transdyn Controls

Williams Corporation

5 What are the main advantages in an Oil & Gas application?

The main benefits of switching to DNP3 and/or IEC 60870-5 protocols are the ability to receive time stamped sequence of events reports, data can be monitored with a faster response time, easier integration based on improved interoperability, and better data security.

DNP3 supports an “Unsolicited” reporting mode, where remote devices can report field events without being polled by the master station. This is useful when a high-priority condition occurs at a site that is normally polled at a very low rate (e.g. every few hours). If an alarm condition such as a pump failure or leak is detected, a response message can be immediately sent to the master without waiting for the next cyclic poll.

DNP3 is able to support a "sequence of events" history for alarms (binary data), measured quantities (analog data) and counters (volume per unit time, custody transfer, etc.). This means that even if a remote site is polled infrequently, all significant changes in the data since the previous poll can be reported at that time, possibly including time stamps that indicate the precise order of the field events. This provides functionality normally found in flow computers.

DNP3 supports a high-security two-pass control procedure known as "Select Before Operate" or SBO. SBO controls provide a very high level of assurance that no inadvertent control operation can occur as a result of interference on the communication channel. This reduces operational risks to personnel and the environment.