Advantages of the DNP3 Communications Protocol

Introduction

The purpose of this white paper is to explain the key features of the DNP3 protocol and how these features can help in a water/waste water telemetry system. This white paper is not intended to be a lesson on the DNP3 protocol. We assume the readers have a basic understanding of the protocol. This white paper is intended for: consulting engineers, end users, communication managers, and automation/control system engineers.

DNP3, or Distributed Network Protocol, has been around for close to two decades now. It was developed by Westronic (now part of GE) in 1993 primarily for the power industry. From its inception, DNP3 has been as an open protocol, allowing end users to use a common protocol across many hardware platforms.

The DNP3 protocol has a number of features and advantages. However, the following features are particularly useful for water and wastewater applications.

- Open protocol
- Classification of field data
- Report by exception
- Time-stamped data
- Support for time synchronization
- Secure authentication
- Diagnostic information for each I/O point
- Communication to multiple masters

Why are these features important? How do they enhance a water/wastewater telemetry system? What are the benefits for the end user?

Let’s look at each of the features in detail and try to answer the questions posed above.

Open Protocol

From its inception, DNP3 has strived to be an open protocol. There are many open protocols, including Modbus, probably the most widely used open protocol. So, why is it that being an open protocol is important?

The guardian of the DNP3 protocol is the DNP3 Users Group Technical Committee, which was formed in 1995 and is vendor independent. The committee’s charter not only includes specifying protocol enhancements and new functionality called “DNP Subset Definitions,” but ensures there is backward compatibility and absolutely makes sure there are no vendor specific variants of the protocol. The firm compliance requirement ensures that hardware and software manufacturers who do support DNP3 do so within very well defined parameters. It should be noted that a vendor need not support all DNP3 protocol functionality.

The compliance to DNP3 can be via three different levels — 1, 2 and 3. All vendors who support DNP3 must make available a device profile document that clearly lists the DNP3 features supported by the product and thus the compliance level.

But how does this help customers? What are the benefits?

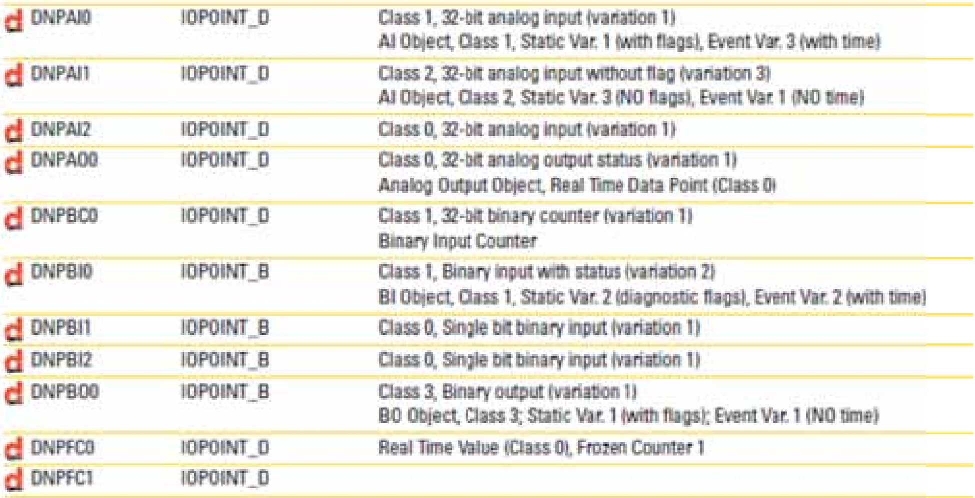
DNP3, being a true open protocol, allows the end customer to use hardware and software from different vendors with the complete confidence that they will be able to communicate with each other and that a common top-end SCADA software package can be used to bring in the data from the different pieces of hardware. This is beneficial not just technically but also commercially, as it provides the end users vendor independence, allowing them to add equipment from different suppliers without the need to replace the entire system every time they want to expand and or change.

Classification of Field Data

In a water or wastewater system there are various assets that require monitoring and control. These include treatment plants, pump stations, valve sites, canals, weirs, tanks, ponds, dams, reservoirs, pipelines, and much more. At these locations, a great deal of normal day-to-day activity exists. For example, at a pump station, it is very normal for the pump to go ON or OFF when the configured conditions are true or false.

The question is — do you want every event reported to the top end? The answer is no, because this will take up bandwidth and possibly prevent information on critical events from getting through to the DNP3 master device.

To prevent this scenario, DNP3 protocol allows users to classify their data into different groups called “Class.” The protocol currently supports four classes of data — 0, 1, 2, and 3. Class 0 data is real-time data. Classes 1, 2 and 3 are reserved for objects that require time stamp information (event data). Each class of data is independent from the other. A class of data also has variation parameters which allow the user to select the type of value, time, and diagnostic information to be recorded.

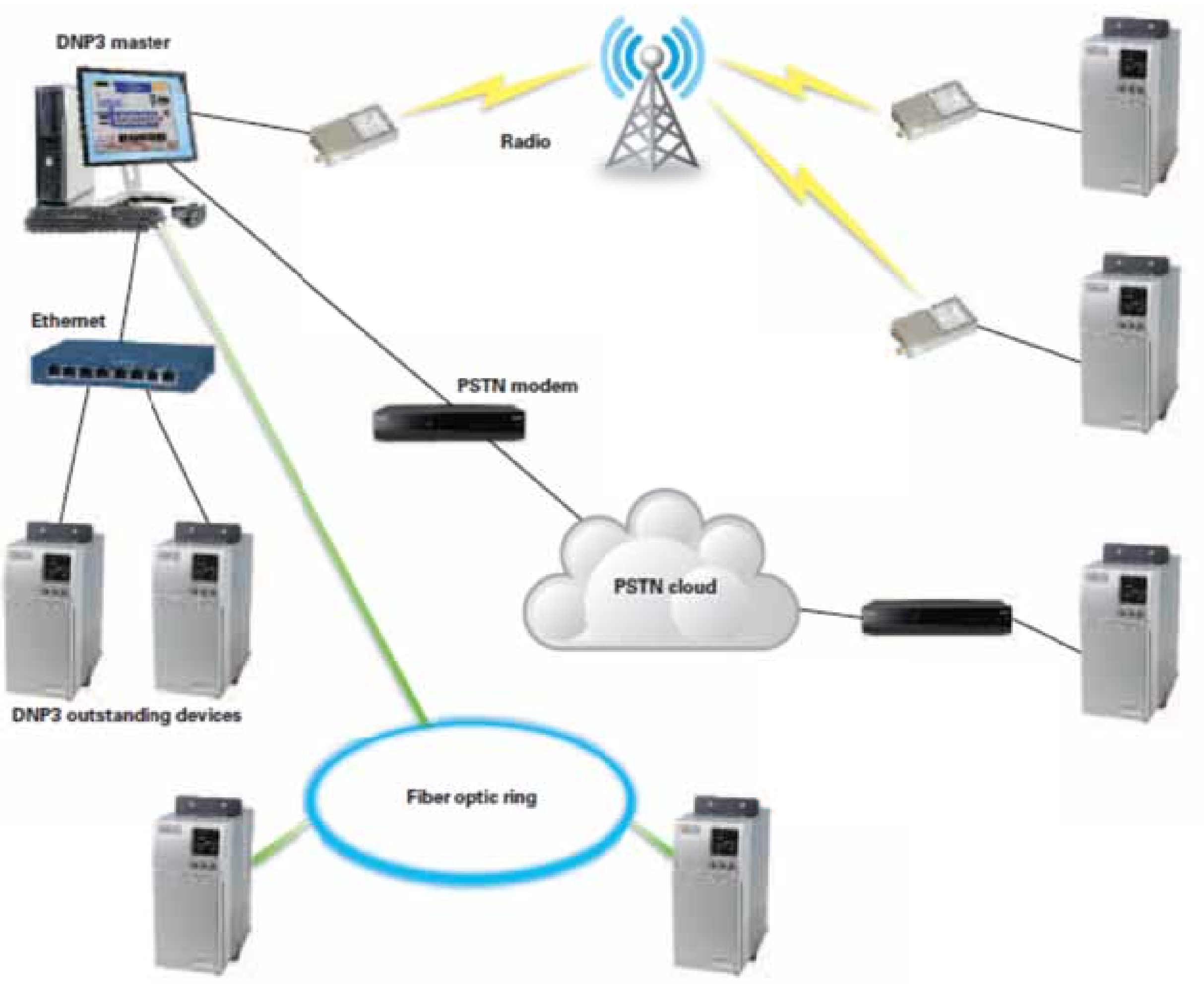


DNPAI0	IOPOINT_D	Class 1, 32-bit analog input (variation 1) AI Object, Class 1, Static Var. 1 (with flags), Event Var. 3 (with time)
DNPAI1	IOPOINT_D	Class 2, 32-bit analog input without flag (variation 3) AI Object, Class 2, Static Var. 3 (NO flags), Event Var. 1 (NO time)
DNPAI2	IOPOINT_D	Class 0, 32-bit analog input (variation 1)
DNPAO0	IOPOINT_D	Class 0, 32-bit analog output status (variation 1) Analog Output Object, Real Time Data Point (Class 0)
DNPBC0	IOPOINT_D	Class 1, 32-bit binary counter (variation 1) Binary Input Counter
DNPBI0	IOPOINT_B	Class 1, Binary input with status (variation 2) BI Object, Class 1, Static Var. 2 (diagnostic flags), Event Var. 2 (with time)
DNPBI1	IOPOINT_B	Class 0, Single bit binary input (variation 1)
DNPBI2	IOPOINT_B	Class 0, Single bit binary input (variation 1)
DNPBO0	IOPOINT_B	Class 3, Binary output (variation 1) BO Object, Class 3; Static Var. 1 (with flags); Event Var. 1 (NO time)
DNPFC0	IOPOINT_D	Real Time Value (Class 0), Frozen Counter 1
DNPFC1	IOPOINT_D	

This DNP3 protocol feature is extremely useful especially in multi-layered systems as it allows the user to categorize field data. For example, normal conditions at a pump station site, like pumps starting and stopping, may be configured as Class 2 type events. Thus, when the pump changes state, an event will be created as a Class 2 type event and stored in memory. Since this is normal operation, an unsolicited report (or Report by Exception) need not be initiated to a DNP3 master device. When the master device performs a routine background poll, it can recover all Class 2 events.

But assume at the same pump station site there is a pump fault indication. This is, in most cases, a critical alarm of which the DNP3 master needs to be aware, so that appropriate action can be taken. Thus, the pump fault status indication can be configured as a Class 1 event, thereby triggering an unsolicited report to the DNP3 master device.

DNP3 protocol's fundamental support for data classification allows the end user to design and operate an efficient telemetry system irrespective of the type of communications media being used.



Report by Exception (Unsolicited Reporting)

Report by Exception refers to a remote device's ability to initiate communications to a top-end master. Traditional telemetry systems are typically poll-only systems. In medium-to-large systems, a polling protocol can lead to loss of data. To prevent the loss of data, communications bandwidth would have to be increased constantly.

Taking the example described in the section "Classification of Data," with DNP3 protocol's inherent support for unsolicited reporting, the pump fault alarm can be sent to the DNP3 master immediately upon occurrence. If the telemetry system were a poll-only system using a different communications protocol, the alarm information would only be seen at the top-end after the outstation has been polled by the master. And even when the master sees the pump fault status indication, it will not have the event time stamp information.

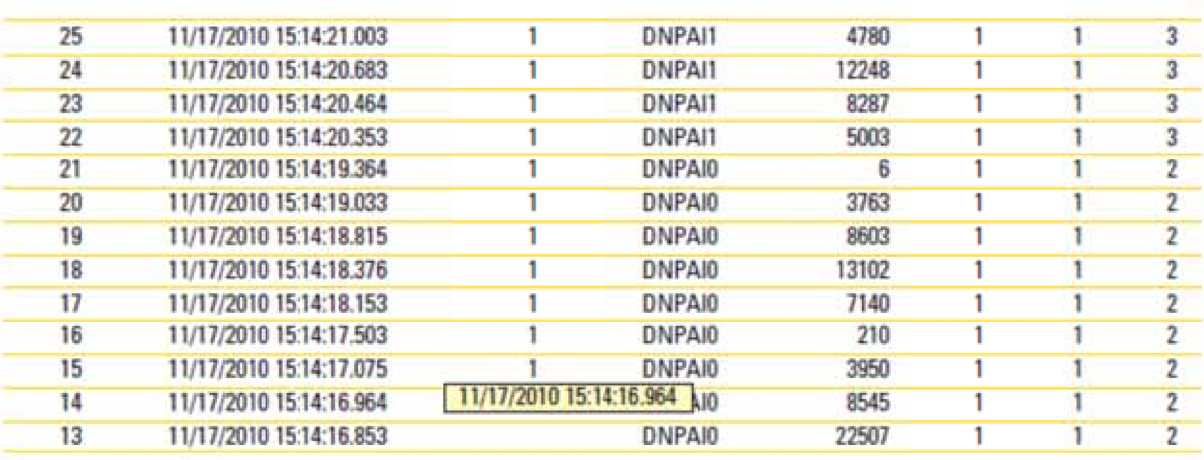
Time-Stamped Data

Time-stamped data is also known as event-logged or event-based data. It is basically where an event such as a pump changing its status from ON to OFF, or a change in the tank level by a certain percentage within a specified time period, will be recorded in the device with a time and date stamp. Sounds simple… well, it is simple, because the DNP3 protocol specification dictates how the time stamping is to be done and which parameters are to be recorded. This standard has to be maintained by all vendors that claim to support DNP3 protocol.

Having access to time-stamped data for an end-user is hugely valuable. There are many reasons, but explained below are the top two.

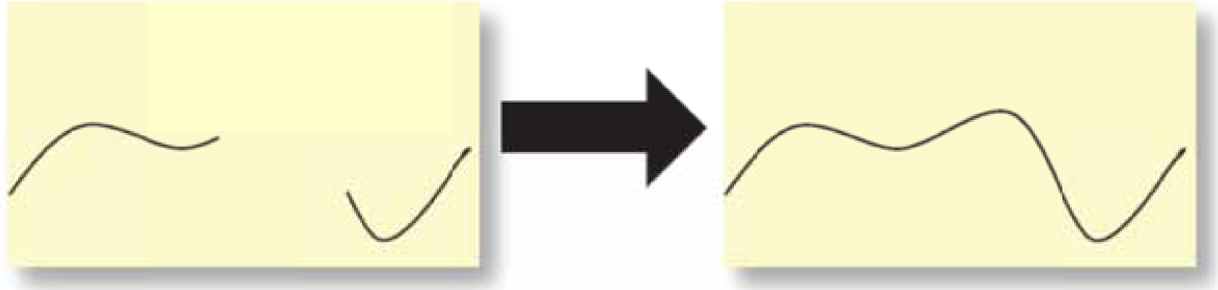
- Many telemetry systems are poll-only systems for a number of reasons — geographical, or by virtue of design, which means that without time stamping, if an event occurs and the device is not polled at that instant in time, the event will be lost. Now, an event like a change of pump status can be stored as the number of times the pump has come ON and the number of times the pump has gone to the OFF state. This is useful information, but it does not provide the time the pumps went ON and OFF. The time information is useful for analysis such as the times during the day the pumps start. Is there a particular time of the day that the pumps start and stop more frequently? Does one pump operate more than the other? If there is a power issue, then correlation analysis can be performed and much more!

- In the event of a communications failure, a device can continue to record the events and store in memory. Once the communication system has recovered, a top-end master will be able to retrieve these events and graphically display, accurately, the events that occurred during the communications failure. This feature is extremely useful for effective maintenance and operation of a telemetry system.



25	11/17/2010 15:14:21.003	1	DNPAI1	4780	1	1	3
24	11/17/2010 15:14:20.683	1	DNPAI1	12248	1	1	3
23	11/17/2010 15:14:20.464	1	DNPAI1	8287	1	1	3
22	11/17/2010 15:14:20.353	1	DNPAI1	5003	1	1	3
21	11/17/2010 15:14:19.364	1	DNPAI0	6	1	1	2
20	11/17/2010 15:14:19.033	1	DNPAI0	3763	1	1	2
19	11/17/2010 15:14:18.815	1	DNPAI0	8603	1	1	2
18	11/17/2010 15:14:18.376	1	DNPAI0	13102	1	1	2
17	11/17/2010 15:14:18.153	1	DNPAI0	7140	1	1	2
16	11/17/2010 15:14:17.503	1	DNPAI0	210	1	1	2
15	11/17/2010 15:14:17.075	1	DNPAI0	3950	1	1	2
14	11/17/2010 15:14:16.964		AI0	8545	1	1	2
13	11/17/2010 15:14:16.853		DNPAI0	22507	1	1	2

11/17/2010 15:14:16.964



Time Synchronization

The DNP3 protocol supports time synchronization. A DNP3 outstation device can be configured to send a time sync request to the master or a DNP3 master can periodically send a time sync command to DNP3 outstation devices. Time sync is part of the DNP3 protocol specification. Key advantages of the time sync function include:

- Accurate and reliable time-based alarm information from a remote device
- Scheduling accuracy — for example, when to switch over from duty to standby pump; generate test unsolicited messages at a particular time
- Most importantly — if time in slave devices is maintained reliably, then it is much easier to implement power saving measures. This is particularly useful in water telemetry systems where it may be less expensive to run pumps at certain times of the day.

Secure Authentication

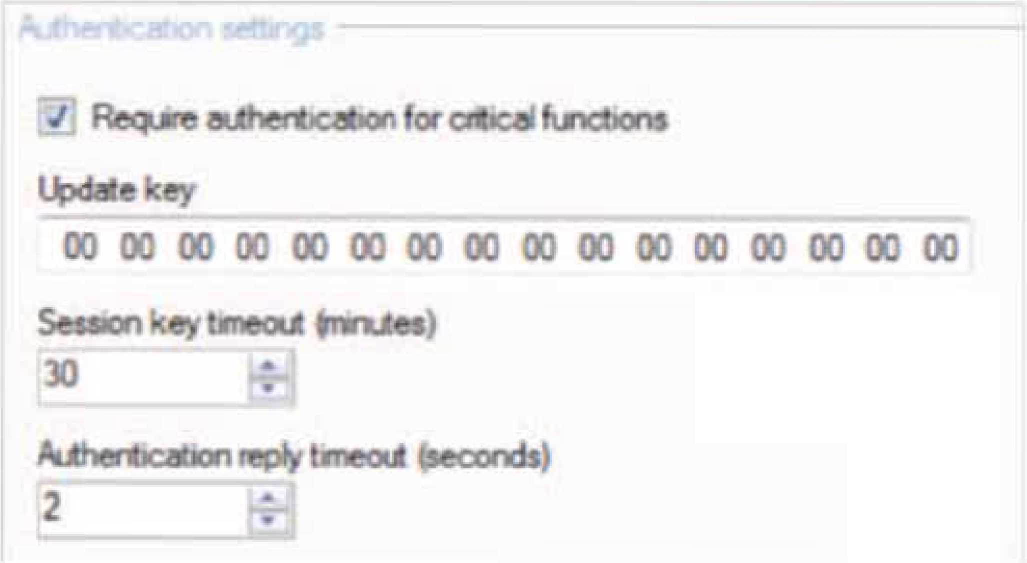
After 9/11, governments around the world have stated that water and wastewater systems are part of the critical infrastructure and as such, must be secured. Also, in the water and wastewater industry, there have been a few well publicized and documented instances of SCADA security breaches that have affected the performance of the systems.

The DNP3 protocol includes IEC62351 version 2 authentication. Authentication is not the same as encryption. Typically, point-to-point encryption is provided by the media (radio, TCP/IP). However, it is entirely possible that at a future date encryption may be an integral part of the

DNP3 protocol. DNP3 secure authentication allows a DNP3 slave or master device to unambiguously determine if it is communicating with the correct DNP3 master or slave.

In water and wastewater systems it is common to issue pump/valve (or similar) operate commands from the top-end master. Without authentication, it is completely possible for someone to intercept a message and relay with modified settings. DNP3 Secure Authentication overcomes this issue, as the DNP3 outstation challenges the DNP3 master to see if the command to operate comes from a legitimate source. The authentication key is updated regularly between a DNP3 master and outstation. This communication is separate and not part of standard DNP3 data transfer messages. If an outstation does not receive an updated key within a specified period of time, or if the key is invalid, then the control commands from DNP3 Master, even if valid, will not be executed by the outstation device.

The DNP3 protocol also uses a more basic form to ensure control commands are executed correctly. This is called "select-before-operate". In this case, a DNP3 Master will first send a "select" command, to which the outstation device will respond and then, if the outstation device does not receive the "operate" command within a specified amount of time, it will not execute the control action.



Authentication settings

☑ Require authentication for critical functions

Update key

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Session key timeout (minutes)

30

Authentication reply timeout (seconds)

2

Diagnostic Information for Each I/O Point

Another inherent feature of the DNP3 protocol is associating diagnostic information for each field object — whether it's pump status, tank level, current flow rate, etc.

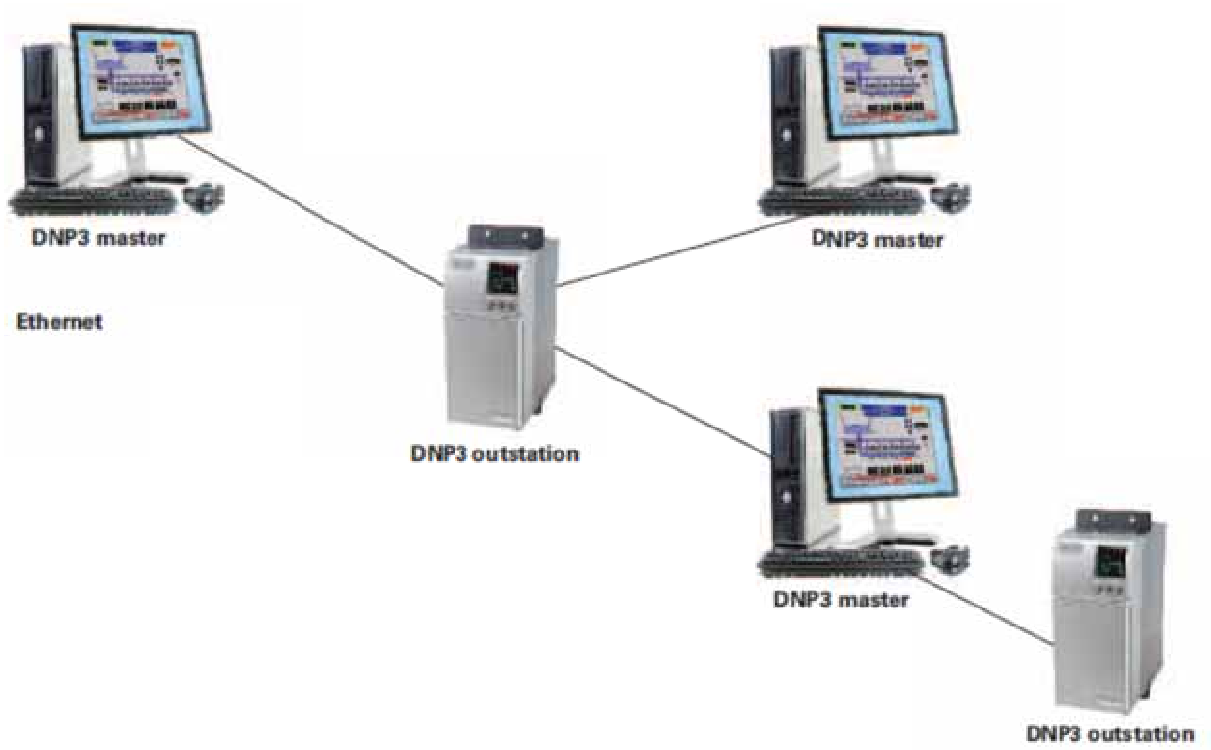
The diagnostic information answers questions such as, is the point online or offline, was it locally forced, chatter- detected, has it been restarted, is the value out of range, and much more? While this is good, what is the purpose and why is it useful?

Again, in typical systems, a status indication for a pump will only show it is ON or OFF, in FAULT, or OK. But when using DNP3 protocol, one can detect if the information regarding the status of the pump is coming from the correct location. This is useful because, remotely, one can tell if wiring is correct. Another example is if the chatter filter bit is SET, then if a field device is going ON/OFF continuously, spurious event logs will not be created. This is very useful when performing maintenance at a location. Individual field I/O points can be isolated, thus eliminating the need to take the entire site out of service.

Communication to Multiple Masters

This is a particularly useful feature, especially in water and wastewater systems. It is typical for a water or wastewater telemetry system to be spread over large areas. This is especially true in countries like the USA, Australia, China, and Brazil. When systems are spread over a large area, it is important for the local operators of the telemetry system to know what is happening, as it will allow them to respond quickly. At the same time, the same data needs to be made available at the system-wide top-end DNP3 master.

DNP3 protocol, with its built in ability to support report-by-exception to multiple masters, can achieve this effortlessly without the need for extensive programming.



Advanced Communications Features for DNP3-Based Telemetry Systems

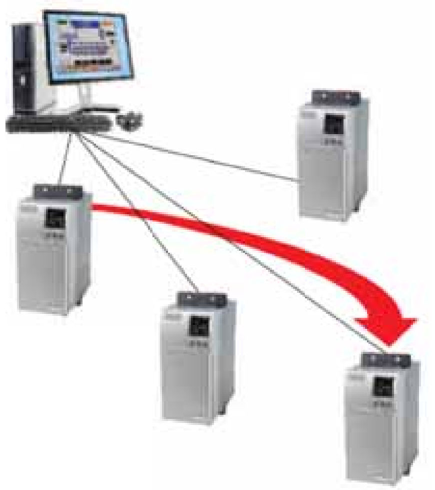
At the very start of this white paper it is mentioned that one of the corner stones of DNP3 protocol is that it is an open protocol with no vendor-dependent variations. Any RTU that claims to support DNP3 protocol must adhere strictly to this rule.

However, the more capable and advanced RTUs have managed to include additional features that do not relate to the actual protocol features/properties or the manner in which DNP3 data in a message is transferred. These additional features focus on the communications itself, which is, getting data from one location to another effectively and efficiently. Some of these features are described below.

- **Peer-to-peer communications.** This allows for local communications between two DNP3 devices. The advantage — if communications to a top-end DNP3 SCADA master is lost, then local RTU systems (like a booster pump station and tank) can continue to operate with all data logged.

- **DNP3 message pass-through.** The DNP3 protocol is primarily a point to point protocol. Point to point type communication architecture is not always feasible in a Water/Waste Water Telemetry system. As such, the more advanced RTUs have the ability to receive a DNP3 message on one port and resend via a second port. Implementation of this feature does not affect the DNP3 protocol compliance requirements. It does however use the advanced communications capabilities of an RTU to provide an effective solution to a multi-layered telemetry system.

- **Data Concentration.** In a multi-layered telemetry system, there are inevitably going to be sub-master RTUs. DNP3 does not have the ability to request local and outstation data from a single RTU. As such, a sub master RTU would have the ability to map data received from an outstation DNP3 device to a new DNP3 object (address), while maintaining all of the original values and properties as provided by the outstation RTU. This ensures DNP3 protocol implementation compliance, but at the same time providing users an effective solution to reduce the complexity in implementing a multi-layered water/wastewater telemetry system.



Conclusion

DNP3 is an exceptional protocol. It is modern, robust, intelligent, and a truly open protocol. While it has been around for close to two decades now, and thus a truly tried and tested protocol, it is still an evolving protocol. This is illustrated by the addition of secure authentication. This white paper has only looked at a fraction of the DNP3 features and how they are useful, in particular, to the water and wastewater industry.

A water and wastewater telemetry system is a complex system with a number of assets and locations to monitor and control. From a communications perspective, it can be a multi-layered system using a variety of communications media such as radio, cellular, PSTN, and fiber to interconnect sites. Then, a top-end graphical SCADA system is required to display all field data in a manner that can be easily understood.

The DNP3 protocol, with its many features listed below, helps enormously in implementing such a complex system and it does help in reducing the complexity of a system. This in turn will help reduce operational and maintenance costs for the end-user.

- Open protocol — allows the end-user to install equipment from different vendors while maintaining a single top end SCADA (or DNP3 master)
- Allows the user to categorize field data, thus allowing for efficient communications and data transfer between a master and outstation
- Ability to log an event with a time and date stamp
- Secure authentication with dynamic key management between a DNP3 master and outstation
- Communication to multiple DNP3 Masters, thus making the same data available at multiple locations