Using DNP3 to Solve Remote SCADA Communication Challenges

by Philip Aubin

Executive summary

The DNP3 protocol has evolved over the last two decades to provide significant advantages for SCADA operations that require communication with remote devices over large distances. This paper highlights the functionality that has made DNP3 such a powerful tool in telemetry applications in the oil & gas and water & wastewater industries, looking specifically at how it can be used to address common communication challenges in the respective industries.

998-2095-04-14-12AR0

Schneider Electric

Summary

Executive Summary

The DNP3 protocol has evolved over the last two decades to provide significant advantages for SCADA operations that require communication with remote devices over large distances. This white paper highlights the functionality that has made DNP3 such a powerful tool in telemetry applications in the Oil & Gas and Water & Wastewater industries, looking specifically at how it can be used to address common communication challenges in the respective industries.

Introduction

Originally developed for the electrical power industry the DNP3 protocol has expanded over the last two decades into industries such as Oil & Gas, Water & Wastewater and Transportation, among others. It has evolved over time with functionalities and capabilities added as the demands of the industries changed and developed with new technologies and requirements. In many areas it has been adopted as a standard.

This paper looks briefly at the features of the DNP3 protocol followed by how these capabilities provide solutions to challenges commonly encountered in the Oil & Gas and Water & Wastewater industries.

Standardisation and Interoperability

As an open, standards based protocol, devices using DNP3 are required to use common data types and a very organized data structure ensuring that all devices handle and present data in the same way. As a multi-layered protocol, each layer is responsible for a specific function so that when communicating with a partner device the interoperability of the two devices is guaranteed.

DNP3 also uses subsets that define a device's minimum requirement for functionality. Four subset levels are defined for a range of device capabilities from small instruments, such as fixed function devices to large multi-purpose RTUs. The result is that vendor's devices conform to one or more of the four subset levels allowing them to communicate with other devices on at least one of the levels. This interoperability supports many types of network architectures and can accommodate a mixture of legacy, new and future equipment.

Flexible Communications

The flexibility of DNP3 is based on the time-stamping and meta-data capabilities of the protocol. Data that is time stamped allows the user to determine the sequence of events and the time of actual process events, such as the start and stop times of equipment. Reliable data transmission is achieved through the use of time-stamping since data can be stored in an RTU in the event of a network problem and re-transmitted once the system is operational.

Meta-data carries additional and meaningful information with the data For example; DNP3 can be used to report not only a value and time-stamp, but also the quality of the data being reported. Data can also be classified into different priority groups known as 'Classes'.

Not all data needs to be collected on a continuous basis. The use of time-stamping and meta-data allows operators to optimise the throughput limits of their communication channels by defining thresholds and rules for data transfer.

The resulting reduction in bandwidth is particularly important for slow communication links but is also relevant for the freeing up of bandwidth to extend network expansion or for other system functions such as peer-to-peer communications, maintenance access, or remote configuration. Time synchronization throughout the communication network allows for greater scheduling accuracy and the potential for energy optimisation when correctly aligned with a high power consuming event.

Critical data and alarms can be sent immediately using a mechanism known as unsolicited reporting, regardless of other pre-scheduled or standard data transfer streams. This allows fast response from upstream or downstream operations.

Security

DNP3 achieves security through the use of both encryption and authentication. Security is provided for data transmission through the use of the AGA12 standard where the original data is combined with a security key to encrypt the message and make it unintelligible to anyone without access to the original key. Authentication provides security for critical actions such as controls and configuration changes by preventing unauthorized users from making changes to the system through the use of a request-challenge-response sequence.

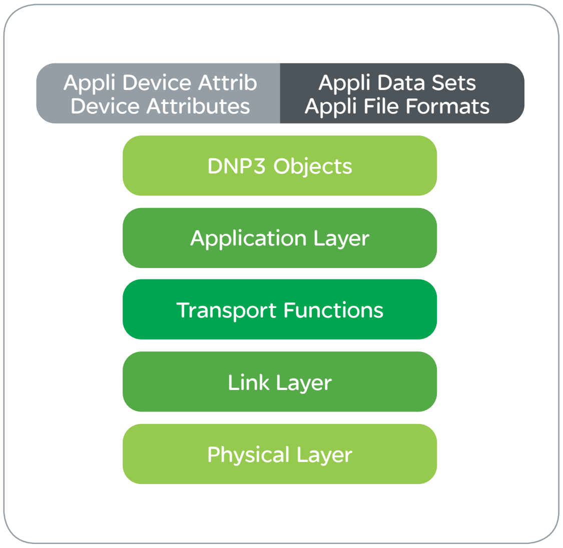
Strong User Support

Since its establishment in 1993, the DNP Users Group has grown to include hundreds of members from both the vendor and user community. This mix of users and vendors increases the level of awareness of DNP3 and allows for more rapid development and acceptance of new extensions to the protocol. It also ensures that developers are working toward enhancements that are meaningful to end-users. With such a broad base of users supporting industry standards and the trend away from proprietary solutions, DNP3 will have continued growth and success.

Customer Challenges in Remote SCADA Communications

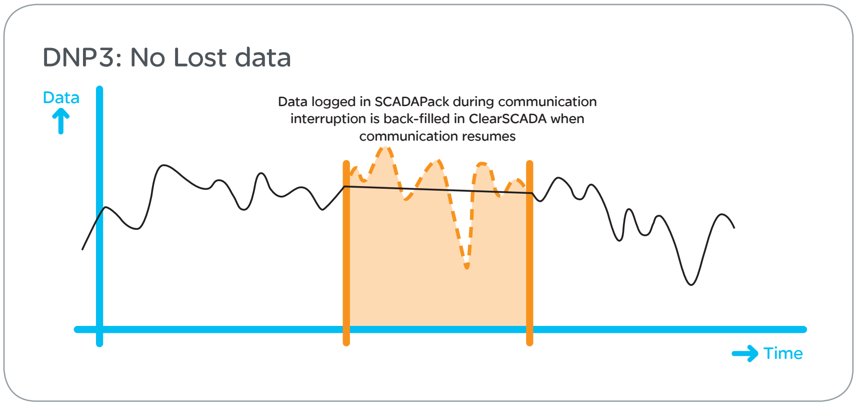
Data Integrity and Reliability

Historically, there have been challenges in guaranteeing the reliability and integrity of data across remote communication networks due to lost messages, occasional communication outages and uncertain operations in the face of adverse weather conditions. This problem is particularly relevant in the oil and gas industry where remote data accessibility and maximum data availability are critical for maintaining a clear picture of how individual assets such as well heads, pads, and rod pumps are operating. Similar advantages are provided in the water and wastewater industry for assets such as pumping stations, tanks, zone pressure control, and so on.



Through the use of meta-data, information about the data other than a simple value such as alarm status or the data quality parameters can be transmitted. When combined with data quality indicators and the ability to time stamp an event, it is no longer a problem if a remote communication system loses messages or goes down. Data can be stored in the RTU until the communication system is available with the time stamp information accurately placing the event in time and sequence. When used with a suitable remote SCADA master station, all events can be properly back-filled in the event audit and historical trending databases. The data is dealt with using the information contained not only in the value but also in the meta-data attached to it.

Since a remote SCADA system is not able to communicate with all devices at once, the use of traditional protocols often required the systems to wait until it was a device's turn to 'speak' before the central SCADA would be aware of a problem. In larger systems, including wastewater systems with networks that support dozens to thousands of remote stations, a significant time could pass before a specific station got its turn to 'speak'. Using unsolicited messaging, fault alerts or other event data collected by the RTU can be sent immediately to the central SCADA system, ensuring the relevant information is received in a timely manner and operations personnel have a complete, accurate picture of the problem that has occurred.



Dynamic Systems Environment

Managing a dynamic system is an essential aspect of modern asset optimisation: dealing with, anticipating and accommodating the on-going changes and upgrades that continually occur. This is particularly true in oil and gas production that thrives on continual improvement and achieving the highest level of production efficiency. Similarly, water & wastewater systems expand in size with growing population, are upgraded for better operational performance, and are renewed in rolling asset replacement programs.

Whether migrating to a new central monitoring and control system or adding new devices or processes to an existing system, the strength of the DNP3 protocol is its flexibility and scalability. DNP3 is extensible which allows configuration to be easily extended to new devices and have all systems running and communicating when migrating from the old system to the new. Files, configurations and control logic program changes can all be transferred to RTUs for a great deal of flexibility within a secure and reliable framework.

Amalgamation of Previously Separate Systems

Before the advent of standardised protocols, system managers often struggled with having multiple devices that were unable to communicate with each other due to proprietary protocols developed by individual vendors. It was often impossible to communicate with legacy equipment, have older and newer equipment interact, or support old and new devices in a unified system. Through the use of the multi-layered protocol architecture and functional subsets that define the minimum functionality level that a device is required to provide, systems deploying DNP3 have successfully addressed these challenges.

Vendor's devices conform to one or more of the four DNP3 subset levels that allows them to communicate with other devices on at least one level. This is a key enabler for interoperability when integrating new equipment during system expansions and upgrades. The open DNP3 protocol drastically reduces the cost of installing a new system, extending or upgrading an existing system when devices are able to communicate regardless of their age and feature set.

Standardising the Transmission of Time-Series Data

Taking gas production or pipeline gas transportation as an example, in order to facilitate the transmission of time-based records, Modbus protocols were often significantly customized to allow for the transport of required historic and audit data over the network. Legislative requirements for auditing and time-series data, in particular through API standards, often resulted in a solution of complex proprietary extensions to existing industrial control system protocols.

One of the early motivators in developing the DNP3 protocol was a market need for standardisation. In the example of time-series data, the standardisation of DNP3 brings significant benefits by avoiding individual vendors drastically customizing protocols. Standardizing the way that time-series data is transmitted mediates some of the problems associated with delivering the data required by legislation. The time-stamping capability of DNP3 provides a big step towards realizing a standard way for the increasing industry requirements for performance and audit data.

Control Integrity

When controlling a remote process from a central location it can be difficult to determine if a desired control command has been carried out, or when. Historically when remote locations were strictly supplying monitoring data, loss of data was inconvenient. In today's remote systems, reliable control is critical for operational, financial and security reasons. The strength of DNP3 is that it has a high integrity control model for sending control commands.

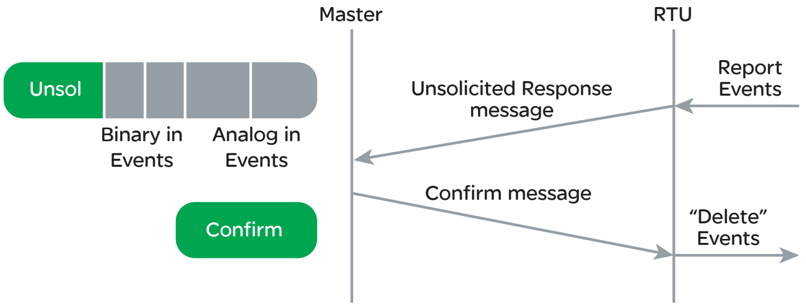
An example is the instance of a gas wellhead using a sales valve. It is one thing to send a signal for the wellhead to close but having rapid feedback to indicate that the valve has operated as required is now necessary functionality. By concise communication processes (such as Select Before Operate controls and output event reporting) between the central SCADA system and the remote field devices, accurate data is provided that reflects and verifies the correct delivery of controls. Further, precise indication on the correct process response is also provided through standard DNP3 mechanisms (input events with time-stamping).

Remotely Monitoring Widely Distributed Equipment

The communication of data between field operations and the control room becomes critical when managing multiple remote sites.

The use of meta-data optimises communication between RTUs and other intelligent system equipment with the RTU determining the priority and importance of the collected data it receives and sending alarm messages or prioritizing transmission based on that content. Prioritized data can be sent through to the master station using unsolicited messaging for rapid feedback.

- Unsolicited event data
  - Field device initiated
  - Delivery Confirmed from Master Station
  - Ensures fastest notification of high priority data
  - Native Collision Avoidance mechanisms



The self-describing feature of the meta-data gives operators a timely view of quality problems that may have occurred, with relevant details (for example, an instrument that is reading over-range or that has gone offline).

Communication optimisation also occurs through bandwidth control. Source and destination device addressing supports multiple masters, peer-to-peer communication, routable and unsolicited messages. This can free up bandwidth, allowing communication capacity for additional devices and systems to be added without having to upgrade the entire communication network.

When combined with object oriented remote SCADA, DNP3 facilitates the completion of operations on a mass scale that previously had to be done on an individual basis. Functions that can be coordinated remotely include logic applications, debugging, diagnostics and RTU configuration either through a dedicated development environment or through SCADA host software.

Regulatory Compliance

Oil and natural gas production and distribution, the supply of potable water, and the handling of wastewater all have increasing requirements for operational safety, compliance with environmental regulations and the overall security of assets.

Industry requirements for both performance and audit data require that data transmission be accurate, consistent and reliable. Time stamping of data and events, to ensure that there is no data loss, is critical when ensuring the correct data is available and calculated for compliance reporting. Smart RTUs, when used with the DNP3 protocol and remote SCADA software, offer automatic data back-filling in case the communications network to the host is interrupted. The added value in the data attributes sent in the meta-data allows for more detailed and comprehensive data.

Doing More With Less

Oil & gas production and transportation organisations, and water and wastewater organisations are continually under pressures to provide increased performance, at the same time as having decreasing man power and a limited budget to accomplish their goals.

Reliable data, provided from the source at remote installations through to the control room and to the business through enterprise systems, can be used by nearly every part of the operations team to improve efficiency and reduce the overall cost of ownership. Operators have access to all assets from a single point. Maintenance staff has accurate reliable data to pin-point problems for expediting fast repairs. Automation technicians have access to control data and standardised communications for rapid deployment when required. Production supervisors can meet regulatory compliance and produce timely production data for delivery commitments and forecasting. Production analysts receive high resolution operational measurements. In gas production this can include detailed plunger arrival logs, accurate gas measurement, and so on. Asset managers can maximise production, for example through new gas opportunities during flow-back periods with same day measurements.

Conclusion

Designed specifically for telemetry applications, the DNP3 protocol has features that provide:

1. Standardisation and Interoperability
2. Flexible Communications
3. Security
4. Strong User Support

The communication challenges in the Oil & Gas and Water &Wastewater industries that these features specifically address include:

1. Data Integrity and Reliability
2. Dynamic Systems Environments
3. Standardizing the Transmission of Time-Series Data
4. Amalgamation of Previously Separate Systems
5. Control Integrity
6. Remotely Monitoring Widely Distributed Equipment
7. Regulatory Compliance.

Schneider Electric

Telemetry & Remote SCADA Solutions
48 Steacie Drive, Kanata, Ontario K2K 2A9 Canada
Direct Worldwide: 1 (613) 591-1943
Fax: 1 (613) 591-1022
Toll Free within North America: 1 (888) 267-2232
www.schneider-electric.com

This document has been
printed on recycled paper