Application Note AN2005-001

WITS DNP3 Usage Overview

Revision 1.6

March 2016

Change history:

Date	Revision	WITS-DNP3 Version	Details
May 2010	1.0	1.0	Incorporating all details up to and including TB #32.
June 7 2010	1.1	1.0	WITS Release 1.0 uses DNP3 secure authentication version 2. Version 5 will be used in a future release later in 2010.
Dec 2010	1.2	1.1	Correct spelling of “Archives” in table 2-1. Update (throughout the notes) to WITS-DNP3 version 1.1
June 2011	1.3	1.2	Rename “Limit Profiles” to “Profiles” and introduce the term “Profile Control Value”. Add the term “Derived Point” to the glossary.
July 2011	1.4	2.0	Correctly capitalise data set names. Introduce DNP3 Secure Authentication version 5.
May 2013	1.5	1.x / 2.x	Remove the requirements of DNP3 Secure Authentication version 5 for the WITS-DNP3 protocol version 1.x stream, creating version “a” of the Application Note. Update to table 2-1 to include the optional sampled data logs in the entry for AN2005-004. Update to table 2-1 to include details of IC record for point number and sample interval (for sampled data logs) in the entry for AN2005-006.
March 2016	1.6	3.0	Merged SAv2 and SAv5 streams back together. Update table 2.1 to include details of IC records for extended logging.

1 Introduction

This Application Note is subject to change. Any questions or comments should be sent to wits@witsprotocol.org.

In 2004 a feasibility study was commissioned to investigate the most appropriate way forward for the UK Water Industry to adopt a standard communications protocol for its telemetry and SCADA applications. The resulting feasibility report recommended that the existing DNP3 open protocol is adopted and should be used in a specified way in order to introduce interoperability and facilitate additional functionality and consequently deliver benefits to each UK Water Management Organisation that adopts it. This WITS Standard Protocol shall be referred to as "The Standard" where applicable within the set of application notes. For further detail on the requirement for The Standard and the results of the feasibility Study, please refer to the WITS website: www.witsprotocol.org.

Within the detailed design phase of the standard protocol project there were a number of discrete pieces of work which were delivered that together provide a sufficient level of detail to enable any vendor of telemetry or SCADA related products to develop their own products to meet the specification for The Standard.

This application note is an introduction to a set of notes used to fully describe the application of DNP3 within the UK Water Industry.

This document describes version 3.0 of the WITS Standard Protocol. Future releases may extend the functionality of the protocol.

2 Details

2.1 Application Notes

The following table describes the full range of WITS application notes used to define The Standard:

Table 2-1, Details of WITS Application Notes

Application Note	Name	Description
AN2005-001 (this note)	WITS DNP3 Usage Overview	Provides an introduction to the WITS group and outlines how DNP3 is used to facilitate the telemetry functionality required by the UK Water Management Organisations. Also serves as a reference point for all of the application notes in the set which together form The Standard.
AN2005-002	WITS Interoperability	This application note is used to describe the mechanisms through which vendors of different Master Stations and Field Devices can interoperate with each other and conform to The Standard. It looks at a generalised technical view of The Standard and the mechanisms used to configure Master Stations from vendor specific Configuration Applications.
WITS AN2005-003	WITS Use of Object Group 0	The use of DNP3 Object Group 0 is fully defined in this note. Its role is to assist with the achievement of the key objectives for asset management and interoperability of Field Devices through device identification (based on product manufacturer name, device type etc.). WITS have defined the use of 2 attribute sets, the standard index 0 and a WITS attribute set. The WITS attribute set is used to facilitate WITS protocol version number. This Application Note lists the specific variations which are mandatory, optional and 'ignored' and details how they are used. The usage information includes additional details which will allow vendors to be aware of the type of data expected and the maximum length of any message.
WITS AN2005-004	WITS Data Logging	Log files store data with a timestamp which is read by a Master Station via DNP3 File Transfer at a later date. This Application Note defines a standard file structure and provides information which Field Device historic log files must conform to in order to be WITS compliant. It is not necessary for a Field Device to have the overhead of supporting a full file system, this is especially important for small devices. The relevant log information is requested via means of a defined file naming convention which, for the periodic and event log files, allows for only destructive read of a time log for all points for all time. Examples of file header and contents are given in the Application Note and log file sizes are discussed. The Application Note also describes the optional process for the ad-hoc retrieval of high speed sampled data on a selective basis – protocol versions 1.3 / 2.1 and higher.

Application Note	Name	Description
WITS AN2005-005	WITS Data Sets	This Application Note details the use of DNP3 Data Sets used to report data to a Master Station. Each Data Set is registered and has a prototype UUID. There are 7 defined Data Sets in WITS: • Analogue Events • Counter Events • Binary Events • Field Device Health Check • Callback • Application Manager • Action Inhibit The Point Event Data Sets provide the facility to transfer information regarding a point event, such as a change of state (i.e. a limit transgression for an analogue point) and includes the new state and a time stamp in addition to the actual captured value. The Health Check Data Set contains flags which are used to provide device health information to a Master Station. Information contained within the Field Device Health Check Data Set is comprised of a range of WITS flags and a range of user defined flags specific to the Field Device assigned by the vendor. The note describes the Health Check Data Set format. The Callback Data Set provides the facility to initiate an inbound connection from a Field Device to the Master Station. This can be used to test alternative communication channels. A Field Device may support application programs. The Application Manager Data Set is used to identify and control the application programs that are running on the Field Device. The Action Inhibit Data Set is used to control the reporting of point changes (i.e. state, DNP3 object flags or other changes) for a single point or all points on a Field Device.
WITS AN2005-006	WITS Incremental Configuration	It is recognised that Bulk Configuration of a Field Device for every small parameter change is not a suitable mechanism, especially for medium and large devices. This Application Note describes the use of file transfer to provide Incremental Configuration updates to Field Devices through a WITS defined file format. Each of the following Incremental Configuration items are described in detail in the Application Note: • Device on/off scan • Connection details • Scheduled connection • Point on/off scan • Override point • Analogue range/scaling • Analogue Limits • Counter Limits • Point archives • Binary States • Profiles • Rate of change calculations • DNP3 Object Flag Actions • Minimum • Maximum • Mean • Integral • State Counter • State Runtime • Profile Control Value • High speed sampled data • Incident Logs • Significant change of value
WITS AN2007-001	WITS Detailed Interoperability	Further to the interoperability document [AN2005-002] this document describes more detailed aspects of interoperability. In particular it contains the detailed configuration process and a full DNP Implementation Table.

2.2 Design Philosophy

The following is a summarised view of how The Standard is defined within the application note set.

2.2.1 Configuration

File transfer of Bulk Configuration is used for the initial configuration download from Master Station to Field Device. The contents of this file are entirely vendor specific as it was found impractical to impose one standard to a wide variety of Field Devices from different manufacturers. As a minimum, this file must contain a point database.

Although the DNP3 standards define an XML Device Profile, it has been decided (in 2006) that this document is insufficiently stable, therefore it is not used. Instead WITS specifies its own XML Device Profile to express the capabilities of a Field Device or Master Station.

File transfer is used to download Incremental Configuration update files containing a defined range of information such as historic logging rates etc. This file is not vendor specific and the contents are defined as part of The Standard [AN2005-006].

File transfer is also used to download application programs to the Field Device. Management of application programs is achieved through the use of an Application Manager Data Set that reports the version of the application, its status and possible controlling actions. The Application Manager Data Set is defined as part of “The Standard” [AN2005-005].

2.2.2 Data Logging, Point Changes etc.

A defined file format has been specified to facilitate the transfer of historic data logged at the Field Device [AN2005-004].

Data Sets are used for Field Devices which support functionality to annunciate point changes and provide an indication of Field Device health [AN2005-005]. WITS devices do not use the standard DNP3 event objects to report changes of binary states and analogue or counter values. WITS defines the term “point changes” to mean:

- A change in a point’s **DNP3** object flags
- A state change (e.g. a change into a specific binary state, a change of value that transgresses a limit value)
- Other changes, for example a significant change in point value (e.g. change of value by more than the configured deadband)

Instances of WITS data set event objects or entries to the WITS data log file may be used to report point changes.

WITS incremental configuration records [AN2005-006] provide a method to configure an action to be taken when there is a change in the DNP3 object flags or the state of point (binary state or transgression of a limit). The action to be taken for other changes cannot be configured using WITS incremental configuration records and therefore must be configured by a proprietary method.

WITS data sets provide a method to inhibit the level of reporting of point changes by temporarily reconfiguring the actions of a point. An inhibit applies to all point changes regardless of whether the action for the particular point change was configured by WITS incremental configuration records or by a proprietary method.

2.2.3 Interoperability

A key focus has been placed on interoperability to allow a wide range of vendors and Field Devices to adopt The Standard. This is largely achieved through the use of a specified mechanism of configuration [AN2005-002 & AN2007-001], predefined data sets [AN2005-005] and defined file formats for incremental configuration [AN2005-006] and data logging [AN2005-004].

2.2.4 **Security**

The DNP3 Secure Authentication (SA) standard has been adopted by WITS. WITS-DNP3 protocol versions 1.x implemented SA version 2 (SAv2), as defined by the DNP3 volume 2 secure authentication supplement (DNP3 Vol2-Supp1 Secure Authentication v2 2008-07-31.pdf).

In 2011 the DNP User Group published SA version 5 (SAv5 - now documented in IEEE 1815-2012) and deprecated SAv2. WITS-DNP3 protocol versions 2.x implemented SAv2. The “deprecation” of SAv2 means that its use is discouraged in new devices but may exist in current implementations. SAv5 provides authentication with:

- Improved resilience to denial of service attacks
- Improved collection of potential cyber-attack statistics
- The option for remote “update key” changes. This option is currently under discussion by the DNP User Group and may change. WITS devices are not expected to support this until the details are finalised by the DNP User Group.

Because the adoption of SAv5 is not mandatory (but recommended by both the DNP User Group and the WITS PSA Committee) devices implementing WITS-DNP3 version 3.0 should:

- If a new Master Station implementation, support both SAv2 and SAv5 (to ensure interoperability with new Field Devices that choose to implement SAv5).
- If a new Field Device, support SAv5. However, if there are no WITS Master Stations yet supporting SAv5 then the Field Device may implement SAv2.
- If an existing Master Station or a legacy Field Device, optionally upgrade to support SAv5.

The implementation of security is discussed in further detail within [AN2005-002 and AN2007-001].

2.3 Glossary of Terms

The following terms are commonly used throughout the set of application notes.

Table 2-2, Glossary of terms

Term	Description
Archive data	Also called historic data. E.g. The periodic logging of analogue points.
ASDU	Application Service Data Unit. Contains enough information to pass to an application program to identify the data and to process it into the database.
Bulk Configuration	The file used by a Field Device containing any proprietary configuration required to meet the Field Device's operational requirements.
Configuration Application	The vendor specific software tool used to generate Bulk Configuration for Field Devices.
Derived Point	A point in the Field Device or Master Station database whose state/value is not determined from a physical item of plant. The state/value is determined by logic, internal to the Field Device or Master Station.
Download	The process of data being transferred from a Master Station to a Field Device.
Field Device	The telemetry device located on site. This could refer to a single instrument interface, outstation, RTU, PLC etc.
File transfer	The process of transferring files from one DNP device to another.
Incremental Configuration	The files used by a Field Device containing WITS Field Device configuration.
Master Station	The product provided by a vendor containing a centrally managed database of configuration, alarm handling etc.
The Standard	The WITS standard protocol.
Upload	The process of data being transferred from a Field Device to a Master Station.
User	One of the UK Water Management Organisations.
UUID	Universally Unique Identifier.
Vendor	A supplier of Field Devices and/or Master Station equipment.
WITS	Water Industry Telemetry Standards.
XML	eXtensible Markup Language.