SOFTWARE SECURITY FOR U-NII DEVICES

Pursuant to FCC Part 15E 15.407(i) and KDB 594280 D02 U-NII Device Security, applicant must describe the overall security measures and systems that ensure that only:

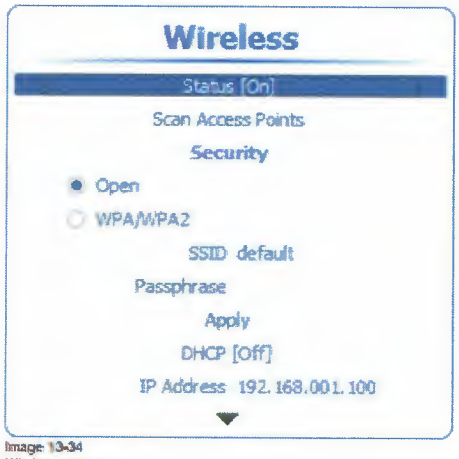
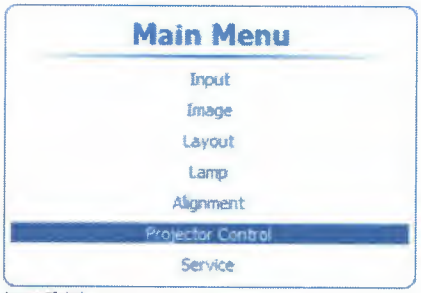
1. Authenticated software is loaded and operating the device.
2. The device is not easily modified to operate with RF parameters outside of the authorization

The description of the software must address the following questions in the operational description for the device and clearly demonstrate how the device meets the security requirements.

General Description	1. Describe how any software/firmware updates for elements than can affect the device's RF parameters will be obtained, downloaded, validated and installed. For software that is accessed through manufacturer's website or device's management system, describe the different levels of security as appropriate.
	Pulse software updates are made available on the public Barco website www.barco.com on the product portal. Once the user gets the update notification, they can update software/firmware automatically.
	2. Describe the RF parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited such that any other software/firmware changes will not allow the device to exceed the authorized RF characteristics?
	All limitations to comply with legal regulations are controlled within the device's software and hardware. The user can only change the following parameters related to WLAN: - Wireless SSID - WPA2-PSK passphrase The user has no access to any RF related parameters which could compromise the grant of authorization
	3. Describe in detail the authentication protocols that are in place to ensure that the source of the RF-related software/firmware is valid. Describe in detail how the RF-related software is protected against modification.
	Firmware updates on the target device are performed by uploading a firmware package. All firmware packages that are made available for the device are encrypted using an encryption key. When the device receives such a package (either through USB or through a network interface) it will first decrypt and inspect it. The decryption will fail if the package was created with an unknown key or if the package has been tampered with.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.

	Firmware packages are encrypted using a passphrase protected 2048 bit RSA keypair using GPG.
	5. For a device that can be configured as a master and client (with active or passive scanning), explain how the device ensures compliance for each mode? In particular if the device acts as master in some band of operation and client in another; how is compliance ensured in each band of operation?
	Not applicable, this device is a client-only device.

3rd Party Access Control	1. Explain if any third parties have the capability to operate a U.S.-sold device on any other regulatory domain, frequencies, or in any manner that may allow the device to operate in violation of the device's authorization if activated in the U.S.
	No, units sold into the USA market are pre-programmed with the US regulatory domain limiting its operation into the allowed domain and frequencies. The user or installer cannot change this.
	2. Describe, if the device permits third-party software or firmware installation, what mechanisms are provided by the manufacturer to permit integration of such functions while ensuring that the RF parameters of the device cannot be operated outside its authorization for operation in the U.S. In the description include what controls and/or agreements are in place with providers of third-party functionality to ensure the devices' underlying RF parameters are unchanged and how the manufacturer verifies the functionality.
	No, the device cannot be upgraded by 3rd party firmware or Software. The Pulse unit does not permit third-party software or firmware installation. The Pulse unit operates with Barco NV software only. All 3rd party software cannot access any RF parameters, because users do not need to know and access any RF parameters.
	3. For Certified Transmitter modular devices, describe how the module grantee ensures that host manufacturers fully comply with these software security requirements for U-NII devices. If the module is controlled through driver software loaded in the host, describe how the drivers are controlled and managed such that the modular transmitter RF parameters are not modified outside the grant of authorization.
	Not applicable, this device is not a module. The device follows a system level certification and does not rely on the modular transmitter certification.

User Configuration guide	1. Describe the user configurations permitted through the UI. If different levels of access are permitted for professional installers, system integrators or end-users, describe the differences.
	The UI is accessible to Barco trained personnel only. None of the RF parameters which could compromise the grant of authorization are accessible. Barco NV does not have any UI for RF parameters.
	a) What parameters are viewable and configurable by different parties?
	Through the OSD menu on the Pulse, WiFi can be configured (scan access points/ WPA or WPA2 / DHCP ON or OFF. 2. Press **ENTER** to select.  Image 13-34 Wireless, status For GSM/3G module only SIM pincode + subscription is available.  Image 13-141 Main menu, projector control  Image 13-142 Projector control, GSM configuration  Image 13-143 SMS subscription  Image 13-144 Subscriber

	b) What parameters are accessible or modifiable by the professional installer or system integrators?
	Wifi: scan access points/ WPA or WPA2 / DHCP ON or OFF GSM/3G: Pincode SIM + SMS subscription
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	All above parameters have pre-defined ranges according to the certification test result. None of the RF parameters which could compromise the grant of authorization are accessible.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	All above parameters have pre-defined ranges according to the certification test result. None of the RF parameters which could compromise the grant of authorization are accessible.

User Configuration guide	c) What parameters are accessible or modifiable to by the end-user?
	No RF parameters which could compromise the grant of authorization are accessible or modifiable to the end-user.
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?
	All accessible parameters can only be changed according to the certification tests performed on this device
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	No RF parameters which could compromise the grant of authorization are accessible or modifiable to the end-user.
	d) Is the country code factory set? Can it be changed in the UI?
	The country code cannot be changed in the UI.
	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
	N/A
	e) What are the default parameters when the device is restarted?
	The configuration is the same as the previous operating configuration.
	2. Can the radio be configured in bridge or mesh mode? If yes, an attestation may be required. Further information is available in KDB Publication 905462 D02.
	No, the radio cannot be configured in bridge or mesh mode.
	3. For a device that can be configured as a master and client (with active or passive scanning), if this is user configurable, describe what controls exist, within the UI, to ensure compliance for each mode. If the device acts as a master in some bands and client in others, how is this configured to ensure compliance?
	Not applicable, this device is a client-only device.
	4. For a device that can be configured as different types of access points, such as point-to-point or point-to-multipoint, and use different types of antennas, describe what controls exist to ensure compliance with applicable limits and the proper antenna is used for each mode of operation. (See Section 15.407(a))
	Not applicable

Product Name: Pulse

The applicant: Barco NV

FCC ID: 2AOUF-R8767900X

Name: / Title: Ignace Rombaut /VP Projection Division
Signature: