POINT TO POINT WIRELESS SOLUTIONS GROUP

MOTOROLA

Technical Report

PTP250 Regulatory Software Summary supporting the FCC approval

phn-2423 001V002

John Sharman

Abstract

This document demonstrates the methods used by Motorola Solutions to ensure that operation of the PTP5X250 product in the field guaranteed to conform to FCC regulations and how unauthorised software upgrades are prevented.

Version details

Version	Date	Change	Author
001V002	2 October 2011	Removed reference to QWP58250 from Appendix	Clem Fisher
001V001	12 October 2011	Modified Document to refer to software controls rather than an FCC Class II change. Makes document more generic	Clem Fisher
001v000	26 Sept 2011	Issued version	John Sharman
000v002	19 Sept 2011	Various changes after initial review	John Sharman
000v001	8 Sept 2011	Initial	John Sharman

Table of Contents

1. Introduction

Motorola is releasing a product which will operate in the 5.8GHz band under FCC Part 15C and in the 5.4GHz band under FCC Part 15E. This product will be known as the PTP5X250 and when made available for sale in the USA must only be capable of operation in accordance with FCC rules. Motorola identifies in this document the controls in place to ensure that only software released by Motorola can be used on this product and therefore how it will ensure continuing compliance with FCC rules in the event of future changes.

2. References

International standards

[1] FCC Part 15 Subpart E UNII Devices (15.401 ff)

[2] Not used

National standards

[3] FCC KDB 594280, “Restrictions on Software Configuration for devices not approved as Software Defined Radios” V 01: 6/8/2011

[4] FCC KDB 442812, “Software Defined Radio Application Guide” V02: 2/24/2011

[5] FCC KDB178919, “Permissive Change Policies” V 05: 6/8/2011

[6] FCC KDB634817 “Frequency Range Listings for Certification Grants” V 02: 5/20/2011

Motorola documents

[7] Phn 2418, PTP250 Operational Description

3. Background

The FCC guidance KDB 594280 opens up the possibility for a manufacturer to add functionality to an approved product on non-SDR approvals. This KDB states -

“The commission may allow grantees to permit specific parties, such as operating system providers, service providers or parties under the direct control of the grantee to enable software upgrades for field deployed non-SDR devices if the details of such arrangements are provided in a Class II permissive change filing made directly with the Commission.”

Based on this, Motorola wishes to identify by the original submission and not by a Class II change the methods that would be used to comply with FCC guidelines in the KDB in the event of future changes.

The Motorola products sold in North America (USA and Canada) are different products to those sold in the Rest of the World. RoW products have different Motorola part numbers and do not carry FCC ID markings. See detailed listing in Product Operational Description document Phn 2418, ref [7].

Motorola is submitting the PTP5X250 for approval under FCC Part 15.407 to operate at 5.4GHz and Part 15.247 to operate at 5.8GHz. Motorola addresses below the basic methods that would used to comply with the provisions of under the Permissive change KDB178919 V5.0 in the event that future field upgrades would be required.:

The data that follows contains information required by the FCC in support of the proposal and provides evidence of how compliance to FCC rules will be maintained for all the PTP250 products.

It includes a description of how such control is implemented to prevent third party modifications.

Appendix A -

Software Security Description Guide

The numbering in this appendix follows the numbering of the table in Part II of the SDR Application Guide, KDB442812.

A.1 Description Software

A.1.1 General software operation description

Software Configuration

A digital signature algorithm (DSA) is used to secure the software. An SHA-1 cryptographic hash of the software image is generated, and then signed with a 1024 bit asymmetric cipher. The private key is known only to the Motorola Solutions Point-to-Point Fixed Wireless Solutions Group. The public key is embedded in the software image, which allows a software image to check its own integrity and the integrity of another software image e.g. one uploaded for a software upgrade.

The signature of a software image is checked before it is allowed to run on a specific PTP250 model. An incorrectly signed software image is not allowed to run. This mechanism (and the secrecy of the private key) ensures that only software images produced by Motorola Solutions Point to Point radio group can run on PTP250 equipment.

Normal Operation

Referring to the block diagram in section A1.3, frames arriving on the Ethernet LAN port are processed by the Ethernet driver and passed to the packet routing function. Frames arriving on the wireless port are processed by the radio driver and passed to the packet routing function. The packet routing function routes packets to the management function, Ethernet LAN or wireless port.

Frames from the packet routing function destined for the wireless medium are processed by the radio driver and transmitted by the radio. Frames from the packet routing function destined for the Ethernet LAN are processed by the Ethernet driver and transmitted via Gigabit Ethernet.

The management function provides the operator, via SNMP or HTTP, with the ability to configure the equipment; monitor the operation of the equipment; and upgrade the operational software. The management function is responsible for maintaining the configuration supplied to the configuration server. The configuration server provides operational configuration for the radio and Ethernet drivers.

A.1.2 Radio frequency parameters modified by the software without any hardware changes.

The software has the ability to modify the following radio parameters:

- Channel bandwidth – 20 or 40 MHz
- Channel frequency (within the bounds of the band of operation)
- Power output level, according to band of operation
  - In operation in the 5.4GHz band the Power Output level cannot be increased beyond the factory preset level which complies with the EIRP limits in 15.407

- Modulation and coding scheme

The operator of the equipment is permitted to:

- Select the country of operation – noting that there is a limited list available, all of which configure the equipment in a way that is compliant with FCC regulations
- Select channel bandwidth – 20 or 40 MHz
- Select either 5.4GHz or 5.8GHz band operation
- Bar specific channel frequencies (to avoid interference or in the presence of a TDWR)
- Reduce power output from the maximum permitted by the regulations
- When using external antennas, to use the antenna gain and feeder cable loss to further limit the max Conducted Power permitted not to exceed the 1W EIRP of 15.407 with the higher gain antenna.
- Cap the modulation and coding scheme
- The software only ever permits the operator to operate within regulatory limits. For example when operating in the 5.4 GHz band, it is not possible to turn off DFS (radar detection). There is no facility to modify DFS functionality or the detection level. In particular, operation in the band 5600-5650MHz is permanently barred in the products placed on the market in the USA (and Canada).

A.1.3 High level (simplified) block diagram of the software architecture.

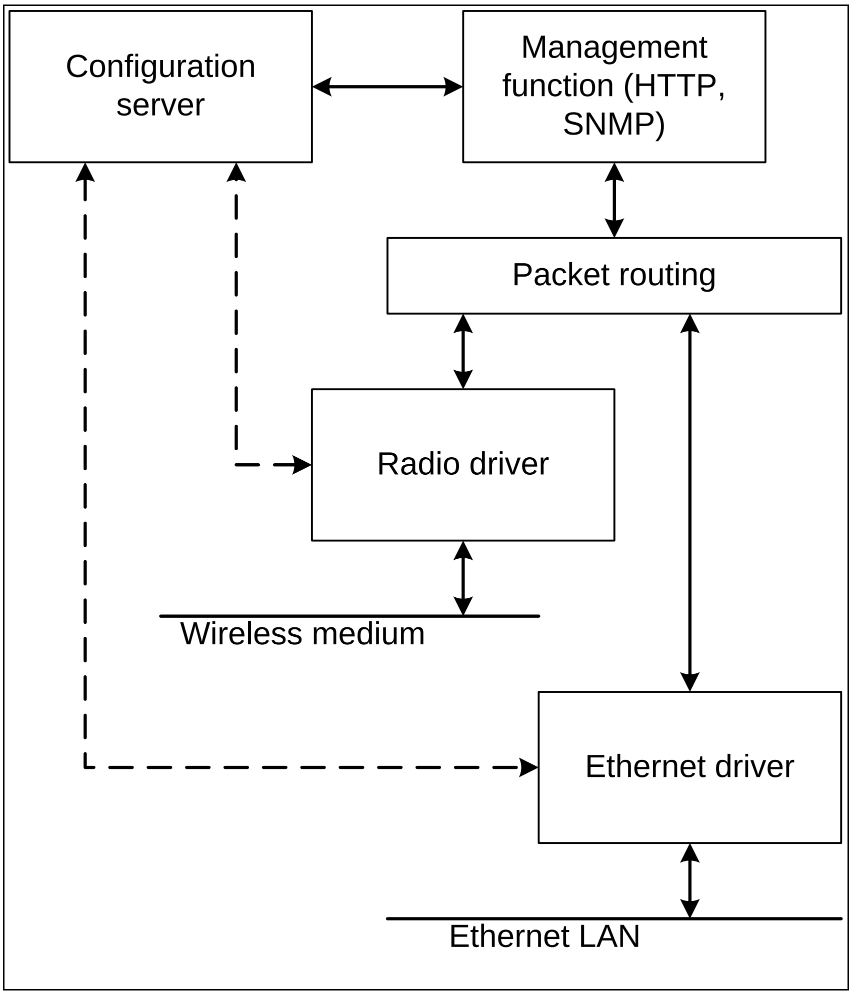


Figure 1: Software Architecture

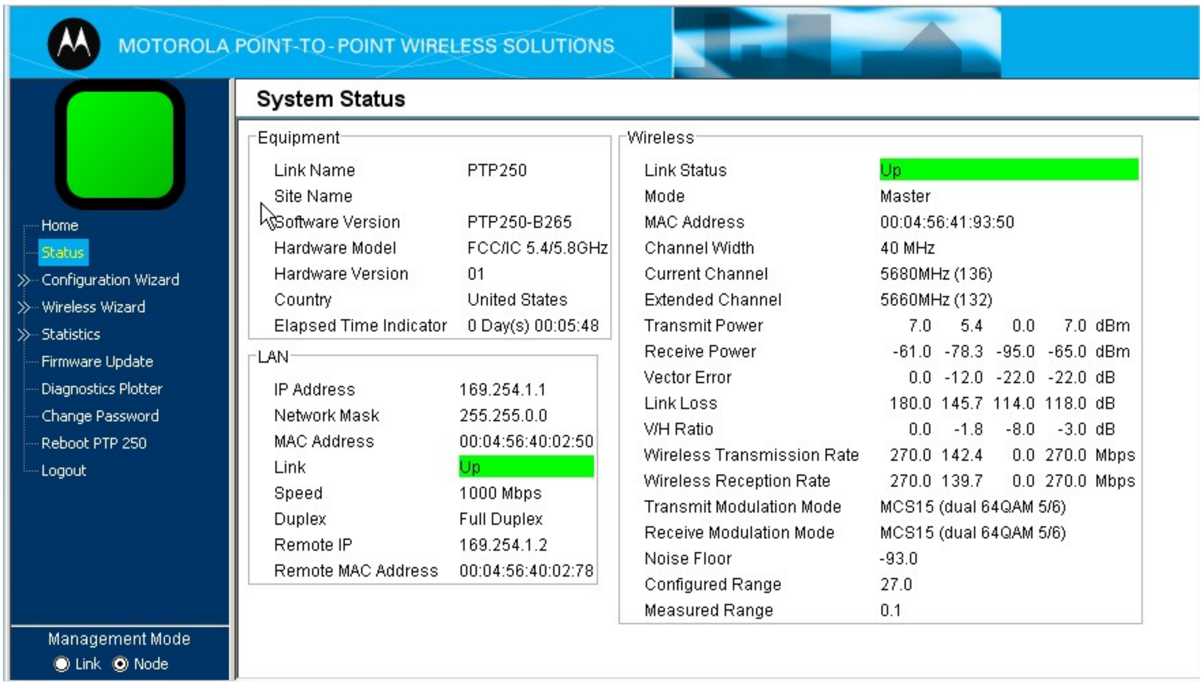
A.2 Labelling

A.2.1 How will the device be labelled?

The device will be fitted with a label on the casing showing the FCC ID 'QWP5X250' . The label also shows the product part numbers specific to the region of sale. Details of the labels are shown in ref [7].

A.2.2 Verifying the correct version of software is running

The operational software version is determined by looking at the user GUI. Using any standard web browser, enter the IP address of the unit, login with the username and password and examine the Status page. The software version is listed in the Equipment section, under “Software Version”.



System Status

Equipment

Link Name	PTP250
Site Name	
Software Version	PTP250-B265
Hardware Model	FCC/IC 5.4/5.8GHz
Hardware Version	01
Country	United States
Elapsed Time Indicator	0 Day(s) 00:05:48

LAN

IP Address	169.254.1.1
Network Mask	255.255.0.0
MAC Address	00:04:56:40:02:50
Link	Up
Speed	1000 Mbps
Duplex	Full Duplex
Remote IP	169.254.1.2
Remote MAC Address	00:04:56:40:02:78

Wireless

Link Status	Up				
Mode	Master				
MAC Address	00:04:56:41:93:50				
Channel Width	40 MHz				
Current Channel	5680MHz (136)				
Extended Channel	5660MHz (132)				
Transmit Power	7.0	5.4	0.0	7.0	dBm
Receive Power	-61.0	-78.3	-95.0	-65.0	dBm
Vector Error	0.0	-12.0	-22.0	-22.0	dB
Link Loss	180.0	145.7	114.0	118.0	dB
V/H Ratio	0.0	-1.8	-8.0	-3.0	dB
Wireless Transmission Rate	270.0	142.4	0.0	270.0	Mbps
Wireless Reception Rate	270.0	139.7	0.0	270.0	Mbps
Transmit Modulation Mode	MCS15 (dual 64QAM 5/6)				
Receive Modulation Mode	MCS15 (dual 64QAM 5/6)				
Noise Floor	-93.0				
Configured Range	27.0				
Measured Range	0.1				

Figure 2: GUI status page

Selecting the Status page will also display information, including Hardware Model, and the Country selected.

A.2.3 Software Version numbering system.

Numbers in the format PTP250-Bnnn (as shown in the above figure) are development versions, released software versions are as follows -

01-00 Software version for the initial grant for the product operating at 5.8GHz only.

01-03 Software update added codes for operation in South America countries

Any version between 01-00 and 02-09 (e.g. 01-03, 01-99, 02-00 or 02-09) is fully representative of the equipment exhibits in the initial grant.

Versions 02-10 and greater (e.g. 02-11; 03-00) would represent the version as modified by the Class II change.

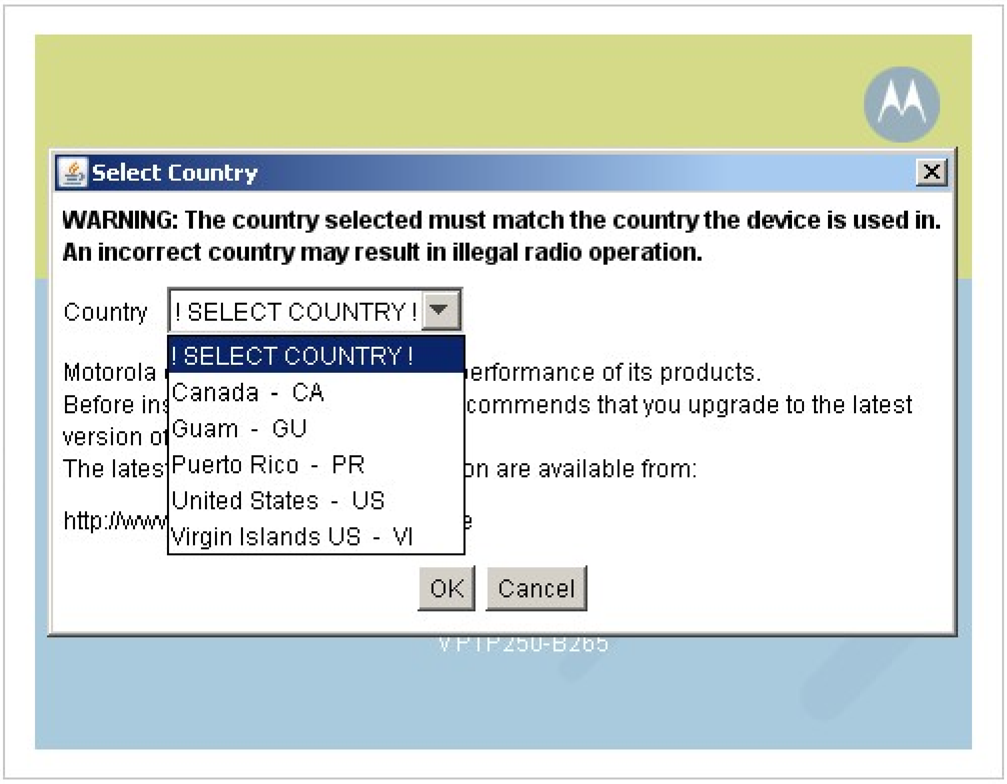
A.3 Security

A.3.1 Third party operation

Question - Procedure to ensure third parties cannot operate US sold devices on any other regulatory domain frequencies, or in any manner that is in violation of the certification.

A hardware model is programmed into non-volatile storage during manufacture. The software uses the hardware model to determine which regulatory domains are presented to the operator. Only software released by Motorola can be used by the product as the software is digitally signed and the signature is checked when new software is loaded. For devices sold in USA, only regulatory domains which comply with FCC regulations are available as options in the software.

On the first login to a new unit, or on the first login to a unit that has been reset to full default configuration, the *Select Country* page is displayed. The user must select the appropriate country (regulatory domain) of operation.



Select Country

WARNING: The country selected must match the country the device is used in. An incorrect country may result in illegal radio operation.

Country ! SELECT COUNTRY !

- ! SELECT COUNTRY !
- Canada - CA
- Guam - GU
- Puerto Rico - PR
- United States - US
- Virgin Islands US - VI

Motorola erformance of its products.
Before ins commends that you upgrade to the latest
version of
The lates on are available from:

http://www e

Figure 3: Country of operation selection

A.3.2 Third party capability

Question - Explain if any third parties have the capability to operate a US sold device on any other regulatory domain frequencies, or in any manner that is in violation of the certification.

A PTP250 device sold in the USA (and hence marked with an FCC ID) cannot be operated in a manner that is in violation of FCC certification because the hardware model type is programmed into non-volatile storage during manufacture.

A.3.3 Software updates

Question -Describe how the software updates are distributed for all regulatory domains and what procedures ensures that a product sold in the US can only operate as granted on US frequencies and at authorized radio

There is a single software image for all regulatory domains. This is available for download from the Motorola Solutions web-site. A hardware model is programmed into non-volatile storage during manufacture. The software uses the hardware model to determine which regulatory domains are presented to the operator. For FCC hardware models, only regulatory domains which comply with FCC regulations are available.

A.3.4 Modification by third parties

Question - If the product cannot be modified by third parties and can only operate as granted on US frequencies and with authorized radio parameters, explain how this is achieved.

A hardware model is programmed into non-volatile storage during manufacture. The software uses the hardware model to determine which regulatory domains are presented to the operator. For FCC hardware models, only regulatory domains which comply with FCC regulations are available. Additionally the software images are digitally signed to ensure unauthorised modification of the software is impossible and 3rd party software cannot be used

A.3.5 Non US software version

Question - What stops third parties from loading non-US versions of software onto products intended for US sale?

See answers to questions 3.3 and 3.4 above.

A.3.6 Factory level changes

Question - Can third parties make factory level changes to reload non-US domain codes, etc.

Access by the user to re-programme, for example the hardware model type, is prevented by requiring a password challenge/response authentication. Access to this challenge/ response generator is closely controlled by Motorola Solutions Point to Point radio group and restricted to those Motorola employees with a strict need. The challenge/ response generator software has a list of MAC addresses built into it and will only run on computer hardware with one of those MACs.

A.4 Unauthorised software changes

A.4.1 Open source software

Question - Describe how open source is the operating code for granted RF properties. Describe the difficulty and proprietary nature of the code that controls the RF parameters as granted.

As detailed in sections 3.3 and 3.4 above, code that has not been signed by Motorola will not run on PTP250. A part of the software is based on open source code: the kernel is open source, as are the shims we use to connect to our proprietary radio drivers. However it is not possible for a third party to modify the software and build an image that will run on PTP250 - the image would need to be digitally signed by Motorola Solutions.