

# SOFTWARE SECURITY INFORMATION

**FCC ID:** U4GDL35US                      **IC**        : 3862E-DL35US

Pursuant to:  
FCC Part 15E 15.407(I) and KDB 594280 D02 UNII Device Security v01r03 / IC RSS-247article 6.4(4).

The information within this section is to show compliance against the SW Security Requirements laid out within KDB 594280 D02 U-NII Device Security v01r03. The information below describes how to maintain the overall security measures and systems so that only:

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

SOFTWARE SECURITY DESCRIPTION		
	Requirement	Answer
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.	Datalogic introduces new SW after a complete SW verification and validation process. The SW is delivered through a Datalogic SW delivery system/ Datalogic uses proprietary radio that can only runs Datalogic SW.
	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 the radio frequency parameters are transmit power, operating channel, carrier bandwidth, modulation type, frequency band edge. Some parameters are fixed after factory calibration, such as transmit power, frequency band edge. Only authorized parameters are available and can be set in software. These authorized parameters do not make device exceed the authorized RF characteristics.
	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.	The SW runs a load validation during the SW upgrades process to ensure that the SW is legitimate, unaltered, and downloaded correctly. The software image contains a proprietary digital signature. The SW, radios, and load validation are proprietary. SW images and loads are only available through the Datalogic SW delivery system. If device be out of factory, transmit power, frequency band edge cannot be modified anymore.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Software images are encrypted using Google N’s default encryption methods.
	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?	The device is a slave only.

	<b>Requirement</b>	<b>Answer</b>
<b>Third Party Access Control</b>	1. Explain if any third parties have the capability to operate a U.S./Canada -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./Canada.	The device cannot be configured in any manner which would violate the authorization of the country in which it is operated.
	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./Canada. 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.	The device does not permit third party SW or firmware installation. The SW, firmware and radios are Datalogic proprietary. The SW runs a load validation procedure during the SW upgrades process to ensure that the SW is legitimate, unaltered, and downloaded correctly. The software image contains a proprietary digital signature and any SW image will be rejected if the digital signature is not correct. SW images and loads are only available through the Datalogic SW delivery system.
	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.	This product is not a module

This section is required for devices which have a "User Interface" (UI) to configure the device in a manner that may impact the operational parameter. The operation description must address if the device supports any of the country code configurations or peer-peer mode communications discussed in KDB 594280 D01.

<b>SOFTWARE CONFIGURATION DESCRIPTION</b>		
	<b>Requirement</b>	<b>Answer</b>
<b>USER CONFIGURATION GUIDE</b>	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 only accessible to the professional installer.
	a) What parameters are viewable and configurable by different parties?	The professional installer can change the RF channel and adjust Tx power level to a lower level.
	b) What parameters are accessible or modifiable by the professional installer or system integrators?	
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	The RF channel can only be set to FCC approved channels. The TX power level can be set up to the approved RF power levels (or less). The MCC determines the authorized valid range of values that the professional installer can configure.

(2) What controls exist that the user cannot operate the device outside its authorization in the U.S./Canada?	All radio parameters are limited by SW settings pre-determine by the FCC radio regulatory approval process. These parameters are in a drop-down list in the GUI and cannot go outside of these approved values.
c) What parameters are accessible or modifiable by 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?	The MCC determines the authorized valid range of values that the operator can configure
(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S./Canada?	All radio parameters are limited by SW settings pre-determine by the FCC radio regulatory approval process.
d) Is the country code factory set? Can it 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./Canada?	The country code can not change.
e) What are the default parameters when the device is restarted?	The device cannot become operational until the professional installer configures the country code (MCC). The device goes to a default (approved) Tx channel and power level based on factory country setting.
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.
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?	The device is a slave only.
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)).	The device cannot be configured as different types of access points

Name and surname of applicant (or authorized representative): Ruggero Cacioppo

Date: October 28, 2020

Signature: 