Application Note AN2005-002

WITS Interoperability

Revision 1.7

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	Correction to data set name in 2.6.3
December 2010	1.2	1.1	Modified change history table layout
June 2011	1.3	1.2	Rename “Limit Profiles” to “Profiles” and introduce the term “Profile Control Value”. Added new section at end of part 2 “Data Derivation”. Added section about “Backwards Compatibility”.
July 2012	1.4	2.0	Correctly capitalise data set names. Added statement about static objects to be included in class 0 poll responses. Introduce DNP3 Secure Authentication version 5.
May 2013	1.5	1.3	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 section 2.6.3 to introduce the concept of counter values being reset after a periodic log. Add section 2.4.7 describing the use of locally applied action inhibits. Update to section 2.6.3 to introduce the concept of logging of high speed sampled data.
February 2015	1.6	1.x / 2.x	Clarify the priority of connection records in section 2.3. Add “sampled data” to the list of IC topics in 2.5.2. Clarify the statement about the use of standard DNP3 event objects in section 2.4.2. Added section 2.4.8
March 2016	1.7	3.0	Merged SAv2 and SAv5 streams back together. Added details of the additional logging functions (incidents and significant changes). Added section 2.7 – optimised use of the protocol

1 Introduction

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

The Water Industry Telemetry Standards (WITS) group is a body representing users and vendors within the UK that have together defined how the DNP3 standard should be implemented in a coherent manner within the UK water industry. As a result of the detailed design project, a set of application notes have been generated that define the methodology of the implementation. Application note [AN2005-001] provides an overview and an introduction to the set of notes which together define The Standard.

This application note describes the WITS approach to configuring Field Devices to achieve interoperability of Field Devices and Master Stations from the widest possible range of vendors.

In this context a Field Device may be a Remote Telemetry Unit, a data logger or any other device used by the WITS members to collect asset information (process data, static asset data, images, etc) from remote sites. A Master Station is a software application that is used to collect and process data from Field Devices. The main aim of WITS interoperability is to enable users to configure Field Devices from a range of vendors on their Master Station with minimal additional software.

The process and applications should be such that configuration can be initiated from the Master Station or the Field Device.

The process must be secure from the threat of electronic attack, such as spoofing valid Field Devices or Master Stations or denial of service of Field Devices and/or Master Stations.

1.1 References

[AN2005-001] Application Note AN2005-001 - WITS DNP3 Usage Overview

[AN2005-003] Application Note AN2005-003 - WITS Use of Object Group 0

[AN2005-004] Application Note AN2005-004 - WITS Data Logging

[AN2005-005] Application Note AN2005-005 - WITS Data Sets

[AN2005-006] Application Note AN2005-006 - WITS Incremental Configuration

[AN2007-001] Application Note AN2007-001 - WITS Detailed Interoperability

2 Details

2.1 General

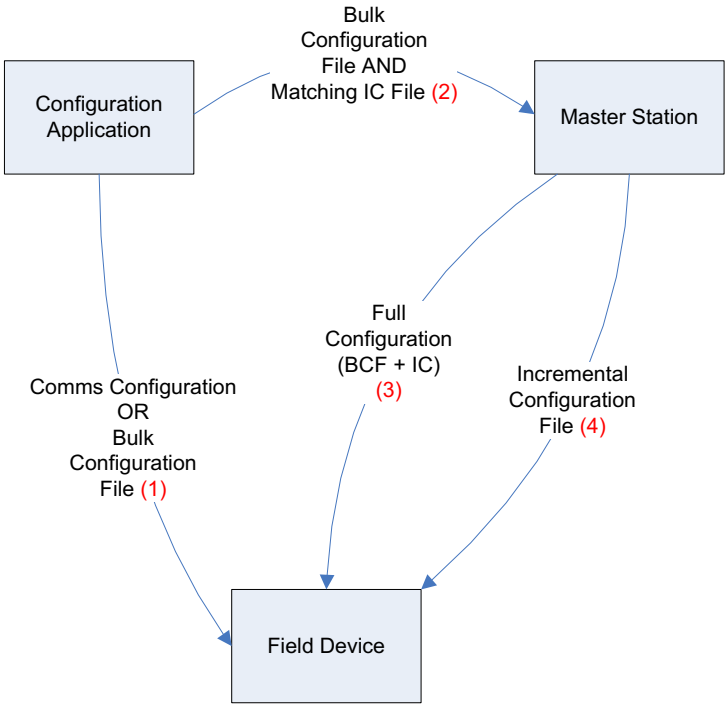

Figure 1, Overview of automated Master Station configuration and interoperation

Figure 1 shows an overview of the process of Field Device configuration within the context of WITS. The data flows are as follows:

(1) The Configuration Application either:

1. Provides the Field Device with enough communications configuration to allow the Field Device to contact a Master Station and download a Full Configuration.
2. Prepares a Bulk Configuration file and configures the new Field Device.

(2) The Bulk Configuration file from flow (1) and an Incremental Configuration file matching the WITS configuration in the Bulk Configuration file can be taken from the Configuration Application and made available to the Master Station and then (3) the Master Station sends the Full Configuration (Bulk Configuration file, any application programs and any Incremental Configuration) to the Field Device to configure the Field Device to a known state.

(4) Once configured using either method thereafter the Master Station uses Incremental Configuration to change the Field Device as required by the user.

After initial configuration, Bulk Configuration, Application Program and Incremental Configuration changes executed from the Master Station will be performed using file transfer (see [AN2005-006]). Any local changes executed from the Configuration Application will result in the device becoming marked as 'Configuration Changed'. This allows the Master Station to optionally reconfigure a Field Device marked as 'Configuration Changed' with its known full configuration and restore the device to a known configuration state.

Any changes required to the configuration of the Field Device, which are outside the scope of Incremental Configuration changes detailed in [AN2005-006], will require a further Bulk Configuration or Application Program download.

It may be the case that associated devices such as HMIs, PLCs, etc could be configured using the vendor's Configuration Application although the WITS focus will remain on Field Devices such as RTUs and data loggers until such time as this is established.

2.2 Use of DNP3

The WITS protocol builds on the industry standard DNP3 Protocol to provide the extra functionality required by the users. A level of compliance to DNP3 Level 2 is assumed. Other functions and object groups beyond Level 2 are also required for WITS. These are detailed in an implementation table contained in [AN2007-001].

WITS does not seek to change the DNP3 protocol at all. However where open interpretation is allowed for within DNP3, WITS may specifically define an interpretation to support a WITS function. So, for example, the ONLINE flag for a point is used by a Field Device to signify whatever the Field Device vendor normally indicates as well as that the Field Device has the point on or off scan with respect to WITS.

The thrust of the WITS protocol design effort has been towards using DNP3 to implement the WITS functions. Vendor specific meanings for DNP3 protocol points which were open to interpretation may not carry forward to a WITS implementation.

2.3 Controlling Connections

DNP3 does not overtly address the subject of device connections to the Master Station, when the connections are created and when they are destroyed. Within the scope of DNP3 this was not necessarily a requirement as the common mode of deployment is in an always connected WAN/LAN, for example, within an electricity substation.

Within the water industry, this level of connection is not normally maintained to Field Devices. Master Stations would connect to Field Devices or vice versa only occasionally to allow the device to be serviced or point changes to be sent. This normally disconnected mode of operation has required a model for connection to be considered within the WITS protocol.

If a Field Device needs to connect to the Master Station to allow the collection of DNP3 events or because it is scheduled to do so, the WITS Field Device must internally assert a "WITS request to connect" to the appropriate internal vendor specific Field Device connection subsystem. Subject to its own rules this subsystem should attempt to connect to the Master Station if possible. Should no reason preventing it be asserted, the subsystem should connect immediately. The rules for asserting the "WITS request to connect" signal are defined within the WITS protocol. Note that this need not be the only reason for the Field Device connecting to the Master Station other vendor specific reasons may exist. Further details on the connection regime can be found in [AN2007-001].

In making a connection the Field Device will use a prioritised list of possible connections. This list is set up using Incremental Configuration; see [AN2005-006]. The Field Device should use the list as a prioritised list, with the first entry in the list being assumed the one with the highest priority.

2.4 Data Set Definitions

Application note [AN2005-005] defines the use of DNP Data Sets for reporting point changes and health status. An overview of data sets is presented in this section.

2.4.1 Data Sets on the Master Station and Field Devices

All WITS data sets will be defined on the Field Device.

All WITS data sets are prototypes and therefore the structure is independent of any specific Field Device.

2.4.2 Point Event Data Set Definition

In WITS, these data sets are used in place of standard DNP3 event objects. In particular they are used to convey analogue, counter and binary state changes, but they are also used to convey any other point events. The following data sets are used to capture the state changes described:

- Analogue Event Data Set: A data set event based on this data set may be created on transgression of a defined limit. The data set has an implied direction derived from the limit which is positive or negative going. The terms raise and clear are used to indicate transgression of the limit as a point enters and leaves a state respectively. Level thresholds (hysteresis) and persistence may be defined against this state change.
- Counter Event Data Set: A data set event based on this data set may be created as a defined level is reached by the counter. The terms raise and clear are used to indicate transgression of the limit in the defined direction and the opposite direction respectively. Counters will continue to generate data sets as they increment into each of the defined states. A counter limit that is in a raised state can be cleared when the counter is set to a value beneath the limit for a state. Changes to the counter value can be from DNP3 commands such as FC9 (freeze and clear) and FC10 (freeze and clear no acknowledge) to set the counter value to zero. Other mechanism such as IEC-61131 programs may also set an arbitrary value for a counter.
- Binary Event Data Set: A data set event based on this data set may be created whenever a binary or double binary point changes state.

For any state change, the point's configuration defines whether a DNP3 event should be generated and when such an event is generated, whether a connection is required from the Field Device to the Master Station.

WITS devices use these Data Sets to report events instead of using the standard DNP3 object groups:

- Object Group 2, Binary Input Events
- Object Group 4, Double-Bit Binary Input Events
- Object Group 11, Binary Output Events
- Object Group 22, Counter Events
- Object Group 32, Analog Input Events
- Object Group 42, Analog Output Events

WITS devices use the standard DNP3 object groups to report other events.

Multiple individual state change levels can be set for any analogue or counter point, the exact instance of the state change reported is given by a unique point limit index which is set when the state change is configured on the device.

When any point event is reported using any of these point event data sets the Field Device must ensure that the static value of the point is included in all class 0 poll responses (i.e. the class 0 poll responses contains the relevant g1, g3, g10, g20, g30 and g40 DNP3 objects for every point reported with these data sets). The DNP3 option to not include the static objects in the class 0 poll response shall not be used.

2.4.3 Health Check Data Set Definition

A Health Check Data Set consists of a 32 bit mask for WITS defined status indicators and a 32 bit mask defined by the Field Device vendor for expressing Field Device specific conditions. These bit masks will be available to allow vendors to report the status of Field Devices using individual bits of each double word (allowing 64 possible status details to be reported). Each bit is allocated to specific state change conditions:

- Data set event with connection request (e.g. battery voltage low)
- Data set event (e.g. configuration changed)
- Or to static conditions (e.g. device off scan)

The meaning of the Field Device specific health check data bits is detailed in the device profile provided by the Field Device vendor. Note that this Data Set is mandatory for a WITS compliant Field Device.

2.4.4 Callback Data Set Definition

The Callback Data Set is provided as a means to testing a Field Devices ability to raise an unsolicited response on a specified communications path to the Master Station.

2.4.5 Application Manager Data Set Definition

The Application Manager Data Set is used to identify and control the application programs that are running on the Field Device. This data set can be used to query the status of a running application, provide information on the allowed control operations on the program (initialise, start, stop, pause and resume) and issue commands to change the state of the application.

2.4.6 Action Inhibit Data Set Definition

The Action Inhibit Data Set is used to control the reporting of point changes (i.e. state, DNP3 object flag or other changes) for either a single point or all points on a Field Device. A maximum duration for the inhibit may be specified. A point that has actions inhibited is still able to report current values when requested and continue periodic logging of values.

2.4.7 Locally applied action inhibits

Protocol versions 1.3 / 2.1 and higher describe how a Field Device may apply action inhibits itself, by simulating the receipt of an Action Inhibit Data Set. There may be scenarios where the Field Device knows that it needs to suppress some data reporting to the Master Station (for example during times of site power fail or when the site is manned and is being exercised for maintenance). In this case the Field Device may apply action inhibits to data points to stop them being reported to the Master Station.

2.4.8 Values and states

WITS-DNP3 has the concept that I/O points have a ***value*** and a ***state***. This is easily understood for analogue and counter points: these points have a ***value*** and a ***state*** which is either “normal” or defined by where the value lies within bands set by configured threshold values. When persistence is configured then a point may have a ***value*** which lies within one of the threshold bands but the new value may not have persisted long enough for the ***state*** to correspond to that threshold band. The WITS-DNP3 protocol uses standard DNP3 objects to show the ***value*** of the point and uses the WITS Analogue Event Data Set to show the changes in ***state*** of the point.

This concept of ***value*** and ***state*** is not so obvious for binary points (single-bit binary input points, double-bit binary input points and binary output points).

If a binary point is currently set to 1 is this its ***value*** or its ***state***? With no persistence configured then 1 would be both its ***value*** and ***state***. If persistence is configured then the ***value*** would be 1 and the

state would only be 1 after the point has had a ***value*** of 1 for the persistence time. However, standard DNP3 objects only carry information which relates to the point's ***value*** (although the DNP3 documentation refers to this as the state). Likewise the WITS-DNP3 Binary Event Data Set, and a WITS log file entry for a binary point, only shows the current ***value*** and an indication that the ***state*** may have changed to be the same as the ***value***. There is no static object that can be read to determine the current ***state*** of a point.

2.5 Configuration

2.5.1 Config Corrupt IIN

This is the standard DNP3 internal indication (IIN), "CONFIG_CORRUPT". A Field Device that requires configuration data from the Master Station is expected to assert this indication. When the Master Station detects that this is set on the Field Device, it will initiate a download of Full Configuration. The Master Station will then activate the configuration using FC31. The Field Device will clear the CONFIG_CORRUPT indication after successfully processing the activation command.

2.5.2 Field Device Configuration

Field Devices may be configured by one of two methods:

- Initially, via a vendor specific Configuration Application attached locally to the Field Device. The Configuration Application will use proprietary commands to configure the Field Device. Once configured by the Configuration Application, the Field Device will enter one of two states:
    - Comms Configured – the device does not contain a valid configuration to run telemetry but is capable of contacting the MS to receive a full configuration. Once a configuration has been received from the MS the device can run telemetry.
    - Independently Configured – the device is capable of running telemetry immediately. When in contact with the Field Device the Master Station will detect the current configuration as loaded by the Configuration Application and may elect to a) download a full configuration to the device, b) continue with the current Field Device configuration or c) upload the configuration from the Field Device and populate its configuration database. Options a) and c) allow the Master Station to maintain known configurations of all Field Devices on the system.
- After initial configuration the Master Station uses DNP file transfer of Incremental Configuration, Application Programs or Full Configuration to download subsequent configuration changes. "Activate Configuration" is then used to commence use of the new configuration on the Field Device.

A fully configured Field Device will be configured with Bulk Configuration, along with any necessary application programs and Incremental Configuration. The Bulk Configuration must at a minimum include:

- A point database containing information on the number of points configured for use with DNP3. This indicates to a Field Device the number of points that should be returned in a standard DNP3 integrity poll. Only points from within this range should be set up on the Master Station.

Only one Bulk Configuration File (BCF) can exist on a WITS Field Device. The contents of the BCF are vendor specific and not interpreted by the Master Station. As such vendors can choose to create a single BCF which represents a series of files for use at the Field Device. However such details are outside the scope of WITS. The Master Station is responsible for managing the association of each BCF and corresponding Field Device.

The user creates Field Devices and configures points on those devices via the Master Station (or in some cases the Master Station may use the configuration from the Field Device to achieve this). The Master Station uses this information to configure the Field Device using Incremental Configuration as defined in [AN2005-006]. Field Device properties that can be configured using Incremental Configuration are:

- Device on and off scan. Suspends data set events being generated (and any connection requests) and data logging for an entire Field Device.
- Connection information. Provides the Field Device with a list of possible connections to use to communicate with the Master Station.
- Scheduled connection configuration. For those Field Devices who must connect to the Master Station at regular intervals, provides details of when those connection times are.
- Point on and off scan. Suspends data set events being generated (and any connection requests) and data logging for an individual point on a Field Device.
- Override point. Allows the Master Station to force the Field Device to report and log the override value until the override is released.
- Analogue point range/scaling information
- Analogue limits configuration
- Counter limits configuration
- Binary states configuration
- Point archive configuration
- Profile configuration
- Rate of change calculations
- DNP3 object flag actions
- Minimum. Allows a minimum value to be calculated for a specified analogue point.
- Maximum. Allows a maximum value to be calculated for a specified analogue point.
- Mean. Allows a mean value to be calculated for a specified analogue point.
- Integral. Allows an integral value to be calculated for a specified analogue point.
- State Counter. Allows state changes for a specified point to be counted.
- State Runtime. Allows the amount of time a particular point spends in specific states to be measured.
- Profile control value. Allows the current value from a profile to be stored in a point and then used as a control value or set-point.
- High speed sampled data. Allows analogue input points to be configured to have high-speed sampling and data storage.
- Incident logging. Allows incidents to be configured that result in additional logging of point values.
- Significant changes. Allows a Field Device to be configured with a deadband value to be used to determine if a significant change of value has occurred, as well as configuring the action to take when a change does occur.

If the Field Device is replaced by the same type of device then the Master Station should download a Full Configuration exactly as it was configured just before replacement. When the new Field Device is next in contact with the Master Station it will be in either the Independently Configured or Comms Configured states which will indicate to the Master Station that the Field Device requires reconfiguration.

If a Field Device rejects a configuration change because it is invalid, the Field Device may continue to operate with the old configuration and therefore is still in the previously configured state.

If a Field Device fails to apply configuration then the Field Device should assert CONFIG_CORRUPT.

2.5.3 Configuration Application

The Configuration Application may be a part of a vendor's Master Station application or it may be a stand-alone tool provided by a Field Device vendor. The Configuration Application must be capable of generating Bulk Configuration Files (and matching Incremental Configuration Files) for the Field Devices that they support.

2.6 General

2.6.1 Security

Experts from a number of standardisation bodies (including the IEC, IEEE, DNP3 Technical Committee) have collaborated to develop standards for implementing security features into SCADA protocols. Details of these standards can be found in IEC62351. The DNP3 Technical Committee created a document: DNP3 Vol2-Supp1 Secure Authentication v2 2008-07-31.pdf. This standard has been adopted by WITS in the WITS-DNP3 protocol versions 1.x. The document is intended to deliver the following:

- A mechanism for authenticating Field Devices
- A mechanism for implementing message sequencing

A mechanism for the remote changing of the pre-shared "update" keys has been developed and, with other security enhancements, is now documented as SAv5 (see IEEE 1815-2012). Support for SAv5 is now adopted in the WITS-DNP3 protocol versions 2.x.

Devices supporting WITS-DNP3 protocol versions 3.0 and higher may support either or both versions of secure authentication. The version that they are currently configured to support is reported in a device attribute object (see AN2005-003).

Master Stations may be required to communicate with legacy Field Devices that implement SAv2. WITS compliant Master Stations will therefore be required to support both SAv2 and SAv5 (and any future versions of Secure Authentication as they are released from the DNP User Group).

Technical details of the implementation of Secure Authentication in WITS-DNP3 can be found in section 4.10 of AN2007-001.

2.6.2 Cold and Warm Start Behaviour

A Field Device must support cold restart (function code 13) and warm restart (function code 14). These are defined in the DNP3 documentation. After either restart the Field Device must attempt to start with basic configuration present such as DNP3 address, connection information etc. This functionality is described in [AN2007-001].

2.6.3 Log Files

A Field Device may support the time logging of analogue and counter points for collection via DNP3 file transfer routines (often referred to as periodic logging).

Optionally, the Field Device may be configured (using incremental configuration, see AN2005-006) to reset a counter value back to zero after it has been periodically logged. This enables the Field Device to provide log details of specific counter point values seen per log period.

Binary points should use the Binary Event Data Set for reporting state changes. The periodic logging is set up via incremental configuration and reported back to the Master Station using file transfer (see AN2005-004).

A Field Device may also support event logging where an event could be a change of state or a significant change in value. Event logging may be used with any type of point.

Selected input points may also be subjected to a higher speed logging process, independent from the periodic logging, and referred to as high-speed sampled data logging. These sampled data log files are normally available in the Field Device for a shorter length of time from the periodic log files – and operate in a cyclic form (newest data overwriting the oldest). The contents of the sampled data log files have the same record structure as the periodic log files (see AN2005-004). The sampled data log files are only retrieved by the Master Station on an ad-hoc basis, normally initiated by the user at the Master Station.

Finally, a Field Device may also log data as a result of an incident. Incidents are defined as changes of state of a point.

2.6.4 Local Time / Universal Time

All time values sent between the Master Station and the Field Device will always be in UTC. However, the Field Device may need to use a local time which differs from UTC, for example when sending data to a local display. It is the responsibility of the Field Device to manage local / UTC time, and any configuration of these attributes will be achieved through the vendor specific Bulk Configuration.

Note that, unless stated to the contrary, all references to time in the WITS application notes refer to UTC.

2.6.5 Scaled Values

All analogue point values will be reported to and from the Field Device as scaled values using single precision floating point number representation. Counters and binaries are not scaled.

2.6.6 Binary Coded Decimals

WITS Field Devices will locally manage Binary Coded Decimals (BCDs), and translate them to analogue points or counter points for presentation to the Master Station. This principle will apply for all the mechanisms used to communicate data to the Master Station, including data transfer via polls and data transfer via log files.

2.6.7 Data Transfer

All multi octet fields are little Endian.

2.6.8 Date Alignment

For any WITS-compliant systems, the start of the week is defined as Monday at 00:00:00 (i.e. midnight between Sunday and Monday).

2.6.9 Data Derivation – continuous or periodic

WITS-compliant Field Devices may be computing derived data values such as state runtime. Some devices are capable of computing these values on a continuous basis i.e. for state runtime computing the values every 1 second and thus maintaining an accurate derived value. Other devices may only be able to compute the values on a periodic basis where the period is greater than 1 second. In this latter case the derived value is only as accurate as the computing period. The Device Profile for a WITS-compliant Field Device shows if data derivations are computed **continuously** or **periodically**.

2.6.10 Backwards Compatibility

It is recommended that a Field Device have a setting that defines which version of the WITS standard it will use in order to allow it to fully interoperate with Master Stations that only support an older version of the WITS standard. This setting may be stored in the Bulk Configuration file.

Log files and configuration files generated by the Field Device can then use the appropriate format for the version of WITS supported by the Master Station.

2.7 Optimised use of the WITS-DNP3 protocol

When a communications session between the Master Station and Field Device is first established there can be a significant number of messages being exchanged. Analysis of these messages has shown that the number of messages can be reduced if the Master Station can make some assumptions about the Field Device behaviour. Details of using the protocol in this “optimised” mode can be found in [AN2007-001]. Field Devices show that they behave in this assumed manner with an indication in their Device Profile.

The sizes of some of the messages used in the optimised mode can also be affected by how the Master Station and Field Device is configured. Suggestions for optimising the configuration can be found in [AN2007-001].