PROCEDURE

FIELDCOMM GROUP™

Connecting the World of Process Automation

HART®

COMMUNICATION PROTOCOL

WirelessHART Device Registration Procedure

HCF_PROC-14, PD20014
Revision 2.0

Release Date: 9 May 2020

Release Date: 9 May 2020

Document Distribution / Maintenance Control / Document Approval
To obtain information concerning document distribution control, maintenance control and document approval, please contact the FieldComm Group at the address shown below.

Trademark Information
HART® and WirelessHART® are registered trademarks of the FieldComm Group, Austin, Texas, USA. Any use of the term HART or WirelessHART hereafter in this document, or in any document referenced by this document, implies the registered trademark. All other trademarks used in this or referenced documents are trademarks of their respective companies. For more information contact the FieldComm Group Staff at the address below.

FieldComm Group
9430 Research Boulevard
Suite 1-120
Austin, TX 78759, USA

Voice: +1 512-792-2300
FAX: 1-512-792-2310

http://www.fieldcommgroup.org

Use of imperatives
The key words (imperatives) "must", "required", "shall", "should", "recommended", "may", and "optional" when used in this document are to be interpreted as follows:

Must	**Must**, **Shall**, or **Required** denotes an absolute mandatory requirement. For example, "All HART Field Devices must implement all Universal Commands"
Should	**Should** or **Recommended** indicates a requirement that, given good cause/reason, can be ignored. However, the consequences of ignoring the requirement must be fully understood and well justified before doing so.
May	**May** or **Optional** identifies a requirement that is completely optional and can be supported at the discretion of the implementation. May can be used to identify optional Host Application or Master functionality and, when this is the case, does not imply the function is optional in Field Devices.

Intellectual Property Rights
The FieldComm Group does not knowingly use or incorporate any information or data into the HART Specifications which the FieldComm Group does not own or have lawful rights to use. Should the FieldComm Group receive any notification regarding the existence of any conflicting Private IPR, the FieldComm Group will review the disclosure and either (a) determine there is no conflict; (b) resolve the conflict with the IPR owner; or (c) modify this specification to remove the conflicting requirement. In no case does the FieldComm Group encourage implementers to infringe on any individual's or organization's IPR.

Table of Contents

Index to Tables

Preface

This preface is included for informational purposes only.

The WirelessHART Device Registration Procedure is part of the overall FieldComm Group Quality Assurance, and Registration Program (FCG PD10026).

The WirelessHART Device Registration Procedure Revision 2.0 ensures that devices registered with the FieldComm Group meet the requirements outlined in the Protocol. All HART products must demonstrate Protocol conformance and be validated against the Specification requirements.

This WirelessHART Device Registration Procedure defines procedures for testing and registering conformant WirelessHART-enabled devices. This procedure is intended to guide members through the registration process and provide member companies with a way to elevate the prominence of devices registered with the FieldComm Group. All devices must be tested by the supplier prior to submittal to the FieldComm Group for testing.

Testing by the FieldComm Group validates that the device data submitted meets Protocol requirements. Manufacturers successfully completing the registration process will be provided with and are encouraged to use the "HART Registered" mark on their registered products.

Both Manufacturers and Users rely on the FieldComm Group to confirm that the Protocol requirements are implemented in a conforming way, thus ensuring quality and interoperability of all devices that claim to be HART compliant. The elements of the procedure include:

- All device submissions must be complete with test data to support test performed
- All submissions will be tested by the FieldComm Group to be consistent with the Specification
- FieldComm Group may perform additional tests on devices submitted
- Use of the “HART Registered” mark is limited to registered device only
- Registered products will be promoted on FieldComm Group’s Product Registry website

Introduction

This introduction is included for informational purposes only.

The WirelessHART capabilities introduced in Revision 7 of the HART specifications marks a significant enhancement to the HART technology. WirelessHART is a networked solution of devices and therefore WirelessHART enabled devices must interoperate with all other devices that may be part of the same network. It is essential that all manufacturers ensure their devices are compliant to the HART Protocol Specification, passing all conformance tests and registering products with FieldComm Group.

Products undergo many levels of testing, normally, the tests themselves must be developed and deployed by the manufacturer, and only then, can the tests be performed. The tests requirements outlined in this document, standardize and eliminate the need for each manufacturer to develop their own tests to confirm Protocol compliance. In addition, test automation and check lists are provided to further reduce the manufacturers testing costs.

Manufacturers must perform the tests and certify the results before submitting the device to the FieldComm Group for independent testing. A manufacturer may elect to contract with the FieldComm Group to perform the tests. Complete documentation must be provided to the FieldComm Group as part of the device submittal for testing by the FieldComm Group. After successfully completing the registration procedure manufacturers are granted permission to use a special "HART Registered" mark, their product is listed on the FieldComm Group website and they are provided a Certificate of Registration.

Registration of a device assures end users that the product has been tested and validated against HART Protocol requirements. Refer to the FieldComm Group Product Registration Policy (FCG PD10026) for the program requirements.

1 SCOPE

This document defines the procedures and requirements for testing, validation and registration of WirelessHART devices. This Procedure is designed to assure the high standards of interoperability and performance expected of HART and WirelessHART devices in the field. All products claiming to be WirelessHART compatible must successfully complete the testing, validation and registration process defined in this Procedure.

The testing, validation and registration of WirelessHART field devices and adapters must adhere to the requirements and procedures in this document. The testing, validation and registration procedures for WirelessHART Gateways and Network Managers will be addressed in future revisions of this document.

> **HART and WirelessHART are trademarks of FieldComm Group. The FieldComm Group is committed to protecting and ensuring the integrity of these trademarks. Products that do not comply with HART Communication Protocol requirements will not be allowed to represent themselves as HART (or WirelessHART) compatible.**

Products must successfully complete all tests specified for the particular device type under test as defined in this Procedure. Required tests are organized into three categories – 1) tests that are common to all WirelessHART device types; 2) tests that are specific to WirelessHART field devices; and 3) tests that are specific to WirelessHART adapters.

This Procedure:

- Overviews the entire testing, validation and registration process for WirelessHART devices;
- Defines the procedure that must be followed in registering a WirelessHART device;
- Identifies the tests that must be successfully performed to register a WirelessHART device;
- Specifies the deliverables that must be included in the Registration Package to submit a WirelessHART device for independent testing.

This Procedure does not include EDD or FDI Device Package testing and registration requirements, these are separate policies available from FieldComm Group.

2 REFERENCES

The following documents and tools are referenced in this procedure.

2.1 The HART Communication Protocol Specifications

The following HART Communication Protocol Specifications define requirements pertinent to the WirelessHART devices discussed in this document:

HART Communication Protocol Specification. HCF_SPEC-13, FCG TS20013

FSK Physical Layer Specification. HCF_SPEC-54, FCG TS20054

Wireless Physical Layer Specification, HCF_SPEC-065, FCG TS20065

TDMA Data-Link Layer Specification, HCF_SPEC-75, FCG TS20075

Token-Passing Data Link Layer Specification, HCF_SPEC-81, FCG TS20081

Network Management Specification, HCF_SPEC-85, FCG TS20085

Command Summary Specification, HCF_SPEC-99, FCG TS20099

Universal Command Specification, HCF_SPEC-127, FCG TS20127

Common Practice Command Specification, HCF_SPEC-151, FCG TS20151

Common Tables, HCF_SPEC-183, FCG TS20183

Wireless Command Specification, HCF_SPEC-155, FCG TS20155

Wireless Devices Specification, HCF_SPEC-290, FCG TS20290

2.2 Related FieldComm Group Documents

The following FieldComm Group documents supplement the HART Communication Protocol Specifications in defining test procedures and requirements relevant to the testing, validation and registration of WirelessHART devices.

HART Product Registration Procedure. HCF_PROC-12, FCG PD20012

Product Registration Policy. FCG PD10026

HART Field Device Test Report. HCF_FRM-156, FCG FR20156

Slave Token-Passing Data Link Layer Test Specification, HCF_TEST-1, FCG TT20001

FSK Physical Layer Test Specification, HCF_TEST-2, FCG TT20002

Slave Universal Command Test Specification, HCF_TEST-3, FCG TT20003

Slave Common Practice Command Test Specification, HCF_TEST-4, FCG TT20004

2.3 HART Test Tools

The following standard tools are referenced throughout this procedure.

Wi-Analys Network Analyzer. HCF_KIT-190. FCG TK20190

HART Test System. HCF_KIT-192. FCG TK20192

WirelessHART Test System. HCF_KIT-193. FCG TK20193

2.4 Related Reference Documents

The following are applicable IEEE documents:

IEEE 802.15.4-2006 *Wireless Medium Access Control and Physical Layer Specifications for Low-Rate Wireless Area Networks.*

ANSI/IEEE Std 829. *IEEE Standard for Software Test Documentation*.

3 DEFINITIONS, ACRONYMS AND SYMBOLS

This section provides information on the Definitions, Acronyms and Symbols used throughout this document.

3.1 Definitions

The HART Protocol Specifications must use a common and consistent vocabulary both within a specification and across all specifications. This section incorporates (by reference) definitions from the HART Field Communications Protocol Specification and defines the terms unique to this specification. Vocabulary or phrases used in more than one specification must be defined in the HART Field Protocol Specification. Sometimes key definitions found in there are repeated and amplified in this section (rather then simply incorporating by reference).

Some of the following definitions are included in the HART Field Communications Protocol Specification. However, these definitions are critical to the understanding of this specification. As a result, they are included and their meaning amplified.

Acknowledge	Explicit Data-Link response to the successful reception of a directed, non-broadcast DLPDU from a Data-Link source device. The second DLPDU of a two-DLPDU transaction.
Application Layer	Topmost layer in the Open System Interconnect (OSI) model. In the HART Protocol this layer includes: the definitions of data types; revision rules; application procedures; and the HART Commands.
Bridge Device	A device that acts as a bridge between the HART network and another network. The other network could be another HART network. Gateways and Adapters are two types of bridge devices.
Byte	8-bits, sometimes called an Octet.
Channel Hopping	Regular change of transmit/receive frequency to combat interference and fading.
Clear Channel Assessment	Clear Channel Assessment (CCA) is used to avoid initiating a transaction while the RF channel is in use. CCA is performed by listening to the channel prior to sending the first DLPDU of a transaction.
Coexistence	Coexistence is the ability of one system to perform a task in a given shared environment in which other systems have an ability to perform their tasks and may or may not be using the same set of rules (IEEE).
Data Link Layer	Layer 2 in the OSI model. This layer is responsible for the error-free communication of data. The Data Link Layer defines the message structure, error detection strategy and bus arbitration rules.
Device Variable	A uniquely defined data item within a Field Device that is always associated with cyclical process information. A Device Variable's value varies in response to changes and variations in the process.
Dynamic Variable	The connection between the process and an analog channel. All HART field devices may contain Primary, Secondary, Tertiary, and Quaternary Variables that are mapped to the first 4 analog channels in a field device.
Field Device	Field Devices are connected to the Process and their Device Variables vary as process conditions change.
Frame	A Data-Link Layer "packet" which contains the header and trailer information required by the physical medium. That is, Network Layer packets are encapsulated to become frames.
Generic Host Generic Master	A host meeting the requirements of, at least, Host Conformance Class 3 (see the Command Summary Specification)

Hop	A term used to describe the data being passed from one device to another as a means to lengthen the transmit distance. Also used to denote the function of changing channels
Host	One of (possibly) several applications that can be executed sequentially or simultaneously on a Master.
I/O System	A device, accessed by an application via the HART Protocol, which supports multiple connections to underlying HART-enabled sub-devices.
Interoperability	Interoperability is the ability for like devices from different manufacturers to work together in a system and be substituted one for another without loss of functionality at the host system level.
Latency	The time it takes for a packet to cross a network connection, from sender to receiver. Latency specifications shall (unless otherwise noted) represent a 2-sigma value. i.e., the latency shall be achieved 95% of the time.
Link	The full communication specification between adjacent nodes in the network, i.e., the communication parameters necessary to move a packet one hop.
Logical Link Control	Logical Link Control (LLC) is the higher of the two data link layer sublayers defined in the OSI Model. The LLC sublayer handles error control, flow control, framing, and addressing.
Long Tag	A 32 character ISO Latin-1 string used to identify the field device. See Tag.
Medium Access Control	A sub-layer found with the OSI Data-Link Layer (OSI Layer 2) used for arbitrating access to the communication channel.
Neighbor	An adjacent node in the network such that the Receive Signal Level (RSL) suggests communication in at least one direction is possible.
Network Device	A device with a direct Physical Layer connection to the network. Each network device (e.g., field device or gateway) has a HART Unique Address that is used in communication with the device.
Network Manager	A Network Manager is responsible for configuration of the network, scheduling communication between network devices, management of the routing tables and monitoring and reporting the health of the network. There must be one and only one network manager per WirelessHART Network. Although the network manager need not have a direct Physical Layer connection it still must have a HART Unique Address.
Not-A-Number	A floating point number that cannot be interpreted. A single, specific non-signaling NaN (0x7F, 0xA0, 0x00, 0x00) is allowed in some Command Specifications to indicate that the field device does not support certain data values.
Packet	A generic reference to the set of data communicated across a network
Physical Layer	Layer 1 in the OSI model. The Physical Layer is responsible for transmission of the raw bit stream and defines the mechanical and electrical connections and signaling parameters for devices.
Request Data Bytes	The sub-field returned in the Data field that contains the Application Layer message data being transmitted from the Master to the Slave.

Response Data Bytes	The sub-field returned in the Data field that contains the Application Layer message data being transmitted from the Slave to the Master. The first byte in the HART Data Field that is not a Response Code, Communication Status, Device Status or Extended Command Number.
Slot	A fixed time interval that may be used for communication between neighbors.
Sub-Device	A HART compatible device communicated to via a Bridge Device. See the Command Summary Specification for more information.
Superframe	A collection of slots repeating at a constant rate. Each slot may have several links associated with it.
Time Constant	A measure of the responsiveness to an input step change. The time constant difference between the start of the step change to when the response has reached 63% of the final steady-state value.
Transaction	A complete, atomic cycle of Data-Link activity. A transaction consists of (a) a single DLPDU transmission from a source device, or (b) two DLPDUs: one from the Data-Link source followed by an second, link-level acknowledgement DLPDU from the destination.
Unique Identifier	The concatenation of the Device Type and Device ID used in constructing the long frame address (see the Data Link Layer Specification). These data, when combined, uniquely identify a specific field device. No two devices ever manufactured may have the same combination of these data.
Validation	The process of establishing evidence that provides a high degree of assurance that a product, service, or system accomplishes its intended requirements.

3.2 Acronyms and Symbols

All Symbols and Abbreviations used in this specification are listed in this section.

DUT	**D**evice **U**nder **T**est
MWT	**M**anual Wireless Test
STO	Slave Time-Out
SOM	Start Of Message
APDU	Application Protocol Data Unit
DPDU	Data-link Protocol Data Unit (not written DLPDU so as to match other xPDUs
DUTm	Device Under Test, using wired FSK maintenance link
DUT	Device Under Test, except when using wired FSK maintenance link (e.g., when using wireless TDMA data link or no communications at all)
NPDU	Network Protocol Data Unit
TPDU	**T**ransport **P**rotocol **D**ata **U**nit
VDn	**V**irtual **D**evice number n (where n = 1)
VD	**V**irtual **D**evice number 1 (for tests using only a single virtual device)

4 REGISTRATION PROCEDURE

This section defines the process that must be followed to register a WirelessHART product. This procedure builds on the requirements found in the *HART Product Registration Procedure* and tailors them for WirelessHART products. The basic process for registering a WirelessHART product consists of:

Manufacturer -

- Developing the product to comply with all requirements of the HART Communication Protocol Specifications;
- Testing the product per the test requirements defined in this Procedure (see Section 4.2);
- Assembling the Registration Package including all deliverables specified in Section 6 and a sample device for independent testing at FieldComm Group; and
- Submitting the Registration Package and sample device to FieldComm Group along with a purchase order for the registration fee.

FieldComm Group - Upon receipt of the Registration Package, the FieldComm Group will review the package and independently assess device compliance. The basic procedure performed by the FieldComm Group includes:

- Assessing the registration package submission to confirm completeness with all deliverables;
- Confirming sample device matches the registration request;
- Filing the registration package materials;
- Auditing the manufacturer's test reports and data;
- Independent retesting of the sample device (100%) to verify results;
- Assessing and validating results to confirm success;
- Generating the registration report;
- Preparing the HART Registered certificate; and
- Updating FieldComm Group records and website

Any inconsistency or anomaly at any of these steps may result in the suspension or termination of the test campaign cycle. Completion of the registration process for a WirelessHART device will take approximately 8 weeks from receipt of a complete registration package. Suspension of the registration process may result in extension of the registration time beyond the nominal 8-week interval.

4.1 Product Registration - Manufacturer Responsibilities

Product manufacturers are responsible for developing compliant products, testing the product to confirm compliance and registering the product with the FieldComm Group. Registering the product with the FieldComm Group requires submission of a registration package complete with sample device and all required deliverables and purchase order (billing information) for the registration fee.

4.1.1 Test Requirements

Except when noted otherwise, manufacturers must perform all tests specified in Section 5. When performing the tests, all log files must be retained and all forms and checklists completed.

4.1.2 Registration Package Submission

Except when noted otherwise, manufacturers must submit all deliverables indicated in Section 6. In addition, the manufacturer must submit all required forms and documents, a sample product for FieldComm Group testing, and a purchase order for the registration fees. The registration package must include:

- HART Product Exhibits.xls for WirelessHART Product Registration.
- Completed *Token-Passing Data-Link Test Summary*. HCF_FRM-156.1, FCG FR20156
- Completed *FSK Physical Layer Test Data Sheets*. HCF_FRM-156.2, FCG FR20156
- Completed *Slave Universal Command Test Summary*. HCF_FRM-156.3, FCG FR20156
- Completed *Slave Common Practice Command Test Summary*. HCF_FRM-156.4, FCG FR20156
- The product specification including device specific details as per *Field Device Specification Guide* (HCF_LIT-18)
- Specific instructions for manipulating the device (Write Lock, More Status Available, etc)
- All the log files generated by the test automation including the
    - BA000xxx.OUT (Token-Passing Data-Link) files;
    - DLL039a.qa.log and DLL039b.qa.log files;
    - UALxxx.qa.log (Universal Command) files;
    - CALxxx.qa.log (Common Practice Command) files;
    - TMLxxx.log, TMLxxx.txt, TMLxxx_testlog.txt (WirelessHART device-level) files; and
    - SLTxxx.log, SLTxxx.txt, SLTxxx.doc (WirelessHART system-level) files.
- FCC test results and antenna transmit power plots
- Proof of IEEE STD 802.15.4-2006 transceiver compliance
- Sample of device
- EDD Source (and FDI Device Package required after 31 December 2020)
- Purchase order for testing and registration fee.

All of the documents and test data must be provided electronically via support request at https://support.fieldcommgroup.org/ (e.g., uploaded to FieldComm Group's ShareFile, or on CD or memory stick included with the sample device). The documents and log files must be organized into the directory structure shown in Figure 1.

The Registration package must be sent to the FieldComm Group at:

FieldComm Group
Attention: Product Registration
9430 Research Blvd. Suite 1-120
Austin, TX 78759
USA

Phone Number: +1-512-792-2300

After the registration package is received at the FieldComm Group, its completeness will be assessed, and a confirming email will be forwarded to the manufacturer.

File or Directory Name	Description
▸ *product-name*	Directory should be bear product's name
▸ EDD	The EDD Source directory
▸ DOCS	The docs directory
HCF_FRM-156.PDF	Completed Token-Passing Data-Link testing checklist. Completed FSK Physical Layer testing checklist Completed Slave Universal Command testing checklist (wired) Completed Slave Universal Command testing checklist (wireless) Completed Slave Common Practice Command testing checklist (wired) Completed Slave Common Practice Command testing checklist (wireless)
product-name.r.pdf	Product specification document (see *Field Device Specification Guide* HCF_LIT-18) where ".r" is the device revision level
▸ MFRLOGS	The test data log directory
▸ CAL-TP	The directory with all the Common Practice Command test data logs from testing via the Token-Passing channel
the CAL summary file	The CAL test result summary file (i.e., *eeee*_CALSummary_FSK.txt[1])
the calxxx.qa.log files	
▸ CAL-UDP	The directory with all the Common Practice Command test data logs from testing via the wireless channel (via UDP)
the CAL summary file	The CAL test result summary file (i.e., *eeee*_CALSummary_UDP.txt[1])
all calxxx.qa.log files	
▸ SLT	The directory with all the system-level test data logs
slt-info.txt	The file containing the network information including Network ID and Join Key.
all SLTLxxx.log files	WiAnalys raw data log files
all SLTLxxx.txt files	The decoded WiAnalys data log files
all SLTLxxx.doc files	The system-level test log files
▸ TML	The directory with all the wireless device-level test data logs
all tmlxxx.log files	WiAnalys raw log files
all tmlxxx.txt files	The decoded WiAnalys files
all TMLxxx_testlog.txt files	The files generated by the TML scripts on the WirelessHART Test System
▸ TPDLL	The directory with all the Token-Passing Data-Link test data logs
the TP-DLL summary file	The Token-Passing Data-Link Layer test result summary file (i.e., *eeee*_DLLSummary_FSK.txt[1])
all BA000xxx.OUT files	HSniffer binary communications captures
all dllxxx.qa.log files	Converted (text) HSniffer files.
all dllxxx_testlog.txt files	Output from compliance assessment (post-processing)
dll039a.qa.log	
dll039b.qa.log	
▸ UAL-Token-Passing	The directory with all the Universal Command test data logs from testing via the Token-Passing channel
the UAL summary file	The UAL test result summary file (i.e., *eeee*_UALSummary_FSK.txt[1])
all ualxxx.qa.log files	
▸ UAL-UDP	The directory with all the Universal Command test data logs from testing via the wireless channel (via UDP)
the UAL summary file	The UAL test result summary file (i.e., *eeee*_UALSummary_UDP.txt[1])
all ualxxx.qa.log files	

Figure 1. Electronic files and directory organization for Product Registration

[1] eeee is the Expanded Device Type code for the DUT

4.2 Product Registration - Initial FieldComm Group Assessment

Upon receipt of the Registration Package, FieldComm Group will assess the package for completeness and audit the test data. The package must contain:

- EDD Source;
- All required checklists and documentation;
- Complete set of test data logs;
- Sample device;
- The product specification document (HCF_LIT-18); and
- Purchase order and billing information for the testing services and registration fees.

Data logs for each required test must be present. The required tests are listed in Section 5. Each data log will be audited for completeness. In addition, the data logs shall be reviewed to confirm the correct version of the test automation was used for testing. Please refer to the online Change Log for the latest released version of test automation to be used.

Upon completing the initial assessment, FieldComm Group shall confirm receipt of the registration package to the submitter. The confirmation shall include either: 1) an estimated timeline for completion of the product registration cycle, or 2) a list of deficiencies that must be corrected for the registration process to resume (see Subsection 4.5).

4.3 FieldComm Group Testing and Validation

Upon completing the initial assessment, the product shall be validated against the HART Protocol requirements. Validation consists of:

- Detailed review of the data logs provided by the manufacturer; and
- Independent 100% validation testing of the sample device per tests specified in Section 5 applicable to the product.

4.3.1 Review of data logs provided by the product's manufacturer

The following data review shall be performed during validation:

- UAL, CAL data logs shall be reviewed, and the indicated results compared with those summarized in the corresponding checklist.
- Token-Passing Data-Link Test data logs shall be processed by the corresponding compliance assessors and the results recorded. The results are then compared to the Token-Passing Data-Link Testing Checklist and any discrepancies noted.
- The TMLxxx.txt and SLTxxx.txt files shall be reviewed, key function-points identified, and the product operation summarized.
- Physical Layer test data shall be reviewed and summarized. The FCC and IEEE 802.15.4 compliance reports shall be reviewed, and results summarized.

Inconsistencies between the summary checklists provided by the manufacturer and the findings of the detailed Registration Package review may result in the suspension / termination of the test campaign.

4.3.2 Testing of Sample Product

Product testing and validation must be reproducible. To this end, FieldComm Group will independently 100% test the sample device to verify reproducibility of test results on all products submitted for registration.

Once the review of the data provided by the product's manufacturer is complete, the FieldComm Group will perform all applicable tests in Section 5 and record the test result as per the requirements in Section 6.

The test data shall be reviewed and checklists generated to summarize the findings. The FieldComm Group-generated checklists shall be compared to the submitted checklists and any differences noted. Any differences between the manufacturer and FieldComm Group findings may result in the suspension / termination of the test campaign.

4.4 FieldComm Group Assessment and Validation

The test data and findings provided by the manufacturer and the independent FieldComm Group verification testing provide objective evidence of a product's compliance with HART Protocol requirements.

4.4.1 Pass / Fail Criteria

For each test performed a finding shall be determined. The finding shall indicate "FAIL" should the data indicate a deficiency that:

- May cause interoperability problems or failures in networks containing a mixture of products and WirelessHART stacks from different companies;
- Materially undermines network integrity or device security;
- Requires special behavior or knowledge on the part of a Network Manager or Gateway to accommodate the device in the network;
- May negatively impact the behavior or performance of another device in the network or the network overall; or
- Is defined as a FAIL in an approved, released Test Specification applicable to that product.

Any finding not indicating a FAIL shall indicate "PASS".

In all cases the Pass/Fail determination shall be based upon the Protocol Specification requirements.

4.4.2 HART Registered Certificate

All findings for all tests shall be reviewed and validated by FieldComm Group. A HART Registered Certificate will be prepared and issued for the product only if all findings are validated as PASS.

4.4.3 Notification of Result

Upon completion of the test campaign, a summary report shall be generated and conveyed to the product's manufacturer (submitter). The report will include all findings from the validation testing and any conclusions drawn from the test data.

Provided the findings confirm all registration requirements have been successfully met, the HART Registered certificate will be issued and included with the product registration report.

Should corrective action be required, deficiencies will be clearly highlighted in the registration report.

4.5 Suspension Criteria and Resumption Requirements

The test campaign shall be suspended if:

- The registration package is incomplete.
- Any of the checklists are not properly completed.
- The Common Practice Command checklist indicates a mandatory command is not implemented.
- The wrong revision of test automation was used for the manufacturer pre-testing.

Should the process be suspended, the submitter shall be notified and report generated listing deficiencies that must be corrected to continue testing. Once all corrections have been received and verified by FieldComm Group, the process shall be restarted and the submitter notified. The notification of resumption will include the revised timeline and cost estimate for completing the product test campaign.

The product test campaign shall be complete if:

- A HART Registered certificate is issued.
- The device or EDD fails the compliance validation.

In either case, a test report shall be provided to the submitter summarizing tests performed and FieldComm Group findings. Any product that fails the compliance assessment must be corrected and resubmitted under a new test campaign.

5 REQUIRED TESTS

The HART Communication Protocol specifications define requirements for which all HART (and WirelessHART) products must comply. This section describes required tests to validate compliance of WirelessHART products. Required tests are prescribed for each protocol layer as follows:

- **Physical Layer** – both wired interface (maintenance port) and wireless interface tests
- **Token-Passing Data-Link Layer** – both slave and master tests, both wired and wireless interface for some tests
- **TDMA Data-Link** and **Mesh Network Layer** – both device and system level tests
- **Application Layer Universal Commands** – both wired interface and wireless interface tests
- **Application Layer Common Practice Commands** – both wired interface and wireless interface tests, both mandatory and optional commands

The required tests are further organized into three subsections:

- **Required Tests Common to all WirelessHART Devices** – core tests that must be performed on both WirelessHART field devices and WirelessHART adapters.
- **Additional Required Tests for WirelessHART Field Devices** – additional tests beyond the core tests that must be performed on WirelessHART field devices.
- **Additional Required Tests for WirelessHART Adapters** – additional tests beyond the core tests that must be performed on WirelessHART adapters.

Data, checklists and other information required to properly document the testing and submit the product Registration Package is discussed in Section 6.

Specific guidance and procedures for conducting the tests are provided in Section 7.

5.1 Required Tests Common to all WirelessHART Devices

The HART Communication Protocol specifications define a common minimum set of requirements applicable to all WirelessHART devices. The tests described in this subsection are required to demonstrate compliance of WirelessHART devices to requirements.

5.1.1 Physical Layer

All WirelessHART devices must include an IEEE 802.15.4 wireless interface. Additionally, WirelessHART field devices are required to have (at a minimum) a maintenance port. The maintenance port must support one of the Physical Layers identified in the *Token-Passing Data Link Layer Specification* (HCF_SPEC-81, FCG TS20081). Both the wireless interface and the maintenance port interface must be tested to demonstrate compliance.

5.1.1.1 Wireless Interface

For the IEEE 802.15.4 Wireless Physical Layer, the device must

- Be implemented using a tested, compliant IEEE 802.15.4 transceiver; and
- Successfully complete RF (FCC, ETSI or equivalent) certification

RF testing is required. Results from both IEEE 802.15.4 and RF testing must be provided with the Registration Package (see Test and Registration Deliverables, Section 6)

In addition, the device must demonstrate support for at least the following transmit signal levels: +10dBm, and 0dBm and the device should support -10dBm.

5.1.1.2 FSK Interface

An FSK interface is most often supplied to meet the requirement for all devices to have (at least) a maintenance port. All tests in the *FSK Physical Layer Test Specification* (HCF_TEST-2, FCG TT20002) are applicable and must be successfully performed on the maintenance port and/or FSK interface of a WirelessHART device.

5.1.2 Token-Passing Data-Link Layer

Tests in the *Slave Token-Passing Data Link Layer Test Specification* (HCF_TEST-1, FCG TT20001) that are required for WirelessHART devices are identified in Table 1. All tests in Table 1 must be performed successfully through the maintenance port and/or FSK interface of the WirelessHART device. Burst-mode services tests (DLL036, DLL037, DLL043, DLL044 and DLL045) must also be performed successfully through the wireless interface of the WirelessHART device.

Table 1. Required Token-Passing Data-Link Layer Tests

Test	Test	Test	Test	Test
DLL001	DLL007	DLL013	DLL020	DLL035
DLL002		DLL014	DLL024	DLL038
DLL003	DLL009	DLL015		DLL039
DLL004	DLL010		DLL032	DLL040
DLL005	DLL011	DLL017	DLL033	DLL041
DLL006	DLL012	DLL018	DLL034	DLL042

5.1.3 TDMA Data-Link and Mesh Network Layer

Validating proper behavior and compliance with requirements for WirelessHART device in the WirelessHART mesh network requires the combination of both device level tests and system level tests.

Required system level tests are denoted in Table 2. Test definitions, test set-up, pass/fail criteria, test procedure and detailed guidance for conducting the system level tests is provided in Section 7. The system level tests enable proper device behavior to be validated within an operating mesh network under normal, abnormal and stress conditions.

Required device level tests are identified in Table 3. Test definition, test procedure and pass/fail criteria for each test is detailed in the *TDMA Mesh Test Specification* (HCF_TEST-6, FCG TT20006). Automated test scripts with FieldComm Group test tools support proper execution of each device level test.

Table 2. Required TDMA Mesh System-Level Tests

Test	Test	Test
SLT000	SLT001	SLT003

Table 3. Required TDMA-Mesh Device-Level Tests

Test	Test	Test	Test	Test
TML100A-C	TML206A-F	TML214A-F	TML224A-B	TML307A-D
TML101			TML225A-B	
TML102A-C	TML208A-F	TML216A-F		TML309
TML201A-B			TML302A	
TML202A-C	TML210A-C	TML220A	TML303A-E	TML311A-C
TML203A-F,H	TML211A-B		TML304A-E	
TML204A-B	TML212A-D	TML222A-E	TML305A-C	TML314A-B
TML205A-F	TML213A-E	TML223		

5.1.4 Application Layer - Universal Commands

All tests in the *Slave Universal Command Test Specification* (HCF_TEST-3, FCG TT20003) are required for WirelessHART devices. Universal Command tests must be successfully performed through both the maintenance port (wired interface) and wireless interface of the device.

5.1.5 Application Layer - Common Practice Commands

All tests in the *Common Practice Command Test Specification* (HCF_TEST-4, FCG TT20004) are applicable to WirelessHART devices. All Common Practice Commands implemented in the device must successfully complete the corresponding Common Practice Command test.

In general, Common Practice Commands are optional except for those designated “required” and/or “mandatory” for WirelessHART devices. Required Common Practice Commands are tested by the combination of Token Passing Data Link Layer tests, Universal Command tests and the required Common Practice Command Tests denoted in Table 4.

Table 4. Slave Common Practice Tests (Required)

Test	Test	Test	Test	Test
CAL000	CAL050	CAL103	CAL107	CAL108
CAL041	CAL078	CAL104	CAL109	CAL115

Common Practice Command tests CAL000, CAL041, CAL050, CAL078 must be successfully performed through both the maintenance port (wired interface) and wireless interface of the device.

Common Practice Command tests CAL103, CAL107, CAL108, CAL104, CAL109, and CAL115 must be successfully performed through wireless interface of the device.

CAL000 must indicate device supports Commands 90 and 106.

5.2 Additional Required Tests for WirelessHART Field Devices

5.2.1 Physical Layer

WirelessHART field devices may contain a standard HART interface designed for connection to the Process Automation System or a maintenance port. When the field device has only a maintenance port:

- The maintenance port must be clearly labeled as such;
- The maintenance port must have a 500 Ohm characteristic impedance

Labeling must be confirmed visually and the impedance is confirmed as part of the standard Physical Layer testing.

5.2.2 Token-Passing Data-Link Layer

No additional test requirements.

5.2.3 TDMA Data-Link Layer and Mesh Network Layer

No additional test requirements.

5.2.4 Universal Commands

No additional test requirements.

5.2.5 Common Practice Commands

Some Common Practice commands that are mandatory for WirelessHART devices are specific to WirelessHART field devices. Table 5 denotes additional required Common Practice Command tests that must be successfully performed on WirelessHART field devices.

Table 5. Additional Common Practice Command Tests for WirelessHART Field Devices (Required)

Test	Test
CAL054	CAL079

5.3 Additional Required Tests for WirelessHART Adapters

5.3.1 Physical Layer

WirelessHART adapters must be designed for permanent operation of the wired FSK interface (as opposed to being only a maintenance port). The wired interface of WirelessHART adapters must meet all FSK physical layer requirements.

5.3.2 Token-Passing Data-Link Layer

WirelessHART Adapters are hybrid devices that function as both a Token-Passing master and slave. Consequently, both modes of operation must be tested.

5.3.2.1 Token-Passing Slave

No additional test requirements.

5.3.2.2 Token-Passing Master

All tests in the *Master Token-Passing Data Link Layer Test Specification* (HCF_TEST-5, FCG TT20005) must be successfully performed.

WirelessHART Adapters must also demonstrate the longer Link Quiet Timeout (RT1) and duplicate master back-off timeout requirements as per the WirelessHART Device Specification.

5.3.3 TDMA Data-Link Layer and Mesh Network Layer

No additional test requirements.

5.3.4 Universal Commands

No additional test requirements.

5.3.5 Common Practice Commands

Some Common Practice Commands that are mandatory for WirelessHART devices are specific to WirelessHART Adapters. Table 6 denotes additional Common Practice Command tests that must be successfully performed on WirelessHART adapters.

Table 6. Additional Common Practice Command Tests for WirelessHART Adapters (Required)

Test	Test
CAL074	CAL101

6 TEST AND REGISTRATION DELIVERABLES

This section specifies the checklists, test data and documentation that must be captured and preserved by the manufacturer in their pre-testing of a candidate product for FieldComm Group Registration. The deliverables specified in this section must be included in the Registration Package submission. Furthermore, the deliverables specified in this section will also be generated and preserved during the independent testing and validation phase of the Device Registration process at FieldComm Group.

Every time a candidate product is received at FieldComm Group for testing, a Test Report must be produced. The Test Report summarizes the results of the registration process. The Test Report is sent to the product's manufacturer (submitter) and included in the test campaign archive. The archive will also contain:

- The Registration Package submitted by the product manufacturer
- All test summaries, test data, documentation and reports generated at FieldComm Group during the product test campaign.

This section specifies deliverables that must be provided in Product Registration Package submissions. Registration Package deliverables must be provided as electronic files organized in the file / directory structure depicted in Subsection 4.1, Figure 1.

Section 5, specifies the tests to be performed. Detailed guidance on conducting the tests is provided in Section 7, Test Procedures.

Complete test records must be maintained for the DUT including summaries of the findings from each test and all test data. Wireless tests require both the raw log files and the deciphered export files to be maintained. The test summaries will include:

- Who performed the tests
- The product identification information
- When the testing was completed
- The finding for each test (PASS/FAIL)

The test summaries (see example in Annex B) along with the test data files provide a detail record of the testing sufficient to satisfy most Quality Assurance Audits. In addition, they provide sufficient detail to allow the test results to be reproduced.

Note: The *FSK Physical Layer Test Data Sheets* (HCF_FRM-156.2, FCG FR20156) both summarize the FSK test results and provide the test data itself.

Specific deliverables for the Physical Layer wired and wireless interface, slave Token-Passing Data-Link Layer, TDMA Data-Link and Mesh Network Layer, Universal Commands, Common Practice Commands are specified.

6.1 Physical Layer

6.1.1 Wireless Interface

For the wireless physical layer, the device implementer is required to submit the following:

- Antenna Transmit Pattern

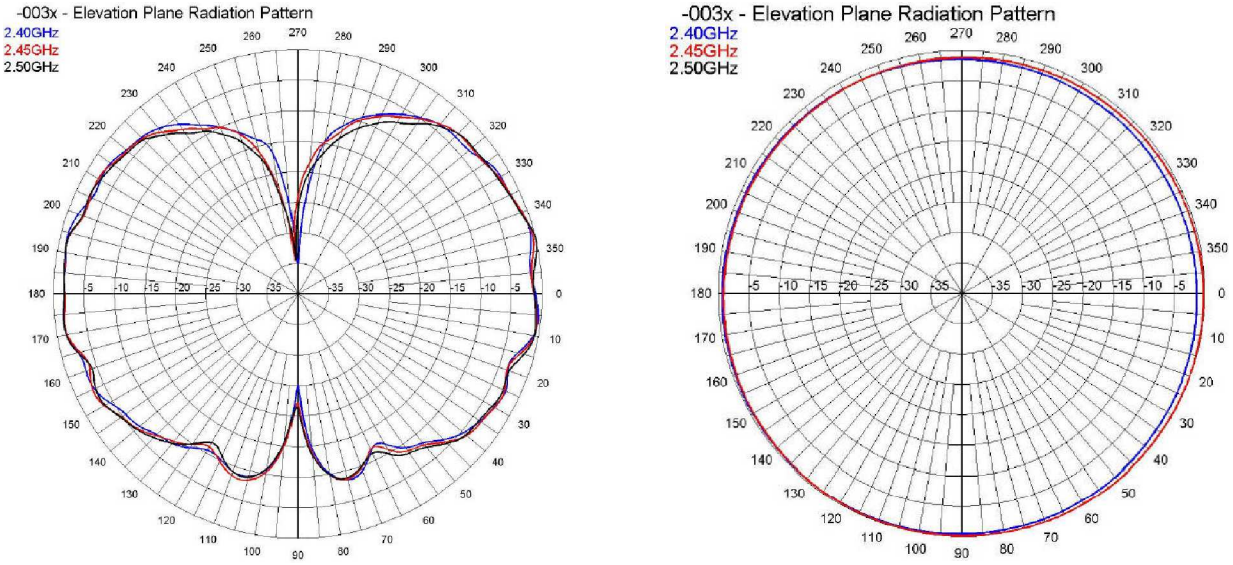

Figure 2. Example antenna pattern plots

- Measurements showing the wireless interface meets minimum 802.15.4 receive sensitivity (-85dBm or greater)
- A copy of the FCC, R&TTE or equivalent test report; and
- A copy of the IEEE 802.15.4 transceiver (i.e., radio) certification.

6.1.2 Wired Interface (Maintenance Port or FSK Interface)

The HART FSK interface is most often supplied to meet the requirement for all devices to have (at least) a maintenance port. When an FSK-Based interface is present the completed *Physical Layer Test Data Sheets* (HCF_FRM-156.2, FCG FR20156) must be provided

6.2 Token-Passing Data-Link Layer

Token-Passing Data-Link Layer tests are performed on the wired interface (maintenance port or FSK interface) of the device. In addition, several burst mode services tests are performed through both the wired interface and wireless interface of the device.

The completed *Slave Token-Passing Data-Link Test Summary* form must be provided along with the test data log files in the BMODE-TP, BMODE-UDP and TPDLL directories. The files shown in Table 7 must be included the TPDLL directory. These files are generated by HSniffer. In addition, the two log files dll039a.qa.log and dll039b.qa.log must also be included in the TPDLL directory.

Table 7. Required Token-Passing Data-Link HSniffer (binary) files in the TPDLL directory

Data Log	Data Log	Data Log	Data Log	Data Log
BA00001A.OUT	BA00006.OUT	BA00016.OUT	BA00024C.OUT	BA00033B.OUT
BA00001B.OUT	BA00007.OUT	BA00017.OUT	BA00025.OUT	BA00033C.OUT
BA00001C.OUT		BA00018.OUT	BA00026.OUT	BA00033D.OUT
BA00001D.OUT	BA00009.OUT	BA00019.OUT	BA00027.OUT	BA00033E.OUT
BA00001E.OUT	BA00010.OUT	BA00020.OUT	BA00028.OUT	BA00034.OUT
BA00001F.OUT	BA00011.OUT	BA00021.OUT	BA00029.OUT	BA00035.OUT
BA00002.OUT	BA00012.OUT	BA00022.OUT	BA00030.OUT	BA00038.OUT
BA00003.OUT	BA00013.OUT	BA00023.OUT		BA00040.OUT
BA00004.OUT	BA00014.OUT	BA00024A.OUT	BA00032.OUT	BA00041.OUT
BA00005.OUT	BA00015.OUT	BA00024B.OUT	BA00033A.OUT	BA00042.OUT

Table 8. Required Token-Passing Data-Link HSniffer (converted) log files in the TPDLL directory

Data Log	Data Log	Data Log	Data Log	Data Log
dll001a.qa.log	dll006.qa.log	dll016.qa.log	dll024c.qa.log	dll033b.qa.log
dll001b.qa.log	dll007.qa.log	dll017.qa.log	dll025.qa.log	dll033c.qa.log
dll001c.qa.log		dll018.qa.log	dll026.qa.log	dll033d.qa.log
dll001d.qa.log	dll009.qa.log	dll019.qa.log	dll027.qa.log	dll033e.qa.log
dll001e.qa.log	dll010.qa.log	dll020.qa.log	dll028.qa.log	dll034.qa.log
dll001f.qa.log	dll011.qa.log	dll021.qa.log	dll029.qa.log	dll035.qa.log
dll002.qa.log	dll012.qa.log	dll022.qa.log	dll030.qa.log	dll038.qa.log
dll003.qa.log	dll013.qa.log	dll023.qa.log		dll040.qa.log
dll004.qa.log	dll014.qa.log	dll024a.qa.log	dll032.qa.log	dll041.qa.log
dll005.qa.log	dll015.qa.log	dll024b.qa.log	dll033a.qa.log	dll042.qa.log

Table 9. Required Token-Passing Data-Link HTest Script output files in the TPDLL directory

Data Log	Data Log	Data Log	Data Log	Data Log
dll001a_testlog.txt	dll006_testlog.txt	dll016_testlog.txt	dll024c_testlog.txt	dll033b_testlog.txt
dll001b_testlog.txt	dll007_testlog.txt	dll017_testlog.txt	dll025_testlog.txt	dll033c_testlog.txt
dll001c_testlog.txt		dll018_testlog.txt	dll026_testlog.txt	dll033d_testlog.txt
dll001d_testlog.txt	dll009_testlog.txt	dll019_testlog.txt	dll027_testlog.txt	dll033e_testlog.txt
dll001e_testlog.txt	dll010_testlog.txt	dll020_testlog.txt	dll028_testlog.txt	dll034_testlog.txt
dll001f_testlog.txt	dll011_testlog.txt	dll021_testlog.txt	dll029_testlog.txt	dll035_testlog.txt
dll002_testlog.txt	dll012_testlog.txt	dll022_testlog.txt	dll030_testlog.txt	dll038_testlog.txt
dll003_testlog.txt	dll013_testlog.txt	dll023_testlog.txt		dll040_testlog.txt
dll004_testlog.txt	dll014_testlog.txt	dll024a_testlog.txt	dll032_testlog.txt	dll041_testlog.txt
dll005_testlog.txt	dll015_testlog.txt	dll024b_testlog.txt	dll033a_testlog.txt	dll042_testlog.txt

6.3 TDMA Data-Link and Mesh Network Layer

Both individual device and system-level tests are mandatory. Data is collected for each test performed. The next two subsections specify the data log files that must be provided for the device and system-level testing, respectively.

6.3.1 Device-level tests

The following tmlxxx.log and tmlxxx.txt files indicated in Table 10 and Table 11, respectively, must be provided in the TML directory. The required (raw) WiAnalys log that must be provided are shown in Table 10 and the corresponding (deciphered) WiAnalys export files to be provided are listed in Table 11. For each test there is a Test System log tmlxxx_testlog.txt that must be included in the submission.

Table 10. Required Device-Level (raw) data log files in the TML directory

Data Log	Data Log	Data Log	Data Log	Data Log
tml100a.log[2]	tml205a.log	tml210c.log	tml216d.log	tml304a.log
tml100b.log	tml205b.log		tml216e.log	tml304b.log
tml100c.log	tml205c.log	tml211a.log	tml216f.log	tml304c.log
tml101.log[2]	tml205d.log	tml211b.log		tml304d.log
tml102a.log	tml205e.log	tml212a.log	tml220a.log	tml304e.log
tml102b.log	tml205f.log	tml212b.log		
tml102c.log	tml206a.log	tml212c.log	tml222a.log	tml305a.log
	tml206b.log	tml212d.log	tml222b.log	tml305b.log
tml201a.log	tml206c.log	tml213a.log	tml222c.log	tml305c.log
tml201b.log	tml206d.log	tml213b.log	tml222d.log	
tml202a.log	tml206e.log	tml213c.log	tml222e.log	tml307a.log
tml202b.log	tml206f.log	tml213d.log	tml223.log	tml307b.log
tml202c.log		tml213e.log	tml224a.log	tml307c.log
tml203a.log	tml208a.log	tml214a.log	tml224b.log	tml307d.log
tml203b.log	tml208b.log	tml214b.log	tml225a.log	
tml203c.log	tml208c.log	tml214c.log	tml225b.log	tml309.log
tml203d.log	tml208d.log	tml214d.log	tml302a.log	
tml203e.log[2]	tml208e.log	tml214e.log		tml311a.log
tml203f.log	tml208f.log	tml214f.log	tml303a.log	tml311b.log
tml203h.log			tml303b.log	tml311c.log
tml203g.log		tml216a.log	tml303c.log	
tml204a.log	tml210a.log	tml216b.log	tml303d.log	tml314a.log
tml204b.log	tml210b.log	tml216c.log	tml303e.log	tml314b.log

[2] Wi-Analys logs are not generated for this test.

Table 11. Required Device-Level (deciphered) data log files in the TML directory

Data Log	Data Log	Data Log	Data Log	Data Log
tml100a.txt[3]	tml205a.txt	tml210c.txt	tml216d.txt	tml304a.txt
tml100b.txt	tml205b.txt		tml216e.txt	tml304b.txt
tml100c.txt	tml205c.txt	tml211a.txt	tml216f.txt	tml304c.txt
tml101.txt[3]	tml205d.txt	tml211b.txt		tml304d.txt
tml102a.txt	tml205e.txt	tml212a.txt	tml220a.txt	tml304e.txt
tml102b.txt	tml205f.txt	tml212b.txt		tml305a.txt
tml102c.txt	tml206a.txt	tml212c.txt	tml222a.txt	tml305b.txt
	tml206b.txt	tml212d.txt	tml222b.txt	tml305c.txt
tml201a.txt	tml206c.txt	tml213a.txt	tml222c.txt	
tml201b.txt	tml206d.txt	tml213b.txt	tml222d.txt	tml307a.txt
tml202a.txt	tml206e.txt	tml213c.txt	tml222e.txt	tml307b.txt
tml202b.txt	tml206f.txt	tml213d.txt	tml223.txt	tml307c.txt
tml202c.txt		tml213e.txt	tml224a.txt	tml307d.txt
tml203a.txt	tml208a.txt	tml214a.txt	tml224b.txt	
tml203b.txt	tml208b.txt	tml214b.txt	tml225a.txt	tml309.txt
tml203c.txt	tml208c.txt	tml214c.txt	tml225b.txt	
tml203d.txt	tml208d.txt	tml214d.txt	tml302a.txt	tml311a.txt
tml203e.txt[3]	tml208e.txt	tml214e.txt		tml311b.txt
tml203f.txt	tml208f.txt	tml214f.txt	tml303a.txt	tml311c.txt
tml203h.txt			tml303b.txt	
tml203g.txt		tml216a.txt	tml303c.txt	
tml204a.txt	tml210a.txt	tml216b.txt	tml303d.txt	tml314a.txt
tml204b.txt	tml210b.txt	tml216c.txt	tml303e.txt	tml314b.txt

6.3.2 System-level tests

Data recorded while executing the system level tests must be recorded. The required (raw) WiAnalys log files that must be provided are shown in Table 12 and the corresponding (deciphered) WiAnalys export files to be provided are listed in Table 13. These files must be placed in the SLT directory

Table 12. Required System-Level (raw) data log files in the SLT directory

Data Log	Data Log	Data Log
slt001.log	slt002.log	slt003.log

Table 13. Required System-Level (deciphered) data log files in the SLT directory

Data Log	Data Log	Data Log
slt001.txt	slt002.txt	slt003.txt

While performing the test, the Test Log must be generated (see Table 14). These files must be placed in the SLT directory along with the slt-info.txt file containing the network information (e.g., Network ID and Join Key).

[3] Wi-Analys logs are not generated for this test.

Table 14. Required System-Level Test Logs in the SLT directory

Data Log	Data Log	Data Log
slt001.doc	slt002.doc	slt003.doc

6.4 Universal Commands

Universal Command tests must be performed twice – once via the maintenance (or wired) port and once over the wireless channel. The test data log files generated from these tests are identified in Table 15. The data log files from these tests must be in both the UAL-TP and UAL-UDP directories.

Table 15. Required data log files in the UAL-TP and UAL-UDP directory

Data Log	Data Log	Data Log	Data Log	Data Log
ual000.qa.log		ual008.qa.log	ual011b.qa.log	ual038b.qa.log
ual001.qa.log	ual005.qa.log	ual009.qa.log	ual012.qa.log	
	ual006.qa.log	ual010.qa.log	ual013.qa.log	ual048a.qa.log
	ual007.qa.log	ual011a.qa.log	ual038a.qa.log	ual048b.qa.log

6.5 Stress Test (DLL039)

The DLL039 Stress-Tests must be performed twice, once via the maintenance (or wired) port and once over the wired channel (via UDP). The test data log files generated from these tests are identified in Table 16. The data log files from these tests must be in both the TML and TPDLL directories.

Table 16. Required Stress-Test data log files

Data Log	Data Log
dll039a.qa.log	dll039b.qa.log

6.6 Common Practice Commands

Common Practice Command tests must be performed twice, once via the maintenance (or wired) port and once over the wired channel (via UDP). The test data log files generated from these tests are identified in Table 17. The data log files from these tests must be in both the CAL-TP and CAL-UDP directories.

Table 17. Required data log files in the CAL-TP and CAL-UDP directory

Data Log	Data Log	Data Log	Data Log	Data Log
cal000.qa.log	cal046.qa.log	cal072.qa.log	cal107a.qa.log	cal524a.qa.log
cal033.qa.log	cal047.qa.log	cal073.qa.log	cal107b.qa.log	cal524b.qa.log
cal034.qa.log	cal049.qa.log	cal074a.qa.log	cal108a.qa.log	cal524c.qa.log
cal035.qa.log	cal050.qa.log	cal074b.qa.log	cal108b.qa.log	cal524d.qa.log
cal036.qa.log	cal051.qa.log	cal074c.qa.log	cal108c.qa.log	cal524e.qa.log
cal037.qa.log	cal052.qa.log	cal074d.qa.log	cal108d.qa.log	cal524f.qa.log
cal040.qa.log	cal053.qa.log	cal103a.qa.log	cal109a.qa.log	cal526a.qa.log
cal041.qa.log	cal054.qa.log	cal103b.qa.log	cal109b.qa.log	cal526b.qa.log
cal042.qa.log	cal055.qa.log	cal103c.qa.log	cal109c.qa.log	cal526c.qa.log
cal043.qa.log	cal056.qa.log	cal104a.qa.log	cal523a.qa.log	cal526d.qa.log
cal044.qa.log	cal071a.qa.log	cal104b.qa.log	cal523b.qa.log	cal526e.qa.log
cal045.qa.log	cal071b.qa.log		cal523c.qa.log	cal526f.qa.log

7 TEST PROCEDURES

All devices must complete all test procedures specified in Section 5 even if the automation is not available for a particular test case. When the test automation is not utilized, the testing methodology must be described in sufficient detail to reproduce the test at the FieldComm Group office. Any specialized tools must be specified. Any custom software or tools must be included along with the registration of the test results (see *FieldComm Group Quality Assurance and Device Registration Procedure* for more information).

Prior to beginning any testing confirm all FieldComm Group supplied tools are the current version (see the Change Log at http://go.fieldcommgroup.org/whart-test-system-documentation). Basic device testing must be performed first and in the following order.

- The FSK Physical Layer testing of the wired or maintenance port must be successfully completed prior to running any of the automated tests.
- It is essential that the Token-Passing Data-Link Layer tests (with the exception of DLL039A and DLL039B) be completed prior to running any Application Layer tests. The Application Layer test automation is certain to operate incorrectly if the Token-Passing Data-Link requirements are not met.
- The Slave Universal Command Tests (UAL) must be completed before running the either Slave Common Practice Command Tests or the Device-Level wireless tests.
- Device-Level wireless tests (except TML501) should be performed after adherence to Universal Command requirements has been validated.
- The Slave Common Practice Command Tests (CAL) must be performed next.

Once the basic, core operation of the device has been validated the stress tests and systems level test must be performed including:

- The stress tests (DLL039A; DLL039B); and
- The System-Level wireless tests (SLT000-SLT002) must be completed.

An overview of the standardized tests is provided in 7.1 and the Master Token-Passing Data-Link Layer in 7.2. A detailed list of the Device-Level tests that must be performed is in Subsection 7.3. Finally, the System-Level test procedures are provided in Subsection 7.4

7.1 Standardized FieldComm Group Tests

An extensive set of standardized test procedures is available for Slave Token-Passing Data-Link, FSK Physical Layer, Slave Universal Command and Slave Common Practice Command. Standardized test procedures are specified in the following test specifications:

- *Slave Token-Passing Data Link Layer Test Specification*, HCF_TEST-1, FCG TT20001
- *FSK Physical Layer Test Specification*, HCF_TEST-2, FCG TT20002
- *Slave Universal Command Test Specification*, HCF_TEST-3, FCG TT20003
- *Slave Common Practice Command Test Specification*, HCF_TEST-4, FCG TT20004

As indicated in Subsection 5.1, these tests must be performed on WirelessHART Field Devices and Adapters to assess device compliance. Test automation is available and must be used to perform the test procedures in the Slave Token-Passing Data-Link, Universal Command and Common Practice Command test specifications. These tests are performed using the *HART Test System* (which is a subset of the *WirelessHART Test System*).

7.1.1 Slave Token-Passing Data-Link Testing

Data Link Layer testing requires The *HART Test System* to be connected via RS-232 to HART interface (see Figure 3) to the DUT. Token-Passing Data Link Layer testing requires detailed timing of responses and the detection of invalid data, improper addressing or invalid message structure. Consequently, the test procedures are executed using HTest scripts while HSniffer records the master-slave interaction as an independent observer. HSniffer is connected via separate RS-232 to the HART interface of the DUT.

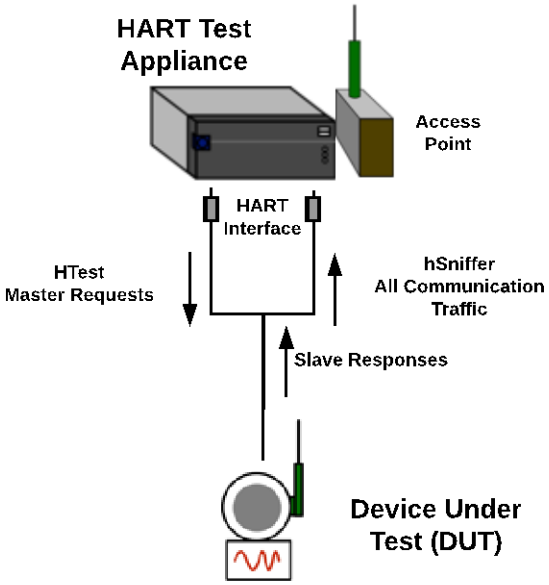

Figure 3. Setup for Automated Token-Passing Data Link Layer Testing

The Data Link Layer test script suite invoked via the HART Menu. This application is invoked automatically when the HART Test System is powered up of by typing "`hartmenu<cr>`" at the Linux prompt. All tests are available via the HART Menu application.

7.1.2 Universal and Common Practice Command Testing

The setup for Application Layer command testing is simpler then that required for Token-Passing Data-Link Layer testing. Universal Command testing and Common Practice Command testing are performed twice: once via the wired or maintenance port and again via the wireless channel. In both cases the tests are run from the HART Test System. The first tests should be performed via the wired or maintenance port by connecting the HART Test System via an RS-232 to HART interface (see Figure 4) to the DUT. The tests can be run using the HART Menu built into the HART Test System.

Once this testing is successful, the testing must be repeated via the wireless channel. Connecting the HART Test System via a HART over UDP (Access Point) (see Figure 5) to the WirelessHART network allows the operation of the Universal and Common Practice commands to be tested. Once again, the tests can be executed using the HART Menu.

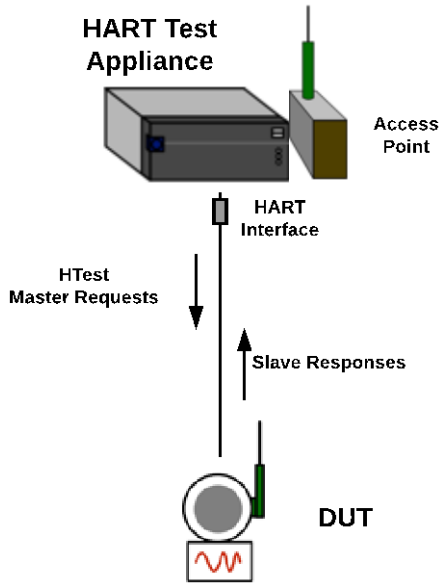

Figure 4. Setup for Automated Application Layer Testing via Wired or Maintenance Port

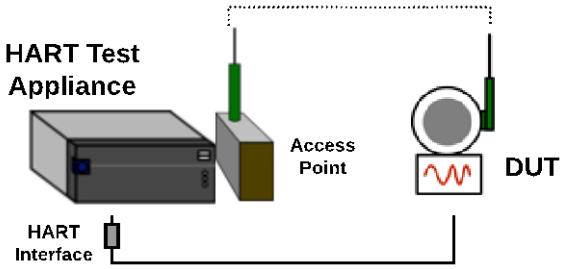

Figure 5. Setup for Automated Application Layer Command Testing Wirelessly

Each time an Application Layer test is performed, the required log file is automatically created. For example, running UAL000 creates the log file "UAL000.qa.log". When using HART Menu to run all Application Layer tests all the required log files are created.

7.2 Master Token-Passing Data-Link Testing

WirelessHART Adapters are hybrid devices that must act as both a Token-Passing Data-Link master and slave. Compliance with slave Token-Passing Data-Link requirements is confirmed using the test procedures in the *Slave Token-Passing Data Link Layer Test Specification*. Master Token-Passing Data-Link requirements must also be assessed.

The *Master Token-Passing Data Link Layer Test Specification* (HCF_TEST-5, FCG TT20005) is a draft version of standardized test procedures for verifying master compliance with Token-Passing Data-Link Layer requirements. All test procedures in this draft test specification or their equivalent must be performed manually.

7.3 Device-Level Wireless Tests

The *TDMA-Mesh Test Specification* (HCF_TEST-6, FCG TT20006) is a draft version of standardized test procedures for validating compliance with TDMA Data-Link Layer and Mesh Network Layer requirements. To get 100% test coverage a combination of Device-Level and System-Level (see Subsection 7.4) test musts be performed. The Device-Level tests are performed using Wireless Test System plus WiAnalys (see Figure 6). The Wireless Test System connects to the DUT both wirelessly and via the DUT's wired or maintenance port. HART FSK communications is used to perform the basic provisioning of the DUT prior to it joining the network. While the network physically only consists of the DUT and the Wireless Test System, the Wireless Test System will simulate the presence of several virtual devices (represented by devices a-f in Figure 6).

Since TDMA-Mesh testing requires detailed timing of responses and the detection of invalid data, improper addressing or invalid message structure. Consequently, the test procedures are executed using WiHTest scripts while WiAnalys records all wireless communications as an independent observer. Prior to initiating each test (e.g., via the HART Menu), WiHTest must manually be configured to record the communications to the correct log file. In addition, the export file must also be configured. For a list of the files that must be recorded see Subsection 6.3.1.

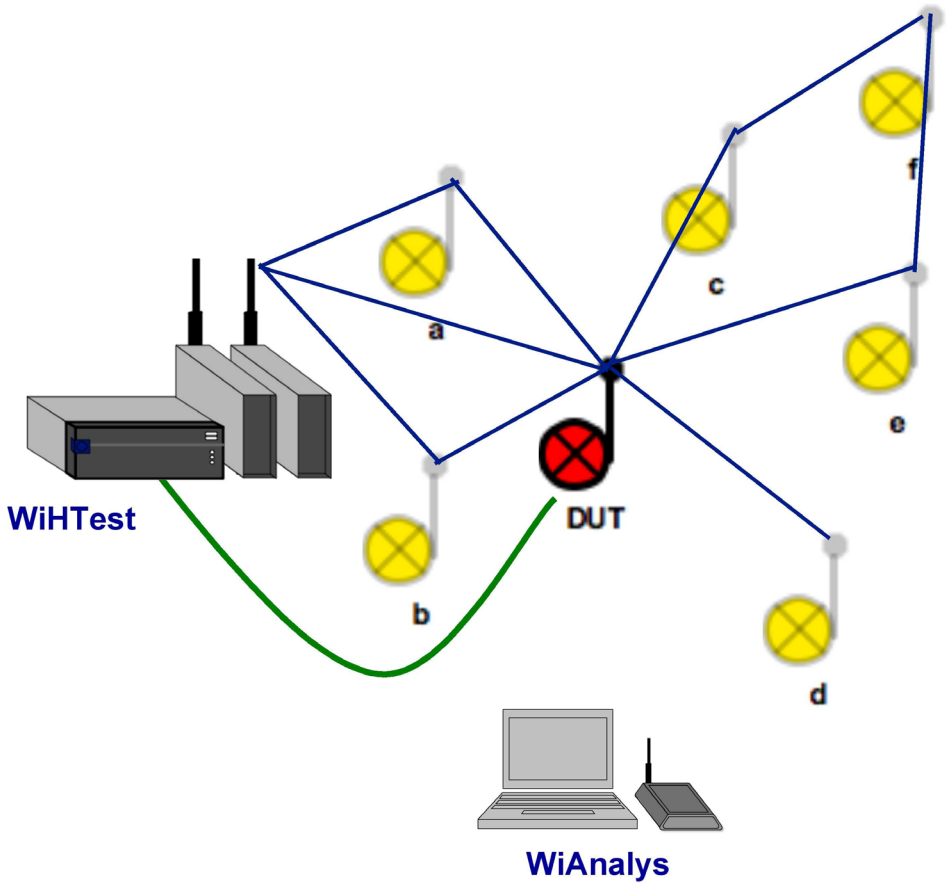

Figure 6. Basic Setup for Automated Wireless Data Link Layer and Network Layer Testing

Key test procedures from this draft test specification have been automated and must be used for testing and registering WirelessHART Field Devices and Adapters. The following tests must be performed from the draft TDMA-Mesh Test Specification.

Table 18. TDMA-Mesh Test Procedures Used for Validation

Test	Description
TML100	Command Audit A Audit via Maintenance Port B Audit via Wireless Connection C Audit Wireless vendor specific commands
TML101	Provisioning
TML102	Joining A Direct Join B Join Retry C Join Retries
TML201	Link Management A Basic Add and Remove Link Test B Check Link Table Response Codes
TML202	Neighbor Table Management A Basic Add and Remove Neighbor B Test Response Codes C Combined Link and Neighbor Table Test
TML203	Superframe Table Management A. Randomly add and delete inactive superframes B. Randomly add superframes with random initial activation status C. Manipulating the length and properties of Superframes D. Delete all Superframes E. Write Superframes and Delete Superframe through the maintenance port F. Manipulating Handheld Superframe H. Test superframe response codes
TML204	Session Table A. Basic Session Table Manipulation B. Session Response Codes
TML205	Route and Graph Table Management A. Route Table Management B. Route Response Codes C. Source Routes D. Graph Route and Edge Management E. Superframe as Graph Equivalence F. Write Device Nickname
TML206	Timetable Management A. Timetable Manipulations B. Timetable Response Codes C. Device Requesting Burst Timetable D. Requesting Event Notification Timetable E. Requesting Block Transfer Timetable F. Requesting Maintenance Timetable
TML208	Basic publishing A. Configure Burst Mode through the maintenance port B. Configure Burst Mode through the Wireless Connection C. Validate that the device requests Burst Mode after it is reset D. NM Adjusts Resource Commitments E. NM removes Links F. Service Request with Invalid Route ID
TML210	Transmit back-off handling A. DUT's ability to use and restrict different back-off exponent values B. DUTs ability to infer collisions, back-off, and retry transmissions C. Configure and honor different back-off exponent limits
TML211	Time-To-Live (TTL) Management A. Test the DUT's ability to restrict different "TTL" hop-count limits B. Test of DUT's TTL value processing for received NPDUs
TML212	ASN Snippet and maxPacketAge A. Test the DUT's ability to restrict different NPDU age limits B. Test of DUT's ASN snippet value processing for received NPDUs C. Test of DUT's ASN snippet processing for NPDUs addressed to it D. Test of DUT's ASN snippet value processing for DUT-originated NPDUs
TML213	NPDU nonce formation A. Nonce sliding window management B. Duplicate NPDU detection C. Testing gaps in to the nonce counter D. Nonce Counter Roll-over E. Determining if the PDU is new or old
TML214	Session Key Management A. Change Network Key B. Change NM Unicast Session Key C. Change NM Unicast Broadcast Key D. Change GW Unicast Session Key E. Change GW Unicast Broadcast Key F. Change Network Key & GW Broadcast Session Key at same ASN
TML216	Configurable timers A. Advertisement timer B. Keep-Alive timer C. Path Failure timer D. Health Report timer E. Broadcast timer F. Discovery timer
TML220	Device disconnection A. Disconnect during normal operation
TML222	Basic DLPDU Construction A. Validate Superframe Header (0x41) B. Validate Address Specifier C. Validate MIC Calculations D. Validate Sequence Number E. Validate Network ID
TML223	DLPDU Specifier
TML224	Device buffer management A. Test NACK response codes B. Test packet precedence and tie-breakers.
TML225	Device join scenarios A. Device joins with new join key B. Device joins with new network id
TML302	Handheld Communications A. DUT communicates with DUT using handheld superframe
TML303	Graph Routing A. Graph Routing - Upstream B. Graph Routing - Downstream C. Graph Routing - Broadcast not acknowledged D. Graph Routing - Broadcast acknowledged E. Graph Routing - Destination is Neighbor
TML304	Source and Proxy routing A. Source routing - destination reachable B. Source routing - destination not reachable (end

Test	Description
	destination not a neighbor) C. Source routing - destination reachable (end destination is a neighbor) D. Proxy routing - proxy is not a neighbor E. Proxy routing - proxy is a neighbor
TML305	Superframe Routing A. Superframe Routing B. Source + Superframe C. Source + Graph Routing
TML307	Routing and Transport Layer Alarms A. Path Down Failure B. Source Routing Failure C. Graph Routing Failure D. Transport Failure
TML309	Buffers and Forwarding Delay
TML311	Packet precedence and priority

Test	Description
	A. Arbitrate amongst receive messages B. Rejects messages when receive buffers depleted C. Packet precedence & priority - rejects according to priority threshold
TML314	Acknowledged Broadcast Communications A. Process & ACK broadcast messages B. Forward on graph

7.4 System-Level Wireless Device Tests

The mesh is the key to WirelessHART's high availability and reliability. System-level testing confirms the DUT correctly and completely participates in the operation of a real, physical WirelessHART network. Many HART requirements are demonstrated during both routine and abnormal network operation.

7.4.1 Test setup

All system-level tests are performed with the DUT installed near the center of a medium-sized network. The equipment required for system tests include:

Table 19. Equipment List for System-Level Tests

Item	Qty	Description/Purpose
1	1	DUT. The device to be tested.
2	1	Network Manager/Gateway/Access Point (Gateway). The Gateway must be HART-over-UDP compliant. The Gateway provides wireless access to the DUT.
3	1	WiHTest. WiHTest is the FieldComm Group's WirelessHART reference implementation and is used for a variety of purposes, depending on the test being performed.
4	1	WiAnalys. WiAnalys is used to record and decipher all network communications.
5	15-25	WirelessHART devices. These devices, along with the Gateway, constitute the test network. The DUT is located mid network such that is has many neighbors.
6	1	The HART-IP Client (not shown in Figure 7) is used to provision and access the DUT during testing.
7	1	HART-Registered interface (modem). The interface connects the MS Windows computer running the HART-IP Client access to the maintenance port on the DUT.

All System-level testing uses a medium size network with a topology like the following.

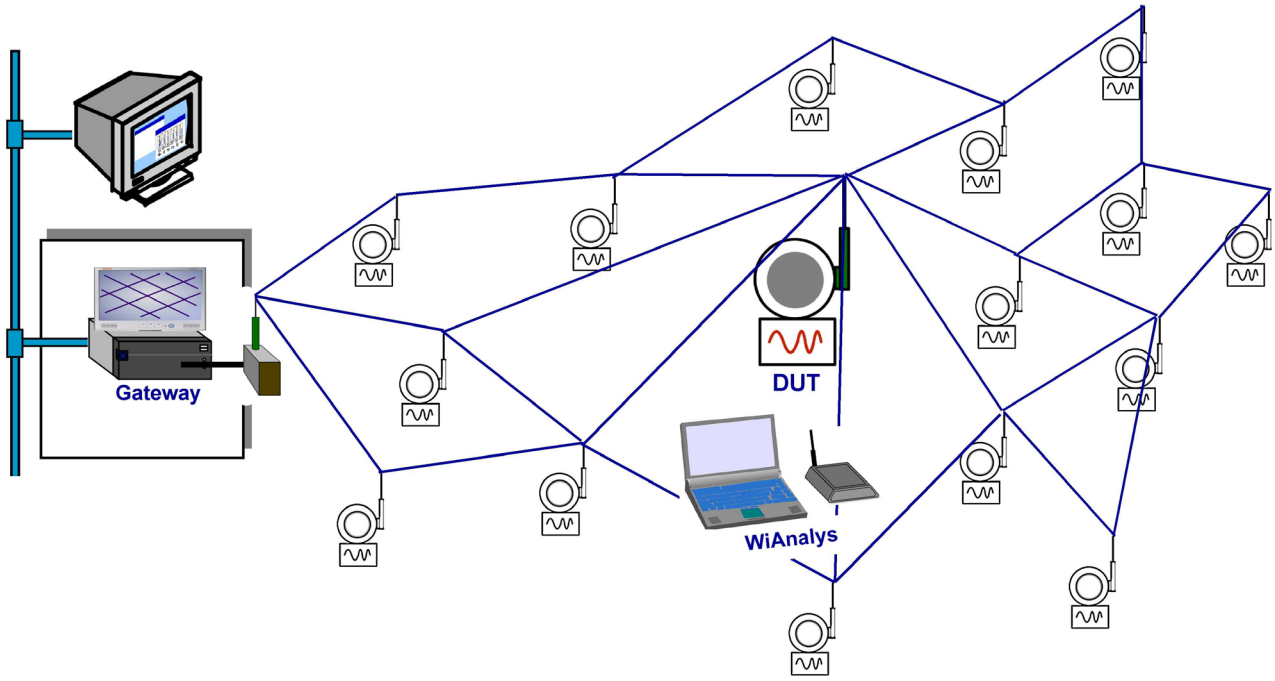

Figure 7. Typical WirelessHART Network Topology Required for System-Level Tests

For this testing, the DUT must be centrally located in the network. It must have at least two parent devices, neither of which can be the Gateway. It must also have several descendants. WiAnalys must be located near the DUT.

7.4.2 Overview of System-Level Test Procedure

The same basic procedure is used for all System-Level tests. Table 20 outlines the basic process that must be followed for each System-Level test. The basic procedure for each System-Level test is similar and includes: provisioning the DUT; configuring WiAnalys; performing the tests and analyzing the data captured during the test. During each test a test log must be created (see Subsection 7.4.3).

Table 20. Generic Procedure for System-Level Testing

Step	Action
1	Create the test log and complete the initial information.
2	Provision the DUT. The DUT must be provisioned with the Network ID and Join Key. The Network ID and Join Key should be the same for all System-level tests. The DUT should be configured for Command 9 and a 16 second burst period.
3	Configure WiAnalys. WiAnalys must be configured with the Network ID ad Join Key. The data log and export files must be configured with the file names specified in the System-Level test (e.g., slt001.log and slt001.txt). WiAnalys must be configured to include all packets (i.e., all filters turned off).
4	Perform the test procedure. Record in the test log any pertinent events that occur during the test execution.
5	Stop WiAnalys.
6	Review the data captured by WiAnalys. Apply the assessment criteria defined in the System-Level Test to determine whether the DUT passes or fails the test.
7	Complete the test log indicating whether DUT passed or failed the test.

WiAnalys records all network communications during the test. The data captured by WiAnalys is the basis for determining successful test completion. Consequently, ensuring WiAnalys records the data and decodes the data is essential.

WiAnalys must be running prior to the DUT joining the network and records data uninterrupted through the entire test. Otherwise the test and WiAnalys must be restarted.

Once the test has been performed and the data successfully captured the test result must be determined. Each test has its own Data Analysis Requirements and Pass/Fail Criteria. The data must be manually assessed, and the result manually determined.

7.4.3 System-Level Test Logs

A test log must be completed for each System-Level test performed. The test log is a Microsoft Word based document and is the record of the test. The test log includes:

- Identification;
- Operational; and
- Activity/Event Journal.

Identification data includes: System-level test being performed; the location where the test is being performed; the person conducting test; and environmental conditions (e.g., indoors, outdoors, plant facility).

Operational data includes device identification and network configuration. Device identification for the Gateway Network Manager and DUT must be provides and includes

- Unique ID (Command 0)
- Revision of device, software and hardware revisions (Command 0)
- HART revision supported (Command 0)
- Revision of radio firmware/hardware (Command 64512)
- Device Wireless Nickname (Command 832 to the GW)

Network configuration data includes:

- Network ID and Join Key;
- Network Topology (Command 834);
- Number of hops from DUT to the nearest Access Point;
- Number of devices upstream (i.e. between the DUT and the Access Point); and
- Number of devices downstream (descendants).

The Activity/Event Journal is a chronological record completed as the test is performed. For example, the first Activity/Event should be provisioning of the DUT and the last should be stopping WiAnalys. Each entry must include the date; time; and description of the event.

7.4.4 Test Procedures

The individual system test procedures are specified in this section. Each test consists of an overall test description, one or more test cases and the corresponding test case procedures, data analysis requirements, pass/fail criteria and suspension/resumption criteria.

7.4.4.1 SLT000 Network Reboot

This test determines how long a group of devices takes to reform a network. A full network reboot is a very chaotic and stressful event for the DUT. All the DUT's neighbors disappear over a period of time and the device must begin to look for advertisements, build a neighbor list and to get itself back into the network. With all the other devices around the DUT doing the same thing, the DUT may need to do prioritized join, back-off and/or proxy route for other joining devices. The DUT will likely participate in message source routing as well as Graph/Superframe routing for devices publishing data through the DUT while the network continues to form.

Description

This test establishes confidence that a device will rejoin a network if the network was temporarily shut down. It tests the capability of the device to recognize potential neighbors and see that it is capable of changes to its network connections (neighbors, superframes, links).

Features to be Tested

A network reboot is very chaotic. This test demonstrates the DUT implementation of the join procedures and state machines are robust. For example, join retries and collision back-off operation will be stressed.

This test verifies that the device correctly reports its join status / wireless mode if the network is removed.

It also verifies correct operation when the network becomes operational again.

This test also confirms neighbor discovery is working (capture discovery links and validate against reported neighbors in the health reports). It will be verified that the device will find the same neighbors.

Verify acceptance of new superframes/links/graphs/services written by the network manager.

The keep-alive rate must be reduced if packets are generated at an interval that is shorter than the keep-alive time. It must be verified that only keep-alives to neighbors are send where no exchange of packets occurred within the keep-alive interval.

Data Analysis Requirement

The following events are extracted from the Test Log and confirmed by review of the WiAnalys data log files.

- Time for the DUT to initially join the network before the GW was restarted.
- Time for the DUT to join after the GW was restarted.
- Time for the DUT to start publishing data
- Time for the DUT to have two neighbors

Review the WiAnalys data log files to confirm the DUT sends Keep-Alive messages to neighbors as required.

Test Procedure

Table 21. SLT000 Test Procedure

Step	Action
Prologue	Test Network must be formed and operational. Provision the DUT. Configure WiAnalys.
1	Join the DUT to the system test network. Force the DUT to join the network using Command 771; Monitor the join process using Command 769 and note when the DUT joins.
2	After the DUT has joined the network the network must be operated for a minimum of 30 minutes before proceeding to the next step in this test procedure. Confirm the DUT is publishing at the configured burst rate using WiAnalys (annotate the Activity/Event Journal accordingly).
3	Via the Gateway, read and record the neighbor table of the DUT using Command 787 and 780 for each neighbor.
4	Record the response to Command 840 sent to the Gateway for the DUT and its neighbors.
5	Power down the Gateway for at least 30 minutes. At the end of this interval confirm there is no traffic associated with the system test Network ID (using WiAnalys).
6	Turn on the Gateway and allow the network to reform.
7	Monitor the network and note when: A. The DUT joins the network (use Command 769 sent to the DUT maintenance port) B. The DUT begins publishing process data (using WiAnalys) C. The DUT has at least 2 operational neighbors (monitor Command 780 and 787 using WiAnalys)
8	After completing the previous step, operate the network for a minimum of 60 minutes
9	Record the network statistics including: A. The health reports using WiAnalys (Commands 779, 780 and 787) B. Response to Command 840 sent to the Gateway for the DUT and its neighbors.
Epilogue	Stop WiAnalys

Pass/Fail Criteria

1 DUT joins the network in less than 10 minutes: PASS

2 DUT joins the network after gateway restart in less than 30 minutes: PASS

3 DUT begins publishing data after rejoin in less than 10 minutes: PASS

4 DUT has two neighbors after rejoin listed in second health report after rejoin: PASS

5 DUT latency is less than one-third its configured burst rate: PASS

6 DUT sends Keep-Alive messages to neighbors as required: PASS

Suspension criteria and resumption requirements

If the DUT does not initially join or does not rejoin the network after the gateway restart the test must be suspended until a cause can be determined.

7.4.4.2 SLT001 Neighbor Abnormal Behavior

This test determines the DUT's ability to recognize a neighbor has fallen out of the network or failed in some way and subsequently recognizes the neighbor's attempts to re-join the network.

Description

This test ascertains that the DUT will send path failure alarms if neighbors are no longer reachable. It will also expose the DUT's ability to track neighbors in the health reports.

Features to be Tested

Health reports are correct, even if time sources are removed.

Path down alarms are generated but links are still probed (keep-alives or normal packets) until neighbor is removed.

Different neighbor RSL signal strength reporting with different transmit power settings.

It may be possible to observe flow control handling if time sources are removed. It should be checked that at least the packet priority is observed.

Test Procedure

Table 22. SLT001 Test Procedure

Step	Action
Prologue	Test Network must be formed and operational. Provision the DUT. Configure WiAnalys.
1	Join the DUT to the system test network. Force the DUT to join the network using Command 771; Monitor the join process using Command 769 and note when the DUT joins.
2	Via the Gateway, using Command 780 (to the DUT) and 832 (to the Gateway), identify the Unique ID and Nickname a linked descendant neighbor of the DUT. Record neighbor Unique ID and Nickname.
3	Remove power from the neighbor selected in the previous step.
4	Via the Gateway, poll command 780 to determine when the lost neighbor is removed from the neighbor table. Simultaneously, monitor the DUT communications with WiAnalys and note when: A. The DUT issues Command 788 for the lost neighbor. B. The DUT publishes Command 780 without the lost neighbor.
5	Operate the network in this new state for at least 30 minutes.
6	Apply power to the lost neighbor.
7	Via the Gateway, poll command 787 to determine when the lost neighbor reappears. Simultaneously, monitor the DUT communications with WiAnalys and note when the DUT publishes Command 787 with the lost neighbor.
8	Let the network run in this new state for 30 minutes.
9	Via the Gateway, using Command 780 (to the DUT) and 832 (to the Gateway), identify the Unique ID and Nickname a linked time source neighbor of the DUT. Record neighbor Unique ID and Nickname.
10	Remove power from the neighbor selected in the previous step.
11	Via the Gateway, poll command 780 to determine when the lost neighbor is removed from the neighbor table. Simultaneously, monitor the DUT communications with WiAnalys and note when: A. The DUT issues Command 788 for the lost neighbor. B. The DUT publishes Command 780 without the lost neighbor.
12	Operate the network in this new state for at least 30 minutes.
13	Apply power to the lost neighbor.
14	Via the Gateway, poll command 787 to determine when the lost neighbor reappears. Simultaneously, monitor the DUT communications with WiAnalys and note when the DUT publishes Command 787 with the lost neighbor.
15	Let the network run in this new state for 30 minutes.
Epilogue	Stop WiAnalys.

Data Analysis Requirement
Review Wi-Analys data log files and record the times for each of the following events

- The DUT sends Command 788 (Alarm Path Down).
- The Network Manager sends Command 967/969/971/974 to the DUT to re-route messages away from the lost neighbor.
- The DUT no longer reports the lost neighbor in Command 780.
- The DUT begins to publish the lost neighbor in Command 787.

This analysis must be performed for both the removal of a descendant and a time source parent (i.e., there will be two sets of times). The times extracted from the WiAnalys data log files shall be compared to those determined by polling the device.

Pass/Fail Criteria

1	DUT sends Command 788 Alarm "Path Down" when neighbors are removed:	PASS
2	Time difference between the neighbor being removed from Command 780 response polled and published is greater than 1 health report period:	FAIL
3	DUT recognizes the new neighbor and adds it to its neighbor table:	PASS
4	Time difference between the neighbor being added to Command 787 response polled and published is greater than 1 health report period:	FAIL
5	The DUT rejoins during the test	FAIL

Suspension criteria and resumption requirements
When the neighbor is removed, if the DUT does not transmit Command 788 or remove it from the neighbor table the test must be suspended. Also, if the neighbor is powered back up and the DUT never reports it as a neighbor the test must be suspended.

If the Network Manager never removes the links to the list neighbor, the test must be suspended.

The test may be resumed when the DUT manufacturer has corrected the issue (fixed the DUT or replaced the Network Manager).

7.4.4.3 SLT002 Long-term System Test

This test checks the Long-Term Reliability of a WirelessHART DUT. The test is conducted over 2 week period with the DUT participating in a well-formed, operational WirelessHART network.

Description

This test will verify the stability of the device in a normal network. The main focus is to ensure that the device adheres to the network manager commands, the published schedule (update rate, health reports) and stays in the network over an extended period of time publishing burst messages at the configured rate. In addition, the accessibility is checked daily over the wireless link.

Features to be Tested

The number of joins is monitored (should be 1 join request and it remains joined to the network). If abnormal conditions are observed during the test, they must be analyzed and the FieldComm Group will assess whether the test can proceed or must be terminated.

The publish burst data and health report rates must be validated. The ability for the device to continue to respond to general host system requests is also tested.

Test Procedure

Table 23. SLT002 Test Procedure

Step	Action
Prologue	Test Network must be formed and operational. Provision the DUT. Configure WiAnalys.
1	Join the DUT to the system test network. Force the DUT to join the network using Command 771; Monitor the join process using Command 769 and note when the DUT joins.
2	After the DUT has joined the network, the network must be operated for a minimum of 120 minutes before proceeding to the next step in this test procedure. Confirm the DUT is publishing at the configured burst rate using WiAnalys.
3	Via the Gateway, read initial state of DUT network configuration parameters: A. Read UTC time mapping – Command 794 B. Read Time values – Command 796 (using enumerations 0 – 6) C. Read radio output power – Command 798 D. Read CCA mode – Command 804 E. Read Packet Time-to-live – Command 808 F. Read Join Priority – Command 810 G. Read packet priority – Command 812 H. Read back-off exponent – Command 819
4	After joining and every workday thereafter, confirm (using WiAnalys) the DUT is publishing as specified.
5	After joining and every workday thereafter, via the Gateway, issue the following cached DUT commands: A. Command 9. Include Battery Life (i.e., Device Variable 243) B. Command 48
6	After joining and every workday thereafter, via the Gateway, issue the following non-cached DUT commands: A. Command 779 B. Command 780 (for all neighbors) C. Command 782 (for all sessions configured) D. Command 783 (for all superframes configured) E. Command 784 (for all links configured) F. Command 785 (for all graphed configured) G. Command 787 (for all neighbors) H. Command 800 (for all services) I. Command 802 (for all routes configured) J. Command 840
7	Via the Gateway, after joining and every workday thereafter, Record the network statistics including: A. The health reports using WiAnalys (Commands 779, 780 and 787) B. Response to Command 840 sent to the Gateway for the DUT
Epilogue	Stop WiAnalys

Data Analysis Requirement
The following events and data are extracted from the Test Log and by review of the WiAnalys data log files.

- Number of DUT joins (from WiAnalys and Command 840).
- Burst data statistics including: number of burst messages generated; number of burst messages expected; and latency.
- The variation in Device Variable values and status.
- Variation or changes in device status.
- Request/Response statistics including: number of requests; number of responses.
- Device state (e.g., neighbors, graphs, superframes, links, etc).
- Device capacities (e.g., number of superframes, links, neighbors, packet buffers; etc.). Commands to extract from data log file include 782, 802, 780, 785, 783, 800, 784, 779.
- Network Management and grooming events. Commands to extract from data log file include 961, 962, 963, 965, 967, 969, 971, 973, 974, 976.

Pass/Fail Criteria

1	The DUT rejoins during the test.	FAIL
2	The DUT consistently publishes at the specified rate.	PASS
3	The device variable time stamp is always consistent with the time the burst message was published.	PASS
4	DUT latency is less than one-third its configured burst rate.	PASS
5	If there are significant variations in the device variable values or status or device status (Note: If appropriate justification is provided, an exception to this rule may be granted).	FAIL
6	The device responds to every request made via either the maintenance port or wireless interface.	PASS
7	As the network is groomed, the DUT properly responds to and acts on Network Management commands.	PASS
9	The DUT uses all frequency channels.	PASS
10	The DUT correctly requests bandwidth prior to beginning publishing process data (i.e., using Command 799).	PASS

Suspension criteria and resumption requirements
The test will be suspended if at any time during the test the DUT fails to respond to a test system command request or a burst message is missed. The test may be resumed immediately if it is determined that the DUT did respond or burst appropriately and some other network phenomenon caused the message to be lost.

If however it is determined that the DUT was the source of the lost message, the test will be suspended and cannot be restarted until the DUT issue is addressed.

ANNEX A. REVISION HISTORY

A1. Revision 2.0

Updated to align with WirelessHART Test System v1.9 including:

- Updating connection drawings
- Updating test lists (e.g., alignment with Common Practice Burst Mode Tests)
- Aligning with FieldComm Group document formats, replaced HART Communication Foundation with FieldComm Group. Updating to include FieldComm Group document and tool numbers.
- Update tooling used for SLT.

A2. Revision 1.0

Initial version.