

Rhein Tech Laboratories, Inc.
360 Herndon Parkway
Suite 1400
Herndon, VA 20170
<http://www.rheintech.com>

Client: HandEra, Inc.
Model: WF-100
Standards: FCC 15.247 & RSS-210
FCC/IC ID: URZ-WF10011/6827A-WF10011
Report #: 2006180

Appendix I: Manual

Please refer to the following pages.



1007-00028
Revision 0.3

WF-100-1-1
Specification

Re ision Date
11/14/2006



CONTACT INFORMATION

Company: HandEra Inc.
2859 104th Street
Des Moines, IA 50322

Phone: (515)-252-7522
Fax: (515)-252-7525
Web: www.HandEra.com

DOCUMENT MODIFICATION LOG

Description of changes	Rev.	Date
Preliminary	0.1	9/28/2006
Minor typos fixed	0.2	9/29/2006
Agency Certifications added, removed preliminary & confidential status, and minor typos fixed	0.3	11/14/2006

Copyright © 2006 HandEra, Inc. All rights reserved. No part of this documentation may be reproduced or transmitted in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without express written consent from HandEra.

Windows CE is a registered trademark of Microsoft.

Palm OS® is a registered trademark of Palm Trademark Holding Company, LLC.

HandEra reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of HandEra to provide notification of such revision or changes.

HandEra makes no representations or warranties that the documentation is free of errors. The documentation is provided on an 'as is' basis.

1	General Description.....	4
1.1	Features	4
2	Electrical.....	5
2.1	Bloc Diagram.....	5
2.2	Connector Pin out	6
2.3	DC C aracteristics	6
2.4	Inter ace Selection	7
2.5	SPI Timing Diagram.....	7
2.6	Host Sc ematic E ample SPI	8
2.7	WLAN Bluetooth Co-location	8
2.8	Regulator Appro als.....	8
2.9	Per ormance	9
3	Mec anical.....	10
3.1	Dimensions	10
3.2	En ironmental	11
4	So t are	12
4.1	Plat orm Support.....	12
4.1.1	Intel PXA270.....	12
4.1.2	Freescall MX21	12
4.1.3	Samsun S3C2410	12
4.2	Feature Matri	12
4.3	De initions	12
4.3.1	WEP	12
4.3.2	WPA	12
4.3.3	WP1.....	13
4.3.4	WPA2.....	13
4.3.5	CCX.....	14
5	Appen i A Agenc Certi ications	15
5.1	Unite States FCC	15
5.1.1	OEM La eling Re uirements	15
5.1.2	FCC Notices	15
5.2	Canaa IC	16
5.2.1	La eling Re uirements	16
5.2.2	RFI Statement	16
5.3	Sample La el	17

1 General Description

HandEra's WF-100 802.11b embedded module is the world's smallest fully type-approved module for use in embedded designs. It can be integrated into OEM products without the need for costly, time consuming FCC approvals.

The WF-100 offers complete drivers for embedded operating systems such as WinCE and Linux. Additional security can be added to the WF-100 by using the optional security supplicant software offered by HandEra

1.1 Features

- IEEE Std 802.11b compliant
- Fully Type-Approved module pre-certified to FCC intentional radiator standards
- Simple, high speed SPI interface
- Low power design
 - Sleep: 200 μ W
 - Receive power: 500 mW
 - Transmit power: 850 mW
- Bluetooth coexistence Packet Traffic Arbitration (PTA) support
- Data Rates 1,2, 5.5 11 Mbps (802.11B)
- RoHS 2006 compliant
- Support for IEEE 802.11i and WPA security enhancements
- EEPROM to Store MAC address

2 Electrical

2.1 Bloc Diagram

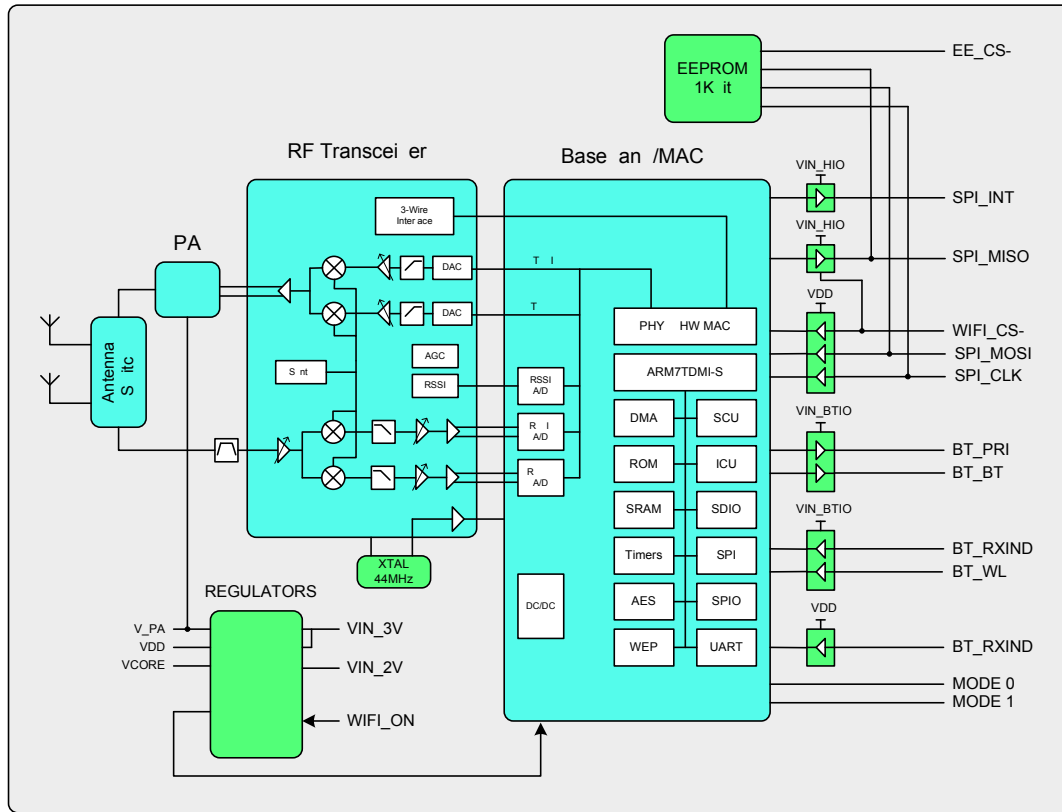


Figure 1 - Block Diagram

2.2 Connector Pin out

Pin	Name	Type	Power Domain	Description
1	SPI_INT	O	VIN_HIO	SPI Interrupt
2	SDAT2 ¹	I/O	---	N SD data bit[2]
3	SPI_MOSI	I	VIN_HIO	SPI Master Out/Slave In
4	SDAT3 ¹	I/O	---	SD data bit[3]
5	SPI_MISO	O	VIN_HIO	SPI Master In/Slave Out
6	SD_CMD ¹	I/O	---	SD Command
7	SPI_CLK	I	VIN_HIO	SPI Clock
8	SD_CLK ¹	I	---	SD Clock
9	WIFI_CS-	I	VIN_HIO	SPI Chip select for WIFI module
10	SDAT0 ¹	I/O	---	SD data bit[0]
11	MODE0 ⁵	I	2.85V	SPI/SDIO interface selection
12	SDAT1 ¹	I/O	---	SD data bit[1]
13	MODE1 ⁵	I	2.85V	SPI/SDIO interface selection
14	EE_CS- ²	I	VIN_HIO	EEProm Chip Select
15	VIN_HIO	PWR	VIN_HIO	SPI I/O Ring Power Supply
16	NC	-	---	NC
17	VIN_2V	PWR	VIN_2V	Core Power Supply
18	BT_PRI ³	I	VIN_BTIO	Bluetooth high priority traffic indicator
19	MODE2 ⁴	I	---	NC
20	BT_BT ³	I	VIN_BTIO	Bluetooth arbitration signal
21	WIFI_ON	I	VIN_HIO	Enable Module
22	BT_RXIND ³	O	VIN_BTIO	WLAN receive indicator
23	MODE3 ⁴	I	---	No Connect
24	BT_WL ³	O	VIN_BTIO	WLAN arbitration signal
25	MODE4 ⁴	I	---	NC
26	VIN_BTIO	PWR	VIN_BTIO	Bluetooth I/O Ring Power Supply
27	GND	PWR		Ground
28	VIN_3V	PWR	VIN_3V	Main Power Supply
29	GND	PWR		Ground
30	NC	-	---	No Connect

Table 1 - Connector Pin out

Notes:

1. WF-100-1-1 only supports SPI, SDIO reserved for future models.
2. Not required if host stores the MAC address.
3. Optional. Used on systems with co-located Bluetooth device.
4. MODE2, MODE3 and MODE4 reserved for future products.
5. MODE0 and MODE1 must be tied low for SPI.

2.3 DC Characteristics

Symbol	Parameter	Min	Nom	Max	Unit
V _{IN_3V}	Main Power Supply	3.1	-	3.6	V
V _{IN_2V}	Core Power Supply	2.25	-	3.6	V
V _{IN_BTIO}	Bluetooth I/O Ring Power Supply	1.2	-	3.6	V
V _{IN_HIO}	SPI I/O Ring Power Supply	0.9	-	3.6	V
I _{IN_3V}	Main supply current			375	mA
I _{IN_2V}	Core supply current			85	mA
I _{IN_BTIO}	Bluetooth I/O Ring current			500	μA
I _{IN_HIO}	SPI I/O Ring current			500	μA

Table 2

2.4 Inter ace Selection

The pins MODE0 and MODE1 are used to select between SPI and SDIO. The WF-100-1-1 only supports SPI, therefore, MODE0 and MODE1 should be set low.

Interface	MODE0	MODE1
SPI	0	0

Table 3 - Interface selection

2.5 SPI Timing Diagram

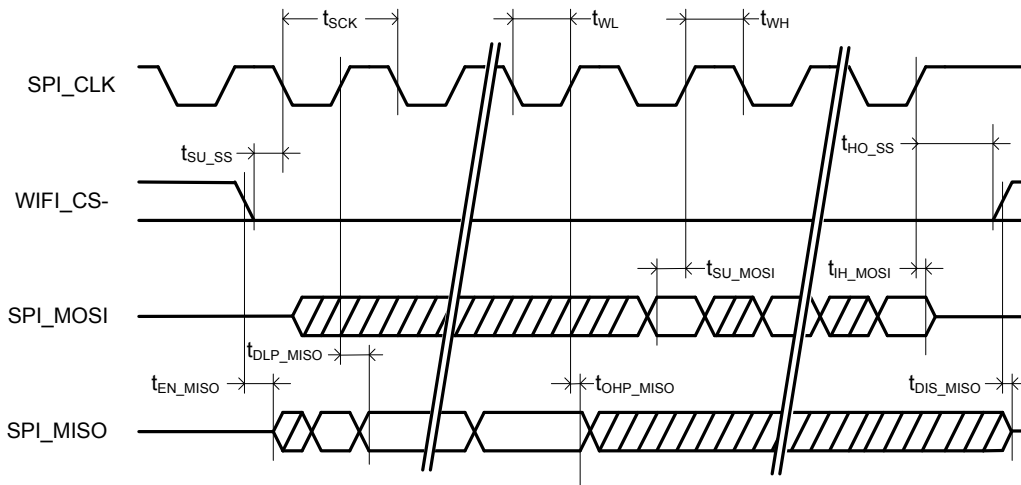


Figure 2 – SPI Timing Diagram (SPI_MISO clocked on rising edge of SPI_CLK)

Symbol	Parameter	Min	Typ	Max	Units
t_{SCK}	Period of SPI_SCK	15.0	-	-	ns
t_{WH}	Clock high time	7.0	-	-	ns
t_{WL}	Clock low time	7.0	-	-	ns
t_{SU_SS}	Setup time for WIFI_CS-	3.0	-	-	ns
t_{HO_SS}	Hold time for WIFI_CS-	0.0	-	-	ns
t_{SU_MOSI}	Setup time for SPI_MOSI	4.0	-	-	ns
t_{IH_MOSI}	Input hold time for SPI_MOSI	0.0	-	-	ns
t_{EN_MISO}	Output enable time for SPI_MISO	-	-	8.0	ns
t_{DIS_MISO}	Output disable time for SPI_MISO	-	-	6.0	ns

Table 4 – AC Characteristics for SPI

2.6 Host Schematic Example SPI

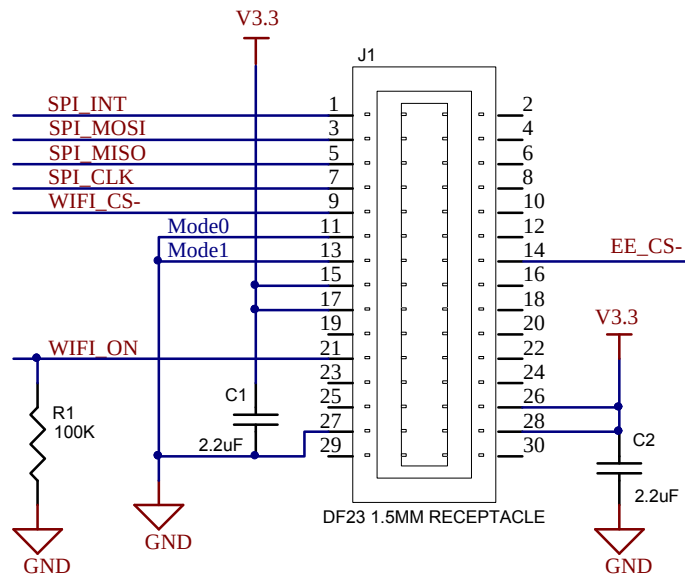


Figure 3 - Simple Host Example (SPI)

2.7 WLAN Bluetooth Co-location

The WF100-2-1 supports the IEEE 802.15 recommended practice of Packet Traffic Arbitration (PTA) to avoid simultaneous transmission with co-located Bluetooth devices. PTA is a system protocol that employs an arbitration algorithm by which WLAN and Bluetooth contend for the medium. PTA is implemented using a simple four-line interface on the WF-100-1-1.

- BT_WL
- BT_BT
- BT_PRI
- BT_RXIND

Note: For systems that do not contain a co-located BT device, these lines can be left unconnected.

2.8 Regulator Approvals

- FCC Part 15 Class B
- FCC Part 15.247, 15.205, 15.209 in USA
- ETS 300 328 in Europe
- CE Mark

2.9 Performance

Receiver

802.11B	1Mbps	2Mbps	5.5Mbps	11Mbps	Units
Sensitivity ¹	-91	-87	-83	-83	dBm

¹Typical values, PER < 8%

Transmitter

802.11B	1Mbps	2Mbps	5.5Mbps	11Mbps	Units
Output Power ²	16.1	16.1	17.6	17.6	dBm

²Typical values, channel 6.

3 Mechanical

3.1 Dimensions

Note: All dimensions in inches.

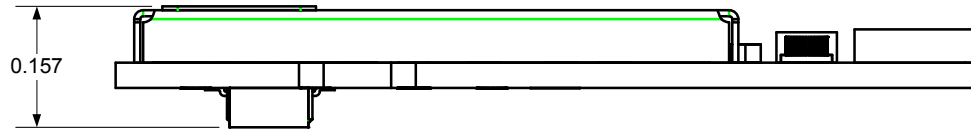


Figure 4 – Side View

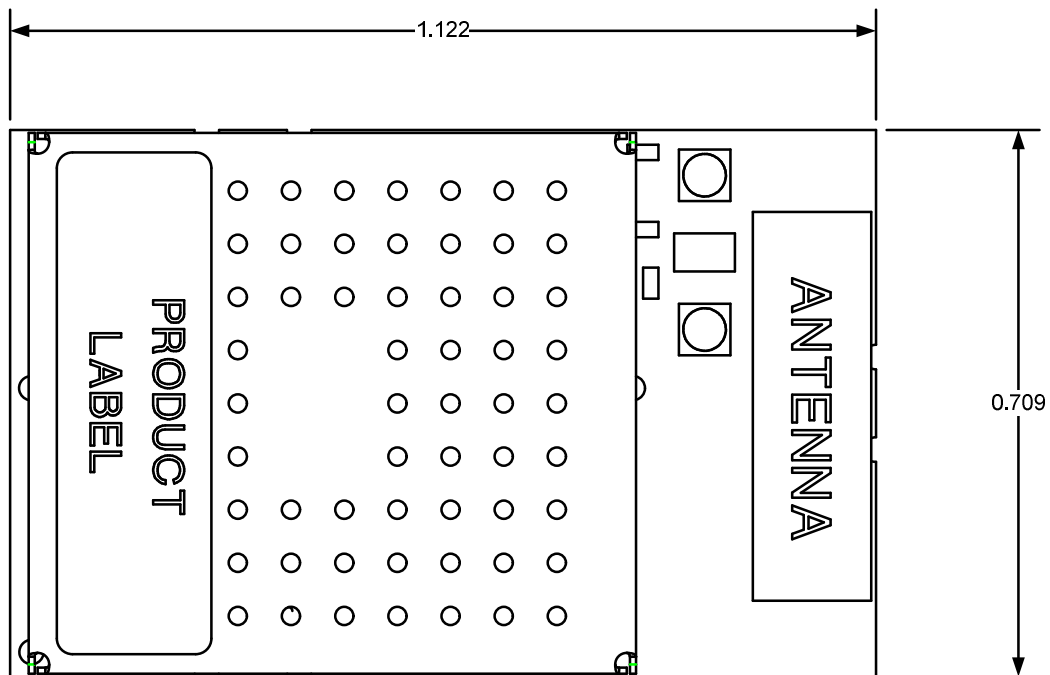


Figure 5 – Front View

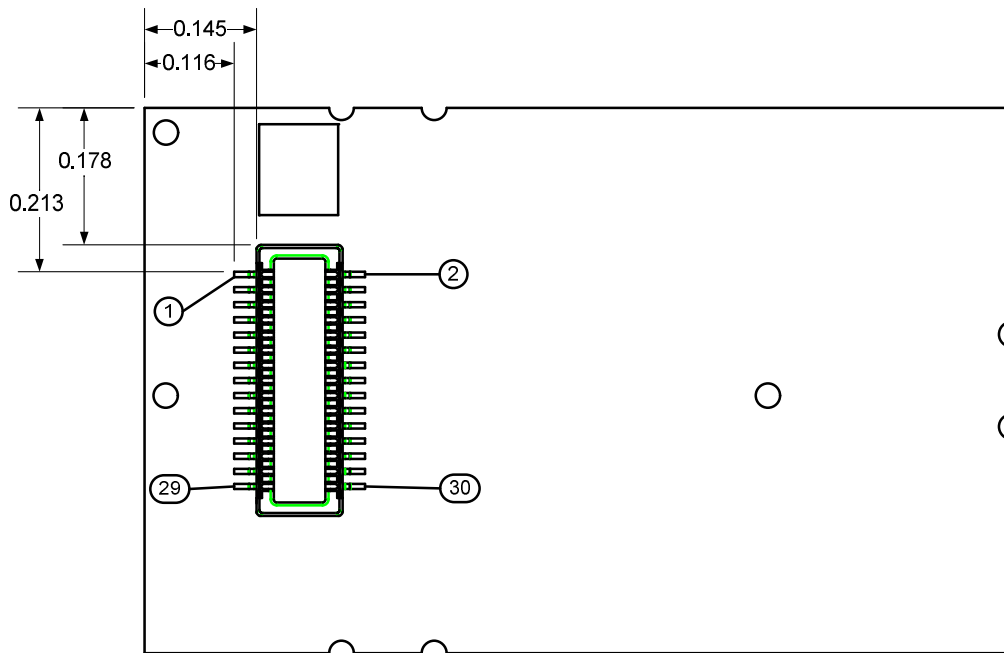


Figure 6 – Bottom View



Figure 7 - Host to Module

WF-100-1-1 connector: Molex 55560-0307, or Hirose DF23C-30DP-0.5V(92)
 Host PCB connector: Molex 54722-0307, or Hirose DF23C-30DS-0.5V(92)

3.2 Environmental

Non-Operational Conditions:

Ambient temperature: -30°C to +125°C.

Relative humidity: 5-95%, non-condensing.

Operational Conditions:

Ambient temperature: -30°C to +85°C.

Relative humidity: 5-95%, non-condensing.

4 Software

4.1 Platform Support

Drivers for the following platforms currently exist for the WF-100-1-1 module.

4.1.1 Intel PXA270

- WinCE 5.0
- Linux 2.6
- MX21

4.1.2 Freescale MX21

- PalmOS 5.4
- WinCE 5.0

4.1.3 Samsung S3C2410

- WinCE 5.0

4.2 Feature Matrix

Feature	Palm 1	Palm 2	WinCE
WEP	Yes	Yes	Yes
WPA1	No	Yes	Yes
TLS	No	Yes	Yes
PEAP	No	Yes	Yes
MD5	No	?	Yes
LEAP	No	No	No
WPA2	No	Yes	No
CCX	No	No	No
Roaming	No	?	?
PowerSave	Yes	Yes	Yes

4.3 Definitions

4.3.1 WEP

- 40 bit / 64 bit encryption keys
- 104 bit / 128 bit encryption keys
- RC4 encryption standard is used to encrypt data using encryption keys entered by the user

4.3.2 WPA

There are several meanings for WPA (Wi-Fi Protected Access). WPA is a commercial term developed by the Wi-Fi consortium to add better security to legacy or WEP products. The core of WPA1 is the TKIP key management protocol. WPA1 was designed to run on legacy wireless hardware.

4.3.3 WP1

- TKIP – Temporal Key Integrity Protocol is used by WPA as a method to periodically generate new keys. This helps to provide protection so that keys cannot be easily broken by surveillance. TKIP was devised to upgrade security on existing WEP products without requiring new encryption support in hardware.
- RC4 – Encryption standard used to encrypt data using TKIP managed keys. RC4 is generally implemented in the 802.11 chipset for speed.
- 802.1X – Access Control method, used to determine if a device is allowed access to the network. 802.1X provides a family of protocols for user authentication, including PAP, MS-CHAP, and EAP. EAP (Extensible Authentication Protocol) does not actually perform authentication itself, but rather provides a framework for processing higher-level authentication methods, such as TLS and PEAP. The authentication server may reside locally in an access point, or in a remote server which communicates to the access point (and the supplicant) through the RADIUS (Remote Access Dial Up Server) protocol.
- High-level authentication methods (EAP-methods) – Protocols such as TLS and PEAP that perform authentication using the EAP protocol as a transport. These authentication methods often include encryption key generation and two-way authentication (both device and network). TLS (Transport Layer Security) is a standardized version of the Netscape security protocol SSL, and uses digital certificates for user authentication. PEAP (Protected-EAP) is an encrypted version of EAP in which the EAP exchanges are performed in a protected “tunnel.”
- LEAP – Cisco Light-EAP, developed before the 802.1X standard was complete. LEAP provides the same functionality as 802.1X, with the authentication server implemented inside Cisco access points. LEAP is considered more secure than WEP but less secure than WPA1.
- MIC – The Message Integrity Checker is used to detect tampering with packets on an active wireless link. The MIC can also invoke countermeasures if tampering is detected, such as temporarily shutting down the network.
- WPA “Personal” usage model: WPA-PSK
 - This configuration is sometimes called “WPA Personal”. PSK stands for “Pre-Shared Keys” and refers to a manual process of initial key distribution. The word “distribution” is used because a single key is provided to many users of the same access point. For example, a system administrator might distribute the key to many users of a single access point. The users need to manually enter the key provided by the system administrator into their computers through a preferences panel. Afterwards, TKIP takes over management of the keys.
- WPA “Enterprise” usage model: WPA-EAP
 - This configuration provides automatic key management using an 802.1X authentication server. This is sometimes called “WPA Enterprise”, and requires more sophisticated infrastructure. Generally special software such as a RADIUS Server program is required to run on a server. This software is responsible for authenticating users.
- There are many high-level authentication/key distribution methods that can be used with WPA-EAP. The method specified by WPA is TLS.

4.3.4 WPA2

- WPA2 (Wi-Fi Protected Access 2). WPA2 is a commercial term developed by the Wi-Fi consortium to refer to the more generic IEEE 802.11i suite of security protocols. The core of WPA2 is the CCMP key management protocol and the AES encryption engine.
- CCMP – Counter Mode-CBC MAC Protocol is used as a superset replacement of TKIP in WPA2.
- AES - Advanced Encryption Standard is an encryption method that is used to encrypt data using CCMP managed keys. AES is provided by the 802.11 chipset.
- RSN – A network in which all stations use 802.11i advanced security protocol is called a Robust Security Network. If legacy devices are allowed to connect, the network is called a TSN (Transitional Security Network).
- WPA2 cannot be implemented on legacy 802.11 chipsets because of the required hardware AES support.

4.3.5 CCX

Cisco Compatible Extensions(CCX) are a collection of protocols defined by Cisco for wireless security, forming a super-set of WPA and 802.11i. In addition to authentication and encryption, CCX includes specifications for power management, roaming, and VOIP. As of 2005 there are four different versions, each version adding extensions to the previous version.

- V1 – 802.11, 802.1X, WEP, LEAP, CKIP (Cisco TKIP), multiple SSID support.
- V2 – WPA, roaming, power management.
- V3 – WPA2, EAP-FAST, Wi-Fi multimedia.
- V4 – PEAP-MSCHAP, voice metrics, AP-directed roaming.

5 Appendix A: Agency Certifications

5.1 United States FCC

The WF-100 802.11b Module complies with Part 15 of the FCC rules and regulations. Compliance with the labeling requirements, FCC notices and antenna usage guidelines is required. To fulfill FCC Certification requirements, the OEM must comply with the following regulations:

1. The system integrator must ensure that the text on the external label provided with this device is placed on the outside of the final product [5.3].
2. The HandEra WF-100 802.11b Module may only be used with antennas that have been tested and approved for use with this module. All other antennas must be tested to comply with FCC 15.203 (Unique Antenna Connectors) and 15.247 (Emissions).

5.1.1 OEM Labeling Requirements

5.1.1.1 Verification / Certification

The labeling requirements for a device subject to the Verification or Certification procedures are specified in FCC Part 2, Subpart J and 15.19(a). These labeling requirements are:

- One of three compliance statements specified in FCC 15.19(a);
- If the device is subject only to Verification, include a label bearing a unique identifier not to be confused with the FCC Identifier (FCC ID) required on devices subject to Certification – FCC 2.954;
- If the device is subject to Certification, 1) FCC 2.925 contains information on identification of the equipment; 2) include a label bearing an FCC Identifier (FCC ID) - FCC 2.926.

If the labeling area for the device is so small, or it is not practical to place the required statement on the device, then the statement can be placed in the user manual or product packaging - FCC 15.19(a)(5). Generally, devices smaller than the palm of the hand are considered small. However, the device must still be labeled with the unique identifier (Verification) or the FCC ID (Certification).

5.1.1.2 Declaration of Conformity (DoC)

The labeling requirements for a device subject to the Declaration of Conformity (DoC) procedure are specified in FCC 15.19(b). The label should include the FCC logo along with the Trade Name and Model Number, which may satisfy the unique identifier requirement of FCC 2.1074 if it represents the identical equipment tested for DoC compliance. For personal computers assembled from authorized components, the following additional text must also be included: “Assembled from tested components,” “Complete system not tested.” When the device is so small or when it is not practical to place the required additional text on the device, the text may be placed in the user manual or pamphlet supplied to the user. However, the FCC logo, Trade Name, and Model Number must still be displayed on the device - FCC 15.19(b)(3).

5.1.2 FCC Notices

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.

Important: The WF-100 802.11b Module has been certified by the FCC for use with other products without any further certification (as per FCC 2.1091). Modifications not expressly approved by HandEra, Inc. could void the user's authority to operate the equipment.

Important: OEMs must test final product to comply with unintentional radiators (FCC 15.107 & 15.109) before declaring compliance of their final product to Part 15 of the FCC Rules.

Important: The RF module has been certified for remote and base radio applications. If the module will be used for portable applications, the device must undergo SAR testing.

Note: 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 or more of the following measures:

- Re-orient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect equipment and receiver to outlets on different circuits,
- Consult the dealer or an experienced radio/TV technician for help.

The use of shielded I/O cables is required when connecting this equipment to any and all peripheral or host devices. Failure to do so may violate FCC rules.

Note: Changes or modifications not covered in this manual must be approved in writing by the manufacturer's Regulatory Engineering Department. Changes or modifications made without written approval may void the user's authority to operate this equipment.

RF Exposure Note: Under normal operating conditions, the antenna is designed to maintain a separation distance of 20 cm from all persons. The EUT is mobile and fixed.

5.2 Cana a IC

5.2.1 Labeling Requirements

Labeling requirements for Industry Canada are similar to those of the FCC. A clearly visible label on the outside of the final product enclosure must display the following text:

Contains Model WF100-1-1, IC: 6827A-WF10011

The integrator is responsible for its product to comply with IC ICES-003 & FCC Part 15, Sub. B - Unintentional Radiators. ICES-003 is the same as FCC Part 15 Sub. B and Industry Canada accepts FCC test report or CISPR 22 test report for compliance with ICES-003.

5.2.2 RFI Statement

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

5.3 Sample Label

Warning: The Original Equipment Manufacturer (OEM) must ensure that FCC labeling requirements are met. This can be achieved by the following.

Figure A-1. Required FCC Label for OEM products containing the WF-100 802.11b Module

Contains FCC ID: URZ-WF10011
The enclosed device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (i.) this device may not cause harmful interference and (ii.) this device must accept any interference received, including interference that may cause undesired operation.

Figure A-2 depicts a sample label to satisfy the requirements of both the FCC Part 15 and IC requirements. This label should be used when the end product is large enough to display the content of Fig. A-1 in a conspicuous location.

Figure A-2. Large sample label for WF-100 802.11b Module

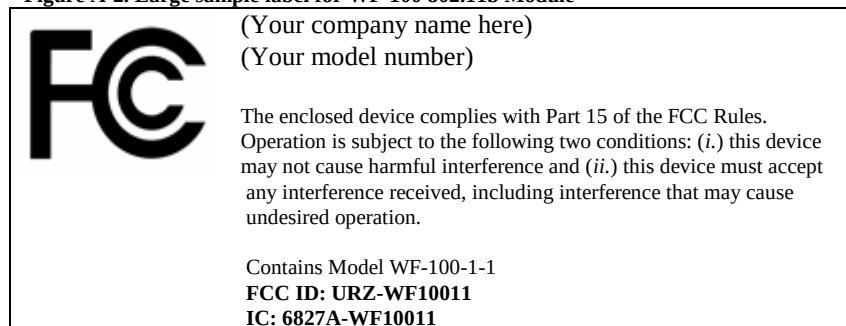


Figure A-3 depicts a sample label to satisfy the requirements of both the FCC Part 15 and IC requirements. This label should be used when the end product is too small for the full label. When this label arrangement is used, the contents of Fig. A-1 must be placed in a prominent location in the instruction manual or pamphlet supplied to the user or, alternatively, shall be placed on the container in which the device is marketed.

Figure A-3. Small sample label for WF-100 802.11b Module

