Starrett®

DataSure™

Wireless Manager

Operator's Manual

Contents

Section 1 Overview

1.1 Introduction

The Starrett *DataSure*™ wireless network is designed to allow the transfer of data from electronic measuring tools to computers where measurements can either be easily logged or conveyed to an SPC software package. The wireless network environment allows tool operators to move freely without the constraints of data cables. The *DataSure*™ wireless manager software provides a convenient user interface for network configuration, management, and inspection.

Since many SPC packages are intended for use with wired data collection systems that utilize multiplexers to connect a variety of tools together through an RS232 communications port, the *DataSure*™ software utility also fully emulates this approach. The *DataSure*™ utility software enables operators to configure their wireless network, and manage the flow of tool data to their target applications. Measurements can be initiated either by the operator of the tool or solicited via computer software.

The following statement applies to each of the *DataSure*™ wireless devices (EndNode, Router, Gateway):

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by the L.S. Starrett Company could void the user's authority to operate the equipment.

1.2 Features

- 916 MHz RF technology
- Freedom of movement and from data cables
- Up to 32 tools per virtual multiplexer
- Up to 5 virtual multiplexers
- A variety of exportable log file formats
- USB or RS 232 Gateway - PC interface
- Operating distance up to 25 meters (80 feet) for EndNodes
- Broadcast range up to 30 meters (97 feet) for Gateway and Routers
- System status feedback on the EndNode, including acknowledge of data received
- Adapts to electronic tools from various manufacturers
- No line-of-sight limitation
- Temporary data retention at the EndNode while outside the network
- Routers enlarge network range and improve robustness against radio interference
- Optional wall mount for Routers
- Routers equipped with a rechargeable battery backup

- EndNodes offer a choice of battery selection (CR2450 or CR2477)
- Gateway and Router antenna can be angled and swiveled to improve reception

1.3 Care & Maintenance

- Cleaning and handling instructions

External plastic surfaces of EndNodes, Routers, and Gateways may be cleaned with Isopropyl Alcohol and a non-abrasive cloth. Care should be taken not to wet internal surfaces or conductive cable ports. Antennae are delicate, and should be handled with caution.

- Plug in cautions
- Environmental bounds of use, humidity, temp, etc.
- Battery replacement

1.4 Hardware Definitions

- Gateway

The Gateway is a radio device which provides a point of entry for the wireless network to interface with software running on PC. Only one Gateway may be used for a group of network elements. There are two status indicators on the Gateway; one is a power indicator, and the other shows radio activity. The red is a power indicator, and the green shows radio activity. The Gateway can be turned on or off via a sliding power switch. Gateways are available with either an RS232 DB-9 connector, or a USB port. Only RS232 enabled Gateways must be powered via an external AC wall adapter (included). The power cable may be looped around the posts located near the power entry jack on the rear of the Gateway. This provides strain-relief to guard against accidental shutoff if the cable should become snagged and pulled away unintentionally.

- Router

Routers are radio devices which provide robustness, range, and scalability to the wireless network. They serve as intermediary steps between the EndNodes and a Gateway. Routers should be installed within range of a Gateway, or else within reaching distance of other Routers. EndNodes can be carried freely throughout a network environment bounded by the overlapping ranges of Routers and the Gateway. Adding more Routers to a network-enabled space further strengthens a network by providing multiple paths for data transmissions to follow. Routers operate automatically; they require no further operation beyond proper placement, antenna orientation, and supplying of power. There are two status indicators on the Router; one is a power indicator, and the other shows radio activity. The Router can be turned on or off via a sliding power switch. Routers are powered via an external AC wall adapter (included), and are also equipped with a rechargeable battery backup. The power cables may be looped around the posts located near the power entry jack on the rear of the Gateway. This provides strain-relief to guard against accidental shutoff if the cable should become snagged and pulled away unintentionally.

- EndNode

  An EndNode is a radio which links a tool to the wireless network. EndNodes connect into the tool's data port in the same way that conventional wired cables do. Use the pushbutton on the EndNode to send tool data. There are two status indicators on the EndNode; one is green and the other is red (refer to Appendix B for instruction of their meanings). When not in use, turn the EndNode off via the sliding power switch to conserve battery life.

1.5 Network Elements and Topologies

Starrett's EndNodes, Routers, and Gateways together form what is termed a wireless mesh network. The mesh network topology is a robust approach to covering large areas with radio connectivity. The robustness offered by the mesh network topology cannot be equaled by any of the other common network topologies. In a mesh network, the reach or range can be extended, redundancy added, and the general reliability of the network enhanced by simply adding more routers. This may be needed to provide a "best route" for the radio signal, thereby increasing throughput and reducing congestion. All routers in a mesh network can communicate with two or more other routers. Thus, a mesh network is very robust in terms of reliability and redundancy. If one radio/network node can no longer operate, all the rest can still communicate with each other, directly or through one or more intermediate nodes. This precludes the practicality of point-to-point or daisy chain network approaches. The latter has single point of failure. If one router in this configuration ceases to function, then there is no capability for the network to recover. Additionally, the data to be sent will never reach its destination. Mesh networks "self-heal" in that if interference enters the environment, such as a strong and localized plume of RF noise, the network has alternate paths for the data to traverse and therefore can reach its intended destination.

Wireless network layouts vary depending on a wide variety of purposes, structural, geographical and environmental conditions. Users may have a variety of needs from their wireless data collection system, such as robustness and assured reliability, while others need many end-nodes supported and added radio coverage in terms of range or reach.

1.5.1 Routing Network - MESH

Mesh networks work best when arranged in a cluster which inherently allow for multiple and redundant links to be established between routers, thereby providing best penetration within common geographical areas. This would normally be the case in an area such as a large milling operation where measurements are taken in work cells spread around the area. Additionally, in QA inspector roles where the inspector roams the shop floor, radio coverage offered by the MESH allows autonomous EndNode sensor or measurement connectivity with the network while within range of the nearest router. The MESH is the most robust of network topologies in that there are many paths for the radio signals to traverse in the event of EMI or mechanical interference.

1.5.2 Routing Network - STRING

Networks consisting of routers in a common line or 'string' dramatically increase radio range, but at the cost of loosing redundancy or alternate link paths between the network routers.

Placement of the network routers to achieve the best reach or range, but redundancy is generally affected.

Routers in this ‘string arrangement’ fall outside the definition of Mesh network topology, but remain compatible with and support the network as a whole (See HYBRID MESH - STRING networks below). STRING routing, while not a MESH, does offer additional network flexibility in layout for remote buildings or measuring stations away from the general area.

Product Note: With the Starrett DataSure™, multiple networks can exist and operate under one roof, but must have separate Group Numbers.

For example, in-line routing may be required in applications that follow a common line or STRING, such as a production aisle where measuring stations flank both sides of the way. Other applications where a common in-line system may be required are building-to-building networks, remote measuring, and portable or ad hoc networks.

1.5.3 Hybrid MESH - STRING Networks

Networks consisting of both MESH and STRING combinations assure added flexibility needed to meet specific user needs. The characteristics of the MESH and STRING layouts remain the same as discussed above.

A Hybrid MESH and STRING network can be laid out to employ the mesh network attributes in a common geographical area, while providing a string of routers to achieve additional reach or range. User environments that might require a combination network would include access to multiple buildings, work cells separated by large obstructions, remote measurement, parking areas separating common operations, QA lab separated by production areas, and large electrical interference fields.

1.5.4 Network Options

Covering large geographical areas is sometimes necessary but can be expensive to deploy the many routers required to cover that space with adequate radio coverage.

Further, additional network traffic generated by the routers and the continual updating of each node increase as the mesh becomes larger. This can result in unsatisfactory network performance. When performance or cost is a concern, multiple work cells across a production/lab area need not deploy a single, large and fixed network. Conflicting requirements in metrology methods or budgets may also preclude a single ubiquitous *DataSure™*.

When autonomous operations or unrelated work cells have no need to have combined wireless network management and/or data collection capabilities, then it may be prudent to install multiple and separate *DataSure™* systems. Since the Starrett *DataSure™* systems may have wired IP network (LAN) connectivity, measurement data can be merged in a common, LAN based database or file server, if needed. In this scenario, the individual networks can be made more efficient than a single large mesh and have the benefit of lower cost.

1.5.5 Determining the Network Layout

With the Starrett *DataSure*™, EndNodes broadcast effectively within a 25-meter (80 feet) radius, more or less. Routers and Gateway network nodes have a broadcast radius of 30 meters (97 feet). With this knowledge, you can simply draw out a schematic floor plan of the area for the *DataSure*™ system to be deployed in and superimpose circles of the scaled radio ranges for each network element.

1.5.5.1 Steps to layout your network:

1. Render a floor plan of the shop area to be covered.
2. Locate work cells or locations where the measurements are to be taken on the floor plan.
3. Determine and locate any large obstruction or electrical noise source that radio coverage will be blocked. Typically, radio coverage can be considered zero.
4. Draw scaled circles around the area in which the Gateway and Routers can or will be placed (30 meters to scale).
5. Draw circles around the location or areas in which the EndNode radios will be used (25 meter to scale).
6. Where EndNode broadcast circles overlap or touch, with a Router or Gateway broadcast circle, radio coverage is good.
7. Where gaps occur between Gateway, Routers, and EndNodes, you will have poor to zero coverage. To resolve this gap problem, move the Routers closer to cover the area or add a Router to fill the coverage gap.
8. In order to have contiguous coverage on your floor plan, you should have at least one path from EndNode to Gateway with zero gaps in the diagram.
9. Take your floor plan out to the actual area and physically place routers and the gateway in the locations indicated on the floor plan schematic.
10. Test the network to see if it works. If not, check for gaps in the actual coverage on the shop floor.

1.5.5.2 Tips for best performance:

1. Make sure the batteries are good in the EndNodes. Battery condition and voltage value is indicated on the *DataSure*™ 's Homepage.
2. Place Routers up high above machinery and their enclosures, but no more than 15 – 20 feet off of the floor or area in which measurements are to be taken.
3. If using a STRING configuration make sure radio coverage of adjacent Routers overlap by several meters to insure good connectivity. Ideally the Routers are placed above interference areas. (See #2 above)
4. Locate *DataSure*™ nodes away from known EMI sources:
5. When EndNodes are within the 25 meters distance to the nearest Router, but appearing to not get received by the Gateway, it may be because the EndNode's radio waves are being shielded by a large metal enclosure or there is EMI in the immediate vicinity of the measurement area. Remedies for this; is to either wait for the EMI to subside or insure that the measurement button is pushed when the tool is in plain sight of the Router or Gateway (which ever is closer).
6. Metal shields and blocks radio waves. Be diligent in locating and using all *DataSure*™ components away from metal expanses if possible. There is no danger, but radio reception/broadcast range will diminish significantly. When Routers or Gateways are

mounted on structural/vertical I beams or metal wall panels, radio waves are shielded or blocked behind the mounting plane of the units. Be aware that if you need coverage of 360 degrees around the router, the metal obstruction will limit the radiation of the radio.

7. EMI will disrupt radio waves and therefore be avoided. Be aware of known EMI sources. Locating *DataSure*™ nodes near these will impair reception/broadcast range. Some known industrial EMI sources are: induction hardeners, de-magnetizers, magnetizers, high power electric motors, arc welders, high voltage power lines, high voltage generators, wiring errors in buildings (incomplete ground to neutral connections), MRI and NMR medical magnetic imaging systems. Additionally, structural steel in a building can be magnetized when it is placed in a strong external dc magnetic field. This usually occurs by sending strong DC currents through the material such as grounding welding equipment to the steel during construction.

1.6 Software Definitions

- should/could be a “tour” of what is shown on Homepage

The *DataSure*™ software is structured as a series of web pages. All operation of its menus is enacted within the confines of a web browser. Common to the tops of all pages is a horizontal menu bar, which can be used to navigate from any point to each of the main subject header menus:

Home:
The Homepage serves as a central location for inspection of tool measurements, EndNode status and battery levels, and also shows association maps linking tools, multiplexers, and applications. This is the first page a user will see when the *DataSure*™ software started. The network service can be started or stopped from the sidebar menu.

Tools:
The Network Devices page displays device summary details. It shows a list of all data sources (tools) attached to the wireless network and provides links to their detail pages. All device statistics can be reset from the sidebar menu.

Multiplexer:
The Multiplexers page displays the multiplexer summary details. It lists each virtual multiplexer identified within the *DataSure*™ manager and provides links to their detail pages. New multiplexers can be created from the sidebar menu.

Logs:
The Logs Summary page contains a tally of log details. It lists all network activity logs by day and provides links to their detail pages. Log files can be archived, restored, or viewed selectively sorted from the sidebar menu.

Applications:

The Applications page displays the applications summary details. It lists all software packages associated with network data collection and provides links to their detail pages. New applications can be identified from the sidebar menu.

Nodes:
The Network Nodes page displays the network nodes summary detail, including the Group Number for the network hardware. It lists all the radio elements that make up the wireless network and provides links to their detail pages.

Administration:
The Basic Administration page displays a summary and status of network administration detail. It lists the basic level system settings. The sidebar menu facilitates: Starting/stopping the wireless network, editing/saving/restoring the basic system settings, clearing the log file, backup/restoration of the system configuration database, and access to the Advanced Administration page.

Help:
Clicking on Help displays an interactive help document. It is a .PDF file, external to the web browser.

(Clock):
Displays the current time according to the local system clock.

The *DataSure*™ system is comprised of a variety of software as well as hardware elements. The table below provides a reference aid for clarifying the discussion of them:

Terminology and Abbreviations

TERM	MEANING
Active	The status of an EndNode that is healthy, communicating over the network, and transmitting measurements.
Administration Page	Displays a summary and status of network management detail. It lists the basic level system settings, and provides a link to advanced system settings.
Alert	A warning or error notice regarding the health and/or performance of a network element.
Application	Software (may be 3rd party) that performs data collection, analysis, reporting and other line of business functions.
Association	A relationship that defines the path of data flow between system elements.
Comm Port	Facilitates RS-232 communication between hardware connected to a PC and/or software package(s) running on a PC. A virtual or internal comm port allows two software packages to interface with each other.
Channel	A numbered association between a tool and a multiplexer. This is also often referred to as a multiplexer port, or slot.
CSV	Comma-separated-value – a file format used by Excel for exporting/importing data from flat files.

TERM	MEANING
Database	A collection of all network settings, associations, devices, names, and descriptions.
Device	A tool which is attached to an EndNode.
Disconnected	The status of an EndNode that is not associated with any multiplexers.
EndNode	A radio transmitter/receiver attached to a tool.
Gateway	A radio transmitter/receiver attached to a PC. Only one Gateway may be in use for a group.
Group Number	A partitioning reference for all wireless network elements. Only EndNodes, Routers, and Gateways of the same group number will communicate with each other.
Health	The health of an object is defined as good, marginal, or bad.
Home Page	Provides a central location for inspection of tool measurements, EndNode status and battery levels, and also shows association maps linking tools, multiplexers, and applications.
Localhost	The PC where the where the majority of DATASURE™ software executes. The Gateway must be attached to this computer.
Log	An audit/storage file for errors, warnings, information, status, data, measurements, and other system events.
Meta-data	Wireless system data, specifically not tool readings.
Multiplexer	An instrument enabling the connection of multiple tools to an application running on a PC. Virtual multiplexers within the DATASURE™ software are intended to emulate the Starrett 761A and 761B.
Network	A self-contained collection of wireless nodes with the DATASURE™ software supporting data collection and analysis application(s).
Node	A base network element such as gateways, Routers, and EndNodes.
Object	A Device, Node, or Application. System logs can be viewed by object.
Offline	An offline object is one that was recently idle/active but is currently not healthy and/or communicating due to out-of-range, dead battery, or some malfunction.
Online	The status of a tool that is a part of the wireless network, but is not yet ready to transmit data.
PC	Abbreviation for personal computer (see Localhost and Remote PC).
Port	See Channel.
Ready	The status of a tool that is ready to transmit data.
Real-time	Data/event management "as it occurs".
Remote PC	A PC networked to the localhost computer running the DATASURE™ software.
Router	A network node that extends the communication range by automatically forwarding signals between EndNodes, other Routers, and the Gateway.
Sampling	The periodic rate at which EndNodes are contacted by the Gateway

TERM	MEANING
Interval	
Setting	System configuration parameters that globally affects network function.
Solicited	An event such as a measurement that occurs due to a request made by the PC and/or the PC user.
UID	Read-only unique identifier of a device set in at time of manufacture.
Unknown	The status of a tool that is of undeterminable standing within the network.
Unsolicited	An event such as a measurement that is triggered by the tool operator at the tool as opposed to the PC and/or the PC user.

1.7 Installation

List what baseline is needed to begin an installation
HW requirements
Windows components requirements e.g.: IIS and .NET framework

Microsoft, Windows, Excel, and .NET Framework is either registered trademarks or trademarks of the Microsoft Corporation in the United States of America and/or other countries. All rights reserved.

1.7.1 Initial Startup

1. Begin with install shield procedure,
 and go to first loading of the homepage

System set up

When the *DataSure*™ utility software is initially launched, the first screen shown is the Homepage. From the sidebar menu, the operator should begin by clicking on ‘Start Wireless Network’. This starts the service program which engages the wireless network hardware. The *DataSure*™ software can be configured whether the Network has been started or not. However, interaction with the wireless network can only commence once it has been started.

1.7.2 Device Identification

To bring a tool in the *DataSure*™ network the operator has only to plug an EndNode into the tool’s data port and power them both on. When the EndNode comes within range of a Router or the Gateway, it will be automatically recognized by the wireless service. By default, the device will initially be named “Tool at n”, where n is the UID number assigned to that EndNode at the time of its manufacture.

From the Homepage, the device’s identity can be verified by clicking on the ‘Locate’ button. This will cause the green LED on the targeted EndNode to blink repeatedly until the ‘Stop’ button has been clicked.

To edit a device, click on the ‘Tools’ link in the site navigation menu bar. Then select a tool name from the Device List. It’s also possible to go directly to a specific Device

Detail page by clicking on the tool's icon on the Homepage.

The tool's name, description, device type, and enabled logging may all be entered or customized by clicking on 'Edit Device' and then making the entries in the fields provided. Changing the device type will determine which icon will appear beside the tool on pages where device details are displayed. Finally, from the sidebar click on 'Save Changes'.

1.7.3 Virtual Multiplexers

A multiplexer is an instrument which enables the connection of multiple tools to an application running on a PC. Virtual multiplexers within the *DataSure*™ software are intended to emulate the Starrett 761A and 761B. The emulated multiplexer systems can accommodate up to 32 tool channels. It is possible to run the network service with a maximum of five multiplexers configured at the same time.

If there are no multiplexers currently configured on the *DataSure*™ Homepage, and a new EndNode and tool is powered up in the presence of the wireless network, then a Primary Multiplexer is automatically generated by the *DataSure*™ software. The Primary Multiplexer will be associated with the next available comm. port of the host PC. As new tools are further added to the network, they will also automatically be added to the next available channel in the Primary Multiplexer (or more precisely, to the multiplexer located at the top of the *DataSure*™ Homepage).

In order to create a new multiplexer, click on the 'Multiplexer' link in the site navigation menu bar. Then from the sidebar click on 'New Multiplexer'. In the Multiplexer Detail page, enter a name and description for the new multiplexer. Check all desired tool connections and assign them port numbers. Note: only tools that have been disconnected from other multiplexers are available to be added; tools may not be associated with more than one multiplexer. Next make all desired application associations. All configured applications are available. Finally, from the sidebar click on 'Save Changes'.

To edit a multiplexer, select one from the list on Multiplexers page. From the sidebar of the Multiplexer Detail page, click on 'Edit Multiplexer'. The name, description, tool connections, port numbers, and associated applications are all valid options to change. Note, de-selecting a connected tool makes it available to be added to a different, or new multiplexer. After all desired changes have been made, from the sidebar click on 'Save Changes'.

1.7.4 External Application Setup

SPC software packages and other data collection applications can be directed to interface with *DataSure*™ multiplexers as if they were Starrett No.761 multiplexers.

In order to configure a new application, click on the 'Applications' link in the site navigation menu bar. Then from the sidebar click on 'New Application'. In the Application Detail page, enter a name and description for the new application. The executable file path may also be specified. Logging for the application can be customized to target specific types of data and/or meta-data. Next, check all desired multiplexer associations. Finally from the sidebar click on ‘Save Changes’.

If the correct file path for an application has been specified, then it will be possible to launch the executable from the *DataSure*™ Homepage. Once loaded, applications must be directed to the comm port of the multiplexer they are associated with and set for **9600 baud, 8 data bits, 1 stop bit, and no parity**. See Appendix A to reference the set of supported commands that may be sent to a *DataSure*™ multiplexer from an application.

1.7.5 Basic Network Administration

The Basic Administration page provides a summary detailing *DataSure*™ software version information, wireless service status, and database space used. From the sidebar menu, the operator may Start (or Stop) the Wireless Network service, Refresh the page, Edit the Basic System Settings, Restore Basic System Setting to their defaults, or manage the *DataSure*™ system Database. Under Related Links, access may be gained to the Advanced Administration page (for more information, refer to section 2.3).

The Log file contains measurement and network performance data. It can be erased by clicking on ‘Clear Log’ (note: All log entries will be lost if they have not yet been archived). The Database file contains all configured system settings, devices, nodes, multiplexers, applications, names, descriptions, associations, etc. The complete configured system can be backed up and restored via the Database Commands from the Basic Administration sidebar menu. To save the current configuration, click on ‘Backup Database’. To view the previously backed up Database files, click on ‘Show Database Backups’. They will appear in a list box below the Basic System Settings. Text descriptions can be entered in the fields provided, and saved by clicking on the sidebar Database Command, ‘Save Backup Descriptions’. A check circle is provided for selecting which Database Backup should be restored. Mark an intended target, and then click on ‘Restore Selected Backup’. This action will overwrite the current system configuration with the settings and objects defined in the restored backup file.

<u>Also describe the Windows security hierarchy for access to Basic and Advanced Administration functions. You could elude to Advanced here and say “refer to section 2.3”</u>

The Basic System Settings are detailed below. Each system setting has a range of valid entries and a pre-defined factory-set default. These settings allow the operator to customize the performance of the wireless network and direct the flow of data through *DataSure*™ utility software. It is also possible to impair or impede network operability through inappropriate changes to some settings. Operators are encouraged to proceed with caution, and test their networks after changes are made.

- Sampling Interval

  0.5sec ≥ Valid Entries ≤ 10.0sec

  Default Setting: 1.1sec

The sampling interval is the periodic rate at which EndNodes are contacted by the wireless network. Quicker intervals will provide a swifter response for solicited readings, but will shorten the useable battery life of the EndNode. The sampling interval has no effect on the response time to send unsolicited readings.

- Enabbled Logging

  {Error, Warning, Information, Verbose, Measurement, Message, FirmwareTrace, BadMessage}

  Default Setting: {Error, Warning, Information, Measurement}

  Specify the log types to be enabled as a default for all logs.

- Archive Job Time

  {hh:mm:ss for a 24hour clock}

  Default Setting: 02:00:00 (2 AM)

  Specify the time of day that daily log files are automatically archived. The service must be running during this time, or else the action will not be taken.

- Archive Older Than

  7days ≥ Valid Entries ≤ 90days

  Default Setting: 7 days

  Specify the number of days to allow log entries to age before they are automatically archived at the time set in ‘Archive Job Time’. The service must be running during that time, or else the action will not be taken.

- Purge Older Than

  -1 ≥ Valid Entries ≤ 365days

  Default Setting: 30 days

  Specify the time to allow log archives to age before they are automatically purged. An entry of -1 means the log archives will never be purged.

- Archive Path

  {A valid directory path on the local PC}

  Default Setting: c:\swi\archives\

  Specify the path to the directory where archived files are stored.

- Page Refresh

  -1sec ≥ Valid Entries ≤ 60sec

Default Setting: 2 seconds

Specify the interval at which the Homepage will auto-refresh. Entering -1 causes the Homepage to never auto-refresh.

- Present Measurement Time

  1sec ≥ Valid Entries ≤ 20sec

  Default Setting: 12 seconds

  Define present measurements as younger than this time. Present measurements are displayed on the Homepage with dark green background.

- Recent Measurement Time

  5sec ≥ Valid Entries ≤ 60sec

  Default Setting: 20 seconds

  Define recent measurements as younger than this time. Recent measurements are displayed on the Homepage with light green background.

- Past Measurement Time

  10sec ≥ Valid Entries ≤ 120sec

  Default Setting: 40 seconds

  Define past measurements as younger than this time. Past measurements are displayed on the Homepage with a pale green background.

- Old Measurement Time

  20sec ≥ Valid Entries ≤ 120sec

  Default Setting: 60 seconds

  Define old measurements as younger than this time. Old measurements are displayed on the Homepage with a white background.

Section 2 Operation

2.1 Data Collection

The *DataSure*™ system facilitates several methods of data collection and distribution.

Once the network has been started measurements can be sent by tool operators from the attached EndNode, measurements may be solicited from tools by the operator of the *DataSure*™ software, or by a 3rd party software application.

Measurements transmitted from the tool are initiated by pressing the data-send button on the EndNode. Operators should wait for EndNode acknowledgement before sending successive measurements (refer to Appendix B: LED Blink Tables). These sent values are called 'unsolicited', since they are not requested by the software. The newest received values can be viewed on the Homepage. All received measurements are retained in the log file. Unsolicited measurements are also automatically sent out over the comm. port of multiplexer which their source tool is associated with. In this way applications may monitor and record in-coming tool data.

Measurements may be solicited from tools on the Homepage by clicking on the 'Measure' button next to the target device. The newest received values will be in view on the Homepage, and all are retained in the log file. However, measurements solicited from the Homepage (or from the sidebar menu of a Device Detail page) are NOT conveyed out the multiplexer comm. port to any applications. Only solicited measurements requested by the application software are transmitted over the multiplexer's comm. port (refer the Measure Command in Appendix A: Application Interfaces).

By these processes, data may be dynamically collected from tools residing anywhere within the bounds of the wireless network, or beyond if the internal memory of the EndNode is not exceeded (maximum of 10 stored measurements). Operators have the option to be located at the site of the tool, with the PC hosting the *DataSure*™ software, or at any remote location with a PC networked to the localhost PC. Alternatively, 3rd party software applications (such as an SPC package) running on the localhost PC have the potential to solicit data from tools.

Measurements can also be accumulated in the *DataSure*™ log file, and later exported in a variety of standard file formats (refer to section 2.1.2 Data Logging). Operators are then free to graph or tabulate their recorded data using their preferred data management software packages.

2.1.1 Quick Start (should be at beginning AND on a card inserted in the box)

- Recap in brief the steps to bring up a tool to the homepage,
- take readings from the homepage.
- Describe tool status, battery, and time-since-last measurement indicators.

1) Install and run the *DataSure*™ software
   - Insert the *DataSure*™ CD in the intended host PC's CD-ROM drive
   - Follow the install procedure
   - Launch the *DataSure*™ software

2) Make sure all hardware elements are powered on, and interconnected

- Tools and EndNodes should have fresh batteries, and be connected
- Routers, Gateway, and hosting PC are all plugged in and running
- EndNodes, Routers, and Gateway are all within working range of each other

3) Start the Wireless network service
   - Click on ‘Start Wireless Network’ from the *DataSure*™ Homepage
   - Watch the tools appear on the Homepage
   - In moments the status of the tools will change to ‘Ready'

4) Begin taking measurements
   - Press the data-send button on the EndNode
   - Or click on the tool’s ‘Measure’ button on the Homepage
   - Watch the tool reading and time-stamp appear on the Homepage

5) Export collected data
   - Click on ‘Logs’ from the horizontal *DataSure*™ menu navigation bar
   - Click on ‘View Measurements’ from the Log Summary sidebar menu
   - Click on ‘Export Log As’ from the Log Detail sidebar menu
   - Click on ‘Export Log as .csv’ from the Log Detail sidebar menu
   - Open or Save the file to disk

2.1.2 Data Logging

The *DataSure*™ software is capable of maintaining highly detailed records in regards to many aspects of traffic over the wireless network, including time-stamped measurements received from tools. Data logs can be generated and then sent to SPC packages, or retained as work records. *DataSure*™ administrators can also use the log file as a diagnostic view of network performance.

The main Log Summary page provides a tally of log message types and a top-level list of daily logs for all objects. Clicking on the icon or date hyperlink of a daily log displays the targeted Log Detail page.

Under the Log Events heading are listed the Date, Time, Object Name, Type, Alert, and Event. The Date and Time correspond to the exact time an event enters the log. The Object Name refers to the Device, Node, or Application associated with the event. The Type is a message classification which can enabled/disabled to be shown in the Logs. This can be set as default for all log objects via the Basic System Settings on the Basic Administration page, or for specific objects via their own Detail page. The Alerts column is used to call notice to events pending acknowledgement and have not yet been dismissed by the operator (a summary list of these events will also be displayed on the sidebar under the Alerts header until they have been dismissed). Finally, in the far-right column, the event description is provided in the log.

From the main Log Summary page, sorted logs for all objects may be viewed by Alerts, Errors, Warnings, or Measurement. These are the options given under Related Links from the sidebar menu. Individual alerts pending dismissal may be viewed by clicking on them from the sidebar. By clicking on the sidebar Commands link 'Dismiss Displayed Alerts', all alert events shown on the currently displayed Detail page will be acknowledged. This action removes them from the sidebar list, and also cancels their pending notice from the Log Events. It does not remove the event from the log. It is also possible to view all Log Events for a specific object (such as Device, Node, or Application) by going to its Detail page and clicking on 'Log Summary' under the Related Links in the sidebar menu.

A set of Log Events shown from any Log Detail page can be exported and saved in a variety of text file formats. To choose a format, click on 'Export Log As' from the list of Commands in the sidebar menu. This will expand the view of the available export options: .csv (comma separated value), .tsv (tab separated value), .xls (for use with Microsoft Excel), and .xml (for use with XML-based applications). Choose one of these and a File Download dialog box will appear. The log file may be 'Opened' directly inside the application assigned to that file type in Windows OS, or 'Saved' to any accessible directory.

Daily Logs may also be archived, cleared, and restored within the *DataSure*™ software utility. From the Log Summary page for all objects use the Archive Commands in the sidebar menu. Click on 'Show Archived Logs' to display all the previously archived logs. Click on 'Select Archive/Restore' in order to gain the ability to place a check mark next to the log file intended for either archival or restoration. Mark a selection, and then click on 'Execute Archive/Restore' to initiate the desired action. The log may also be cleared by clicking on 'Clear Log' from the sidebar menu on the Basic Administration page. All log entries will be lost if they have not yet been archived. The directory used to stored archived log files may be specified in the Basic System Settings in the Basic Administration page.

2.1.3 Applications

- Explain the use of the Application Command Set

- Site a generic example of an external application program (terminal program) Way too complicated – I say do an App Note on that one. Try Shop Floor II+ or other SPC app
- Explain the use of the Application Command Set

2.2 Remote Network Monitoring

If the PC running the *DataSure*™ utility software is attached to a computer network, such as a LAN, it is also possible to monitor and manipulate network activity from a remote PC. Using a browser the remote PC can target the PC hosting the *DataSure*™ software locally (the localhost PC must also be the one directly attached to the Gateway device).

The name of the localhost PC is a part of the address used by the remote PC. To obtain this information on the localhost PC: Progress from the Windows 'Start' menu to the 'Control Panel'. Click on 'System', and then the 'Computer Name' tab. Make note of the displayed Full Computer Name.

In the Address field of the browser running on the remote PC, use the Localhost's Computer Name in place of the letters <LCN>:

http://<LCN>/swi/Home.aspx

Through remote access, operators may perform most of same actions as users of the localhost PC. However, there are some noted exceptions in regards to applications. Virtual multiplexers within the *DataSure*™ software use comm. ports internal to the localhost PC. Software applications running on remote PCs cannot make use of those comm. ports, and so cannot interface with the virtual multiplexers.

It is not possible to launch applications from the Homepage via remote access. Remote users are also not given access to browse file directories on the localhost PC while defining a new application in the *DataSure*™ system. Remote users have read-only access to the Basic Administration page, and are banned from reaching the Advanced Administration page.

Remote PC users can collect and record tool data by using the 'Measure' button on the Homepage (or by sending readings from the EndNode itself). Log files of the measurements taken can be downloaded to the remote PC in the same way they are exported to the drive of the localhost PC (refer to section 2.1.2).

2.3 Advanced Network Administration

The Advanced Administration page is accessible via the sidebar menu from the Basic Administration page. It contains options not intended for frequent and/or general use. It is intended for advanced *DataSure*™ system users and administrators only.

Under Database Commands from the sidebar, the *DataSure*™ system configuration can be cleared and all Basic System Settings returned to their default settings. To take this action, click on 'Clear Database'. All data and settings will be lost if they have not been previously backed up.

The Advanced System Settings are detailed below. Each system setting has a range of valid entries and a pre-defined factory-set default. These settings allow the operator to customize the performance of the wireless network and direct the flow of data through *DataSure*™ utility software. It is also possible to impair or impede network operability through inappropriate changes to some settings. Operators are encouraged to proceed with caution, and test their networks after changes are made.

- Module Trace Level
  {None, Errors, Warnings, Informational, Verbose}

Default Setting: {Errors}

Choose the level that triggers trace-log messages from device modules.

- Module Tool Sampling
  10sec ≥ Valid Entries ≤ 60sec

  Default Setting: 30 seconds

  This is the interval at which tools are checked to determine if they are on or off.

- Module GCTS Offline
  10min ≥ Valid Entries ≤ 60min

  Default Setting: 10 minutes

  If an EndNode signals that it is not clear to send data for this many minutes, then sampling will be disabled for that device.

- DB Update Interval Secs
  1sec ≥ Valid Entries ≤ 30sec

  Default Setting: 5 seconds

  This is the time specified to span between automatic database updates.

- Log Update Interval Secs
  1sec ≥ Valid Entries ≤ 60sec

  Default Setting: 5 seconds

  This is the time specified to span between automatic log file updates.

- Log Update Interval Lines
  1 Line ≥ Valid Entries ≤ 200 Lines

  Default Setting: 50 Lines

  The number of lines that triggers a log file update.

- Node Offline Total Time
  5min ≥ Valid Entries ≤ 30min

  Default Setting: 15 minutes

  Generate a log entry/alert when a node has gone offline and remained so for this number of minutes.

- Dismiss Job Time

  {hh:mm:ss for a 24hour clock}

  Default Setting: 01:00:00 (1 AM)

  Specify the time of day that alerts are auto-dismissed on days set by ‘Dismiss Older Than’. The service must be running during this time, or else the action will not be taken.

- Dismiss Older Than

  1day ≥ Valid Entries ≤ 7days

  Default Setting: 3 days

  Specify the number of days to allow alerts to age before they are automatically dismissed at the time set in ‘Dismiss Job Time’. The service must be running during that time, or else the action will not be taken.

- Gateway Comm Port

  {Auto, Com1,.. Com16}

  Default Setting: {Auto}

  Select the comm. port connected to the network Gateway. For USB enabled Gateways, select the internal comm. port associated with the USB connection. ‘Auto’ causes the DATASURE™ software to auto detect for the appropriate comm. port.

- Log Date Format

  {MM/dd/yyyy hh:mm:ss.ff tt}
  {M: month, d: day, y: year, h: hour, m: minute, s: second,
  f: millisecond, tt: AM/PM}

  Default Setting: {MM/dd/yyyy hh:mm:ss.ff tt}

  Enter the format for the date and time fields of the log. These are some common examples that may be used:

Description of Pattern	**Example Format**	**Example Result**
Default	MM/dd/yyyy hh:mm:ss:ff tt	06/15/2005 11:56:04.15 AM
Short Date	MM/dd/yyyy	
Long Date	dddd, dd MMMM yyyy	

Full date and time	dddd, dd MMMM yyyy hh:mm:ss	
Short data and time	MM/dd/yyyy hh:mm	
Month and day	MMMM dd	
Short time	hh:mm	
Long time	hh:mm:ss	

- Ping Interval

    5,000msec ≥ Valid Entries ≤ 60,000msec

    Default Setting: 10,000 milliseconds

    Specify the interval at which the status of nodes is automatically checked. Quicker intervals will provide a swifter notification of status changes, but will shorten the useable battery life of the EndNode.

- Marginal Battery

    2.5V ≥ Valid Entries ≤ 3V

    Default Setting: 2.8 Volts

    Specify the threshold for discriminating the Good/Marginal battery level for EndNodes. A battery of marginal voltage will still provide enough power for full operation of the EndNode. However, operators should take note that the use-able life of the battery will soon be coming to an end.

- Critical Battery

    2.5V ≥ Valid Entries ≤ 3V

    Default Setting: 2.7 Volts

    Specify the threshold for discriminating the Marginal/Critical battery level for EndNodes. Batteries that have dropped below this threshold level should be considered spent and un-useable.

- Retry Count

    0 ≥ Valid Entries ≤ 20

    Default Setting: 3 Retries

    Specify the number of retries that will be attempted before an error is reported

- Excessive Retries

    1% ≥ Valid Entries ≤ 10%

Default Setting: 10%

A warning message will be generated when a series of retries exceeds this percentage.

- Module Enabled Alerts

  {Reset, ToolOn, ToolOff, BufferOverflow, CorruptMessage}

  Default Setting: {Reset, ToolOn, ToolOff, BufferOverflow, CorruptMessage}

  Choose the set of conditions that which will cause device modules to generate alert messages.

- Wireless Diagnostic Monitor Enabled

  {Yes or No}

  Default Setting: {No}

  Determine whether the Wireless Diagnostic Monitor is visible or not.

- Marginal Router Battery

  1.5V ≥ Valid Entries ≤ 2V

  Default Setting: 1.8 Volts

  Specify the threshold for discriminating the Good/Marginal battery level for routers.

- Critical Router Battery

  1.5V ≥ Valid Entries ≤ 2V

  Default Setting: 1.6 Volts

  Specify the threshold for discriminating the Marginal/Critical battery level for routers.

- Backup Path

  {A valid directory path on the local PC}

  Default Setting: c:\swi\backups\

  Specify the path to the directory where backup database files are stored.

Section 3 Troubleshooting

3.1 Common Problems and Solutions

Should you have any questions not addressed by the examples below, or if you desire to contact the L.S. Starrett Company for any reason, please contact the L.S. Starrett Company subsidiary serving your location, or write: The L.S. Starrett Company Sales Support Center 121 Crescent Street Athol, MA 01330. Attention: *DataSure*™ Technical Support.

Common Problems	Potential Solutions
• Tool status remains Online, and will not send measurements.	• Click on 'Reset Device' from the device's Detail Page. • Cycle the power on the EndNode.
• EndNode batteries are used up over a short period of time.	• Make sure the Locate EndNode feature has been Stopp from the Homepage. • Increase the Sampling Interval from the Basic System Settings. • Increase the Ping Interval from the Advanced System Settings. • Take the option to upgrade the EndNode battery to a CR2477.
• Tool will not go to sleep, and is running down its batteries.	• Turn the EndNode off when it is not needed.
• Applications cannot open the comm. port for a multiplexer.	• Make sure no other programs are engaged on that comm port. • Restart the PC.
• The Wireless Network will not start.	• Make sure the Gateway is connected and powered on. • Make sure the Gateway is not assigned to comm. port 9 greater. • Make sure there are no more than 5 multiplexers config in the *DataSure*™ system.
• Not all measurements sent from the EndNode are transmitted.	• Wait for the green LED flashes indicating readings hav been sent and then received before sending another measurement.
• Changing the Sampling Interval from the Basic System Settings does not affect a node.	• Edit the node from the Network Node Detail page, and on 'Use Default'.
• Changing the Enabled Logging from the Basic System Settings does not affect the logging of an object.	• Edit the object (device, application, or node), 'Customi the logging, and click on 'Use Default'.

3.2 Recommended Use Policies

- Useful network administrative tip 1
- Useful network administrative tip 2

3.3 RF 'Does & Don'ts

Describe appropriate methods of RF deployment

Industrial environments demand rugged and reliable solutions regardless of the type of system to be deployed. Electronics as a group, are some of the most mechanically and performance fragile systems that live on the shop floor. Within the shop floor environment there are frequent examples of noise and interference sources that disturbs or otherwise impairs the reliable functioning of electronics. While heavy steel packaging and seal rings keep harmful, volatile and corrosive liquids and particles out of sensitive electronics, they cannot protect the emissions of radio waves in wireless networks. More and more, wireless sensors and metrology instruments are being deployed in production areas. Wireless systems deliver their quality or production data to critical operations downstream and are crucial components of the modern production reality. With this said, wireless data transmission of data is critically needed and simultaneously vulnerable to shop induced interference.

Radio frequency (RF) waves are the carrier for data in a wireless data acquisition system. These waves are simply energy propagated through free space. When free space is cluttered with other energy forms, intentional radio waves are compromised. RF is highly susceptible to corruption and alteration via a variety of Electromagnetic Interference (EMI). EMI has been defined as the *"degradation of the performance of a piece of equipment, transmission channel, or system caused by an electromagnetic disturbance."* (ANSI C63.14, 1992) EMI can occur throughout the EM spectrum from 0 Hz to 20 GHz or higher frequencies. However, EMI problems are most prevalent in the RF spectrum. Since in our application the RF carries the data, then good RF handling must be dealt with to keep the data intact.

EMI types typical of (but not limited to) production shop environments:

DC Fields – Quasi-AC fields and Magnetic: “plumes” or fields generated by rotating spindles, motor armature coils, de-magnetizers, magnetized steel beams in commercial buildings etc.

AC Fields and RF: generated by AC motors, induction hardeners, unshielded electronic devices, cell phones, microwave ovens, and walkie-talkies.

Transient Electromagnetic Fields: produced by the switching of inductive loads such as circuit breakers or motors. Lightning will also cause this type of disturbance. A transient signal in a cable can produce a radiated emission with spectral (frequency) content. Radiation from transient sources is rarely found to have significant energy at frequencies exceeding 500 MHz however.

In the presence of these EMI components, RF based systems must manage their performance relative to interference if they are to be useful. There is no such thing as a 100% noise immune radio system. So with that truth, systems designers must develop robust wireless data collection networks and sensors to be less susceptible to the presence of EMI.

There are many techniques that designers can use to offset the impact of noise in a wireless network. The scope of this section is to discuss the mesh network as a primary means of making robust and reliable wireless networks.

A mesh network is a topology that has some distinctive features. First it has a single and central Gateway function where all system wide commands and network management can occur. Data from the network also returns here. Secondly, the sensor/measurement EndNode radios can be active components of the network. Thirdly, numerous Routers or repeaters are present and can be added to enable multiple paths for OTA transmissions.

The mesh is inherently robust to interference by the very nature of the system configuration. An example of can be explained via looking at what happens to the OTA flight of the RF. (Figure 1a) As the EndNode acquires data from it's measurement tool, and transmits it to the Gateway, a plume of EMI from an induction hardener cancels the RF in the immediate vicinity.

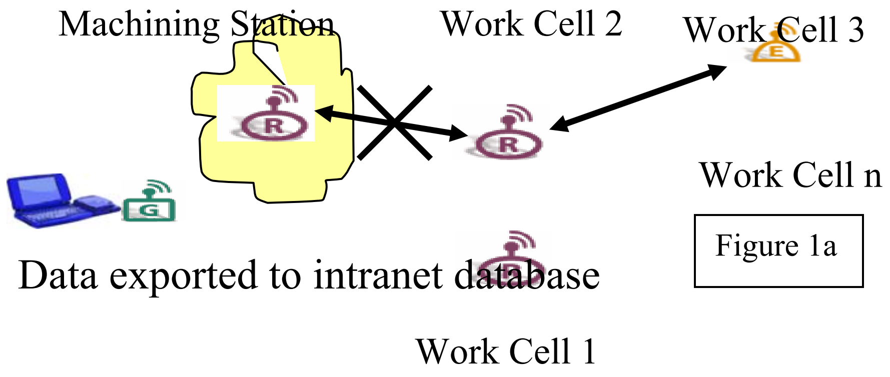

Figure 1a

Adjacent to the first Router, other Routers (Figure 1b) have also received the data transmission. Once the blocked Router has found no data was received, it cannot pass along any data to the Gateway. Simultaneously, the other Routers have the good data and attempt to send that data to the Gateway. The data may make a series of Router hops until it reaches the Gateway. While this is happening, other copies of the data are enroute to the Gateway. When the Gateway sees an exact copy of already received data, the Gateway discards the additional copies. EndNodes on the network have a time stamping capability and unique "address" which allows only the intended data to reach the gateway without duplication.

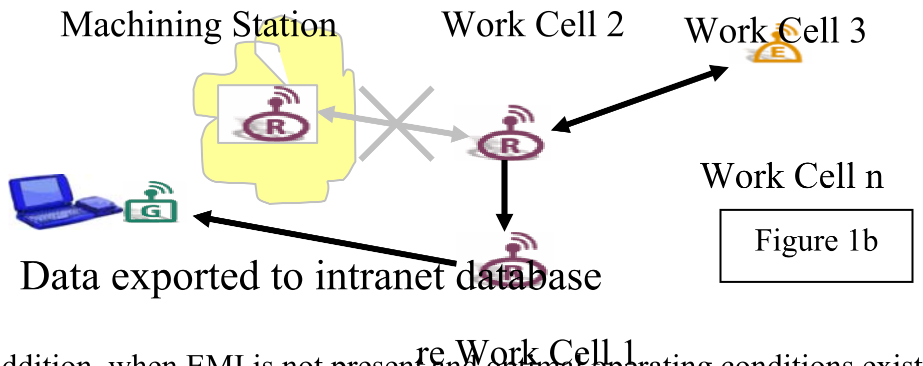

Figure 1b

In addition, when EMI is not present and optimal operating conditions exist, the mesh network speeds OTA transmission by constructing a routing table in each network element. With the Router table there is a predetermined path for data, which allows the other Routers in the network to be either idle or available for other EndNodes to be received.

This example shows that multiple paths in a mesh network provide alternative paths for data thus spatially and temporally avoiding corruption from EMI.

Unlike mesh networks, daisy chain or point-to-point networks suffer from “single points of failure”. See Figure 2. If one link in the chain is corrupted via EMI, then OTA transmission will stop at that break in the “chain”.

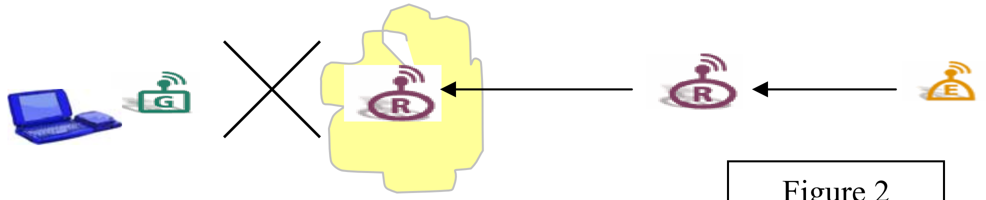

Figure 2

Suffice it to say, if the wireless network is capable of supporting a mesh configuration, then simply adding Routers to the system will make the system more robust.

However, data errors are not isolated to EMI. There are other environmental and user related means to cause data errors. The well informed system installer and network administrator will be able to choose the right system and remedy for certain kinds of data integrity problems.

In paper and pen data recording, it is immediately apparent that data has been recorded. By looking at the paper, you can easily see what was recorded. Wired systems for data collection are typically connected to a local device that displays the most recent reading. Some installations of data collection have PC’s at each work cell or bench showing the data and trend lines for the measurements in progress.

One of the key advantages of wireless data collection is freedom from the bench; host PC’s, wires and the limitations of bringing a part for inspection to the tool.
Therefore, with wireless systems, data being recorded may not be immediately or readily visible. Consider a shop floor operator with a wireless tool. When data is recorded by pressing a button on the tool or data cable, the data shows up at the gateway/PC screen. If the PC is not located in the immediate vicinity of where the data is taken, and often it is not, then the operator is unsure data has been received. Some wireless data systems have no capability to alert the operator of the tool that the data actually made it to the intended destination – here it is the PC/gateway.

Advanced systems for wireless data collection have indicators/enunciators on the data transmission device itself, to show the operator the status of the system and the successful transmission of data. In many systems, the EndNode is “unaware’ that the network or host PC loses power, and therefore, data will not be recorded. However, if the endpoint has the ability to show the user that data transmission has failed, a few good things can result. The operator can immediately see that there is a problem with the network and correct it. Conversely, without any system status indication, the operator can unknowingly corrupt his own data collection. The operator can also stop pressing the data send button, which may send many duplicates of the data. Unfortunately, repeated pressing of a button is a typical or perhaps a natural response when an electronic device does not work as expected. By repeatedly pressing the data send button to "remedy" the problem, the data set will be corrupted and therefore corrupting the data sets statistical significance. Additionally, without system feedback, the operator may continue to think everything is ok for sending data, continuing the data collection process but lose an entire shift worth of data collection. This is an undesirable situation indeed.

With a feedback method of system status oriented to the user, data can have more integrity. However, when the user ignores or misses the feedback, data can still be corrupted. As an additional safeguard to lost data, the endpoint radio can incorporate a means to store data recorded when the main systems is down. Often operators will take measurements quickly, yet accurately in a production environment. After taking e.g. 15 successive measurements with rapid button pushes, and the system crashes on the 10th measurement, then the remaining 5 measurements would be lost. Modern wireless data collection system designs incorporate a storage feature that collects any data "taken" at the endpoint and holds it until the system becomes available again. All the while data is being stored on the endpoint, the endpoint radio alerts the user with the feedback system described above and waits for the system to come back online. Once the system is back on line, the endpoint will dump its data to the gateway/PC host system. No data is lost, even though the main system has failed.

During the OTA (over the air) transmission of data, a wide variety of interferences can occur and modern systems have mechanisms to identify corrupted data and mark the data as such. By using CRC (cyclic redundancy check(ing)) and parity error detection methods, modern systems can tag or discard the corrupted data, unfortunately, most systems today just do that. There is no chance of recovering the intended measurement. Advanced systems, such as The LS Starrett's wireless data collection system, has a system feature communicates between endpoint and gateway that seeks to insure that uncorrupted data arrives at the gateway. If the system tags the data sent with a CRC or parity error, the gateway informs the endpoint to resend the data again from the endpoints temporary memory. Data is then sent again, up to 10 times, to insure good data ultimately gets to the data set. If data is received as good, then the gateway informs the endpoint to discard its temporary memory of that data, so that it doesn't get sent again. The temporary memory is only held until the gateway validates a successful receipt of the data.

These methods are just some of the ways the LS Starrett Wireless Data Collection System insures very high data integrity. Data collected in the field show some remarkable performance figures. Typical successful measurement transmissions up to zero failures in 3.5 million measurements have been recorded.

3.4 Monitoring Device Statistics

Administrators encountering problems with data exchanges over the wireless network have the opportunity to monitor the performance of EndNodes through the Device Statistics table shown on their Device Detail pages. From the information obtained here, corrective adjustments to the Basic or Advanced System Settings may be identified. All statistics for all devices can be reset from the Network Devices page's sidebar menu. Statistics relevant to specific device can be reset from its Device Detail page's sidebar menu.

- Messages Sent
  This is the total number of transmissions sent to the tool. In most cases this is a request for the tool to send data to the EndNode, either for it to be sent out over the network, or to test if the tool on or off.

- Messages Received
  This is the total number of transmissions received by the Gateway from the tool.

- Messages Retried
  This is the number of transmissions requiring some number of retries.

- Messages Retries
  This is the total number of retries sent to the EndNode.

- Messages Corrupted
  This is the number of invalid messages received from an EndNode.

- Last Message Time
  This shows the last time and date that a message was received from an EndNode.

- Module Messages Sent
  This is the total number of transmissions sent by an EndNode.

- Module Messages Received
  This is the total number of transmissions received by an EndNode.

- Module Messages Retried
  This is the number of messages retransmitted at least once by an EndNode.

- Module Messages Retries
  This is the number of message retransmissions sent by an EndNode.

- Module messages Corrupted
  This is the number of invalid messages received by an EndNode.

- Module Up Time
  This shows the total elapsed time since an EndNode was reset ('Reset Device' from the Device Detail page sidebar menu.)

- Offline Events
  This is the total number of times an EndNode transitioned to the offline state.

- Online Events
  This is the total number of times an EndNode transitioned to the online state.

- Offline Time
  This shows the total accumulated time an EndNode has spent in the offline state.

- Online Time
  This shows the total accumulated time an EndNode has spent in the online state.

- Ready Time
  This shows the total accumulated time an EndNode has spent in the ready state.

- Active Time
  This shows the total accumulated time an EndNode has spent in the active state.

- Total Time
  This is the total amount of time spanned by the displayed set of device statistics.

- Total Errors
  This is the total number of device errors logged against an EndNode.

- Total Warnings
  This is the total number of device warnings logged against an EndNode.

- Network Write Failures
  This is the total number of network serial write errors for an EndNode.

- Network Buffer Errors
  This is the total number of network serial write buffer full errors for an EndNode.

- Network Retry Sequences
  This is the total number of write retry sequences initiated for an EndNode.

• Appendix A: Application Interfaces

Virtual multiplexers within the *DataSure™* software are emulations of the Starrett 761A and 761B. Communications with other applications use the same 761 Command Set and RS232 protocol parameters:

9600 BAUD
8 DATA BITS
1 STOP BIT
NO PARITY

Command	**Syntax**	**Default**
Measure	M nn<cr>	
Sequence	S nn,nn,nn,..nn<cr> or S -1<cr>	01
Report	R<cr>	
Auto	A ON<cr> or A OFF<cr>	OFF
Buzzer	B ON<cr> or B OFF<cr> or B n	OFF
Poll	P nn	OFF
Version	V<cr>	
Units	U ON<cr> or U OFF<cr>	ON
Port Number	N ON<cr> or N OFF<cr>	ON
Save	SV<cr>	

Note: Commands are not case sensitive.
<cr> Is the syntax notation for pressing the Enter key (Carriage Return).
n Is the syntax notation for a numeral value 0,1,2,3,4,5,6,7,8, or 9.

- Measure Command:

This command is used to get a reading from any one of the tools that are connected to the multiplexer.

Example:

Transmitted Data	**Received Data**
M 03<cr>	#03 00.7000 in

- Sequence Command:

This command is used to set up the sequence that will be used when the Auto mode is turned ON. When a reading is displayed for the first port number of a sequence, a reading will automatically be taken from the next port number, and continue in turn until the sequence is complete. Polling the first port number of a sequence will cause the string of sequential measurements to repeat.

The port numbers can be in any order, and the same port can be used more than once. The numbers must be entered as two digit sets separated by commas. To clear the sequence, enter S -1<cr>

Example:

Transmitted Data	**Programmed Port Sequence**
S 01,03,05,03<cr>	1, 3, 5, 3

- Report Command:

This command will display the multiplexer name, version, setup values, and the list of EndNode Controller ID's that are associated with ports in the multiplexer.

Example:

Transmitted Data	**Received Data**
R<cr>	Primary Multiplexer on COM2 Emulates Starrett_761 # of Line to TX: ALL A: OFF B: OFF N: ON P: OFF U: ON SEQ: 01 PORT 01: 19970661 VER 1.0 Wireless

- Auto Command:

This command activates the Auto mode of the multiplexer. When ON and a reading is taken by the first tool in the Sequence, it will automatically trigger the remaining tools in the list. The list is specified in the Sequence command.

The initial reading can be activated by the EndNode transmit button, the Measure command, or the Poll command.

Example to turn Auto mode on:	A ON<cr>
Example to turn Auto mode off:	A OFF<cr>

- Buzzer Command:

Speakers or headphones must be attached to the PC if the buzzer tone is to be heard. The Buzzer Command has three forms:

B ON<cr> A tone will sound whenever a reading is received.

B OFF<cr> Disables the buzzer when a reading is received. When OFF, the buzzer will still activate when it receives an invalid command or a solicited reading cannot be obtained.

B n<cr> Causes the buzzer to sound n+1 times (to a maximum of 10).

- Poll Command:

This command will continuously request readings from port n.

Example:

Transmitted Data	**Received Data**
P 01<cr>	#01 00.0020 in
	#01 00.0020 in
	#01 00.0020 in
P OFF<cr>	

If the multiplexer is set up with a sequence and the Auto function is enabled then the output will be a continuous sequence.

Example:

Transmitted Data	**Received Data**
S 01,03,05<cr>	
A ON<cr>	
P 01<cr>	#01 00.0020 in
	#03 00.7000 in
	#05 03.5410 in
	#01 00.0020 in
	#03 00.7000 in
	#05 03.5410 in
	#01 00.0020 in

- Version Command:

The multiplexer will respond with the version of the current *DataSure*™ Wireless Network Manager software.

Example:

Transmitted Data	**Received Data**
V<cr>	1.0 Wireless

- Units Command:

Determines if the multiplexer will send the units of measurement with every transmission.

This feature only works if the tool sends units of measurement as part of its message.

Example:

Transmitted Data	Received Data
U ON<cr>	
M 01<cr>	#01 00.0020 in
U OFF<cr>	
M 01<cr>	#01 00.0020

- Port Number Command:

Determines if the multiplexer will transmit the port number associated with every received the reading.

Example:

Transmitted Data	Received Data
N ON<cr>	
M 01<cr>	#01 00.0020 in
N OFF<cr>	
M 01<cr>	00.0020 in

- Save Command:

This command will save the current setup of the virtual multiplexer. Every time the network is stopped and restarted, the saved settings will be retained. Setups include the ON or OFF status of Auto, Buzzer, Port Numbers, Poll, and Units modes. The Sequence is also saved in the setup.

Example:

Transmitted Data	Received Data
SV<cr>	Save Complete

Appendix B: LED Blink Tables

These tables define the EndNode module's visual response to states and events. States refer to the EndNode's current status of operation within the wireless network. Events occur when nodes actively attempt to transfer data over the wireless network. A blink "combo" is any combination of red & green blinks as defined in the tables below.

State	Green LED	Red LED	Time between Blink Combos (Seconds)	Notes
No network	0	1	10	
Tool OFF/Network ready	1	1	10	First Green then Red
Ready	1	0	10	
Data Stored In EndNode	2	1	5	Green-Red-Green

State	Explanation
No network	There is no network detected, tool on/off status is irrelevant
Tool OFF/Network ready	Tool is off or in sleep mode, the network is up and ready
Ready	The tool is on, network is up and ready
Data Stored In EndNode	The EndNode has unsent tool data stored, waiting for network to be ready

Event	Green LED	Red LED	Time between combos (Seconds)	Notes
Tool does not emit data/network present	1	4	2	5 combos
EndNode sends data	2	0	One combo	
Data successfully received	4	0	One combo	
Data Stored In EndNode/ no network connection	2	1	0.5	2 combos, Green-Red-Green
Data Lost/ no network connection	0	3	0.5	3 combos
Data Lost/network connection ok	0	5	1	5 combos

Event	Explanation
Tool does not emit data/network present	Either the tool has not been used for a while and has gone to sleep or some other failure
EndNode sends data	EndNode has sent data to the Gateway
Data successfully received	Acknowledgement from the Gateway that data was received
Data Stored In EndNode/ no network connection	Network connection has been lost and measurement is being stored in the EndNode
Data Lost/ no network connection	No network connection is present and no more room is left in the EndNode to store measurements
Data Lost/network connection ok	Network connection is present, but data cannot be delivered. Unknown communication error

Appendix x: Network Monitor

Describe the enabling and use of the Millennial iBean Network Monitor