Sensite solutionS

LogiSphere

User Manual

Version 3.8

January 2005

General information
The information in this document is subject to change without notice.

Liability
Sensite Solutions B.V. shall not be liable for technical or editorial errors contained herein: not for incidental or consequential damages resulting from the furnishing, performance or use of this document.

Use of product names
The product names mentioned herein are used for identification purposes only, and may be trademarks and/or registered trademarks of their respective companies.

Copyright

Contact information
Sensite Solutions B.V.
Keizersgracht 23b
5611 GC Eindhoven
The Netherlands
Phone: +31 (0)40 212 87 00
Fax: +31 (0)40 213 06 39
Internet: www.sensite-solutions.com

Table of Contents

1 Introduction

1.1 Purpose and Scope

This document describes the technical aspects of all LogiSphere components and is intended for people responsible for installing and configuring LogiSphere systems.

1.2 Terminology, Acronyms, and Abbreviations

ATEX	*“**AT**mosphere **EX**plosive”*, French acronym for product directives with respect to explosion-hazardous situations
CR	Carriage Return
EIRP	Effective Isotropic Radiated Power
EMEA	Europe, Middle-East and Africa
Intelligent Tag	The name for Sensite Solutions’ transmitter
LF	Line Feed
NTE	Network Termination Equipment, the device that is connected to the WNC’s serial interface
RF	Radio Frequency
RIP	Routing Information Protocol
RSSI	Received Signal Strength Indicator
Sensor Terminal	The name for Sensite Solutions’ wireless transmitter with possibility of connecting external sensors
SRD	Short Range Device
TCP/IP	A suite of commonly used internet data communication protocols
Wireless Network Controller	The name for Sensite Solutions’ receiver/base station (WNC)
WNC	See Wireless Network Controller

1.3 Sensite Solutions

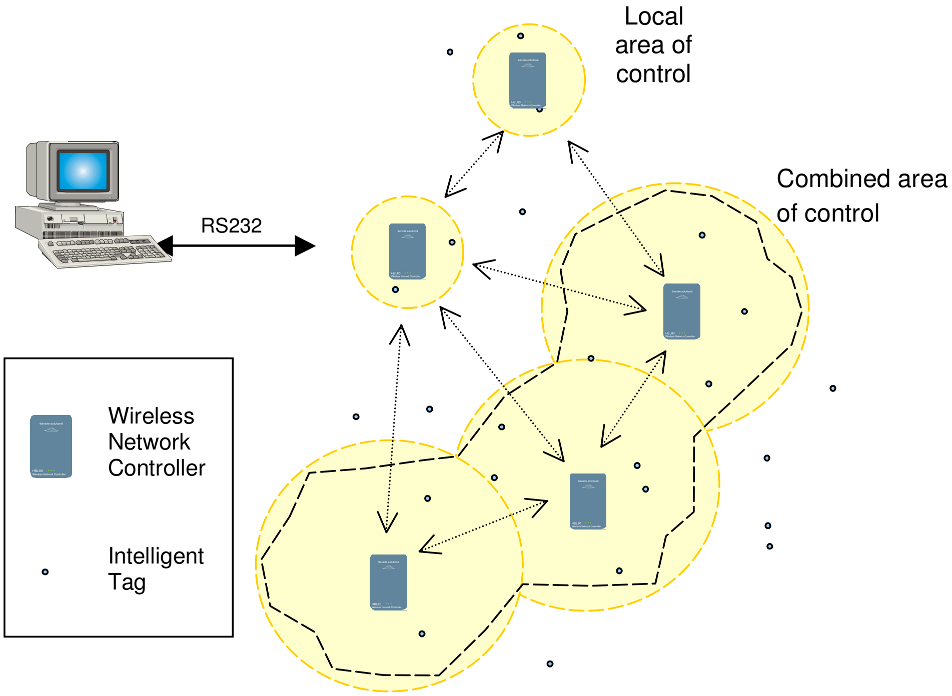
Sensite Solutions B.V. develops and markets complete solutions for wireless local tracing and telemetry applications. The system that provides specific support for logistical processes like transport, distribution, and yard management, is called LogiSphere. The LogiSphere architecture consists of Intelligent Tags (active sensor/transmitters), Sensor Terminals (for wireless transmission of external sensor measurements), Wireless Network Controllers (receiver/base stations), and the associated LogiWare Software Suite (running on windows-based platforms). In addition, the LogiSphere system features configuration utilities consisting of Tag Programmers and Signal Analysers.

1.4 LogiSphere

LogiSphere is the highly innovative wireless tracing and telemetry system providing real-time asset visibility and management for a wide variety of logistical processes.

The LogiSphere components operate on a license-free frequency intended for Short Range Devices (SRD). This frequency is 915 MHz for REGION-I (North- and South America), and 868 MHz for REGION-II (EMEA). With respect to REGION-I, all LogiSphere devices comply with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) the devices may not cause harmful interference, and (2) the devices must accept any interference received, including interference that may cause undesired operation.
With respect to REGION-II, all LogiSphere devices comply with the standards and regulations within CE certification.

The overview below depicts a typical LogiSphere configuration. A LogiSphere wireless communication network is constructed using Wireless Network Controllers (WNC) that can be combined without any limitations. They enable the definition of areas of control, in which both the presence of Intelligent Tags and Sensor Terminals, and the telemetry that they provide can be interrogated. By adding Wireless Network Controllers, the wireless communication network can be expanded by the user to form areas of control in any required form and size. All the information from the LogiSphere network is provided to any computer platform, wireless link, or industrial controller via a Wireless Network Controller of choice.



One of the major concepts of LogiSphere is *Ease of Everything*: all LogiSphere elements have been designed to minimize efforts with respect to installation, configuration, and use. Default values of all LogiSphere parameters have been chosen such that a wide variety of applications can be served without changing any of them. Furthermore, built-in intelligence of the Wireless Network Controllers allows automatic and real-time adaptation of the LogiSphere system to configuration changes like addition or removal of system components. However, the versatility of LogiSphere also allows the configuration of system parameters in Intelligent Tags, Sensor Terminals and Wireless Network Controllers, a detailed description of which is provided in this document

2 Wireless Network Controller

2.1 WNC Product Description

Please refer to the WNC Product Leaflets for a summary of all technical parameters. The Wireless Network Controller is the base station in a LogiSphere configuration. The WNC's main purpose is to report information obtained from Tags and Sensor Terminals. This information can be related to proximity as well as to telemetry. The WNC supports various input and output protocols and filtering techniques.

2.1.1 Telemetry and proximity information

The WNC processes packets from all Intelligent Tags and Sensor Terminals within its reach. In full HBL100 mode, the configuration of the filtering mechanism determines the WNC behaviour with respect to telemetry and proximity information. The types of packets received from Intelligent Tags are:

- Identifier (received from both Intelligent Tags and Sensor Terminals), used for in-range and out-of-range information. Also referred to as Beacon packets.
- Telemetry data (e.g. temperature, motion, contact information, or telemetry data obtained via an external sensor to the Sensor Terminal)
- Auxiliary information from Intelligent Tags and Sensor Terminals (e.g. signal power levels, battery status).

The tracing and telemetry information can be transferred in the following ways, depending on the parameter settings of the WNC:

- The data can be utilised to control and/or trigger internal devices in the WNC (LEDs, auxiliary open collector output) or the data can be filtered and stored in the WNC's internal logging area. A maximum of 5000 range and telemetry entries can be stored in this logging area.
- Direct reporting to a windows-based platform that is connected to the WNC via the RS232 serial interface. In this configuration the WNC acts as so-called *Master* in a network of (one or a multitude of) WNCs.
- To an adjacent WNC; in this way, a WNC network can be built exactly to the size and shape of the area that needs to be monitored and controlled. In this case the WNC acts as a so-called *Slave* in a network of WNCs. A special role exists for mobile Slaves that are used as end-nodes in several different LogiSphere Networks and do not provide further routing of data; this role is called *Nomad*. Please refer to the section on inter-WNC communication for the role of Nomads in a LogiSphere network.

In order for WNCs to communicate they need to be placed within 300 m of each other (for non-line of sight communication this distance is shorter, depending on obstacles; rule of thumb is that a regular brick wall represents 50 m reach). It is also possible for WNCs to communicate in a wired manner via their serial port(s).

The read range of a WNC can be configured from several centimetres to as much as 300 m; the read ranges for Beacon packets and telemetry packets can be configured independently from each other. In this way, the information on whether an Intelligent Tag or Sensor Terminal is within or out of a certain area (so-called “hot-spot”) can be treated completely separate from the reception of its telemetry data.

2.1.2 Filtering

The HBL100 features an advanced filtering mechanism that provides the possibility to process Beacon and telemetry packets from Intelligent Tags and Sensor Terminals in any desired way. All filter settings are stored in non-volatile memory and are restored after a power cycle.

2.1.3 Output rendering

After a packet has successfully passed all filtering stages (i.e. there is a match, the minimum RSSI value is received and, if applicable, a delta is detected), the packet is transferred to WNC output. The following output rendering options are possible:

- Make up a Report. In case the WNC has been configured as a slave in a WNC network (via *set* 02 2), this report is sent (via RF or the serial port(s)) to the designated master. In case the WNC is Master in a WNC network (via *set* 02 1), the report is sent via the serial port to the computer connected. Please refer to the section on WNC reports for details. In case the WNC has been set out for logging (via *set* 20 1), the report is stored in the WNC's logging area. Please refer to the section on logging for details.
- Control the auxiliary output. The WNC provides an electrical output that can be used to switch external equipment (like controllers, electric gates, etc), or to provide sounds.
- Both of the above

2.1.4 Auxiliary output control

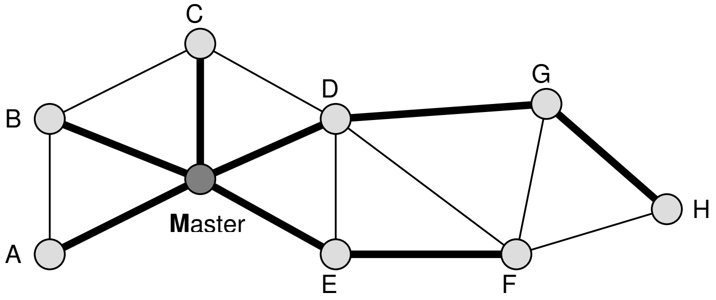
The WNC provides an electrical output that can be used to switch external equipment (like controllers, electric gates, etc), or to provide sound waves to audible devices. It can be used in manual mode (via *set* 1D 0), in which case open/close can only be controlled via the serial link (*set* 17 1 is close, *set* 17 0 is open). If register 1D is set to 4, pulsed control of the open collector output is established: the open collector output will provide a square wave with an amount of pulses as specified in the *set 17* command (0 to 65535).

The Auxiliary output can be set in sound mode (via *set 1D 1*). It this mode, it provides a sound wave to an external speaker. An in-range report results in a high-pitched sound, an out-of-range report results in a low-pitched sound, and a Telemetry report results in a medium-pitched sound.

When the Auxiliary port is set to switch mode (via *set 1D 2*) it can be triggered via a Beacon or Telemetry report using delta processing. In that case, a report is converted to an "auxiliary port state request". By default, the Auxiliary port is not activated. The WNC can be configured in such a way that when a Tag comes In-Range or In-Bound, the port is triggered to be activated. When the Tag goes Out-of-Range or Out-of-Bound, the port is triggered to be deactivated. The Auxiliary port will be activated as long as more activation triggers than deactivation triggers were received.

2.1.5 Routing

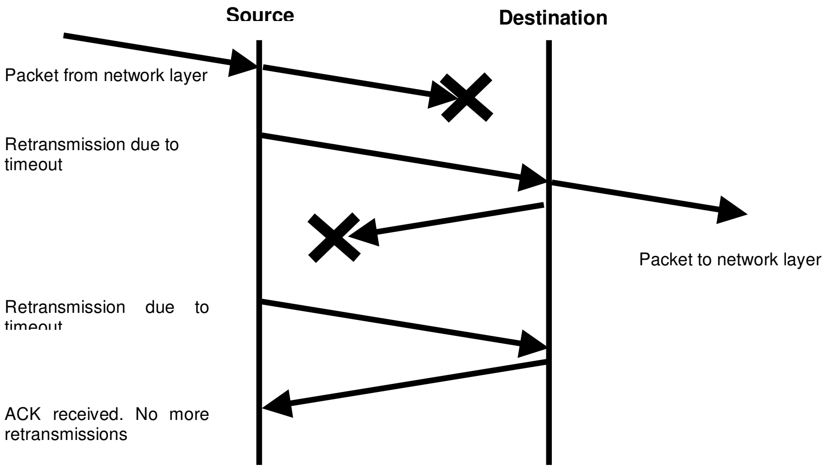
WNCs are capable of wireless communication with each other, both through RF (default) and wired via the serial port(s)). This allows WNC to send range and telemetry reports to another WNC. One WNC can be designated the *Master* which is connected to a computer. Other WNCs are configured so that they will send their reports to the master. These WNCs are called S*laves*. If a slave cannot communicate with the master directly, other intermediate slave WNCs (with a maximum of 15) can be used to forward the reports via an intelligent routing mechanism, as depicted below.



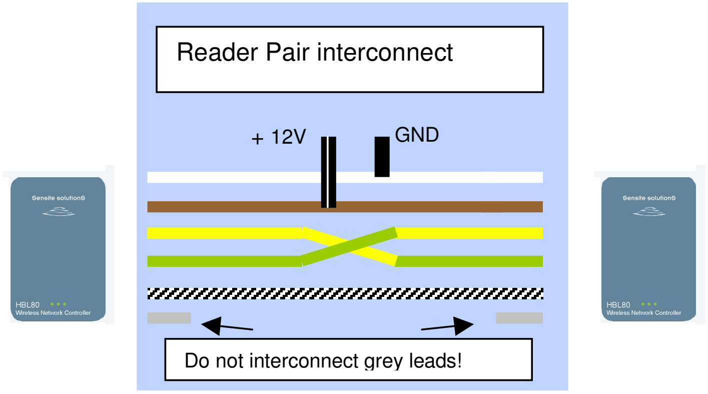
In this figure each circle represents a WNC. One WNC is configured to be the master. All other WNCs are configured to be slaves. All lines represent a possible communication path between <u>two</u> adjacent WNCs directly. The thick lines show which paths will actually be used in Inter WNC communication. So if WNC H sends a report to the master, WNCs G and D will be used as intermediate WNCs.

When the master is to send a command to WNC H then WNC H is called the *Network Destination*. The master looks for WNC H in its routing table and finds WNC D as H's *gateway*. The master will send a report to D containing information that it is addressed to WNC H. On reception of the report WNC D will see that the report is not intended for D itself. WNC D's own routing table dictates that it should send the report to WNC G. Finally, WNC G will send the report to WNC H. WNC H has now received the command that the master sent.
By default, management of routing tables and adding WNCs to a LogiSphere network is done in a <u>static</u> way, i.e. via *radd*, *rdel* and *rclear* commands. It is also possible for LogiSphere networks to build up and tear down components, routes, and connections in a <u>dynamic</u> way.

The communication protocol between WNCs features an acknowledgement mechanism to ensure that messages are properly received. The picture below illustrates the communication between two adjacent WNC's in a situation where first the original packet is mutilated, followed by a mutilation of the eventual acknowledgement.


Source
Destination
Packet from network layer
Retransmission due to timeout
Packet to network layer
Retransmission due to timeout
ACK received. No more retransmissions

In case an RF blockage between two WNC-hops exists (like concrete walls or ceilings between readers, or in the situation that a reader (network) inside a building is to be connected to a reader (network) outside the building), it is possible for the WNCs to communicate in a wired mode via the RS232 port(s). Selecting one of the two RS232 ports of the WNC as communication medium can be achieved by adding a "1" or a "2" to the associated entry in the routing table. (Refer to the commands on routing for details). Please note that only serial port 1 is accessible through the standard WNC cable. For access to serial port 2, a different cabling arrangement is required.
The Rx and Tx lines of the serial ports of the adjacent WNCs need to be crossed. Any of the serial ports of the destination WNC can be used; the WNC detects any traffic, either received from RF, port1 or port 2). As an example, the interconnection scheme for WNC-pairs communicating via their standard serial ports is provided below:


Reader Pair interconnect
+ 12V
GND
Do not interconnect grey leads!
Sensite solutionS
HBL80
Wireless Network Controller
Sensite solutionS
HBL80
Wireless Network Controller

Note that, as the Master in a LogiSphere network utilises serial port 1, it is not possible to configure this port for inter-WNC traffic.

2.1.6 Logging

The WNC supports logging of reports into its internal memory. All telemetry, in- and out-of-range reports are logged. A log entry contains the report including the time (in seconds since the last reboot of the WNC) that the report was added to the log. In order to translate this timestamp into real time, the WNC time since last reboot can be interrogated via the *get 18* command. Each log entry contains the time relative to this value. Logging can be enabled/disabled via the *set* command;

The log contains log entries that all take up the same amount of memory. The size of a log entry can be configured. So when a log entry size is chosen, it limits the maximum number of entries the log can contain. Choose the size such that the largest required logging report will fit.

Telemetry reports have a variable size and are the largest report. Most have only 1 or 2 bytes of data. The table below shows the numbers of log entries as a function of the maximum bytes of data allowed in a logged telemetry report.

Max size of data in telemetry report	Amount of log entries
1	5450
2	5031
4	4360
8	3442
16	2422
20	2109

A telemetry report is not logged when it does not fit in a log entry.

2.1.7 Power management

In order to save the WNC's power consumption, the WNC supports a couple of power saving modes. The following table shows the various levels of power save modes:

Power saving mode	Description
0	No power saving. Full feature support.
1	Like mode 0 but all LEDs are turned off. (reduces power consumption with 8%)
2	To be implemented
3	Like mode 1 but with co-processor and RF transceiver turned off. (reduces power consumption with 60%)

The power saving mode can be changed via register 1E. The power saving mode is remembered during a power cycle or reboot. Power saving modes can always be modified through the RS232 link. Changing modes when in power save mode 3 is not possible via RF communication.

2.1.8 Software upgrades

The WNC contains two processors, a main processor and a coprocessor, each with their own dedicated embedded software version. The current versions of main processor and coprocessor software can be interrogated via the *get 00* command.

The software in both main processor and coprocessor can be upgraded, either via the RS232 serial interface, or wirelessly, via inter-WNC upgrades. Upgrades are provided by Sensite Solutions as stand-alone packages, via e-mail, or via the customer-specific portal on the website. This package, called Software Upgrader is an executable file containing software images for both processors. This ensures a compatible combination of software images. The user should take care that both images are loaded successfully.

The bootloader software download is the fastest way. The new software will be transferred to the WNC in a binary stream and will typically take less than 1 minute. The bootloader is an embedded WNC module that is executed upon a reboot or power cycle. So for bootloader software download, the WNC must be rebooted and will temporarily stop its standard functions during software download.

The console software download is considerably slower. In this case the software will be transferred to the WNC via terminal commands and is ASCII based. Advantage is that the WNC operates normally during software download. However, the WNC must be rebooted after the download via the *reboot* command. Do not use a power cycle for this as the new software is placed in volatile memory. Upon reboot, the software will be programmed and will take a few seconds before normal operation resumes. Another advantage of the console software download is the remote support. A remote WNC can be upgraded via the RF link. A console software download may take up to 30 minutes depending on the size of the software images and the RF link quality.

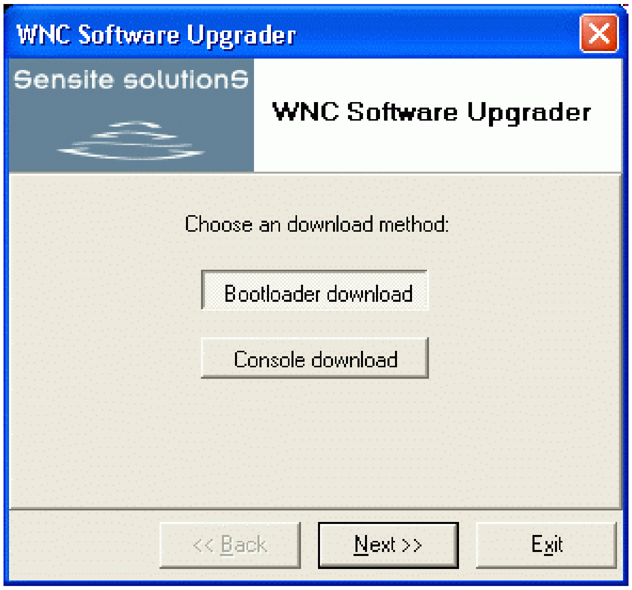
When the RS232 lines and the power lines are accessible, bootloader software download is recommended. Use console software download when a remote WNC needs to be upgraded or when a power cycle is not possible.

2.1.8.1 Bootloader software upgrade

For a bootloader software upgrade, the following steps are taken:

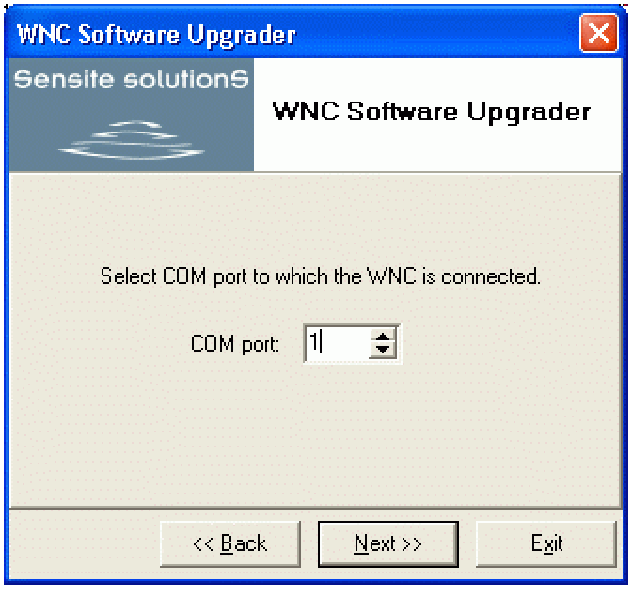
1. Connect a WNC to a free COM port of the computer that has access to the Software Upgrader. Close the programs potentially using the COM port (such as terminals) in order to make sure that the com port is not in use by other programs.

2. Start the Software Upgrader. The following screen is shown:



Choose an download method:

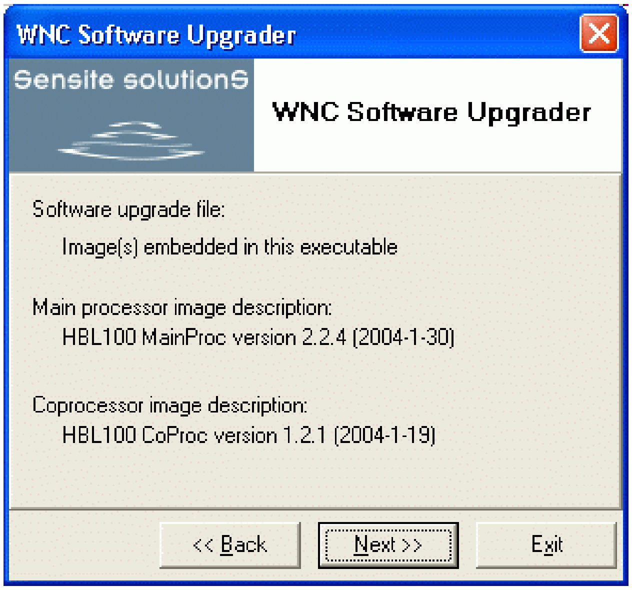
3. Choose Bootloader download as software download method and click “Next”. The following screen is shown:



Select COM port to which the WNC is connected.

COM port: 1

4. Select the correct COM port and click "Next". In the following screen, the version of the images are displayed:

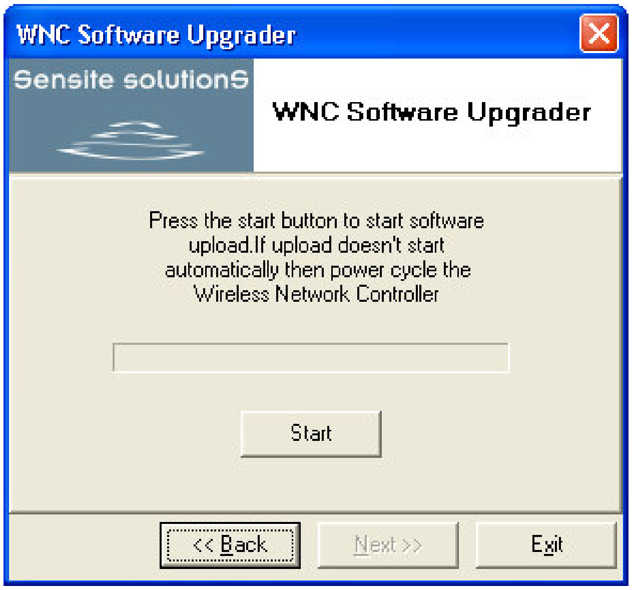


Software upgrade file:
Image(s) embedded in this executable

Main processor image description:
HBL100 MainProc version 2.2.4 (2004-1-30)

Coprocessor image description:
HBL100 CoProc version 1.2.1 (2004-1-19)

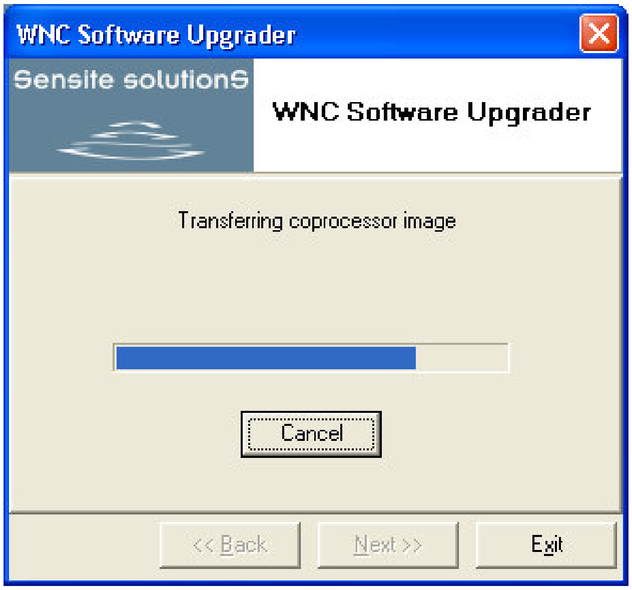
5. Click "Next" if these versions are to be downloaded in the WNC. The following screen is shown:



Press the start button to start software upload.If upload doesn't start automatically then power cycle the Wireless Network Controller

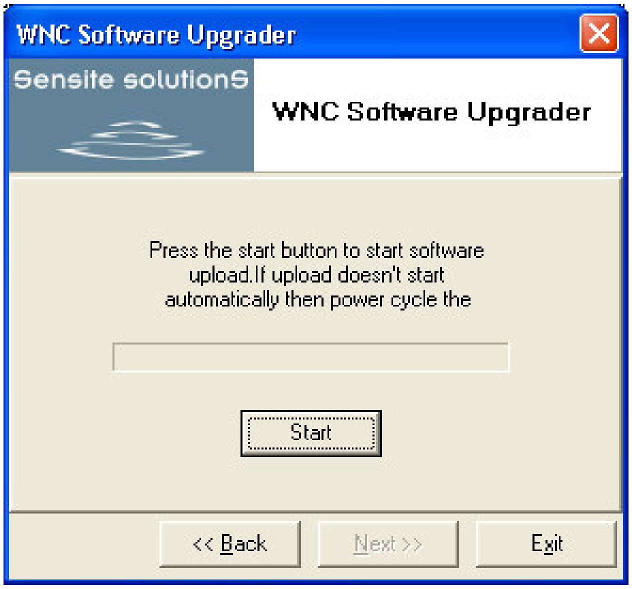
6. Click "Start". Depending on the existing software versions in the WNC the upload will start automatically, or the WNC needs to be power-cycled.

Progress of the coprocessor software upgrade is shown in the progress bar:



Transferring coprocessor image

After the co-processor software upgrade has finished successfully, the following screen is shown:



Press the start button to start software upload.If upload doesn't start automatically then power cycle the

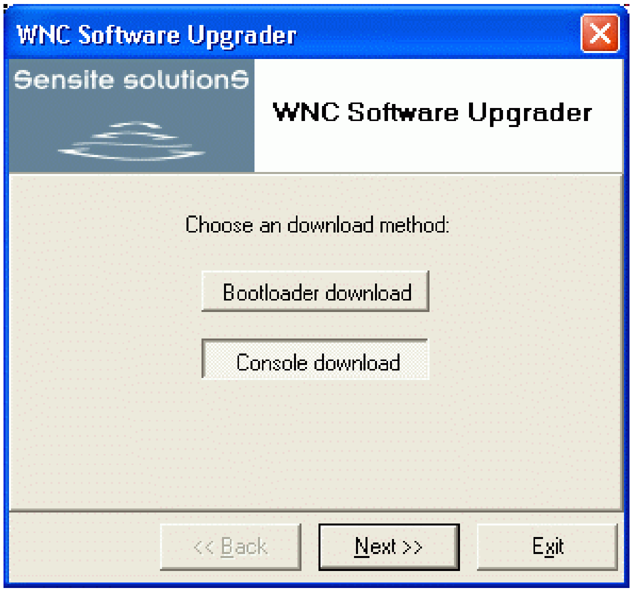
7. Click "Start". Depending on the existing software versions in the WNC the upload will start automatically, or the WNC needs to be power-cycled. Wait until the main processor software upgrade download has finished. If the message 'failed' pops up, re-start from step 1.
8. The WNC is now operational and running the new software versions. This can be verified via the *get 00* command.

2.1.8.2 Console software upgrade

For a console software upgrade, the following steps are taken:

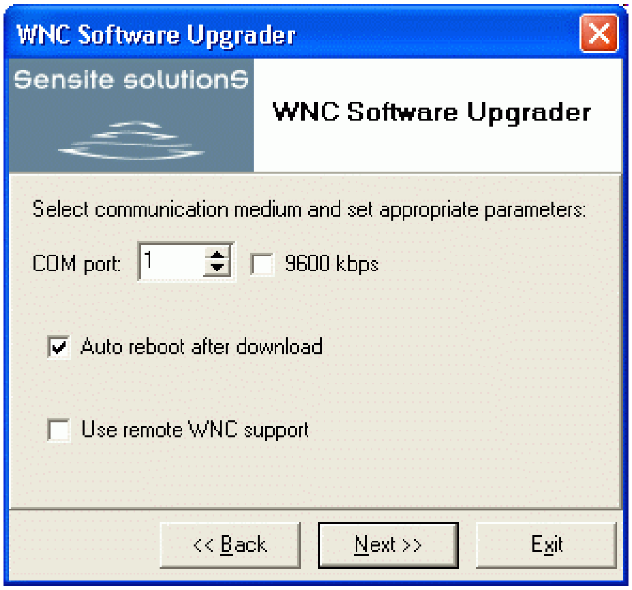
1. Connect a WNC to a free COM port of the computer that has access to the Software Upgrader. Close the programs potentially using the COM port (such as terminals) in order to make sure that the com port is not in use by other programs.

2. Start the Software Upgrader. The following screen is shown:



Choose an download method:

3. Choose Console download as software download method, and click "Next". The following screen is shown:



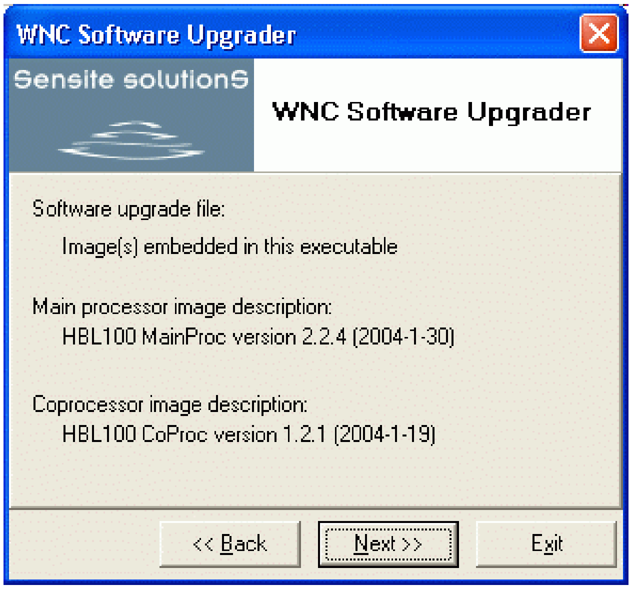
Select communication medium and set appropriate parameters:

COM port: 1 ☐ 9600 kbps

☑ Auto reboot after download

☐ Use remote WNC support

4. Select the correct COM port. Select the 9600 kbps option only if the WNC operates in backward compatibility mode 1 (to be interrogated via the *get 22* command). As a default, the WNC will reboot automatically after the software upgrade process has finished successfully. If this is not desired, un-check the associated box. If a remote WNC needs to be upgraded, enable this by clicking the check box. An additional field is shown where the 6-digit hexadecimal ID of the remote WNC ID is to be filled in. Make sure that the routing tables of both WNCs contain each other's IDs. (Refer to the section on inter-WNC communication for details). Click 'Next". The version of the images will be displayed:

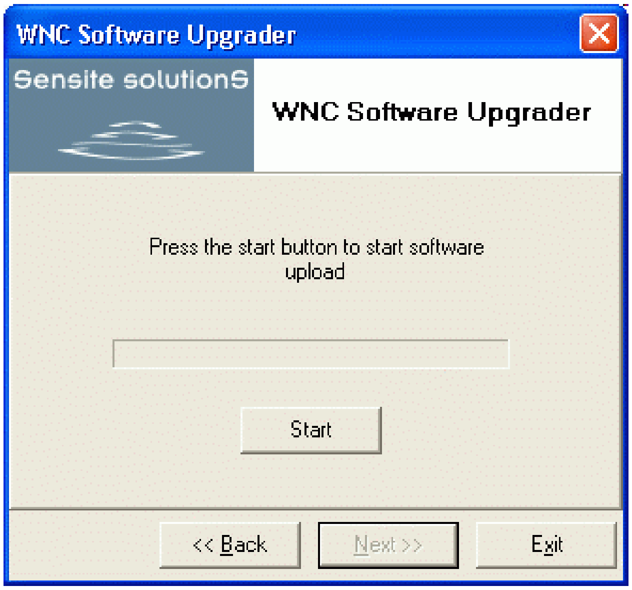


Software upgrade file:
Image(s) embedded in this executable

Main processor image description:
HBL100 MainProc version 2.2.4 (2004-1-30)

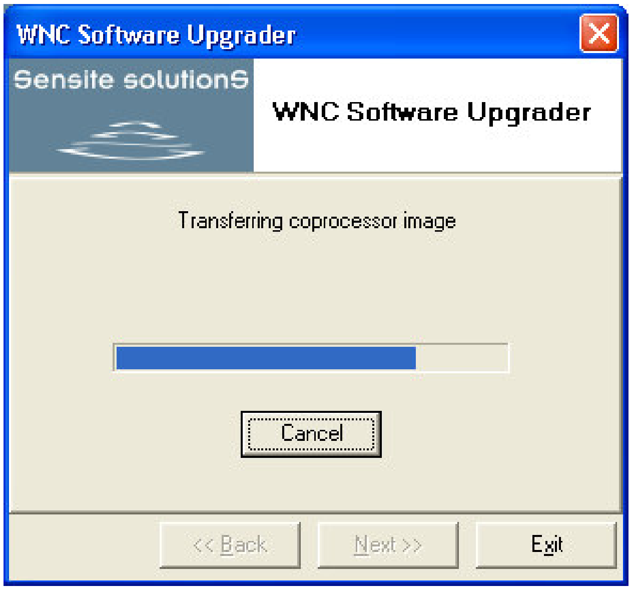
Coprocessor image description:
HBL100 CoProc version 1.2.1 (2004-1-19)

5. Click "Next" if these versions are to be downloaded in the WNC. The following screen is shown:



Press the start button to start software upload

6. Press "Start". Now software images for both main processor and coprocessor will be transferred to the WNC. Progress of the software upgrade is shown in the progress bar:



Transferring coprocessor image

Wait until the transfer is completed. After software upgrade for both processors has finished successfully, both software images are in the WNCs internal volatile memory. Do not power cycle the WNC!

7. As a default, the WNC reboots automatically after a successful software upgrade. If this option has been de-selected in step 4. This reboot is to be issued manually via the *reboot* command. Power is not to be disconnected until 10 seconds after reboot!
9. The WNC is now operational and running the new software versions. This can be verified via the *get 00* command.

2.1.9 WNC Serial terminal communication

The serial interface of the WNC facilitates standard RS232 line with the following configuration:

- 19200 baud
- 8 bits
- no parity
- 1 stop bit
- no flow control

A serial message is defined as the data contained on one line. Messages can be extracted from a serial data stream using the following simple algorithm:

1. Wait for a reception of a CRLF. This identifies the end of a message (of which the data is unknown) and the start of a new message.
2. All data that is now received is part of the current message. The end of the message is encountered when a CRLF is received.
3. Go to action 2.

When the Network Termination Equipment (NTE) is correctly aware of the start and end of messages, the NTE is said to be in *message sync*. The NTE should only lose message sync when errors occur on the physical or MAC communication level.

Messages sent to the WNC have a maximum length of 80 bytes including the CRLF and a minimum of length of 2 (the CRLF). Messages sent by the WNC have a maximum length of 255 bytes including the CRLF and a minimum of length of 4 (the checksum and CRLF).

By default, a checksum is added to all messages sent **by** the WNC (**not** to messages sent **to** the WNC). The checksum is a one-byte straightforward checksum. The checksum is incremented with the ASCII value of the data characters. It is sent after the last data byte and before the CRLF as a two digit hexadecimal number. Example. If the WNC were to send the data “DATA” then the checksum is calculated by adding the ASCII values: 68 + 65 + 84 + 65 = 285. The checksum is 8 bit, so make the checksum modulo 256. 285 mod 256 = 29. Decimal 29 = 0x1D (hexadecimal). So the message would be:

DATA1D↵

(“↵ “ represents the CRLF characters)

The checksum in the WNC message can be suppressed by setting register 33 to 1 with the *set* command

Having a checksum in messages sent **to** the WNC is optional. All messages starting with the ‘*’ character will be checked for a valid checksum. If the checksum is found to be not correct then the message is discarded. The checksum is calculated over the starting ‘* character and the payload behind it. The checksum must be calculated and printed in exactly the same manner as with messages from the WNC (see above).

The WNC/NTE communication consists of exchanging messages at the application level. There are several kinds of messages:

- Command messages. These are messages sent to the WNC by the NTE that instruct the WNC to take a particular action.
- Response messages. These are messages sent by the WNC as a direct (synchronous) response to a command that was issued just before.

- (Negative) Acknowledge messages. These messages are sent by the WNC to the NTE and are the end of the a response:
    - An acknowledge message ('+' <parameters>) tells the NTE that a command has been successfully received and processed. <parameters> contains the parameters that were given behind the command.
    - A negative acknowledge message ('-'<command>) tells the NTE that a command has not been recognized. <command> contains the command that was not recognized.
    - Another negative acknowledge message ('!'<parameters>). With this message the WNC indicates that the given parameters are invalid or that the command could not be executed successfully. <parameters> contains the parameters that were given behind the command.

  When commands are properly sent by the NTE but the WNC responds with a negative acknowledge then the most likely reason for the NACK is that didn't receive the command correctly. The NTE may retry the command and get a positive result.
- Reports. These are the messages sent by the WNC to the NTE at the WNC's own discretion. They contain information of events that the might be of interest for the NTE.

The NTE may have only one outstanding command. This means that no new command can be issued before an (N)ACK message is received of the outstanding command. There is one exception here that will be explained later.

Each command should result in a response by the WNC within 1 second. A response consists of zero or more response messages and is always terminated by a single (N)ACK message. Example:

```
<report message>
          ...
<command message> to WNC
<response message> from WNC
<ACK message> from WNC
          ...
<report message>
<report message>
```

The most likely reason for the WNC not to respond in time is that it didn't receive the CRLF properly, therefore it wasn't aware that the NTE has finished sending the command.

The syntax of commands, responses and reports are provided in the section on WNC command structure.

2.1.10 WNC command structure

This section describes the details of the commands that the WNC accepts. All commands can be provided directly via RS232 or via Inter WNC Communication (using the *remote* command; refer to the set of Generic commands).
Note that parameters in command lines are separated from each other and the command by a single space character.

Command	**factory <operating mode>**
Description	Restores the WNC's non-volatile configuration to its factory defaults. When complete, the WNC will reboot. Note that the execution of this command takes 30 – 60 seconds. The factory configuration of the WNC can be interrogated via the *get* command, (read-only) register 22
Parameters	<operating mode>: "0"/"1"/"2" "0": HBL80 backward compatibility mode "1": HBL80-Navman backward compatibility mode

	“2”: Full HBL100 functionality with advanced filtering If no parameter is provided, default is “0”
Returns	- (a boot report after the reboot) - LEDs in “running light” mode during execution of the command

Command	**reboot**
Description	Reboots the WNC
Parameters	-
Returns	- (a boot report after the reboot) - All LEDs on during execution of the command

Command	**remote** <Remote WNC ID> <Command...>
Description	Executes a command on a remote WNC. The command is send to the remote WNC via Inter WNC Communication.
Parameters	<Remote WNC ID>: The 6 digit hexadecimal identification of the remote WNC. WNC ID “FFFFFF” denotes the broadcast address and should not be used in order to prevent unexpected behaviour of WNCs in reach. <Command...>: The command including parameters to be executed on the remote WNC. Note that for WNCs to communicate, the mutual WNC Ids must be present in their respective routing tables. Refer to the description on the *radd* command for details.
Returns	-
Returns	-

Command	**cancel**
Description	Cancels a WNC command. When a WNC is reporting multiple result lines (e.g. after a “readl” command), it will stop reporting more results. The WNC is now ready to process new commands.
Parameters	-
Returns	-

Command	**ping** <WNC ID>
Description	Ping sends a wireless echo request packet to a remote WNC. The other WNC will respond with a ping reply
Parameters	<WNC ID>: The 6 digit hexadecimal identification of the remote WNC. WNC ID “FFFFFF” denotes the broadcast address (all WNCs in reach)
Returns	- (an asynchronous ping report)

2.2 WNC configuration

The command set as described in the section on the serial interface can be used for both configuration and control of the WNC. Additional WNC Configuration Utilities are provided that provide the possibility to configure all parameters of a WNC, either direct, via the RS232 interface, or remotely via the LogiSphere wireless network.

2.3 WNC Installation

Wireless Network Controllers are installed in the following simple steps:

1. Mount WNC

The WNC can be mounted in any position, using the 4 clamps at the corners on the back. Mount the WNC as high from the ground as possible, preferably above 2 meters. If possible, mount the WNC such that there is a "line-of-sight" between the WNC front and the Transmitting devices. Large metal walls and doors influence the RF behaviour of the WNC. Mounting the WNC with its back flat on a large metal surface generally enhances antenna capability. In all other cases avoid the presence of large metal objects in the vicinity of a WNC as much as possible. The indoor variant needs to be installed at a dry place, within a temperature range of –40 to +60 °C, and a relative humidity range of 0-90% non-condensing.

2. Connect WNC to power

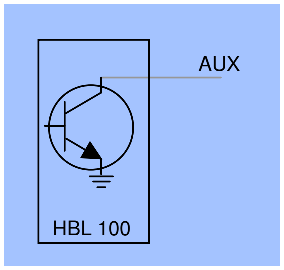
The WNC is powered via 8-30V DC (dissipation max. 370 mW).

3. If applicable, connect WNC to computer

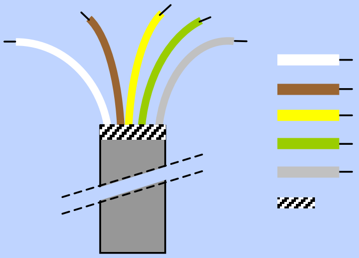
If the WNC is the Master in a wireless LogiSphere network, it is connected to one of the COM-ports of the PC infrastructure via its RS232 interface.

4. If applicable, connect external device to be controlled

The Wireless Network Controller features the possibility to control external devices via an auxiliary, open-collector output on one of its wires, switching to ground. (See schematic). Max. current when closed 2A, and max. voltage when open 30V.



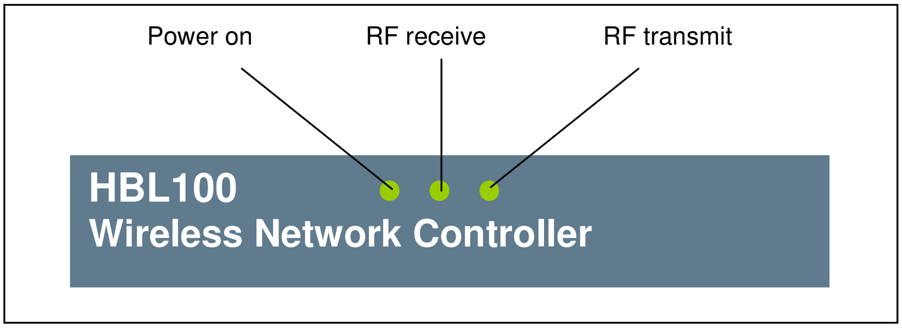
The picture below shows the wiring scheme for the Wireless Network Controller:



White:	Ground (to PC GND, pin 5)
Brown:	+ 5 to + 24V DC
Yellow:	HBL100 RS232 Tx (to PC Rx, pin 2)
Green:	HBL100 RS232 Rx (to PC Tx, pin 3)
Grey:	Aux (open collector, 30V, 2A)
Cable Shielding:	Connect to Ground

For optimal shielding it is recommended to connect the Cable Shielding to Ground.

Proper operation of the WNC can be verified through the PC application, the WNC Configuration utility, and via the three LEDs at the front of the WNC. The default function of the LEDs is described below:



During a reboot, all LEDs are on. During execution of a factory command, the LEDs will be lit one by one, in a "running light" mode.

3 Intelligent Tag

3.1 Intelligent Tag Product Description

Please refer to the Intelligent Tag Product Leaflets for a summary of all technical parameters.

3.1.1 Intelligent Tag types

The Intelligent Tag is the sensor/transmitter in a LogiSphere network and can be attached to any moving object of which location and/or status needs to be monitored.
The list below describes the Intelligent Tag sensor variants:

Type	Sensors
BN208	• Motion sensor
BN215	• High-accuracy temperature sensor • Motion sensor
BN223	• Reed contact
BN283	• High-accuracy humidity sensor

Wireless configuration of Tag parameters can be achieved via the Tag Programmer.

Selected serial numbers of BN208 and BN215 types of Intelligent Tags have been certified to conform to Directive 94/9/EC, which implies that they can be used in potentially explosive atmospheres caused by gases, vapors, or mists. Please refer to the section on Intelligent Tag Installation for all relevant details on safe deployment, use, mounting and un-mounting, maintenance, installation and configuration of these certified Intelligent Tags.

3.1.2 Intelligent Tag packets

The Intelligent Tag can be configured to transmit (combinations of):

- Beacon packets (transmission of the Intelligent Tags unique identification code; this code can be found in the last 6 hexadecimal digits in its serial number, or read via the Tag Programmer)
- Telemetry packets (Beacon signals, enhanced with information like e.g. temperature, relative humidity, motion, magnetic contact, battery status, customer code)

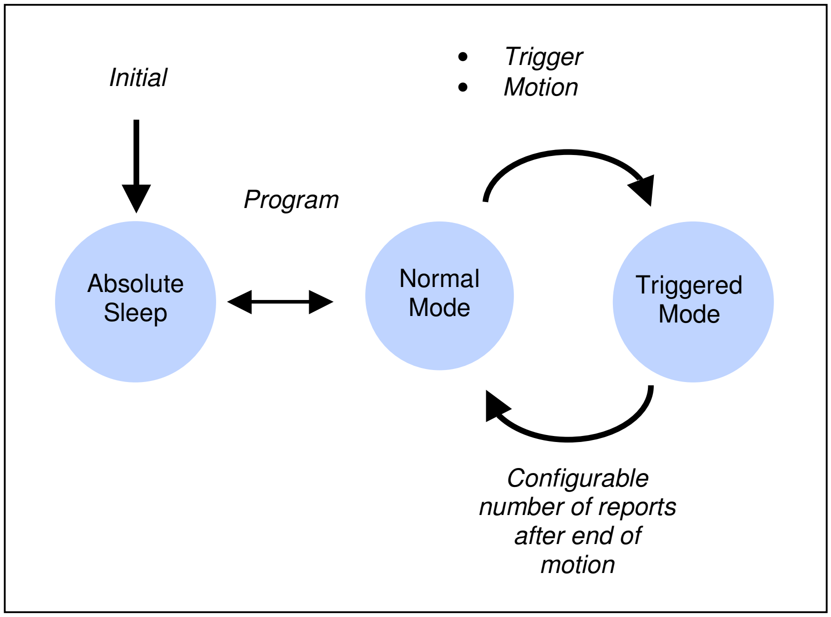
The interpretation by the application of telemetry data from the Intelligent Tag is carried out as follows: Each WNC Report provides, following the WNC ID, Tag ID, and Telemetry Code, a 4-digit hexadecimal report value. Depending on the type of measurement, this report value needs to be converted into the associated physical unit.

3.1.3 Intelligent Tag modes

The Intelligent Tag can be stored or utilized in one of three possible modes:

- **Absolute Sleep**
  In this mode, the Intelligent Tag does not transmit. Extremely low-power mode with an expected battery lifetime >> 15 years.
- **Normal Mode**
  This is the mode the Intelligent Tag is in normal operation. The interval between packets in Normal Mode can be predefined using the Tag Programmer
- **Triggered Mode**
  In this mode, the Intelligent Tag uses different packet intervals. The packets intervals in Triggered Mode can be pre-defined using the Tag Programmer.

The picture below describes possible transitions between the Intelligent Tag modes:

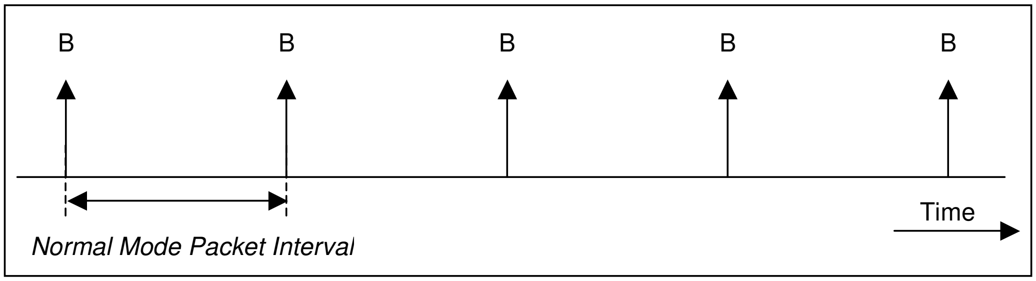


The Intelligent Tag can be programmed to have begin and end of Triggered Mode accompanied by a transmission sequence.

3.1.4 Packet transmissions

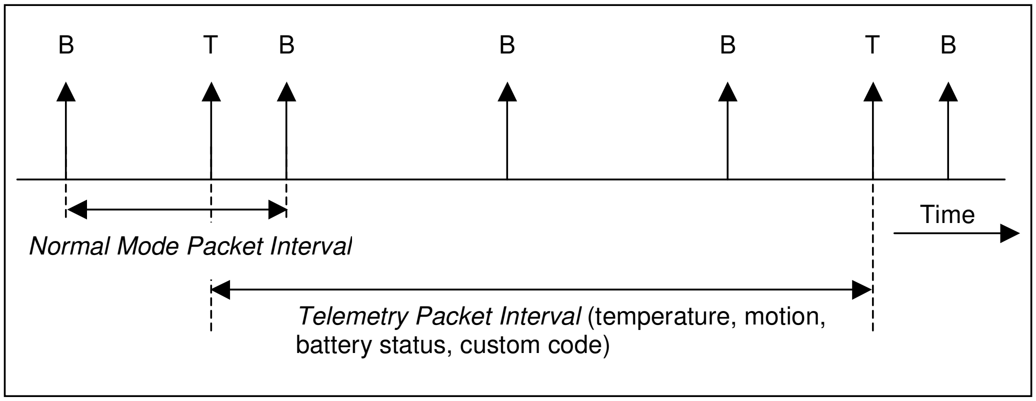
Some examples of the different types and names of Intelligent Tag packets and the associated intervals are provided below. Note that via the settings of the Intelligent Tag, various (combinations of) packets can be achieved. The arrows marked with "B" denote Beacon packets, those with "T" denote telemetry packets (e.g. temperature, motion, etc.), and those with "P" denote any packet (this can be a Beacon Packet or a telemetry packet associated with motion or magnetic contact). Text in *italics* denote parameters that can be programmed into the Intelligent Tag.

Example 1: Beacon packet transmissions only:



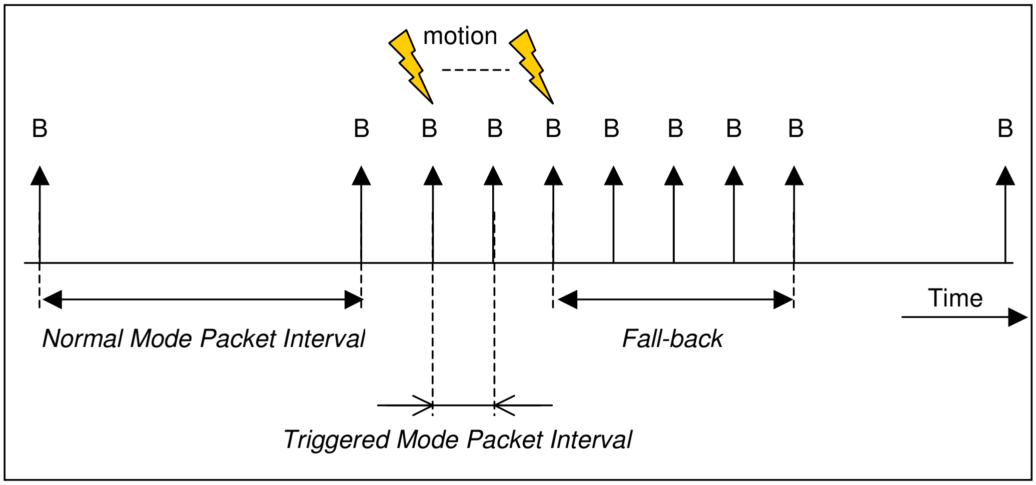
In its simplest configuration, the Intelligent Tag sends Beacon packets, with its unique 3-byte identification code, at regular intervals. This Normal Mode Packet Interval can be set from 1 sec to 18 hours in 1 sec steps.

Example 2: Both Beacon packets and telemetry packets:


B
T
B
B
B
T
B
Time
Normal Mode Packet Interval
Telemetry Packet Interval (temperature, motion, battery status, custom code)

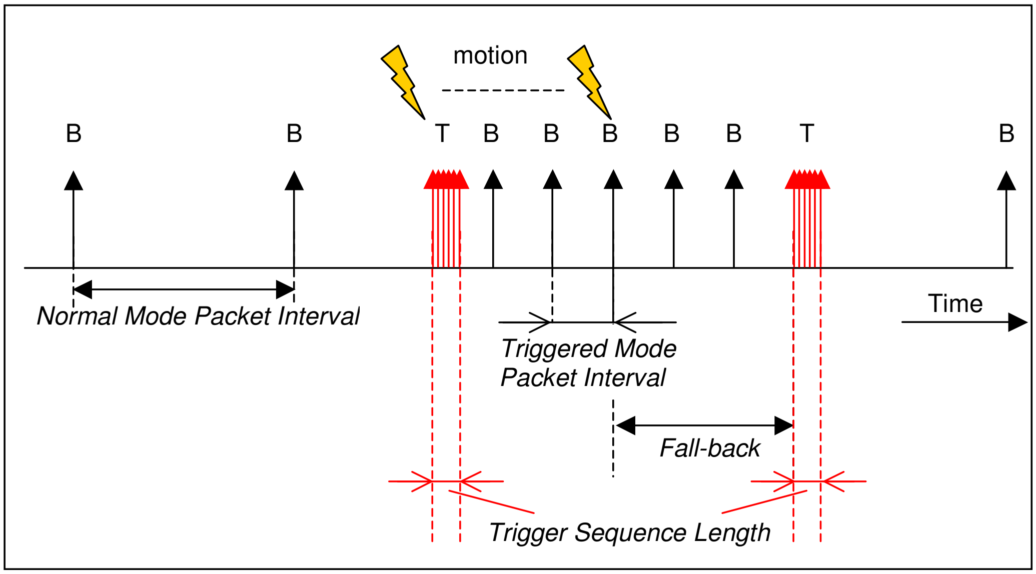
Next to Beacon Signal transmissions, the Intelligent Tag can be set to transmit telemetry packets at their own pre-defined pace. Telemetry packets include high-accuracy temperature, begin- and end-of motion indication, continuous motion indication and magnetic contact information. In addition and if desired, a customer-defined, 2-byte code can also be sent as a telemetry Packet. In order to maintain information on the battery status of the Intelligent Tag, a battery status packet with a predefined interval can be enabled.

Example 3: Normal Mode and Triggered Mode (upon motion)



The Intelligent Tag is equipped with a motion sensor that can be used for e.g. security purposes and for efficient battery use. A sample Intelligent Tag configuration that utilises the motion sensor for transition from Normal Mode to Triggered Mode is depicted above. The Intelligent Tag can be configured to enter Triggered Mode upon motion, resulting in a Triggered Mode Packet Interval that can be programmed into the Intelligent Tag. The Triggered Mode is lifted after a configurable amount of packets after end of motion (so-called Fall-back). Triggered Mode is re-triggerable, i.e. if during the Fall-back period a motion is detected again, Fall-back timing restarts. Triggered Mode is only applicable to telemetry packets associated with motion and **not** to temperature, custom code and battery status packets.

Example 4: Beacon packets in Normal Mode and in Triggered Mode, with Motion and End-of-Motion trigger packets



In the example above, beside a transition to Triggered Mode, an additional sequence of Telemetry packets is sent at the beginning of motion and after Fall-back. The packet sent is of type “Begin-of-Motion” at the beginning of the transition and of type “End-of-Motion” after Fall-back. In order to ensure that the transition packets are received properly, a configurable amount of these packets are sent. (Trigger Sequence Length).
In case of magnetic (door) sensors it is also possible to have the Intelligent Tag transmit its contact status in the Beacon packet for continuous monitoring.

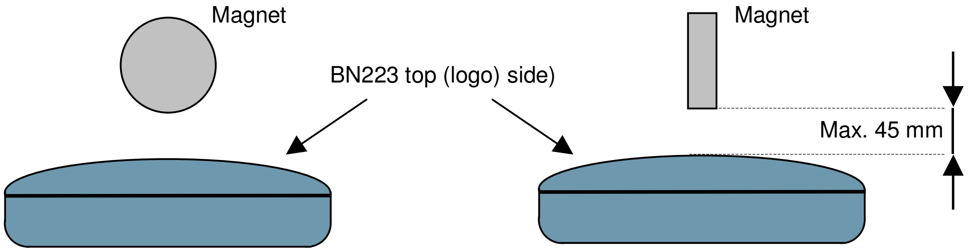
3.2 Intelligent Tag Configuration

During production, the Intelligent Tag is provided with default values of all its parameters. Depending on the nature of the application and the requirements with respect to battery lifetime, these parameters can be modified for optimal Intelligent Tag behaviour. Re-programming of Intelligent Tags can be established via the BCT 50 Tag Programmer.

3.3 Intelligent Tag installation

The Intelligent Tag allows for a wide variety in mounting possibilities. However, the following precautions are recommended:

- Do not mount Intelligent Tags closer than 10 cm above ground. In general, the higher the mounting above ground, the better
- If mounted on a metal surface, make sure the Intelligent Tags mounted at least 2 cm above such a surface
- Near proximity (2 cm) of the Tag should only consist of air or light materials for optimal antenna performance
- If possible, mount the Tag such there is a "line-of-sight" between the WNC and the Intelligent Tag
- The BN 223 (used for proximity measurements) is sensitive to magnetic fields from the top (logo-) side of the Tag. The recommended mounting of BN223 and magnet is depicted below; the magnet is to be mounted on the moving part, whilst keeping the BN223 in a steady position.

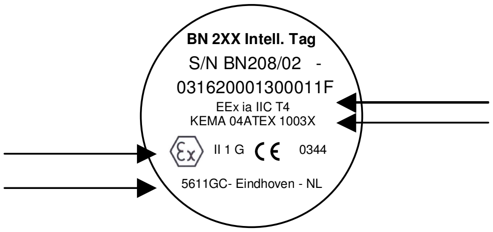


Magnet front view

Magnet side view

- General precautions: Keep magnets separate from all electronic equipment at all times as this may cause damage or malfunction of the equipment. Avoid iron-containing objects in the proximity of magnets. Avoid direct contact of multiple magnets as this may cause damage or injuries due to their unpredictable motions.

Selected serial numbers of BN208 and BN215 types of Intelligent Tags have been certified to conform to Directive 94/9/EC, which implies that they can be used in potentially explosive atmospheres caused by gases, vapors, or mists. The associated Certificate of Conformity Number is KEMA 04ATEX1003 X. The certified Intelligent Tags are marked on the product sticker as shown in the example below:



4 Sensor Terminal

4.1 Sensor Terminal Product Description

4.1.1 Introduction

The ST208 Sensor Terminal turns sensors of any kind and type into wireless devices that can be made part of any LogiSphere telemetry infrastructure in a quick and easy way.

The ST208 accepts open/close information, as well as sensor readings represented by voltage, resistance, or capacitance and transmits this information to any Wireless Network Controller in its vicinity. In this way a virtually unlimited variety of sensors can be combined in a wireless LogiSphere Telemetry network. One of the three analogue inputs (voltage, resistance or capacitance) can be used at the time. The open/close input can be combined with any kind of analogue measurement..

4.1.2 Sensor Terminal packets

The Sensor Terminal can be configured to transmit (combinations of):

- Beacon packets (transmission of the Sensor Terminal's unique identification code; this code can be found in the last 6 hexadecimal digits in its serial number, or read via the Tag Programmer)
- Telemetry packets (data obtained from external sensors providing voltage, resistance, capacitance or contact information)
- Auxiliary packets (power level, battery status, customer code)

Measuring intervals and packet intervals are independent parameters that can be configured individually using the Tag Programmer. In addition, it is possible to define a threshold within the range of the selected measuring unit, above and below which Telemetry packets can be enabled or disabled. Crossing of this threshold can also be marked via a separate telemetry packet. This allows for high measuring rates (the amount of energy required for a measurement is a low as 20% of a regular packet transmission) and low packet rates (heartbeat function) or even reporting above/below threshold only.

4.1.3 Sensor Terminal modes

The Sensor Terminal is stored or used in one of two possible modes:

- **Absolute Sleep**
  In this mode, the Sensor Terminal does not transmit. Extremely low-power mode with an expected battery lifetime >> 15 years.
- **Normal Mode**
  This is the mode the Sensor Terminal is in normal operation. The interval between packets can be predefined using the Tag Programmer. In addition, the pace between Telemetry packets can be made different for Sensor values above and below a pre-defined threshold (threshold definition can be defined using the BCT50 Tag Programmer)

Switching between Absolute Sleep and Normal Mode can be established via the BCT50 Tag Programmer.

4.1.4 Packet transmissions

The Sensor Terminal can be set to transmit Beacon packets and telemetry packets at their own pre-defined pace. Telemetry packets contain a digital representation of the data provided by a sensor external to the Sensor Terminal. As a multitude of physical quantities are accepted (voltage, capacitance, resistance, contact information), a wide variety of external sensors is supported.

In addition and if desired, a customer-defined, 2-byte code can also be sent as a telemetry packet. In order to maintain information on the battery status of the Intelligent Tag, a dedicated Telemetry packet can be enabled.

For all types of external measurements, a threshold can be programmed into the Sensor Terminal, above and below which telemetry packets can be enabled. A dedicated packet that indicates crossing of the threshold can be enabled in the Sensor Terminal.

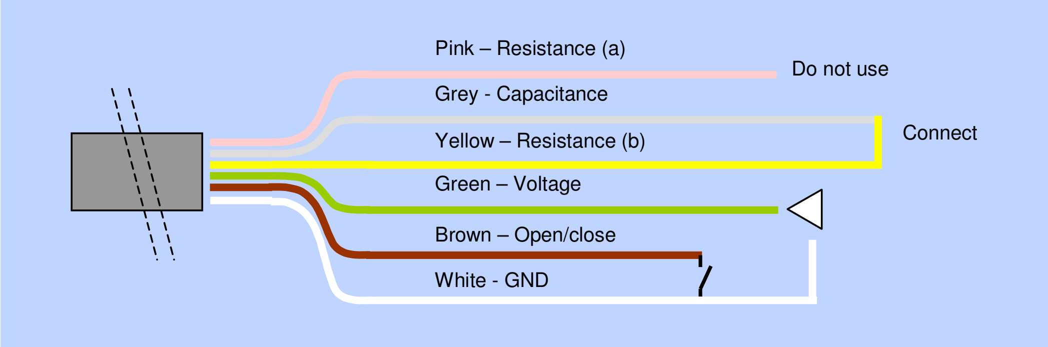
4.2 Sensor Terminal configuration

Please refer to the section on Intelligent Tag configuration for details.

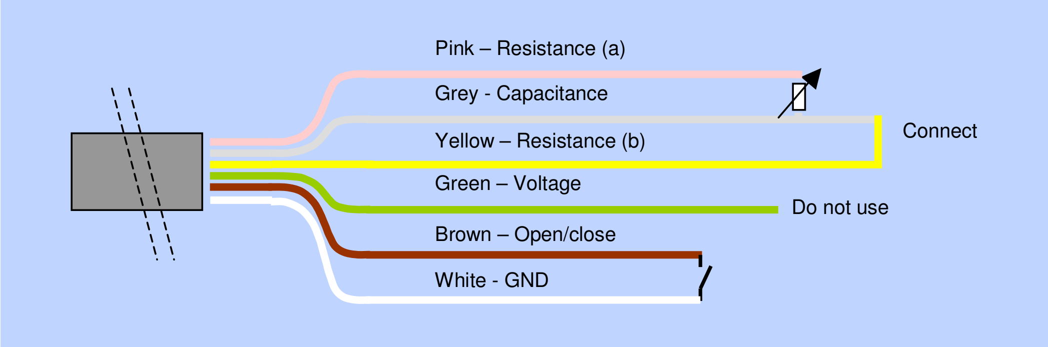
4.3 Sensor Terminal Installation

The Sensor Terminal is capable of measurements with respect to voltage, capacitance, and resistance. In addition, a separate open/close switch lead is provided.
Only one analogue measurment can be utilised at one time. Combination with open/close, however, is always possible.
The connection schemes for the various types of measurements are provided below.

<u>Voltage measurements</u>



<u>Resistance measurement</u>



<u>Capacitance measurements</u>

For capacitance measurements, a dedicated coax cable between sensor and Sensor Terminal is required in order to prevent disturbances from cabling capacitance.

<u>CAUTION: DO NOT CONNECT WIRING OTHERWISE AS SPECIFIED ABOVE</u>