

Panasonic

Date: June, 13th, 2019

to:	from:
Regulatory Certification Body DEKRA Testing and Certification, S.A.U. Parque Tecnológico de Andalucía C/ Severo Ochoa 2 & 6 29590 Campanillas Málaga, España	Panasonic Automotive Systems Company of America 776 Georgia Hwy 74 Peachtree City, GA 30269 – USA

Related to product:

Type of equipment:	High Performance Display Controller for an infotainment system
Brand name:	Panasonic
FCC ID:	ACJ932A-HPDC
IC:	216A-HPDC

To whom it may concern,

We hereby declare that this device is programmed to operate only in the following frequencies:

2.4 GHz Band,

Frequency Range **2.401 - 2.482 GHz**

- Channels 1-11 (BW 22 MHz)
- Channels 1-11 (BW 20 MHz)
- Channels 3 and 11 (BW 40 MHz)

5GHz Band,

In Canada, the device won't operate in the frequency range **5.6 – 5.65 GHz** (channels within this range won't be used)

- Frequency Range **5.170 – 5.330 GHz**
 - Channels 36-64 (BW 20 MHz)
 - Channels 38-62 (BW 40 MHz)
 - Channels 42 and 58 (BW 80 MHz)
- Frequency Range **5.490 – 5.730 GHz**
 - Channels 100-144 (BW 20 MHz) (Except 120, 124, 128 in Canada)
 - Channels 102-142 (BW 40 MHz) (Except channels 118 and 126 in Canada)
 - Channels 106 and 138 (BW 80 MHz) (not in channel 122 in Canada)



Operation modes, DFS and TPC

This device does not support Ad-Hoc / Wi-Fi hotspot mode in 5 GHz frequency band where the device operates as a client device without Radar detection.

Ad-hoc / Wi-Fi hotspot feature is limited to 11 channels available in 2.4 GHz frequency band.

As client device, this product does not initiate transmission of any probes, beacons and does not initiate Ad-Hoc operations when not associated with and under the control of a certified master device, according to Section 15.202 of FCC rules.

Future changes in this device will not change these operational characteristics, in any mode of operation.

Software security description per KDB 594280 D02:

General Description	1. Describe how any software/firmware updates for elements that 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.	Releases are present in PASA's internal artefact storage server but shared to customer on their shared location on a need bases. Software is not present on the manufacturer's website.
	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?	RF parameters are stored in a separate file which can only be modified by PASA's electrical\RF team only. These are also verified by software team before they are integrated into the build.
	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.	As explained above the parameters are modified only by PASA's electrical\RF team and verified before the parameter values are passed on to software. Software team verified and integrates the RF parameters which are part of a single file.

Panasonic


	<p>4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.</p>	<p>RF parameter file is converted to bin format which is not readable but can only be interpreted by software before this file is integrated into the build.</p>
	<p>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?</p>	<p>We do not have any requirement at present to configure HPDC to work both as an access point and in station mode at the same time.</p>
<p>Third-Party Access Control</p>	<p>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.</p>	<p>Third party software is not allowed on the device unless approved by PASA \ end customer.</p>
	<p>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.</p>	<p>The software is signed with production or customer keys, so third party software cannot be installed unless it is signed with the same keys which is known only to customer.</p>

Panasonic

	<p>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.</p>	<p>As explained above the parameters are modified only by PASA's electrical\RF team and verified before the parameter values are passed on to software. Software team verified and integrates the RF parameters which are part of a single file.</p>
--	---	--

Sincerely,

P.A.



By: Benjamin Onambele
Title: Program Manager
Company: Panasonic Automotive Systems of America
Telephone: +1-770-515-1484
e-mail: Benjamin.Onambele@ext.panasonicautomotive.com