Interface Manual
Gateway-In-A-Stick

SignalFire Number: GWS-CBBL

The SignalFire Gateway-In-A-Stick has the following features:

- RS485 connection to Modbus master device (Optional Modbus-TCP interface module)
- Wide range DC power input: 6-36VDC
- Collects and caches Modbus data from all SignalFire remote devices
- Provides configuration and status registers for remote configuration and status monitoring
- Integrated 500mW FHSS 900MHz ISM band radio and high gain antenna
- Stores up to 4700 register values from any combination of remote nodes
- Supports transparent Modbus mode
- Internal Remote Shut Down (RSD) logic control option
- Slave register re-mapping
- Remote configuration of SignalFire devices through an Ethernet gateway connection
- Remote sensor configuration (PACTware and RadarMaster)
- AES-128 Encryption
- Class 1 Division 2 Area certification

Table of Contents

Specifications 3
Connections and Components 4
Gateway-In-A-Stick Connections 4
Status LED 4
Operation 5
Remote Modbus Sticks and Sentinel-Modbus (non-sleeping radio only) Nodes 5
Remote Modbus Stick Node Re-Scan 5
Setup 6
Optional Ethernet Gateway Connections 6
Encryption 8
Checking Remote Nodes 9
Remote Node Configuration 10
Firmware Upgrades 12
Rescue Gateway (ARM) Bootload 12
Remote Shutdown (RSD) Control 13
RSD Configuration 14
Source Node Section 14
Relay Control Logic Section 15
Destination RSD Stick Section 16
Relay Pulse 16
Example 17
Options 18
RSD Event log 18
Slave Register Remapping 19
Use Data Type Floats 20
Fail Mode 21
Load/Save Files 21
Import/Export CSV Files 21
Output Modules 22
RS485 Details 22
Network Map 22
Gateway Event Log 23
Saving the Gateway Log **Error! Bookmark not defined.**

Modbus Gateway Register Map ____ 24
Discrete Registers ____ 24
Holding Registers ____ 25

3

Specifications

Gateway Size	20.5" overall length. 1.45" diameter
Mounting	¾" Female NPT fitting
Power Source	6-36VDC. 25mA @ 12VDC (average), 17mA @ 24VDC (average)
Temperature Rating	-40°C to +85°C
Radio	902-928MHz ISM Band, FHSS radio. IC and FCC Part 15 certified Integrated 5dBi antenna. FCC ID: W8V-M655, IC: 8373A-M655
Compliance	Certified for use in Class I, Division 2 groups C and D. Certified to CSA C22.2-2015 No. 142, CSA22.2 No. 312213, ISA 12.12.01-2015 and UL916

Gateway-In-A-Stick Connections

The Gateway-In-A-Stick is supplied with a 6 conductor cable. The connections are as follows:

Wire Color	Connection
RED	Positive Power (6 to 36 VDC)
BLACK	Ground
GREEN	RS-485 “A”, 9600 Baud
BROWN	RS-485 “B”, 9600 Baud
ORANGE	RS-232 Debug/Programming TX, 9600 Baud
YELLOW	RS-232 Debug/Programming RX, 9600 Baud

Status LED

The Gateway has one LED Available for field diagnostics.

LED	Description
Slow Flash (3 second pause)	System is running and in communication with radio network
Fast Flash (0.5 second pause)	System is running but no network found
Solid On	System Fault needs service or rescue bootload

Operation

The Gateway-In-A-Stick supports all remote SignalFire nodes making all remote sensor data available in Modbus format.

The register data from remote sensor nodes is available by requesting the remote node's Modbus slave ID and register address from that node's register map. The gateway will respond with the most recent copy of the data from the remote node. The gateway will automatically time-out data from a remote node it stops receiving data for.

If the remote node is a Modbus-Stick interface node additional features are supported.

Remote Modbus Sticks and Sentinel-Modbus (non-sleeping radio only) Nodes

Remote nodes that have been pre-configured forward their set of registers to the Modbus gateway on a pre-defined schedule (1 minute to 5 minutes is typical). The register data is then buffered in the gateway and is available to be read by the RTU at any time.

If a Modbus request is received by the gateway for a Modbus ID and address for which buffered data does not exist, but the Modbus ID is known, the Modbus request will be forwarded to the remote Modbus node over the SignalFire network. The response is returned to the RTU.

If a request for multiple registers is issued by the RTU, and if the gateway does not have all registered data buffered, an exception will be returned. The system will not combine buffered and transparent data within a single Modbus response.

Remote Modbus Stick Node Re-Scan

It is possible to cause a remote Modbus Stick to re-scan for attached Modbus devices by writing to one of the gateway's configuration registers. This is useful to discover a Modbus device that is added to an existing Modbus node. The scan may be initiated by one of the two methods. First, if the radio address of the Modbus Stick is known, writing this address to gateway register 3000 will result in a scan. Second, if the Modbus ID of one of the already registered devices attached to a Modbus Stick is known, a scan will be started by writing the ID to gateway register 3002.

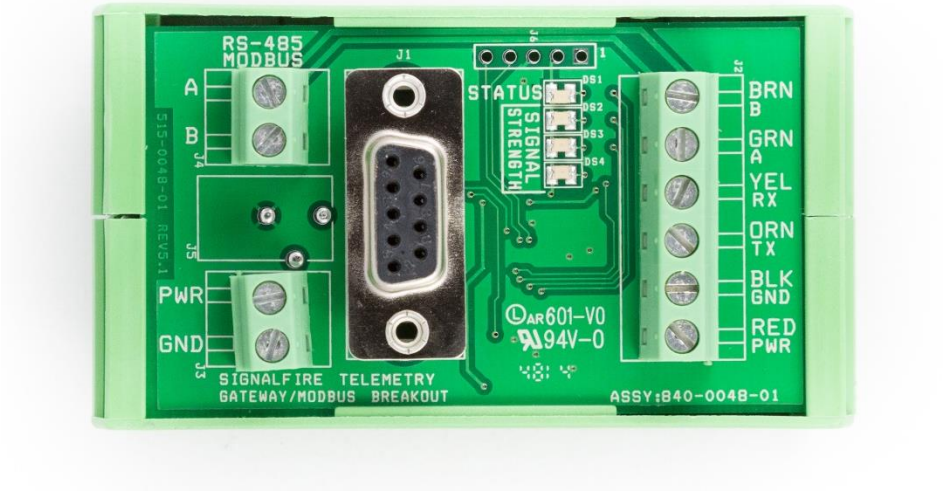
Setup

The Gateway-in-a-Stick requires an initial configuration over RS-232 using the SignalFire Toolkit. Connect a USB-Serial cable (can be purchased from SignalFire) between a computer and the Gateway's DB9 port.

The following items must be configured to set up a SignalFire network:

- Radio Network
- Radio Network Group
- Corporate ID/Encryption Key

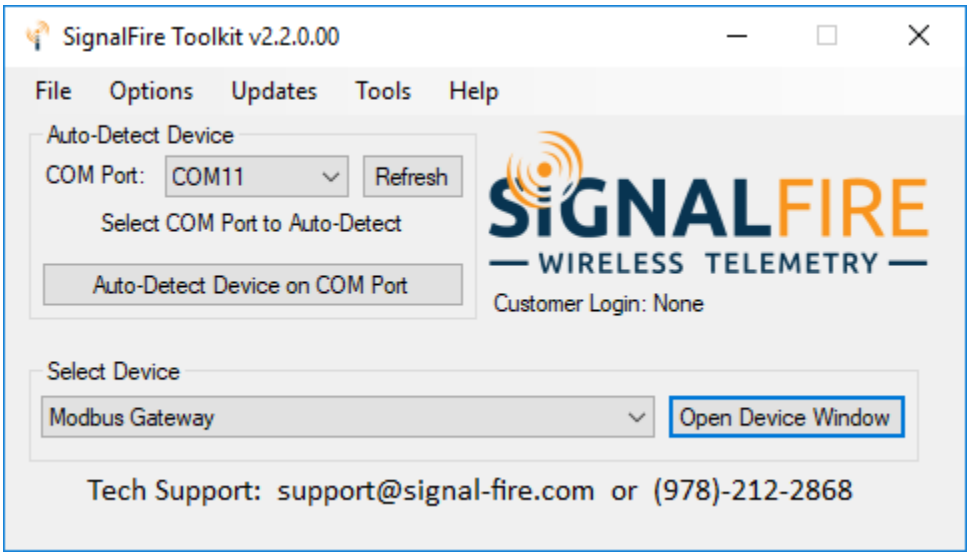
The standard SignalFire Connector-Breakout-Board (CBB), pictured below, provides an easy means to connect to the RS232 lines and power the device while configuring the system. Note that the signal strength LEDs do not light at the gateway as multiple nodes with varying signal strength may be connected at one time.



Optional Ethernet Gateway Connections

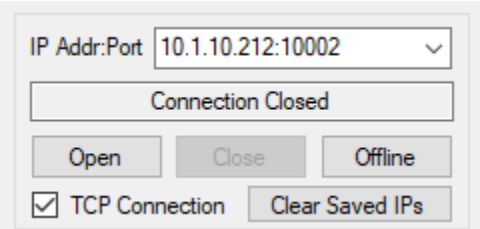
When used with a SignalFire Ethernet Interface Module, the 6 wires should be connected to the color coded "Gateway Stick Connection" connector on the Ethernet Interface Module. Power can be supplied either to the Power Input terminals on the Ethernet Interface Module or via power over Ethernet (PoE). For more information on configuring and using the Ethernet Interface Module, please consult the Ethernet Interface Module manual.

The SignalFire Toolkit application can be downloaded at www.signal-fire.com/customer. After installation, launch the software and the main toolkit window will open:



Select the COM port associated with the Gateway Stick and click "Auto-Detect Device on COM Port." This will open the device configuration window, where all device settings can be configured.

If the Gateway is connected to an Ethernet Module, instead select the Modbus Gateway Stick in the dropdown menu of the main ToolKit window, and click "Open Device Window". In the upper left corner, check off the "TCP Connection" box, type in the IP Address, and click "Open". The port number (10002) will be automatically added, so this is not necessary to enter it.



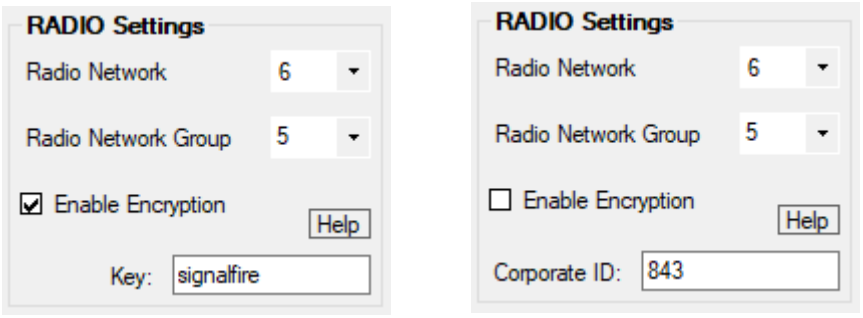
Network Setting

The network is set using the SignalFire Toolkit. There can only be one Gateway per network/group/encryption combination, otherwise they will conflict. In a system with multiple Gateways, each Gateway must be on a separate network/group/encryption combination. **The network, network group, and corporate ID/encryption key settings must match those of its nodes for them to communicate.**

Encryption

To protect your over-the-air data and prevent tampering, SignalFire networks starting with radio version 2.50 and Gateway version 7.93 come with encryption. Legacy products use a Corporate ID, but can be switched over to use an encryption key if the firmware and ToolKit are up to date.

To set up a legacy Gateway to use encryption, click the checkbox labeled **Enable Encryption** inside the **Set Corporate ID** box. All Gateways now default with this option enabled and "signalfire" as the default encryption key.



Radio settings box with and without encryption enabled. For more details, click the Help button.

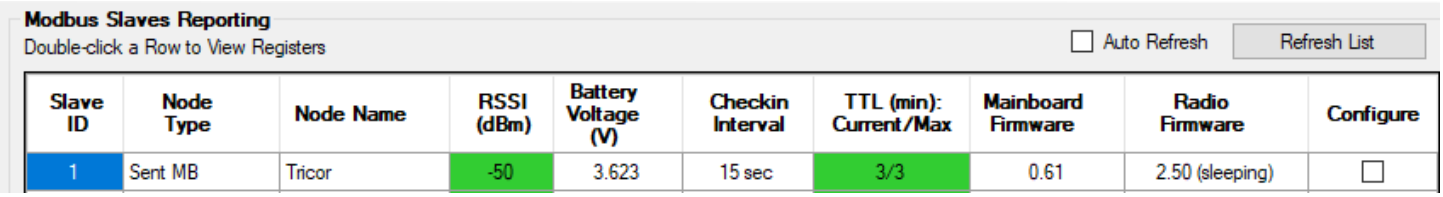
The box will then change into a **Set Encryption Key** box, and it will prompt instead for the encryption key you would like to use. Note that keys may not contain spaces or angle brackets. Enter it and then press **Set**. If you are setting up a new network, you will need to set the encryption key on all of your devices. If you are swapping out the Gateway for a legacy network, you can simply uncheck Enable Encryption and set the Corporate ID, and it will remain compatible with the older system.

It is also possible to hide your encryption key so it cannot be read. This is the most secure option, but if you forget your key, there is no way to recover it – you must reset the key on every device on its network. To enable this option, select **Set Encryption Key Unrecoverable** under the **Settings** menu.

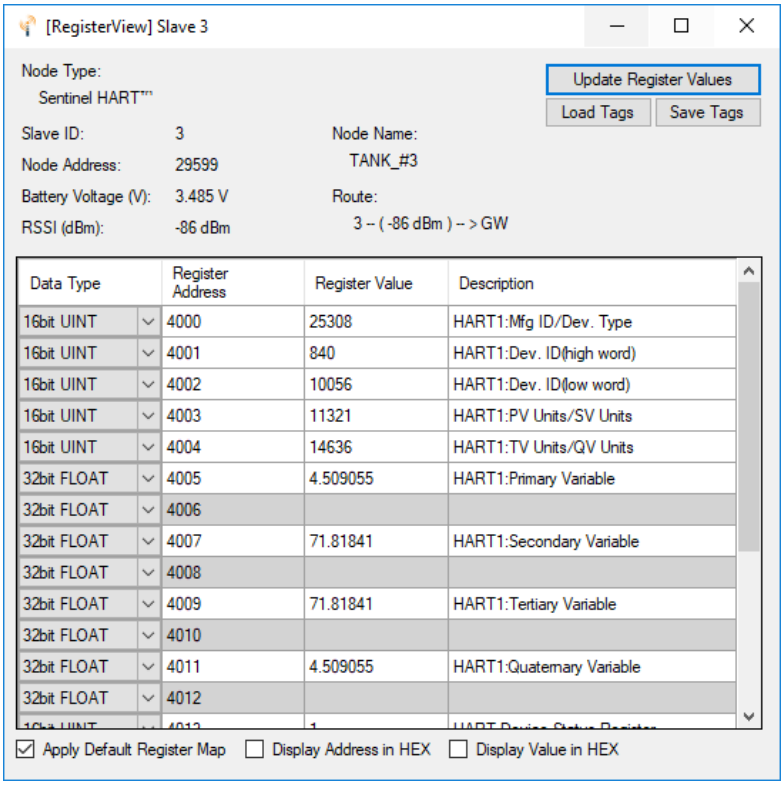
Checking Remote Nodes

If one or more remote nodes are configured with the correct network settings, they will send their data to the gateway. Clicking **Refresh List** will populate the list with all connected remote nodes. The gateway displays the node type, node name (if it has been set), RSSI signal strength, check-in interval, the Time-To-Live (TTL), and the node's radio and main firmware versions.

The RSSI and TTL values are color coded (Green, yellow, orange, red) to indicate relative link quality of a node. The 'TTL Current' indicates the number of minutes remaining until the node will be timed out of the gateway if no updates are received. The 'TTL Max' indicates the maximum TTL for that node and is equal to the node's check-in interval times 5 plus 2. The 'TTL Current' will reset to the 'TTL Max' each time an update is received from that node. The 'TTL Current' will decrement once a minute.



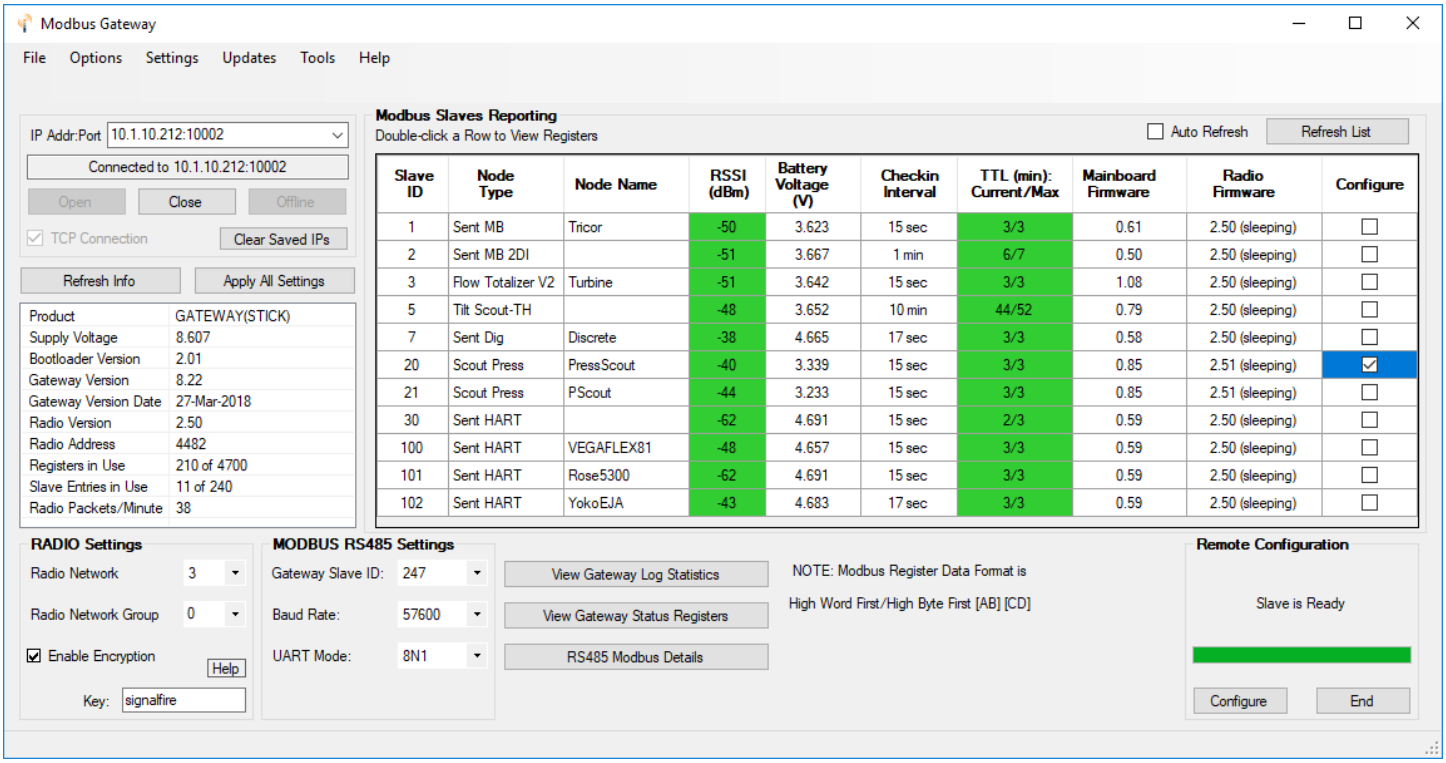
Double clicking on one of the nodes in the list will bring up additional detail including the register data from the remote node.



Remote Node Configuration

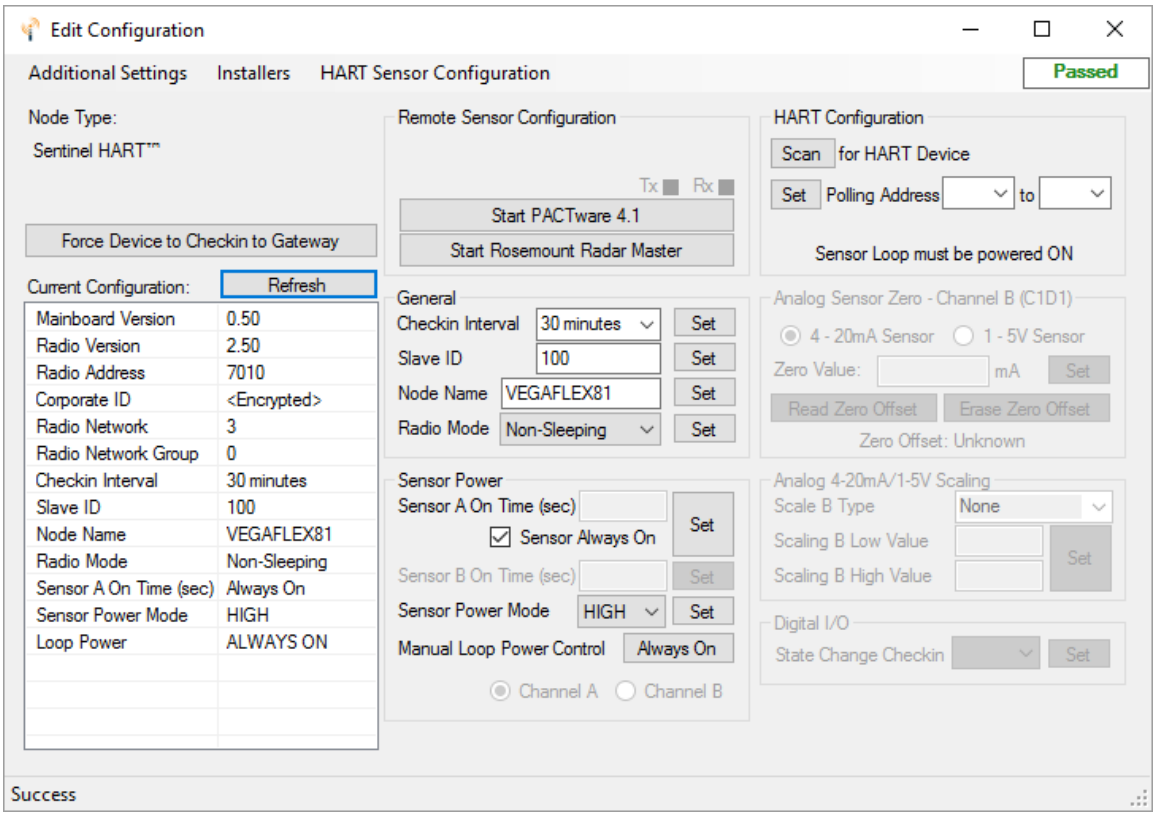
The SignalFire Gateway allows configuration changes to be made to any of the connected SignalFire remote nodes wirelessly. To use this feature, access to the Gateway debug port is required. This may be accessed over a TCP/IP network using a SignalFire Ethernet Gateway module, or by a direct connection to the Gateway RS232 port.

To start a remote configuration session with a remote node, select the check-box next to the node to configure.



If the device has a non-sleeping radio the remote configuration session will be ready immediately. If it is a sleeping device, you must wait for the node to either check-in or send a "beacon" so that it can be commanded to enter configuration mode. The Sentinel/Scout nodes send a beacon every two and a half minutes, while all other sleeping nodes send a beacon every five and a half minutes. When the device has entered a remote configuration session you will see a message indicating the slave is ready. Click **Configure** to open the configuration window (image on next page).

Make any necessary changes and click the corresponding **Set** button to save the changes. When finished with the configuration, close the configuration window and then click the **End** button in the Gateway window to end the session. The session will also automatically time-out after 15 minutes of inactivity and the Node will resume normal operation.



Example Remote Configuration Window

Further information on how to remotely configure a HART device through the ToolKit using PACTware can be found in the "Remote HART Sensor Configuration Manual".

Firmware Upgrades

12

Firmware updates for both the gateway (ARM) and the built-in radio are possible over the RS-232 debug interface using the SignalFire Toolkit, or over a remote TCP connection if an Ethernet Gateway module is used.

Gateway (ARM) Firmware update steps

1. Open the SignalFire Toolkit application.
2. Open the correct COM port connected to the RS-232 port of the gateway.
3. Go to the **Update** menu and select **Update Gateway Firmware**.
4. The latest gateway firmware file will be selected by default.
5. Click **Start Upgrade**.

Gateway Radio Firmware update steps:

1. Open the SignalFire Toolkit application.
2. Open the correct COM port connected to the RS-232 port of the gateway.
3. Go to the **Update** menu and select **Update Radio Firmware.**
4. The latest radio firmware file will be selected by default.
5. Click **Start Upgrade**.

Rescue Gateway (ARM) Bootload

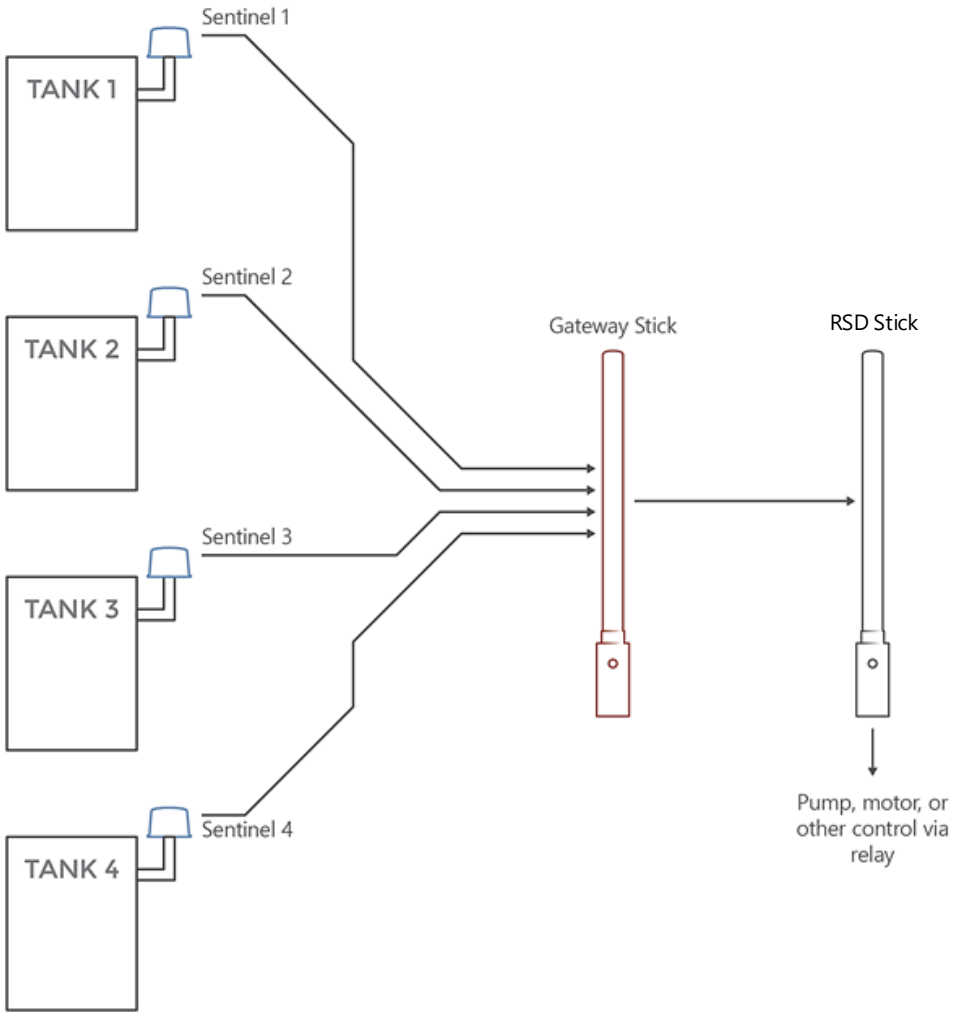
If in the process of a firmware update there is a power failure or other communications failure it may be necessary to do a "rescue bootload." If the base LED is solid on and/or the Toolkit is unable to communicate with the Gateway the following process is necessary.

1. Remove DC power to the Gateway.
2. Open the SignalFire Toolkit application.
3. Open the correct COM port connected to the RS-232 port of the gateway.
4. Go to the **Update** menu and select **Update Gateway Firmware**.
5. The latest gateway firmware file will be selectable by default.
6. Click **Start Upgrade**.
7. Now re-connect the DC power to the gateway. The firmware update process should start. If the firmware update does not start remove power for at least 10 seconds and re-try.

Remote Shutdown (RSD) Control

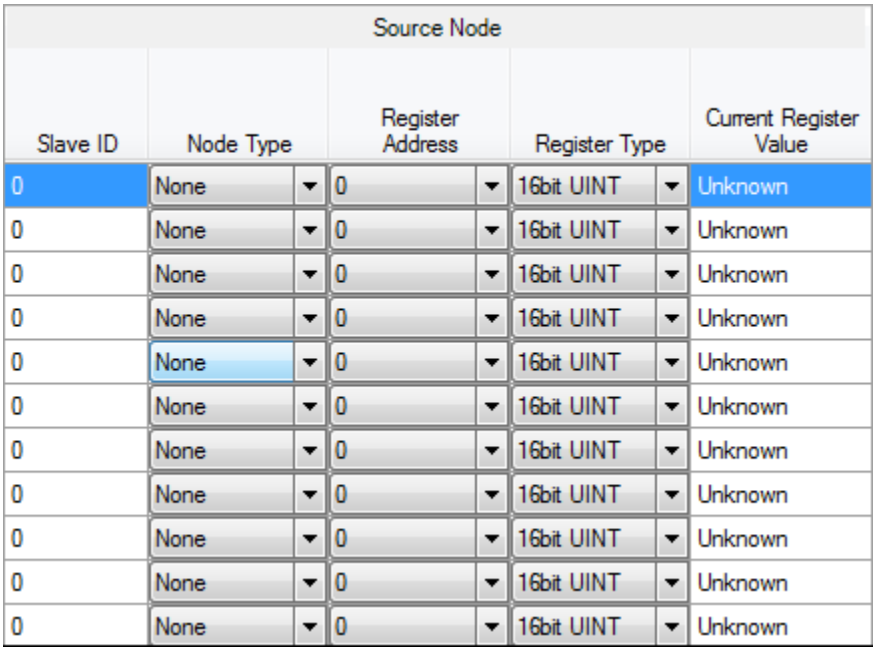
The SignalFire Gateway supports **Internal Logic Control** capability which enables the Gateway to control output relays on SignalFire RSD sticks.

The SignalFire Gateway Stick receives data from multiple remote nodes. It can use the data from those remote nodes to set the relay output on one or more remote RSD sticks. An example of the topology is shown in the following figure:



From the Gateway configuration window within the SignalFire Toolkit, go to the **Settings** menu and select **Remote Shutdown Settings**. This will open the RSD configuration window.

Source Node Section



The source node section is used to select the source register for the logic rule.

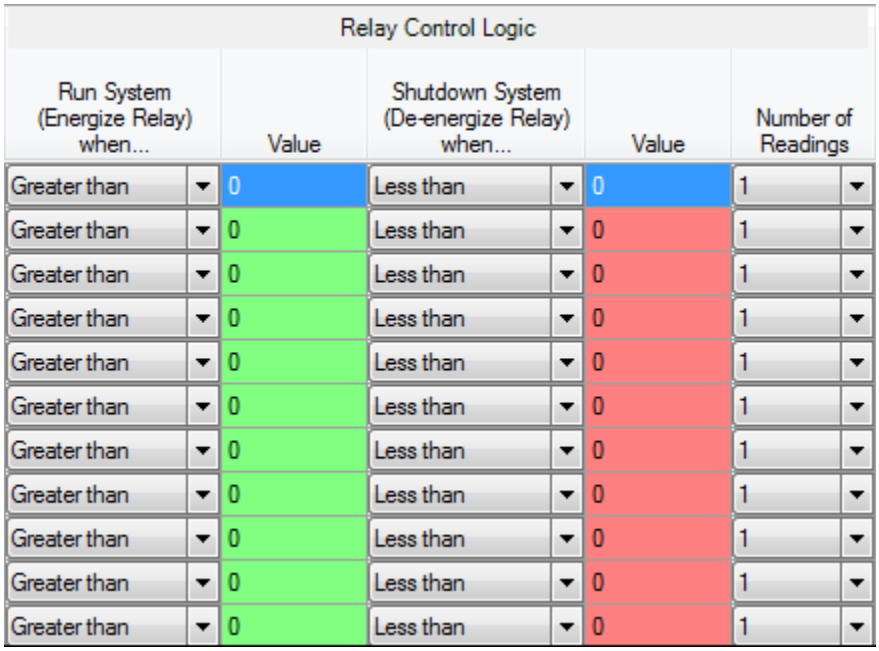
Slave ID – The Modbus Slave ID of the remote source node.

Node Type – Drop-down list of standard SignalFire remote nodes. Select the type of remote node here, or select **Custom** for manual data entry.

Register Address – Select the register address for the data to use for the logic, or manually enter the register address if **Custom** was select for the node type.

Register Type – The correct register data type will automatically be selected unless **Custom** is used. If using a custom register address, select the correct data type here.

Current Register Value – Displays the value of the selected source data register. Clicking the **Update** button will refresh this value.



Relay Control Logic

Run System (Energize Relay) when...	Value	Shutdown System (De-energize Relay) when...	Value	Number of Readings
Greater than	0	Less than	0	1
Greater than	0	Less than	0	1
Greater than	0	Less than	0	1
Greater than	0	Less than	0	1
Greater than	0	Less than	0	1
Greater than	0	Less than	0	1
Greater than	0	Less than	0	1
Greater than	0	Less than	0	1
Greater than	0	Less than	0	1
Greater than	0	Less than	0	1
Greater than	0	Less than	0	1

The relay control logic section is used to set the trigger thresholds for the selected source data register.

Run System (Energize Relay) – Select the logic operand to use for the "energize" logic evaluation.

Value – The value that the relay will be energized. Note that the energized state is the normal "operating" state of the relay.

Shutdown System (De-Energize Relay) – The logic operand to use for the "de-energize" logic evaluation. This will automatically be the opposite of the selection for the energize case. Note that the de-energized state is the SAFE state of the relay.

Value – The value that the relay will be de-energized. Note that the de-energize state is the "safe" state of the relay.

Number of Readings – This field contains the number of check-in packets that must be received in a row that are above (or below) the logic threshold for the de-energize condition. This is useful so that a single (possibly a glitch) reading does not cause a shut-down. The default is 1 where each check-in will cause the rule to be evaluated and acted on. A single reading that satisfies the run system (energize) condition will cause the relay to energize.

Destination Counter/RSD Stick		
Slave ID	Relay Channel	Current Relay State (readonly)
0	1	Unknown
0	1	Unknown
0	1	Unknown
0	1	Unknown
0	1	Unknown
0	1	Unknown
0	1	Unknown
0	1	Unknown
0	1	Unknown
0	1	Unknown
0	1	Unknown
0	1	Unknown

Slave ID – The Slave ID of the destination Counter Stick.

Relay Channel – Select the relay channel to switch

Current Relay State – Shows the last value of the relay as reported to the gateway (except for IO1 module). Clicking the Update button will refresh this value.

After filling out the table click **Write Remote Shutdown Settings to Gateway** to store the setting in the gateway Stick.

Relay Pulse

Starting with ToolKit version 2.2.3, and Gateway Firmware version 8.22, destination relays can be configured to pulse instead of being permanently energized or de-energized. To do so, in the **Relay Channel** drop-down menu, select the same relay but in "(Pulse)" mode. Specify whether to pulse during run or shutdown, and specify the pulse duration.

Destination Relay			Relay Pulse	
Slave ID	Relay Channel	Current Relay State (readonly)	Pulse Relay on...	Pulse Time (sec)
6	1 (Pulse)	De-energized	Run	3

Source Node					Relay Control Logic					Destination Counter Stick		
Slave ID	Node Type	Register Address	Register Type	Current Register Value	Energize Relay when...	Value	De-energize Relay when...	Value	Number of Readings	Slave ID	Relay Channel	Current Relay State (readonly)
1	Sentinel Analog	3001-Current(uA)	16bit UINT	14495	Greater than	14000	Less than	13000	1	5	1	Energized
2	A2 Analog	1003-Digital In	BOOLEAN	1	Equal to	1	Equal to	0	1	5	1	Energized
3	Sentinel HART	4005-HART PV	32bit FLOAT	8.22507	Greater than	3.15	Less than	3.05	1	5	1	Energized
4	Sentinel Digital	3012-Digital In 1	BOOLEAN	0	Equal to	0	Equal to	1	1	5	1	Energized
0	None	0	16bit UINT	Unknown	Greater than	0	Less than	0	1	0	1	Unknown
0	None	0	16bit UINT	Unknown	Greater than	0	Less than	0	1	0	1	Unknown
0	None	0	16bit UINT	Unknown	Greater than	0	Less than	0	1	0	1	Unknown
0	None	0	16bit UINT	Unknown	Greater than	0	Less than	0	1	0	1	Unknown
0	None	0	16bit UINT	Unknown	Greater than	0	Less than	0	1	0	1	Unknown
0	None	0	16bit UINT	Unknown	Greater than	0	Less than	0	1	0	1	Unknown
0	None	0	16bit UINT	Unknown	Greater than	0	Less than	0	1	0	1	Unknown
0	None	0	16bit UINT	Unknown	Greater than	0	Less than	0	1	0	1	Unknown

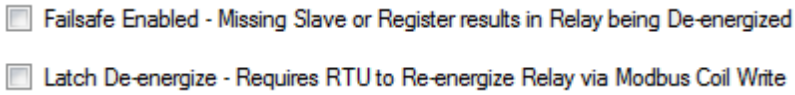
Line 1 has been configured with a source data node as a Sentinel-Analog with the loop current (in µA) as the selected register. The relay will energize when the loop current is above 1400µA (14mA) and de-energize when the loop current is below 1300µA (13mA). Note that this configuration has a 1000µA (1mA) hysteresis factor.

In this example all 4 source nodes are assigned to the same destination Slave ID and relay channel so the following statement applies:

> **If more than one rule is assigned to the same destination RSD Stick and relay channel, then all of the rules must meet the energize condition for the remote relay to be energized.**
>
> **Alternatively, this means that if any one of the four source node's logic results in the "de-energize" condition being true the relay will be de-energized (safe).**

Options

There are two check boxes for additional logic options.



Failsafe Enabled – If this option is selected **all** rules must have valid data for the relay to be energized. If one or more of the nodes times-out or does not exist the relay will be de-energized.

If this option is not selected, then a node that is not installed or fails to check in will be ignored and the relay will be energized using logic only from the units that are active.

Latch De-Energized – If this option is selected the rules may only de-energize the relay. For the relay to be energized again a Modbus write from a PLC to the gateway for the destination Counter stick relay must occur. This is useful if manual intervention is required before the relay is energized after an event. In the example above, a Modbus coil write to Slave ID 5 relay channel 1 (which is register 1) is required to energize the relay. See the RSD Stick manual for a detailed register map.

The "Normal" state of the relay or digital output is the un-energized state and this state should be used to set the controlled system (pump, motor,…) in the "safe" or "off" state.

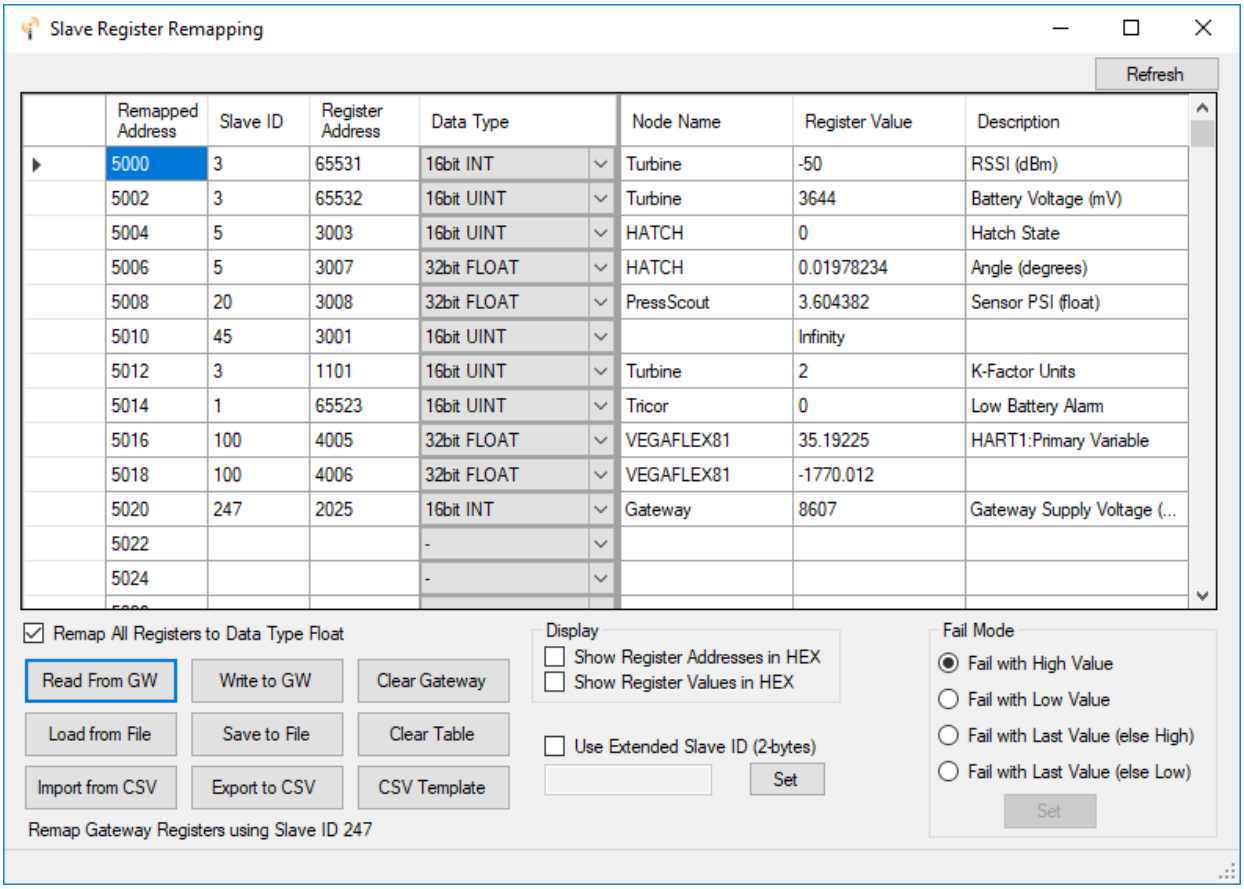
RSD Event log

The RSD events will be stored in the gateway internal event log which can be read using the ToolKit. Additionally, a basic RSD event log containing the last 5 RSD events is available to be read via Modbus from registers 7000-7024. See the Modbus register map for details. The Modbus event log it not maintained through gateway resets.

Slave Register Remapping

The gateway allows any of the remote register data to be remapped to a single block of registers available at the Gateway's slave ID (default is 247). This is useful for collecting a subset of register data from multiple nodes and making it readable in a single block of registers. Up to 1500 registers can be remapped to the gateway's slave ID starting at register 5000.

To configure the remapping, first select **Slave Register Remapping** from the **Settings** dropdown menu.



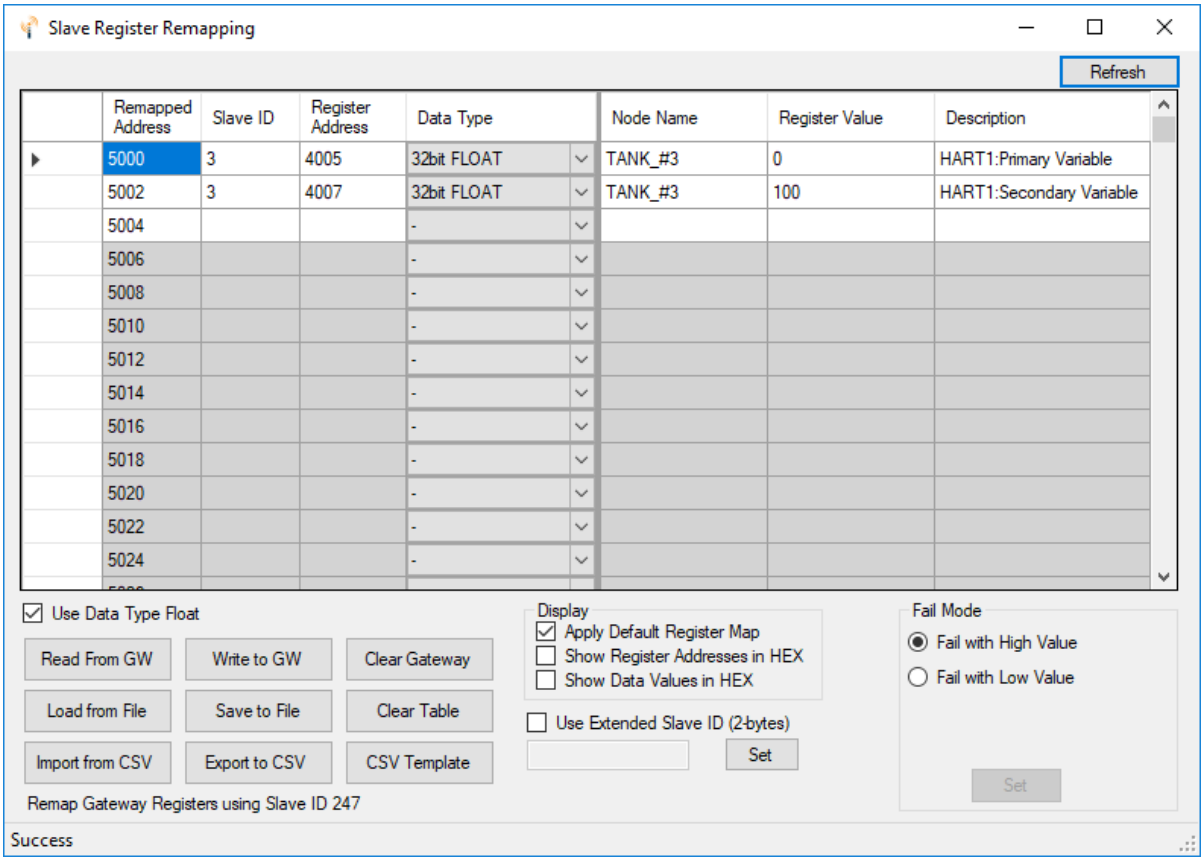
Enter the remote slave ID and register address to map to each gateway register and click **Write Mapping to Gateway** to remap the register(s).

The **Node Name**, **Data Type**, **Register Value**, and **Description** fields will automatically be filled in by the gateway once the mapping is written to the gateway.

Use Data Type Floats

The Modbus Gateway Slave Register Remapping provides an option to remap all registers to 32-bit floats. This allows the user to enter a register and its data type knowing that it will be read from the gateway via Modbus as two 16-bit registers.

To use the floating-point remapping, select the 'Use Data Type Float' check box below the remap table. This will erase the current register remap in the Gateway; the user will be asked to confirm this action before proceeding.

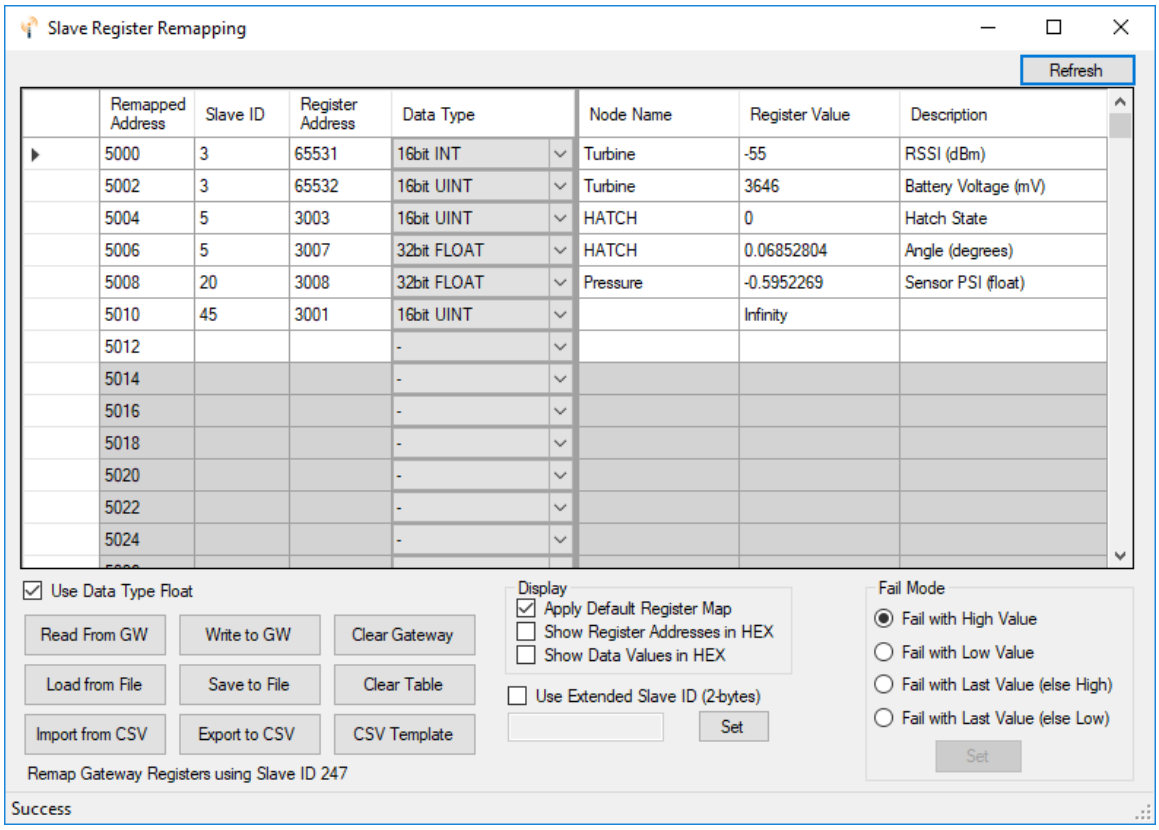


For each even numbered register address in the remap table, enter the Slave ID, Register Address, and select the data type. The data types are provided in a pull-down list. Click the 'Write to GW' button to remap the register(s).

The Node Name, Register Value, and Description fields will automatically be filled in by the gateway once the mapping is written to the gateway.

Fail Mode

If the gateway does not have data for a remapped value it will respond with 0xFFFF, or 0x0000 for the register request, configurable globally with the Fail Mode settings.



Slave 45 isn't reporting in, fail mode set to "high"

Load/Save Files

The displayed remap information can be saved to a proprietary file by clicking the 'Save to File' button. The information may also be loaded from a '.remap' file by clicking the 'Load from File' button.

Import/Export CSV Files

To use 'csv' files, a specific format is required. Exporting the displayed remap information to a 'csv' file automatically writes the file in the required format. When creating a 'csv' file to import, it is recommended to start with the template provided by clicking the 'CSV Template' button.
If the 'Use Data Type Float' checkbox is checked, the pre-formatted template will include the exact strings required for the data type column for easy 'cut & paste' operations.

Output Modules

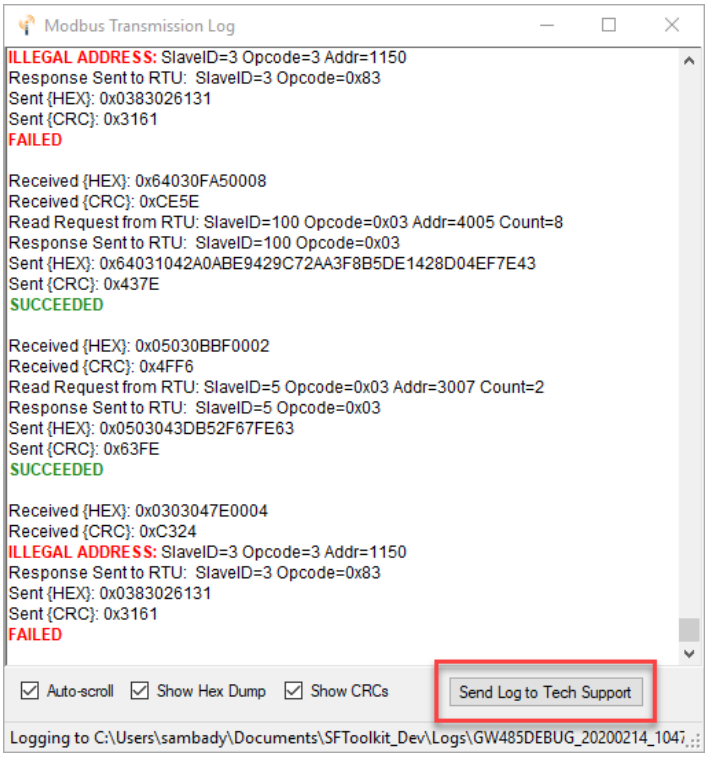
With the purchase of a SignalFire Analog Output Module or Digital Output Module, the Gateway can directly control analog (4-20mA, 1-5V) and digital outputs. The outputs for the module can be controlled through the "Analog/Relay Output Module" window under the Settings menu.

Further information on the modules can be found in their respective manuals.

RS485 Details

The Gateway keeps a log of any Modbus requests made to either itself or any slave nodes connected to it. The Modbus Transmission Log can be viewed under the Tools menu by selecting "RS485 Details".

When the Gateway is open in the ToolKit, this log will be automatically written to the Log folder. The RS485 Modbus Details window also has a 'Send Log to Tech Support' button that opens a window to email SignalFire support with the file attached using your default email client.



Network Map

The ToolKit comes with a graphical display of the network that includes the Gateway, its nodes, their slave IDs and signal strengths, and what path each node takes to communicate with the Gateway (such as hopping through a repeater stick).

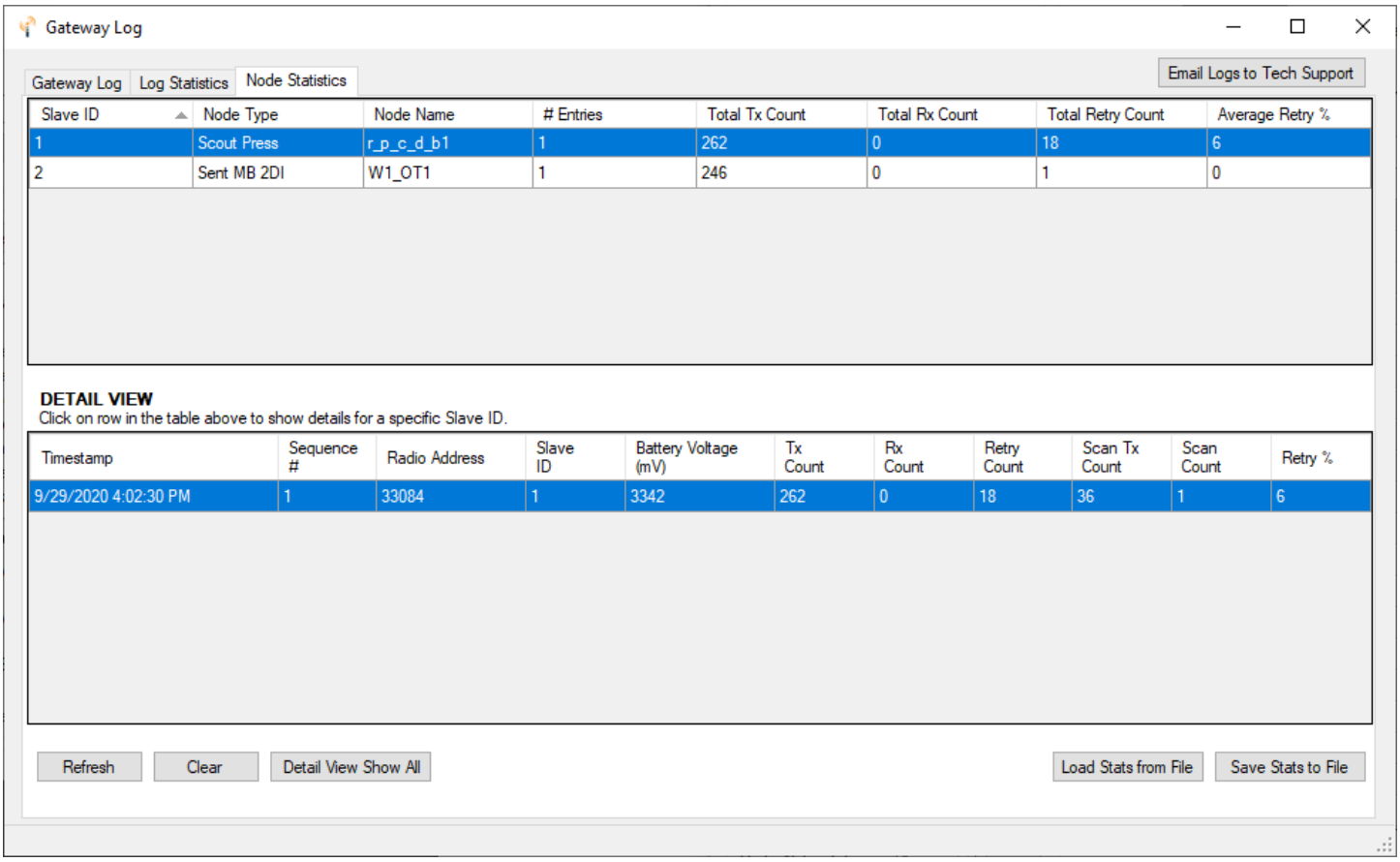
Gateway Event Log

Starting with Gateway Firmware version 7.81 the Gateway keeps an internal log of events.
The event log can be viewed from the gateway window of the ToolKit by clicking 'View Gateway Log' at the bottom of the window. The gateway log events such as reboots, remote nodes joining/timing out, local RSD control events, remote configuration sessions, firmware updates, and more.

The Node Statistics tab shows information reported every four hours from Sentinels, Scouts, and Flow Totalizers to the Gateway with firmware versions from on or after September 21, 2020.

Saving the Gateway Log

Starting with ToolKit version 2.2.21.00, there is a 'Email Logs To Tech Support' button in the upper right hand corner. It will automatically save all the log entries and statistics, and open a window to email SignalFire support with the files attached using your default email client.



Modbus Gateway Register Map

The SignalFire Modbus Gateway by default is assigned Modbus Slave ID number 247. **Only the Gateway status/configuration and remapped registers are read at this address.** All remote node registers are read from the slave ID and register address of the remote node, unless slave register remapping used.

Discrete Registers

Gateway Configuration and Status Messages – These can only be written to by Modbus opcode 0x05 (Write Single Coil). To perform the following resets, write a 0xFF00 to the respective coil. Writing 0x0000 to a coil has no effect.

Register Number	Register Address (Offset)	Description
00001	0000	Resets the gateway and radio
00002	0001	Resets the radio leaving the gateway on
00003	0002	Resets all counters to zero (See Read Only Registers 2026-2031)

Write Only – These can be written to by Modbus opcode 0x05 (Write Single Coil) or 0x15 (Write Multiple Coils). To energize, write a 0xFF00; to de-energize, write a 0x0000.

Register Number	Register Address (Offset)	Description
00102	0101	Analog/Relay Ouput Module 1 Relay 1
00103	0102	Analog/Relay Ouput Module 1 Relay 2
00104	0103	Analog/Relay Ouput Module 2 Relay 1
00105	0104	Analog/Relay Ouput Module 2 Relay 2

Read Only – They can be read by Modbus opcode 0x01 (Discrete Output), and opcode 0x02 (Discrete Input)

Register Number	Register Address (Offset)	Description
02035	2034	State of Digital Output 1. 0=open, 1=closed (function code 0x01)
02036	2035	State of Digital Output 2. 0=open, 1=closed (function code 0x01)
12037	2036	State of Digital Input 1. 0=open, 1=closed (function code 0x02)
12038	2037	State of Digital Input 2. 0=open, 1=closed (function code 0x02)

Holding Registers

Write Only – These can only be written to by Modbus opcode 0x06 (Write Single Holding Register) or opcode 0x16 (Write Multiple Holding Registers).

Register Number	Register Address (Offset)	Description
40122	0121	Analog/Relay Ouput Module 1 Relay 1 Pulse (Seconds to pulse relay on)
40123	0122	Analog/Relay Ouput Module 1 Relay 2 Pulse (Seconds to pulse relay on)
40124	0123	Analog/Relay Ouput Module 2 Relay 1 Pulse (Seconds to pulse relay on)
40125	0124	Analog/Relay Ouput Module 2 Relay 2 Pulse (Seconds to pulse relay on)
40132	0131	Digital Ouput Module 1 Relay 1
40133	0132	Digital Ouput Module 1 Relay 2
…	…	…
40143	0142	Digital Ouput Module 1 Relay 12
40144	0143	Digital Ouput Module 2 Relay 1
40145	0144	Digital Ouput Module 2 Relay 2
…	…	…
40155	0154	Digital Ouput Module 2 Relay 12

Read/Write Registers – These are 16-bit read/write registers. They can be written to by Modbus opcode 0x06 or 0x10 (Write Single and Multiple Registers, respectively) and can be read with Modbus opcode 0x03 or 0x04 (Read Discrete Input and Holding Registers, respectively). The first three registers are identical to the previous three write coils and behave similarly. They will be read as 0x0000 and can be triggered by writing 0xFF00 to them. The remaining must be written with 16-bit values in the range specified in the table below.

Register Number	Register Address (Offset)	Description
41001	1000	Resets the gateway and radio
41002	1001	Resets the radio leaving the gateway on
41003	1002	Resets all GW status counters to zero (See Read Only Registers 2026-2031)

Read Only Registers – These are 16-bit read only registers. They can be read with Modbus opcode 0x03 or 0x04 (Read Discrete Input and Holding Registers, respectively). The register map can be found below.

If the gateway has a large total number of registers approaching 4700, register 2008 should be monitored to ensure that free registers are available before adding a new node.

Register Number	Register Address (Offset)	Description
42001	2000	Upper 16 bits of SFTS GW node address (the radio ID)
42002	2001	Lower 16 bits of SFTS GW node address (the radio ID)
42003	2002	Upper 16 bits of Radio Firmware version number
42004	2003	Lower 16 bits of Radio Firmware version number
42005	2004	Upper 16 bits of gateway firmware version number
42006	2005	Lower 16 bits of gateway firmware version number
42007	2006	Number of slave nodes that data is cached for this gateway
42008	2007	Total number of registers allocated to slave devices
42009	2008	Total number of free registers available for slave devices
42010	2009	Bitmask for active slave IDs 15-0 (LSB is 0)
42011	2010	Bitmask for active slave IDs 31-16 (LSB is 16)
42012	2011	Bitmask for active slave IDs 47-32 (LSB is 32)
42013	2012	Bitmask for active slave IDs 63-48 (LSB is 48)
42014	2013	Bitmask for active slave IDs 79-64 (LSB is 64)
42015	2014	Bitmask for active slave IDs 95-80 (LSB is 80)
42016	2015	Bitmask for active slave IDs 111-96 (LSB is 96)
42017	2016	Bitmask for active slave IDs 127-112 (LSB is 112)
42018	2017	Bitmask for active slave IDs 143-128 (LSB is 128)
42019	2018	Bitmask for active slave IDs 159-144 (LSB is 144)
42020	2019	Bitmask for active slave IDs 175-160 (LSB is 160)
42021	2020	Bitmask for active slave IDs 191-176 (LSB is 176)
42022	2021	Bitmask for active slave IDs 207-192 (LSB is 192)
42023	2022	Bitmask for active slave IDs 223-208 (LSB is 208)
42024	2023	Bitmask for active slave IDs 239-224 (LSB is 224)
42025	2024	Bitmask for active slave IDs 255-240 (LSB is 240)
42026	2025	Gateway power supply voltage in mV
42027	2026	Radio packets received count
42028	2027	Radio packets sent count
42029	2028	RS-485 messages received count
42030	2029	RS-485 messages sent count
42031	2030	Total Modbus errors from master and slaves
42032	2031	Modbus exceptions from slave nodes
42033	2032	Radio packets received/transmitted per minute. Recommended to be less than 60

42034	2033	Radio packets per minute alert. 0 if packets/min <= 60, 1 if packets/min > 60
42035	2034	State of Digital Output 1. 0=open, 1=closed (readable with function code 0x01 or 0x03, writeable with function code 0x05, 0x06, 0x16)
42036	2035	State of Digital Output 2. 0=open, 1=closed (readable with function code 0x01 or 0x03, writeable with function code 0x05, 0x06, 0x16)
42037	2036	State of Digital Input 1. 0=open, 1=closed (readable with function code 0x02 or 0x03)
42038	2037	State of Digital Input 2. 0=open, 1=closed (readable with function code 0x02 or 0x03)
42039	2038	Analog Input 1 (mV)
42040	2039	Analog Input 2 (mV)
42041	2040	Analog Input 3 (mV)
42042	2041	Seconds Since Power On (UINT32 High Word)
42043	2042	Seconds Since Power On (UINT32 Low Word)
42044	2043	Seconds Since Last Reboot (UINT32 High Word)
42045	2044	Seconds Since Last Reboot (UINT32 Low Word)
42101	2100	Address test register. Always returns 2100
42102	2101	Address test register. Always returns 2101
42103	2102	Address test register. Always returns 2102
43001	3000	Write the radio address of a Modbus Stick node to this register to cause that Modbus Stick to perform a scan for attached Modbus sensors
43004	3003	Write Modbus ID for a Modbus Client node to this register to cause that remote node to perform a scan for attached Modbus sensors
44002	4001	Status of Slave ID 1:Returns 1 if Slave is present and 0 if not present
44003	4002	Status of Slave ID 2:Returns 1 if Slave is present and 0 if not present
…	…	…
44241	4240	Status of Slave ID 240:Returns 1 if Slave is present and 0 if not present
47001	7000	Event 1 – RSD Line Number
47002	7001	Event 1 – Source SID
47003	7002	Event 1 – Destination RSD SID
47004	7003	Event 1 – Destination RSD relay channel
47005	7004	Event 1 – RSD Event Type: 1 = Energize, 0 = De-Energize
47006	7005	Event 2 – RSD Line Number
…	…	…
47011	7010	Event 3 – RSD Line Number
…	…	…
47016	7015	Event 4 – RSD Line Number
…	…	…
47021	7020	Event 5 – RSD Line Number
…	…	…
47025	7024	Event 5 – RSD Event Type: 1 = Energize, 0 = De-Energize

Revision History

Revision	Date	Changes/Updates
2.1	11/29/10	Clarified description for register 1002
3.0	-	Added registers and description for “transparent” Modbus mode
3.1	-	Added detail on using SignalFire Toolkit
3.2	-	Updated SignalFire Toolkit screenshots
3.3	-	Added additional detail on register mapping
3.4	-	Updated SignalFire Toolkit screenshots, added RSD control section
3.6	-	Added slave ID status registers
3.7	-	Added section of slave register mapping
3.8	-	Added section on remote node configuration
4.0	-	Updated design, minor edits
4.1	7/6/16	Added section on encryption
4.2	9/7/17	Updated section on register remapping
4.3	8/7/2018	Updated screenshots, rewrote network settings
4.4	9/4/2018	Cleaned up some sections, formatting, clarifications, organization
4.5	10/17/2018	Added RSD pulse settings and registers
4.6	4/9/20	Added Gateway Log support button, Digital Output Module
4.7	9/30/2020	Added Gateway log node statistics
4.8	8/4/2021	Register remap increased to 1500

The Gateway-in-a-Stick is rated Class 1 Division 2 non-Incendive.

WARNING: EXPLOSION HAZARD. DO NOT REMOVE OR REPLACE COMPONENTS UNLESS POWER HAS BEEN DISCONNECTED OR THE AREA IS FREE OF IGNITIBLE CONCENTRATIONS.

AVERTISSEMENT : RISQUE D'EXPLOSION . NE PAS RETIRER OU REMPLACER LES COMPOSANTS QUE L'ALIMENTATION EST DÉBRANCHÉ OU ZONE EST LIBRE DE CONCENTRATIONS IGNITIBLE.

WARNING – EXPLOSION HAZARD Substitution of components may impair suitability for Class I, Division 2

AVERTISSEMENT - RISQUE D'EXPLOSION. La substitution de composants peut rendre ce materiel inacceptable pour les emplacements de classe I, division 2

WARNING – EXPLOSION HAZARD Do not disconnect while circuit is live unless area is known to be nonhazardous

AVERTISSEMENT - RISQUE D'EXPLOSION. Ne débranchez pas lorsque le circuit est en direct , sauf si la zone est connue pour être nonhazardous

WARNING – All wring methods must be in accordance with the NEC

AVERTISSEMENT - Toutes les méthodes de Essorez doivent être en conformité avec la NEC

APPENDIX - FCC and IC Statements

Changes or modifications not expressly approved by SignalFire Telemetry, Inc could void the user's authority to operate the equipment.

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.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

-- Reorient or relocate the receiving antenna.
-- Increase the separation between the equipment and receiver.
-- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
-- Consult the dealer or an experienced radio/TV technician for help.

This deice has been designed to operate with only the permanently attached internal antenna, having a maximum gain of 5 dB. No other antenna may be used.

WARNING!
FCC and IC Radiation Exposure Statement:
This equipment complies with FCC's and IC's RF radiation exposure limits set forth for an uncontrolled environment under the following conditions:

1. This equipment should be installed and operated such that a minimum separation distance of 20cm is maintained between the radiator (antenna) & user's/nearby person's body at all times.
2. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a maximum (or lesser) gain approved for this transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.r.i.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.