

DataNet and DatPass Administration Software

Validation Manual

For compliance with the
United States Food and Drug Administration
Title 21 Code of Federal Regulations Part 11
and with GAMP 4

Revision 1.0
Copyright © fourtec – Fourier Technologies 2011



Contents

Chapter 1: Introduction.....	3
Chapter 2: What is Title 21 CFR Part 11?	4
Title 21 CFR Part 11 Definitions.....	4
Fourtec Software	4
Chapter 3: Compliance with Title 21 CFR Part 11	5
References	9
Chapter 4: DatPass Validation Tests.....	10
1 - Initial Login	10
2 - File Menu.....	10
3 - Administration.....	11
4 - Help.....	14
5 - Toolbar Icons.....	14
Chapter 5: DataNet Validation Tests	15
1 - Login	15
2 - File Menu.....	15
3 - Network Menu	16
4 - Tools Menu.....	17
5 – Analysis Menu	22
6 – Help Menu	23
7 – Upper Toolbar Icons	23
8 - Graph Toolbar	24
9 – Table View.....	26
10 – Statistics View.....	26
11 – Map View.....	27
12 – Change Password dialog	32

Chapter 1: Introduction

This manual will guide you through the process of validating the DatPass and DataNet software package to GAMP 4 and FDA Title 21 CFR Part 11 guidelines. This manual will provide users with a test plan for their own performance and operational qualification of DatPass and DataNet.

The manual comprises two main sections. The first section describes the relevant sections of the FDA Title 21 CFR Part 11 and the implementation of these sections in the Fourtec software package. The second section provides the necessary test sheets for DatPass and DataNet.

It is important to understand that the implementation of these guidelines is not the sole responsibility of Fourtec. The software user must undertake a large portion of the responsibility through the appropriate validation tests.

The software package consists of two programs:

- DatPass – DataNet administration application
- DataNet – Data acquisition and analysis application, supporting Fourtec's DataNet data loggers.

To validate the software package, start by testing DatPass, followed by DataNet. Some of these tests assume that the user is familiar with the Windows interface in addition to the DatPass and DataNet software.

Chapter 2: What is Title 21 CFR Part 11?

The Food and Drug Administration (FDA) issued the regulations *Title 21 Code of Federal Regulations Part 11*. These regulations provide criteria for acceptance by FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper. The regulations apply to all FDA program areas, and are intended to permit the widest possible use of electronic technology, compatible with FDA's responsibility to promote and protect public health. Part 11 applies to any record governed by an existing FDA predicate rule that is created, modified, maintained, archived, retrieved, or transmitted using computers and/or saved on durable storage media.

Title 21 CFR Part 11 Definitions

Electronic Record

Any combination of text, graphics, data, audio, pictorial or other information representation in digital form, that is created, modified, maintained, archived, retrieved or distributed by a computer system.

Electronic Signature

A computer data compilation of any symbol or series of symbols, executed, adopted or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

Digital Signature

An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

Closed System

An environment in which system access is controlled by persons who are responsible for the content of electronic records that is on the system.

Open System

An environment in which system access is not controlled by persons who are responsible for the content of electronic records that is on the system.

Standard Operating Procedures (SOPs)

Guidelines and rules defined by the organization implementing Title 21 CFR Part 11 compliance to instruct users what they are and are not permitted to do and how they are to perform the relevant tasks.

Fourtec Software

The dual program software package achieves compliance with FDA Title 21 CFR Part 11 with: *DataNet* and *DatPass*. The *DatPass* software is the administration software, which includes features that define the users that can log into the *DataNet* software, their passwords and the digital signatures the users are permitted to sign data within electronic records (files). The *DataNet* software is used to access the electronic records, display the logger data, analyze the data and allow the user to add the appropriate digital signatures to the electronic records, in addition to other features. An additional security feature is the serial port dongle, without which the *DatPass* and *DataNet* software packages will not operate.

Chapter 3: Compliance with Title 21 CFR Part 11

Title 21 CFR Part 11 Requirements		Comments on Compliance or Requirements	
§11.10 Controls for Closed Systems			
(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Yes	DataNet will not open invalid or altered data.
(b)	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency.	Yes	To ensure data integrity, DataNet stores data with specific formats (.dat and .dnp). Data can be exported to Excel™ and stored in common formats, such as an Excel workbook or for example comma delimited or tab delimited. Only through the (dat) formats can data be read back into DataNet and only these formats support electronic signatures.
(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	N/A	The customer chooses which data directory to save files to. Otherwise, the default directory <i>C:\Program Files\Fourier Systems\DataNet for DatPass/DataNet</i> data is used. System owners must establish their own SOPs to protect and restore data files.
(d)	Limiting system access to authorized individuals.	Yes	For limited access, the customer must purchase a valid software license and dongle device, preventing access to unauthorized users.
(e)	Use of secure, computer-generated, time- stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	Yes	Every action that generates or alters an electronic record (dat and dnp), automatically generates an entry into an encrypted log file, which can be used in audit trail. The entries are chronologically organized and cannot be edited or deleted. The entries can only be viewed using the DatPass software. It is the system owner's responsibility to create SOPs to protect and restore audit trail files.
(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate	Yes	A smart and user friendly interface ensures all DataNet operations follow a specified order. This ensures all stages are followed.
(g)	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	Yes	When using DataNet, users logon with a valid username and password. Further security is ensured by a Fourier Dongle having to be connected to the workstation. All actions are recorded in an encrypted audit trial log file.

Title 21 CFR Part 11 Requirements		Comments on Compliance or Requirements	
(h)	Use of device (e.g. terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Yes	DataNet checks the status of the logger at each communication – errors are automatically reported.
(i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems has the education, training, and experience to perform their assigned tasks.	N/A	System owners must provide their authorized users with relevant training.
(j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	N/A	System owners must develop written policy in which reliability and responsibility of each user is documented.
(k)	Use of appropriate controls over systems documentation including:		
(k)(1)	Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	N/A	The DataNet and DatPass package for Title 21 CFR Part 11 compliance are supplied with detailed user guides and help files, which can be used to create SOP. Distribution, access and implementation of this documentation are the responsibility of the system owner.
(k)(2)	Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	N/A	This is the responsibility of the system owner.
§11.30 Controls for Open Systems			
	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	N/A	DataNet has been implemented as a closed system.

Title 21 CFR Part 11 Requirements		Comments on Compliance or Requirements	
§11.50 Signature Manifestations			
(a)	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:		
(a)(1)	The printed name of the signer;	Yes	Stored and printed data contains: User login name, time/date stamp, and user signature meaning(s).
(a)(2)	The date and time when the signature was executed;	Yes	
(a)(3)	The meaning (such as review, approval, responsibility, or authorship) associated with the signature	Yes	
(b)	The items identified in paragraphs (a)(1),(a)(2), and (a)(3)of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	Yes	Electronic signatures in DataNet are subject to the same requirements as electronic records. Electronic signatures can be viewed electronically and can be included on a printout.
§11.70 Signature/Record Linking			
	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied or otherwise transferred so as to falsify an electronic record by ordinary means.	Yes	In DataNet, raw data and electronic signatures are permanently linked in a single file, and as such cannot be edited, deleted or separated.
§11.100 General Requirements			
(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Yes	DatPass software contains an authorized user list containing login name, password, and meanings list, making every user unique to the system.
(b)	Before an organization establishes, assigns, certifies or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	N/A	This is the responsibility of the system owner.
(c)	Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.	N/A	This is the responsibility of the system owner.

Title 21 CFR Part 11 Requirements		Comments on Compliance or Requirements	
(c)(1)	The certification shall be submitted in paper form, and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100),5600 Fishers Lane, Rockville, MD 20857.	N/A	This is the responsibility of the system owner.
(c)(2)	Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	N/A	This is the responsibility of the system owner.
§11.200 Electronic Signature Components and Controls			
(a)	Electronic signatures that are not based upon biometrics shall:		
(a)(1)	Employ at least two distinct identification components such as an identification code and password.	Yes	DatPass Software for Title 21 CFR Part 11 compliance uses a unique dual component combination: Login username and password. Every login and new digital signature with DataNet requires a valid username and password. DataNet enforces the user to re-logout after a time period, which is defined by the administrator via the DatPass software.
(a)(1)(i)	When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual	Yes	
(a)(1)(ii)	When an individual executes one or more signings not performed during a single continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.	Yes	
(a)(2)	Be used only by their genuine owners;	N/A	Information confidentiality is the responsibility of the system owner and users.
(a)(3)	Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	N/A	Information confidentiality is the responsibility of the system owner and users.

Title 21 CFR Part 11 Requirements		Comments on Compliance or Requirements	
(b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	N/A	Biometrics are not the basis of electronic signatures generated by DatPass software for Title 21 CFR Part 11 compliance.
§11.300 Controls for Identification Codes/Passwords			
	Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:		
(a)	Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	Yes	Since every user is unique in the DataNet and DatPass systems, duplicate combinations of username and password are impossible.
(b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised, (e.g. to cover such events as password aging).	Yes	Adequate aging of passwords is the responsibility of the system owner. DataNet allows authenticated users to change their own logon password.
(c)	Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	N/A	Unauthorized access is vetoed by the DatPass software since an administrator can disable or remove any user from the system.
(d)	Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	Yes	All unsuccessful logons are recorded in the audit trail log file.
(e)	Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information, to ensure that they function properly and have not been altered in an unauthorized manner.	N/A	This is the responsibility of the system owner.

References

For further information on FDA Title 21 CFR Part 11, please visit the FDA website:

www.fda.gov

For FDA guidance documents:

www.fda.gov/ora/compliance_ref/part11/

Chapter 4: DatPass Validation Tests

1 - Initial Login

Ensure that the DatPass security plug is connected to your computer's USB port.

Note: After installation, the first user to login to the DatPass software is automatically assigned the user name *Admin*. He is classified as an administrator.

Test #	Test Description	Expected Result	Result
1.1	Double click the DatPass icon on the Desktop.	Verify that the <i>User Login</i> dialog box opens.	
1.2	Click New User in the login window.	a. Verify that the <i>New User Login</i> window opens. b. Verify that the <i>New User</i> drop-down menu displays the <i>Admin</i> user name.	
1.3	a. Populate the <i>New User ID</i> , <i>Confirm User ID</i> , <i>New Password</i> and <i>Confirm Password</i> fields, and click OK . b. Exit the DatPass software. c. Launch the DatPass software.	a. Once DatPass is launched, verify that the <i>User Login</i> window opens. b. Verify that the newly created User ID and User Password are correct (click OK and verify successful login to DatPass).	


2 - File Menu

Test #	Test Description	Expected Result	Result
2.1	On the File menu, click Open . Navigate to: <i>My Documents\Fourier Systems\DatPass</i> . Note: You will only find files saved in this directory if data, such as the Audit Trail log, has been previously saved.	a. Verify that the <i>Open</i> dialog box opens. b. Select a file to open, and click Open . c. Verify that the file opens, and the table data is displayed in the main DatPass window.	
2.2	On the File menu, click New .	Verify that the DatPass main window is clear i.e. there is no Audit Trail log data.	
2.3	On the File menu, click Print . Note: For this action to succeed, the main DatPass window must be populated with Audit Trail log data.	Verify that the <i>Print Dialog</i> dialog box opens.	
2.3.1	In the <i>Print Dialog</i> dialog box: a. Select Portrait or	Verify that the <i>Print</i> dialog box opens.	

Test #	Test Description	Expected Result	Result
	Landscape orientation. b. Using the <i>From</i> and <i>To</i> fields, define the date and time range to print. c. Click OK .		
2.3.2	In the <i>Print</i> dialog box, confirm that the correct printer is selected in the <i>Name</i> drop-down menu and click OK .	Verify that the graph was printed with the specific date and time range (as defined in test 2.3.1), at the selected printer.	
2.4	On the File menu, click Print Setup .	Verify that the <i>Print Setup</i> dialog box opens.	
2.5	On the File menu, click Log Off .	Verify that the <i>User Login</i> dialog box opens.	

3 - Administration

Test #	Test Description	Expected Result	Result
3.1	On the Administration menu, click User Administration .	a. Verify that the <i>User Administration</i> dialog box opens. b. Verify that <i>Admin</i> appears under the <i>User Name</i> tab and <i>Administrator</i> appears under the <i>Group</i> tab.	
3.1.1	a. In the <i>User Administration</i> dialog box, click Add User . b. Enter a new user name in the <i>User Name</i> field. c. Select a Group from the Group drop-down menu: Administrator, Approver, or User. Under the <i>Login Settings</i> heading: d. Enter a number in the <i>Password min length</i> field (for example, 4). e. Enter a number in the <i>User ID min length</i> field (for example, 4). f. Enter number of days in the <i>Password expiration time (days)</i> field (for example, 1). g. Use the drop-down menu in the <i>Inactivity Timeout</i> field to select the duration (for example, 00:05:00). h. Click OK .	Verify that a new user has been added to the <i>User Administration</i> dialog box, listing the correct User Name and Group.	

Test #	Test Description	Expected Result	Result
3.1.2	<p>a. Launch the DatPass software and add click New User.</p> <p>b. Using the new user account created in test 3.1.1, fill in the <i>New User ID</i>, <i>Confirm New User ID</i>, <i>New Password</i> and <i>Confirm Password</i> fields.</p> <p>c. Click OK.</p>	Verify that the DatPass software opens.	
3.1.3	<p>Launch the DatPass software. In the <i>User Login</i> dialog box:</p> <p>a. Enter an incorrect user name and a correct password.</p> <p>b. Enter a correct user name and an incorrect password.</p> <p>c. Enter an incorrect user name and password.</p>	Verify that in all three login tests, the DatPass software does not open.	
3.2	In the <i>User Administration</i> dialog box, select the newly added user (see test 3.1.1) and click Properties .	<p>a. Verify that the User Properties dialog box opens.</p> <p>b. Verify that the properties entered when adding the user (in test 3.1.1) are correct.</p>	
3.2.1	<p>a. In the <i>User Properties</i> dialog box, change the user group using the drop-down menu in the <i>Group</i> field. For example, from <i>User</i> to <i>Approver</i>.</p> <p>b. Click OK.</p>	Verify that the user group was successfully changed by reopening the User Properties dialog box and checking the Group field.	
3.2.2	<p>a. In the <i>User Properties</i> dialog box, change the <i>Login Settings</i>.</p> <p>b. Click OK.</p>	Verify that the <i>Login Settings</i> were successfully changed by reopening the User Properties dialog box and checking the relevant Login Settings.	
3.3	In the <i>User Administration</i> dialog box, select a user and click Deactivate .	Verify that the user icon is now marked with a white cross in a red background, as follows: 	
3.3.1	Open the DatPass software and attempt to login with the user name and password of the newly deactivated user.	Verify that a dialog box opens with the message: <i>Your user account was deactivated. Please refer to your system administrator.</i>	







Test #	Test Description	Expected Result	Result
3.3.2	<p>a. In the <i>User Administration</i> dialog box, select the previously deactivated user and click Activate.</p> <p>b. Exit DatPass, then reopen DatPass and login with the user name and password of the newly activated user.</p>	Verify that you are able to successfully login to DatPass.	
3.3.3	<p>a. In the <i>User Administration</i> dialog box, select a user and click Renew Password.</p> <p>b. Exit DatPass, and then reopen DatPass and attempt to login with that user.</p>	<p>a. Verify that a new DatPass dialog box opens with the message: <i>Your password was reset. Please enter a new password.</i></p> <p>b. After clicking OK, verify that a new <i>Change Password</i> dialog box opens.</p>	
3.3.4	<p>a. In the <i>Change Password</i> dialog box, enter a new password and then confirm this password.</p> <p>b. Click OK.</p>	Verify that the DatPass software opens.	
3.3.5	Launch the DatPass software and login using the user name and new password created in step 3.3.4.	Verify that the DatPass software opens.	
3.4	On the Administration menu, click Group Administration .	<p>a. Verify that the <i>Group Administration</i> dialog box opens.</p> <p>b. Verify that the group names <i>User</i>, <i>Approver</i> and <i>Administrator</i> are displayed.</p>	
3.4.1	In the <i>Group Administrator</i> dialog box, click Add Group .	Verify that the <i>Group Properties</i> dialog box opens.	
3.4.2	<p>a. In the <i>Group Properties</i> dialog box, enter a new name in the <i>Group Name</i> field.</p> <p>b. Click the <i>New</i> check box.</p> <p>c. Click OK.</p>	<p>a. Verify that the <i>Group Administration</i> dialog box opens.</p> <p>b. Verify that the newly created group is displayed in the <i>Group Name</i> list.</p>	
3.4.3	In the <i>Group Administrator</i> dialog box, select the newly created group and click Properties .	Verify that there is only one check box selected (in this case, <i>New</i>).	
3.4.4	<p>In the <i>Group Administrator</i> dialog box, select one of the listed groups and click Remove Group.</p> <p>Note: You will not be able to remove a group if there are still users who are members of this group.</p>	<p>a. Verify that a dialog box opens with the message: <i>Are you sure you want to remove <Group Name> group?</i></p> <p>b. Click Yes.</p>	

Test #	Test Description	Expected Result	Result
3.4.5	On the Administration menu, click Group Administration .	Verify that the group you have removed is no longer displayed in the <i>Group Name</i> list.	

4 - Help

Test #	Test Description	Expected Result	Result
4.1	On the Help menu, click About DatPass .	<ul style="list-style-type: none"> a. Verify that the <i>About DatPass</i> dialog box opens. b. Verify that the DatPass version number and copyright are displayed. c. Verify the link http://www.fouriersystems.com/works. 	

5 - Toolbar Icons

Test #	Icon	Test and Expected Result	Result
5.1	Open 	Refer to test 2.1.	
5.2	Print 	Refer to test 2.3.	
5.3	User Administration 	Refer to tests 3.1 to 3.3.	
5.4	Group Administration 	Refer to test 3.4.	
5.5	Refresh 	<ul style="list-style-type: none"> a. Wait several minutes (for users to perform actions) and click Refresh. b. Verify that the Audit Trail data has been refreshed (you will see new actions added to the table). 	
5.6	Calendar 	<p>Use the drop-down menu to open the calendar and select a date. Verify that the data from this date is displayed on your screen.</p> <p>Note: Only those dates with recorded data will be displayed.</p>	

Chapter 5: DataNet Validation Tests

1 - Login

Test #	Test Description	Expected Result	Result
1.1	<p>a. Launch the DataNet software from the desktop shortcut. The <i>User Login</i> dialog box opens.</p> <p>b. In the <i>User ID</i> field, enter the User ID created in test 1.3 of the DatPass Validation Test.</p> <p>c. In the <i>User Password</i> field, enter an <i>incorrect</i> password.</p>	Verify that the DataNet software does not open and an <i>Incorrect Password</i> message window opens.	
1.2	<p>a. In the <i>User Login</i> dialog box, in the <i>User ID</i> field, enter an <i>incorrect</i> User ID.</p> <p>b. In the <i>User Password</i> field, enter the User Password created in test 1.3 of the DatPass Validation Test.</p>	Verify that the DataNet software does not open and an <i>Incorrect User ID</i> message window opens.	
1.3	In the <i>User Login</i> dialog box, enter an incorrect User ID and User Password.	Verify that the DataNet software does not open and an <i>Incorrect User ID</i> message window opens.	
1.4	In the <i>User Login</i> dialog box, login using the User ID and User Password created in test 1.3 of the DatPass Validation Test.	Verify that the DataNet software is launched.	

2 - File Menu

Test #	Test Description	Expected Result	Result
2.1	On the File menu, click Open .	Verify that the <i>Open Data Files</i> window is opened.	
2.1.1	In the <i>Open Data Files</i> dialog box, select a logger according to its Comment and select the date of the data set using the <i>From:</i> and <i>To:</i> fields.	Verify that the selected data set from the specific logger opens, and that the appropriate data is displayed in the graph and table in the History View window.	
2.2	From the <i>History View</i> window, with at least one data set open, go to File menu and click Save Project . Enter the project name in the Save As dialog	Verify that the project has been saved in the selected location.	

Test #	Test Description	Expected Result	Result
2.2.1	On the File menu, click Open Project Files and browse to the location of a previously created DataNet project file. Click Open .	Verify that the DataNet project is opened in the History View window, with the relevant data from all loggers in the selected project.	
2.3	On the File menu, click Exit .	Verify that the DataNet software is closed.	

3 - Network Menu

Test #	Test Description	Expected Result	Result
3.1	Connect the Receiver to the computer USB port and switch the Receiver on. Click Detect Receiver .	Verify that the Receiver is detected and that the connected Receiver icon appears on the Map View.	
3.2	Click Lock Network . Take a DataNet data logger DNL910 or DNL920 and select the Leave Network option on the logger menu. Rescan for new networks.	Verify that the Receiver network is not found during the scan network procedure.	
3.2	Click Form New Network .	Verify that the Receiver forms a new network and that the network ID has changed in the Receiver tool tip in Map View and on the Receiver LCD menu.	
3.3	Click Refresh Network Connections .	Look at the Receiver icon tool tip and verify that the Refresh Network Connections command is in queue and is processed by the Receiver.	
3.4	Click Show Network Paths .	Verify that the network paths between all online devices in the network are displayed as a green, yellow or red path.	
3.5	Click Device Filter .	Verify that the <i>Mini DataNet Device Filter</i> dialog box opens	
3.5.1	Enter a 6 digit number into the Device Filter window and click Add.	Verify that the number has been entered into the main list.	
3.5.2	Select one of the entered numbers and click Remove .	Verify that the selected number has been removed.	

4 - Tools Menu

Test #	Test Description	Expected Result	Result
4.1	Select Define Sensor .	Verify that the <i>Defined Sensors</i> dialog is opened.	
4.1.1	In the Sensor Properties fields, enter a <i>Sensor name</i> and <i>Sensor unit</i> , and select the relevant option from the <i>Base sensor</i> and <i>decimal digits</i> menus. Enter the relevant values in the Define Values fields. Click Add .	Verify that all properties have been entered correctly in the <i>Defined Sensor</i> dialog.	
4.1.2	Go to the Setup window of an online data logger and in the <i>Sensor type</i> drop-down menu, select the Sensor name as defined in 4.1.1.	Verify that the Sensor name appears in the drop-down menu.	
4.1.3	Send the setup to the logger, including the defined sensor name on one of the logger inputs.	Verify that the Sensor name appears in the Logger icon tool tip when sampling data, with the correct values.	
4.2	Go to the <i>Sensor View</i> with online loggers sampling data. On the Tools menu, select Switch Sensor View Mode .	Verify that the Sensor boxes switch between large and small sizes.	
4.3	Click Lock Map View ensuring there is a check mark next to this menu item.	Verify that the icons on the Map View cannot be moved and are locked in position.	
4.3.1	Unselect the check mark next to the Lock Map View menu item.	Verify that the icons on the Map View can be moved freely around the Map View window.	
4.4	Select Options .	Verify that the <i>Options</i> dialog opens.	
4.5	Preferences Tab		
4.5.1	Select the check box next to the <i>Minimized to System tray</i> option. Minimize the DataNet application.	Verify that the application has been minimized and the DataNet icon appears in the Windows system tray.	
4.5.1.1	Double click the DataNet icon in the system tray.	Verify that the DataNet application is opened.	
4.5.2	Select the check box next to the <i>Run DataNet on Windows startup</i> option.	Verify that after resetting the computer, DataNet is automatically launched.	
4.5.3	Toggle the Map View background options between Stretch and Center.	Verify that the Map View background image is centered or stretched, depending on the option selected. Depending on the background image there might not be any noticeable difference.	

Test #	Test Description	Expected Result	Result
4.5.4	In the <i>Set decimal places for</i> option, select a sensor input and change the number of decimal places from the default selection.	Verify that for the selected input, the value is now displayed in a resolution according to the number of decimal places selected.	
4.5.5	Change the <i>Date Format</i> to one of the options available in the drop-down menu.	When viewing online or offline data, verify that the date appears according to the date format selected.	
4.5.6	Change the path where the DataNet data files are saved by clicking Browse next to the <i>Path for DataNet data files</i> option. Click OK .	Once the path has been changed, wait for data to be downloaded from at least one logger on the network. Go to the new path and verify that the folder <i>DataNet data files</i> has been created there.	
4.5.7	Select the <i>Save text data files</i> option.	Verify that the folder <i>DataNet data text files</i> is populated with text files the next time online data is downloaded and saved to this directory.	
4.5.7.1	Change the path where the DataNet text data files are saved by clicking Browse next to the <i>Save text data files</i> option. Click OK .	Once the path has been changed, wait for data to be downloaded from at least one logger on the network. Go to the new path and verify that the folder <i>DataNet data text files</i> has been created there.	
4.5.8	Select the <i>Enable automatic data download when DataNet is launched</i> option.	Verify that when you next launch the DataNet application data is automatically downloaded from all of the online loggers on the network.	
4.6	e-mail Settings Tab		
4.6.1	Select the <i>Send e-mail notifications</i> check box.	Verify that the <i>Server Information</i> and <i>Login Information</i> fields are enabled (not grayed out).	
4.6.2	In the Server Information section, enter the relevant account settings specific to your e-mail account.	Verify that all the settings are entered correctly.	
4.6.3	Ensure the <i>Use authentication login</i> check box is selected and enter the username and password. If your e-mail account does not require login information this step may be skipped.	Verify that these settings are entered correctly.	
4.6.4	Select the Server requires SSL check box (if relevant to your e-mail account).	Verify that the Port number has changed to 465.	

Test #	Test Description	Expected Result	Result
4.6.5	Create an alarm condition on one of the data loggers in the network and select a contact to receive an alarm e-mail notification in the event that the alarm threshold was breached.	Verify that an e-mail notifications was sent to the selected contact/s.	
4.7	e-mail Settings Tab		
4.7.1	Select the <i>Send SMS notifications</i> check box.	Verify that the <i>GSM Connection Settings</i> and <i>Unlock SIM Card</i> fields are enabled (not grayed out).	
4.7.2	In the <i>GSM Connection Settings</i> section, enter the relevant settings specific to the GSM modem you are using.	Verify that all the settings are entered correctly.	
4.7.3	If a PIN code is needed, select the Use PIN code check box and enter the code.	Verify that the Use PIN Code field is enabled.	
4.7.4	Click OK to close the dialog and ensure that the GSM modem is properly connected to the computer and is powered.	Verify that the GSM modem icon in the DataNet upper tool bar is green, indicating modem connection.	
4.7.5	Create an alarm condition on one of the data loggers in the network and select a contact to receive an alarm SMS notification in the event that the alarm threshold was breached.	Verify that an SMS notification was sent to the selected contact/s.	
4.8	e-Mail Alarm Notifications		
4.8.1	Select e-Mail Alarm Notifications .	Verify that the <i>e-Mail Alarm Notifications</i> dialog is launched.	
4.8.2	Select the <i>Contacts</i> tab and click Add Contact .	Verify that the <i>Contact Details</i> dialog is opened.	
4.8.2.1	Select the Vacation check box.	Verify the From and To fields are enabled.	
4.8.2.2	Enter the relevant details in the Contact Details dialog (Name is mandatory). Click OK .	Verify that the contact was created and is listed in the <i>Contacts</i> tab.	
4.8.2.3	Select the Contact created in 4.8.2.2 and click Edit Contact .	Verify that the Contact Details dialog is opened with the same details entered in 4.8.2.2.	
4.8.2.4	Change one of the details in the selected contact. Click OK . Click Edit Contact on this contact.	Verify that the detail has in fact been changed.	

Test #	Test Description	Expected Result	Result
4.8.2.5	Select the contact created in 4.8.2.2 and click Remove Contact .	Verify that the contact has been removed from the list.	
4.8.3	Select the <i>Groups</i> tab and click Add Group .	Verify that the <i>Group Details</i> dialog is opened.	
4.8.3.1	Enter a name in the <i>Group Name</i> field and click OK .	Verify that the group was created and is listed in the <i>Groups</i> tab.	
4.8.3.2	Ensure at least one contact has been created, and click Edit Group . In the Contact section select at least one contact to add to the group. Click OK .	Verify that the contact name has been added to the group by seeing it appear under the Contacts header in the <i>Groups</i> tab, next to the relevant group.	
4.8.3.3	Select the group created in 4.8.3.1 and click Remove Group .	Verify that the group has been removed from the list.	
4.8.4	Select the <i>Notifications Setup</i> tab. Select one logger which is running on the network.	Verify that for the selected logger, the Battery and Reception alarm check boxes are enabled, as well any check boxes for any other input for which an alarm level has been configured in the Setup process.	
4.8.4.1	Select the Battery Alarm check box. Click Contacts and select the contact who should receive e-mail notification of a low battery alarm. Click Close .	Verify that when the battery level goes below 10% on the logger tool tip in Map View, an e-mail notification is received by the selected contact.	
4.8.4.2	Select the Reception Alarm check box. Click Contacts and select the contact who should receive e-mail notification of a low reception alarm. Click Close .	Verify that when the logger goes offline an e-mail notification is received by the selected contact. Verify that when the logger goes back online an e-mail notification is also received by the selected contact.	
4.8.4.3	For at least one of the logger inputs for which an alarm level has been defined, select the check box for <i>Low, Pre-Low, Pre-High</i> or <i>High</i> alarms. Also select the <i>Normalized</i> check box. Click Contacts and select the contact who should receive alarm e-mail notification. Click Close .	Verify that when the logger breaches the defined alarm threshold, an e-mail notification is received by the selected contact. Verify that when the logger value is normalized (not in alarm state), an e-mail notification is also received by the selected contact.	
4.9	SMS Alarm Notifications		
4.9.1	Select SMS Alarm Notifications .	Verify that the <i>SMSAlarm Notifications</i> dialog is launched.	
4.9.2	Select the <i>Contacts</i> tab and click Add Contact .	Verify that the <i>Contact Details</i> dialog is opened.	

Test #	Test Description	Expected Result	Result
4.9.2.1	Select the Vacation check box.	Verify the From and To fields are enabled.	
4.9.2.2	Enter the relevant details in the Contact Details dialog (Name is mandatory). Click OK .	Verify that the contact was created and is listed in the <i>Contacts</i> tab.	
4.9.2.3	Select the Contact created in 4.8.2.2 and click Edit Contact .	Verify that the Contact Details dialog is opened with the same details entered in 4.8.2.2.	
4.9.2.4	Change one of the details in the selected contact. Click OK . Click Edit Contact on this contact.	Verify that the detail has in fact been changed.	
4.9.2.5	Select the contact created in 4.8.2.2 and click Remove Contact .	Verify that the contact has been removed from the list.	
4.9.3	Select the <i>Groups</i> tab and click Add Group .	Verify that the <i>Group Details</i> dialog is opened.	
4.9.3.1	Enter a name in the <i>Group Name</i> field and click OK .	Verify that the group was created and is listed in the <i>Groups</i> tab.	
4.9.3.2	Ensure at least one contact has been created, and click Edit Group . In the Contact section select at least one contact to add to the group. Click OK .	Verify that the contact name has been added to the group by seeing it appear under the <i>Contacts</i> header in the <i>Groups</i> tab, next to the relevant group.	
4.9.3.3	Select the group created in 4.8.3.1 and click Remove Group .	Verify that the group has been removed from the list.	
4.9.4	Select the <i>Notifications Setup</i> tab. Select one logger which is running on the network.	Verify that for the selected logger, the Battery and Reception alarm check boxes are enabled, as well any check boxes for any other input for which an alarm level has been configured in the Setup process.	
4.9.4.1	Select the Battery Alarm check box. Click Contacts and select the contact who should receive SMS notification of a low battery alarm. Click Close .	Verify that when the battery level goes below 10% on the logger tool tip in Map View, an SMS notification is received by the selected contact.	
4.9.4.2	Select the Reception Alarm check box. Click Contacts and select the contact who should receive SMS notification of a low reception alarm. Click Close .	Verify that when the logger goes offline an SMS notification is received by the selected contact. Verify that when the logger goes back online an SMS notification is also received by the selected contact.	

Test #	Test Description	Expected Result	Result
4.9.4.3	<p>For at least one of the logger inputs for which an alarm level has been defined, select the check box for <i>Low, Pre-Low, Pre-High</i> or <i>High</i> alarms. Also select the <i>Normalized</i> check box.</p> <p>Click Contacts and select the contact who should receive alarm SMS notification. Click Close.</p>	<p>Verify that when the logger breaches the defined alarm threshold, an SMS notification is received by the selected contact. Verify that when the logger value is normalized (not in alarm state), an SMS notification is also received by the selected contact.</p>	
4.10	Firmware Update Center		
4.10.1	<p>Ensure a copy of the DataNet firmware is located in the DataNet root directory.</p> <p>Select Firmware Update Center. Enter the system password (default is 1234).</p>	<p>Verify that the <i>Firmware Update Center</i> dialog is launched.</p>	
4.10.2	<p>In the <i>Available Firmware Versions</i> section, check the firmware version displayed.</p>	<p>Verify the firmware version matches the version placed in the DataNet root directory.</p>	
4.10.3	<p>Perform a firmware update on all online units on the network.</p> <p>Select the <i>Update</i> check box next to each of the units listed in the dialog.</p>	<p>Verify that the firmware update process is performed on each of the units (never more than two in parallel).</p>	
4.10.4	<p>If the firmware version was higher than the previous firmware installed on the units, check the Firmware Version listed for each unit.</p>	<p>Verify that the firmware version matches the version listed in the <i>Available Firmware Versions</i> section and that the unit Status is <i>No Update Required</i>.</p>	

5 – Analysis Menu









Test #	Test Description	Expected Result	Result
5.1	<p>Open a data set in History View.</p> <p>Select a plot on the graph and select Histogram.</p>	<p>Verify that the <i>Histogram Settings</i> dialog opens.</p>	
5.2	<p>Enter the relevant settings and click OK.</p>	<p>Verify that the Histogram was created according to the defined settings.</p>	
5.3	<p>Open a data set in History View and select Export to Excel.</p>	<p>Verify that the selected data set is opened in an Excel file.</p>	







Test #	Test Description	Expected Result	Result
5.4	Open a data set in History View and select Export to CSV . In the Save As dialog enter the file name and click Save in the desired location.	Verify that the selected data set is opened in a CSV file and was saved in the correct location.	

6 – Help Menu

Test #	Test Description	Expected Result	Result
6.1	Select Check for Updates .	Verify the <i>Check for Updates</i> dialog is opened.	
6.1.1	Click the Check for Updates icon.	Verify that the update application has established connection with the Fourtec server and confirms is new software or firmware is available.	
6.2	Click User Guide .	Verify that the user guide PDF file is launched.	
6.3	Click About .	<ul style="list-style-type: none"> a. Verify that the <i>About DataNet</i> dialog opens. b. Verify that the DataNet version is 1.2.0.0. c. Verify the link www.fouriersystems.com/works. 	





7 – Upper Toolbar Icons








Test #	Icon	Test Description and Expected Result	Result
7.1	Open File 	Click this icon and verify the <i>Open Data Files</i> dialog opens.	
7.2	Map View 	Click this icon and verify the Map View is displayed in the main window.	
7.3	Sensor View 	Click this icon and verify the Sensor View is displayed in the main window.	
7.4	History View 	Click this icon and verify the History View is displayed in the main window.	
7.5	Alarm Mute/Unmute  	<p>Click the Mute icon  and verify when an alarm is activated the software alarm is muted (through the computer speakers).</p> <p>Click the Unmute  icon and verify when an alarm is activated the software alarm is muted (through the computer speakers).</p>	



Test #	Icon	Test Description and Expected Result	Result
7.6	e-mail Alarm Notifications 	Click the icon and verify the <i>e-mail Alarm Notifications</i> dialog opens.	
7.7	SMS Alarm Notifications 	Click the icon and verify the <i>SMS Alarm Notifications</i> dialog opens.	
7.8	GSM modem indicators  	Connect the GSM modem according to section 4.9 and verify the icon is green when the modem is connected. Verify the icon is grey when the modem is disconnected.	
7.9	Temperature - Celsius 	Toggle the Celsius icon and ensure all online temperature readings are displayed in C.	
7.10	Temperature - Fahrenheit 	Toggle the Fahrenheit icon and ensure all online temperature readings are displayed in F.	

8 - Graph Toolbar

This section tests the Graph toolbar which is available in Graph tab in History View and Online Graph view. Icons specific to each view are noted.

Test #	Icon	Test Description	Expected Result	Result
8.1	Data Map  (in History View only)	Toggle the Data Map icon.	Verify the Data Map is removed/added from the main window left pane.	
8.2	Plot Legend 	Toggle the Plot Legend icon.	Verify the plot legend is removed/added from the Online Graph view.	
8.3	Auto scale 	a. Zoom in on an area of the graph. b. Click the Auto scale icon	Verify that the graph is restored and displayed in full.	
8.4	Zoom in 	a. Click the Zoom In icon. b. Click down and hold the left mouse button and drag the <i>Zoom In</i> cursor over the area of the graph to be zoomed. c. Release the left mouse button to set the zoom area.	Verify that the selected area of the graph is zoomed in.	

8.5	Pan graph 	a. Click the Pan icon. b. Place the <i>Pan</i> cursor over the graph, hold down the left mouse button and proceed to pan the graph up, down, left and right.	Verify that the graph pans up, down, left and right.	
8.6	First cursor 	a. Click the First Cursor icon. b. Drag the graph cursor to any coordinate on the graph.	a. Verify the graph cursor is displayed. b. Verify that the chosen coordinate is displayed in the data pane underneath the graph.	
8.7	Second cursor 	a. Click the Second Cursor icon. b. Drag the graph cursor to any coordinate on the graph.	a. Verify the second graph cursor is displayed. b. Verify that the chosen coordinate is displayed in the data pane underneath the graph.	
8.8	Grid 	Toggle the Grid icon.	Verify the grid lines are added/removed from the graph.	
8.9	Add Custom View  (in History View only)	Click the Add Custom View icon.	Verify the customized graph view is added to the Data Map.	
8.10	Copy Graph 	Click the Copy Graph icon.	Open a word processing application such as Microsoft Office Word, and verify that the copied graph can be pasted into the document.	
8.11	Graph Properties 	Click the Graph Properties icon.	Verify the <i>Graph Properties</i> dialog is opened.	
8.11.1		In the <i>Axis Scaling</i> tab, unselect the Autoscale check box and enter the minimum and maximum time and date for the specific date set. Click OK .	Verify that the scale of the displayed graph is according to the time scale defined.	
8.11.2		In the <i>Axis Scaling</i> tab, select the Group Plots by Unit check box and select a specific axis. Click OK .	Verify that the graph axis is defined according to the selected axis.	

8.11.3		In the <i>Style</i> tab, unselect the <i>Use default line properties</i> check box. Select a specific axis, color and line width. Click OK .	Verify that the line on the graph is displayed according to the defined settings.	
8.12	Export to Excel 	Click the Export to Excel icon.	Verify that the selected data set is opened in an Excel file.	
8.13	Print 	Click the Print icon. In the Print dialog select the relevant printer and click OK .	Verify the <i>Print</i> dialog is opened and that the graph is printed.	

9 – Table View

This section tests the Table view which is available in the Table tab in History View and Online Graph view.

Test #	Test Description	Expected Result	Result
9.1	In History View, click the <i>Table</i> tab. Click the <i>Print</i> icon.	Verify the <i>Print Table</i> dialog is opened.	
9.1.1	In the <i>Print Table</i> dialog, select the relevant data set to be printed using the <i>From</i> and <i>To</i> drop-down menus. Click OK .	Verify the <i>Print</i> dialog is opened.	
9.1.2	In the Print dialog select the relevant printer and click OK .	Verify that the table is printed according to the defined data set.	
9.2	In Online Graph view, click the <i>Table</i> tab. Click the <i>Print</i> icon.	Verify the <i>Print Table</i> dialog is opened.	
9.2.1	In the <i>Print Table</i> dialog, select the relevant data set to be printed using the <i>From</i> and <i>To</i> drop-down menus. Click OK .	Verify the <i>Print</i> dialog is opened.	
9.2.2	In the Print dialog select the relevant printer and click OK .	Verify that the table is printed according to the defined data set.	
9.3	Display the online data from a running logger and select the <i>Table</i> tab.	Verify the logger data is updated in the Table view in real-time, according to the logger transmission time.	

10 – Statistics View

This section tests the Statistics view which is available in the Statistics tab in History View and Online Graph view.

Test #	Test Description	Expected Result	Result
10.1	In History View, click the <i>Statistics</i> tab. Click the <i>Print</i> icon.	Verify the <i>Print</i> dialog is opened.	

10.1.1	In the <i>Print</i> dialog select the relevant printer and click OK .	Verify that the statistics are printed according to the statistics displayed in the <i>Statistics</i> tab.	
10.2	In Online Graph view, click the <i>Statistics</i> tab. Click the <i>Print</i> icon.	Verify the <i>Print</i> dialog is opened.	
10.2.1	In the <i>Print</i> dialog select the relevant printer and click OK .	Verify that the statistics are printed according to the statistics displayed in the <i>Statistics</i> tab.	
10.3	Display the online data from a running logger and select the <i>Statistics</i> tab.	<ul style="list-style-type: none"> a. Verify the Statistics start and end times correspond to the first and last sample time in the <i>Table</i> tab. b. Verify the number of samples corresponds to the number of samples listed in the <i>Table</i> tab. 	


11 – Map View

This section tests all functionality available in Map View, including the Map View icons functionality.

Test #	Test Description	Expected Result	Result
11.1	Map View Background		
11.1.1	Double-click the Map View background to launch the <i>Open</i> dialog. Browse to a new background image. Select this image and click Open .	Verify the image is displayed as the new Map View background.	
11.1.2	Right-click the Map View background and select Load Wallpaper. The <i>Open</i> dialog is launched. Browse to a new background image. Select this image and click Open .	Verify the image is displayed as the new Map View background.	
11.1.3	Right-click the Map View background and select Reset Wallpaper .	Verify the default DataNet background image is displayed.	
11.2	Receiver Icon		
11.2.1	Connect the Receiver to the computer and switch the Receiver on.	Verify that the Receiver icon in the Map View is displayed in Connected (green) status.	
11.2.2	Ensure a copy of the DataNet firmware is located in the DataNet root directory. Right-click the Receiver icon and select Update Firmware . Enter the password and confirm firmware update.	<ul style="list-style-type: none"> a. Verify that the firmware update process is performed on the Receiver. b. Following the firmware update, confirm the firmware version in the Receiver tooltip matches the firmware file that was updated. 	

11.2.3	Right-click the Receiver icon and select Lock Network . Take a DataNet data logger DNL910 or DNL920 and select the Leave Network option on the logger menu. Rescan for new networks.	Verify that the Receiver network is not found during the scan network procedure.	
11.2.4	Right-click the Receiver icon and select Form New Network .	Verify that the Receiver forms a new network and that the network ID has changed in the Receiver tool tip in Map View and on the Receiver LCD menu.	
11.2.5	Right-click the Receiver icon and select Refresh Network Connections .	Look at the Receiver icon tool tip and verify that the Refresh Network Connections command is in queue and is processed by the Receiver.	
11.2.6	Right-click the Receiver icon and select Show Network Paths .	Verify that the network paths between all online devices in the network are displayed as a green, yellow or red path.	
11.2.7	Place the mouse cursor over the Receiver icon to display the tooltip.	Verify the tooltip contains the following information: a. Receiver Part Number: DNR900 b. Receiver Serial Number - matching the Serial Number on the rear of the unit casing c. Network ID – matching the network ID on the Receiver LCD menu d. Version – matching the firmware version displayed on the Receiver LCD menu	
11.3	Repeater Icon		
11.3.1	Connect a Repeater to the DataNet network.	Verify the online Repeater icon is displayed in the Map View.	
11.3.2	Right-click the Repeater icon and select <i>Setup</i> .	Verify the Setup dialog is opened.	
11.3.2.1	Change the Repeater name and click Setup and Run .	Verify the Repeater name has been changed by looking at the Repeater tool-tip.	
11.3.3	Right-click the Repeater icon and select Call Unit (Beep) .	Verify the Repeater unit emits a beep for several seconds.	
11.3.4	Right-click the Repeater icon and select Leave Network . Enter the default password.	Verify the Repeater leaves the network and the icon disappears from the Map View.	

11.3.5	Ensure a copy of the DataNet firmware is located in the DataNet root directory. Right-click the Repeater icon and select Update Firmware . Enter the password and confirm firmware update.	<ul style="list-style-type: none"> a. Verify that the firmware update process is performed on the Repeater. b. Following the firmware update, confirm the firmware version in the Repeater tooltip matches the firmware file that was updated. 	
11.3.6	Right-click the Repeater icon and select Show Network Path .	Verify the network path between the Repeater and the parent node is displayed.	
11.3.7	Place the mouse cursor over the online Repeater icon to display the tooltip.	<p>Verify the tooltip contains the following information:</p> <ul style="list-style-type: none"> a. Repeater Serial Number - matching the Serial Number on the rear of the unit casing b. Repeater name c. Battery Level/Charging status d. Reception Quality e. Version – matching the firmware version displayed on the Receiver LCD menu 	
11.4	Logger Icon		
11.4.1	Connect a logger to the network.	Verify the online logger icon is displayed in the Map View.	
11.4.2	Right-click the logger icon and select Setup . Select the <i>Device Setup</i> tab.	<ul style="list-style-type: none"> a. Verify the <i>Setup</i> dialog is opened. b. Verify the Serial Number and Firmware version are correct in the Device Setup tab. 	
11.4.2.1	<ul style="list-style-type: none"> a. In the <i>Comment</i> field, enter the name of the logger. b. Select the relevant <i>Sampling Rate</i>. c. Select the relevant <i>Transmission interval</i>. d. Select 0 average points. e. Select the relevant Temperature unit. f. Select the relevant inputs to be measured. If selecting In-1, 2, 3 or 4, change the custom sensor name for the selected Sensor type. <p>Click Setup and Run.</p>	<p>Once the logger has been configured:</p> <ul style="list-style-type: none"> a. Verify the Comment has been updated in the logger tooltip. b. Verify the logger is sampling at the defined sampling rate. c. Verify the logger is transmitting at the defined Transmission interval. d. If a temperature sensor was defined, verify the value is displayed in the correct unit in the logger tooltip. e. Verify the custom sensor name is displayed in the logger tooltip and in the Sensor View. 	
11.4.3	Following 10.4.2.1, right-click the logger icon and select Setup . Select the <i>Alarm Setup</i> tab.	<ul style="list-style-type: none"> a. Verify the <i>Setup</i> dialog is opened. b. Verify the same inputs configured in 10.4.2.1 are enabled in the <i>Alarm Setup</i> tab. 	

11.4.3.1	<ul style="list-style-type: none"> a. Select the relevant Alarm delay b. Select the relevant Alarm duration c. For at least one of the enabled sensor inputs, select at least one of the Low, Pre-Low, Pre-High and High alarm check boxes. Enter the relevant value in the alarm field. d. Click Setup and Run. 	<p>Create the alarm conditions as defined in this test and verify the following:</p> <ul style="list-style-type: none"> a. Logger alarm is activated after the defined alarm delay. b. Logger icon displays red alarm status c. Logger emits audible alarm for the defined duration d. DataNet software alarm is audible (ensure the Alarm icon is unmated in the upper toolbar) 	
11.4.4	Place the mouse cursor over the online logger icon when the logger is running, to display the tooltip.	<p>Verify the tooltip contains the following information:</p> <ul style="list-style-type: none"> a. Logger Part Number b. Logger Serial Number - matching the Serial Number on the rear of the unit casing c. Logger Comment d. Battery Level/Charging status e. Reception Quality f. Version – matching the firmware version displayed on the Logger LCD menu g. Last Sample Time – for each of the configured inputs 	
11.4.5	With the logger running, right-click the logger icon and select Display Data .	Verify the online Graph View is opened and that the logger data is updated in real-time.	
11.4.6	Right-click the logger icon and select Download Data .	<p>Verify the data is downloaded from the logger memory to the online Graph View. When the logger is downloading the data, the Logger icon in Map View will display a green progress circle as follows:</p> 	
11.4.7	Right-click the logger icon and select Cancel Download during the download process.	Verify the data download is halted.	
11.4.8	Right-click the logger icon and select Reset Alarm while the logger is in alarm status.	Verify the logger icon changes from alarm status to normal status. If the logger is still in alarm status then the icon will immediately revert back to alarm status.	
11.4.9	Right-click the logger icon and select Call Unit (Beep) (for DNL910 and DNL920 only)	Verify the logger unit emits a beep for several seconds.	

11.4.10	Ensure a copy of the DataNet firmware is located in the DataNet root directory. Right-click the logger icon and select Update Firmware . Enter the password and confirm firmware update.	a. Verify that the firmware update process is performed on the logger. b. Following the firmware update, confirm the firmware version in the logger tooltip matches the firmware file that was updated.	
11.4.11	Right-click the logger icon and select Stop .	Verify the logger has stopped running.	
11.4.12	With the logger in Stop mode, right-click the logger icon and select Calibration > Calibrate . Enter the system password.	Verify the logger <i>Calibration</i> dialog is opened.	
11.4.13	Select the relevant sensor from the <i>Sensor</i> drop-down menu. Select the inputs to be calibrated (All inputs or a specific input) and click Setup .	Verify the <i>Calibration</i> and <i>Logger Data</i> panes are enabled.	
11.4.14	Calibrate the input selected in 10.13.1. Click Send Calibration at the end of the process.	Verify the <i>Logger Data</i> pane displays the correctly calibrated values.	
11.4.15	Repeat 10.13.1 and 10.13.2 for each of the inputs to be calibrated.	For each input, verify the <i>Logger Data</i> pane displays the correctly calibrated values.	
11.4.16	With the logger in Stop mode, right-click the logger icon and select Calibration > Save Calibration . Enter the system password. In the <i>Save As</i> dialog, enter the file name and click Save in the desired location.	Verify the calibration file was saved in the correct location.	
11.4.17	With the logger in Stop mode, right-click the logger icon and select Calibration > Load Calibration . Enter the system password. In the <i>Open</i> dialog browse to the location of the calibration file to be loaded, and click Open .	Verify the software loads the calibration file into the logger memory by looking at the logger tooltip <i>Command Queue Process</i> .	
11.4.18	With the logger in Stop mode, right-click the logger icon and select Calibration > Restore Factory Calibration Defaults . Enter the system password.	Verify the default calibration values were restored to the logger memory.	
11.4.19	Right-click the logger icon and select Leave Network .	Verify the logger leaves the network and the icon disappears from the <i>Map View</i> .	

11.4.20	With the logger in Stop mode, right-click the logger icon and select Run .	Verify the logger icon changes to Run status and the logger tooltip and online graph displays real-time values.	
11.4.21	Right-click the logger icon and select Show Network Path .	Verify the network path between the logger and the parent node is displayed.	
11.4.22	Right-click the logger icon and select Enable Short range Repeater Mode (only for DNL910 and DNL920). Enter the system password.	Verify the logger tooltip displays <i>SR Repeater Mode</i> after the logger part number.	
11.4.22.1	Right-click the logger icon and select Disable Short range Repeater Mode (only for DNL910 and DNL920). Enter the system password.	Verify the logger tooltip no longer displays <i>SR Repeater Mode</i> after the logger part number.	

12 – Change Password dialog

Test #	Test Description	Expected Result	Result
12.1	Open the <i>Password</i> dialog e.g. go to Tools > Firmware Update Center .	Verify the <i>Password</i> dialog is opened.	
12.2	Click Change Password .	Verify the <i>Change Password</i> dialog is opened.	
12.3	Enter the old password and then enter the new password in the <i>New</i> and <i>Confirm</i> password fields. Click OK .	Verify that the new password is accepted and that the dialog originally selected in 11.1 is opened.	