

Operation Description

K20/k21 is based on RockChip RK3576 hardware platform, the device uses Google's Android operating system, support WiFi, Ethernet and NFC functions.

The hardware of the device consists of a motherboard and other components.

SLX-PWL27-P4 is an AC to DC power board with a load capacity of 12V 2A.

The motherboard input voltage is 12V, which can be converted to 3.3V, 1.8V, 0.9V by other DCDC.

As the core of the whole hardware system, the motherboard contains RK3576, RK806S-5, JL2101B and other main components, which realize the main functions of the system baseband and RF through the combination of functions.

As the core control center of the system, the RK3576 features a quad-core Cortex-A72 and a quad-core Cortex-A53 application processor, along with an independent NEON coprocessor and an embedded modem system. The modem subsystem handles functions related to the modem, including traditional wireless device features such as the OTA protocol stack, PMIC control, and audio. The application processor runs the Android system, which includes the Linux kernel, the JAVA virtual machine, and various applications. Touch screen signals can be directly read through the integrated touch screen control function.

RK3576 is connected to EMMC through EMM (External Memory Interface) to realize application and data storage as well as application operation.

AP6256 is a chip with Bluetooth and WIFI functions. Bluetooth: RK3576 is connected to AP6256 through SDIO interface to realize audio and file transmission function.

RK3576 communicates with the power management chip RK809-5 through a dedicated IIC (inter-integrated circuit) interface to manage the power supply of each component on the motherboard.

RK3576 communicates with NFC chip PN7160A1HN-C100E through a dedicated IIC (inter IC) interface, and exchanges near field communication data through NFC antenna.

The RK3576 generates a 24MHz clock internally and stabilizes the clock frequency through an external resonator. The 24MHz oscillator also serves as the primary clock source for the baseband.

32.768KHZ The oscillator is connected to RK806S-5 and used as the clock source of RTC and baseband sleep time.

The AP6256 integrates WIFI and BT RF transceivers as well as protocol processing. WiFi supports 11a/b/g/n/ac and BT supports BT5.2.

WIFI Function:

Frequency:

BT/BLE:2402-2480 MHz

2.4G wifi
2412-2472MHz

5G wifil
5180 MHz to 5240 MHz (U-NII-1)
5260 MHz to 5320 MHz (U-NII-2A)
5500 MHz to 5720 MHz (U-NII-2C)

5745 MHz to 5825 MHz (U-NII-3)

Modulation:

BLE: GFSK

BT: GFSK, $\pi/4$ -DQPSK, 8DPSK

2.4G WIFI: IEEE 802.11b: DSSS(CCK, DQPSK, DBPSK)

IEEE 802.11g/n: OFDM(64-QAM, 16-QAM, QPSK, BPSK)

5G WIFI: IEEE 802.11a: OFDM(64QAM, 16QAM, QPSK, BPSK)

IEEE 802.11n: OFDM(64QAM, 16QAM, QPSK, BPSK)

IEEE 802.11ac: OFDM(256QAM, 64QAM, 16QAM, QPSK, BPSK)

BLE Data Rates:	1Mbps/2Mbps
-----------------	-------------

Supported channels:

BLE:

Channel	Frequency (MHz)						
0	2402	11	2424	22	2446	33	2468
1	2404	12	2426	23	2448	34	2470
2	2406	13	2428	24	2450	35	2472
3	2408	14	2430	25	2452	36	2474
4	2410	15	2432	26	2454	37	2476
5	2412	16	2434	27	2456	38	2478
6	2414	17	2436	28	2458	39	2480
7	2416	18	2438	29	2460	/	/
8	2418	19	2440	30	2462	/	/
9	2420	20	2442	31	2464	/	/
10	2422	21	2444	32	2466	/	/

BT:

Channel	Frequency (MHz)						
00	2402	20	2422	40	2442	60	2462
01	2403	21	2423	41	2443	61	2463
02	2404	22	2424	42	2444	62	2464
03	2405	23	2425	43	2445	63	2465
04	2406	24	2426	44	2446	64	2466
05	2407	25	2427	45	2447	65	2467
06	2408	26	2428	46	2448	66	2468
07	2409	27	2429	47	2449	67	2469
08	2410	28	2430	48	2450	68	2470
09	2411	29	2431	49	2451	69	2471
10	2412	30	2432	50	2452	70	2472
11	2413	31	2433	51	2453	71	2473
12	2414	32	2434	52	2454	72	2474
13	2415	33	2435	53	2455	73	2475
14	2416	34	2436	54	2456	74	2476
15	2417	35	2437	55	2457	75	2477
16	2418	36	2438	56	2458	76	2478
17	2419	37	2439	57	2459	77	2479
18	2420	38	2440	58	2460	78	2480
19	2421	39	2441	59	2461	/	/

2.4G WIFI:

Channel List For Bandwidth=20 MHz							
Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)
1	2412	5	2432	9	2452	13	2472
2	2417	6	2437	10	2457	/	/
3	2422	7	2442	11	2462	/	/
4	2427	8	2447	12	2467	/	/

5G WIFI:

UNII-1 (For Bandwidth=20MHz)			UNII-1 (For Bandwidth=40MHz)			UNII-1 (For Bandwidth=80MHz)		
Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel
36	5180	active	38	5190	active	42	5210	active
40	5200	active	46	5230	active			
44	5220	active						
48	5240	active						

UNII-2A (For Bandwidth=20MHz)			UNII-2A (For Bandwidth=40MHz)			UNII-2A (For Bandwidth=80MHz)		
Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel
52	5260	passive	54	5270	passive	58	5290	passive
56	5280	passive	62	5310	passive			
60	5300	passive						
64	5320	passive						

UNII-2C (For Bandwidth=20MHz)			UNII-2C (For Bandwidth=40MHz)			UNII-2C (For Bandwidth=80MHz)		
Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel
100	5500	passive	102	5510	passive	106	5530	passive
104	5520	passive	110	5550	passive	122	*5610	passive
108	5540	passive	118	*5590	passive	/	/	
112	5560	passive	126	*5630	passive			
116	5580	passive	134	5670	passive			
120	*5600	passive	/	/				
124	*5620	passive						
128	*5640	passive						
132	5660	passive						
136	5680	passive						
140	5700	passive						
/	/							

Notes: * not operational in Canada (5.6-5.65GHz are disabled by software when sold to Canada. There is a country code regulatory parameter to limit the support channel. The country code is factory set when sale out to the Country of destination. For example, when sale to Canada, the factory must select the Canada country code and the 5.6-5.65GHz are disabled by software.)

UNII-3		UNII-3		UNII-3	
Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)

149	5745	active	151	5755	active	155	5775	active
153	5765	active	159	5795	active			
157	5785	active						
161	5805	active						
165	5825	active						

Antenna Type and Antenna Gains:

BT/BLE:

Antenna	Frequency (MHz)	Antenna Type	MAX Antenna Gain (dBi)
1	2402-2480	Dipole Antenna	1

2.4G WIFI:

Antenna	Frequency (MHz)	Antenna Type	MAX Antenna Gain (dBi)
1	2412-2472	Dipole Antenna	1

5G WIFI:

Antenna No.	Frequency Band	Antenna Type	Max Antenna Gain (dBi)
1	5150-5850	Dipole Antenna	1

Max. tune-up power with tolerance:

BT (peak):

GFSK: 7 ± 1 dBm

$\text{π}/4$ -DQPSK ,8DPSK: 4.6 ± 1 dBm

BLE (peak)

LE 1M & LE 2M: 6 ± 1 dBm

2.4G wifi(average)

b mode ANT1: 16 ± 1 dBm

b mode 2472MHz ANT1: 12 ± 1 dBm

g mode ANT1: 14.5 ± 1 dBm

g mode 2472MHz ANT1: 8 ± 1 dBm

n20 ANT1: 14 ± 1 dBm

n20 2467MHz ANT1: 11 ± 1 dBm

n20 2472MHz ANT1: 8 ± 1 dBm

5G wifi(average)

UNII-1

a ANT1: 15.5 ± 1 dBm

n20/ac20 ANT1: 15.5 ± 1 dBm

n40/ac40 ANT1: 15.5 ± 1 dBm

ac80 ANT1: 15 ± 1 dBm

UNII-2A

A ANT1: 15.5 ± 1 dBm

n20/ac20 ANT1: 15 ± 1 dBm

n40/ac40 ANT1: 15.5 ± 1 dBm

ac80 ANT1: 15 ± 1 dBm

UNII-2C

a ANT1: 15 ± 1 dBm

a 5720_UNII-3 ANT1: 4.5 ± 1 dBm

n20/ac20 ANT1: 14.5 ± 1 dBm
n20/ac20 5720_UNII-3 ANT1: 5 ± 1 dBm
n40/ac40 ANT1: 14.5 ± 1 dBm
n40/ac40 5720_UNII-3 ANT1: 1 ± 1 dBm
ac80 ANT1: 14.5 ± 1 dBm
ac80 5720_UNII-3 ANT1: -3 ± 1 dBm

UNII-3

a ANT1: 14.5 ± 1 dBm
n20/ac20 ANT1: 14.5 ± 1 dBm
n40/ac40 ANT1: 14.5 ± 1 dBm
ac80 ANT1: 14 ± 1 dBm

NFC Function:

Frequency: 13.56 MHz

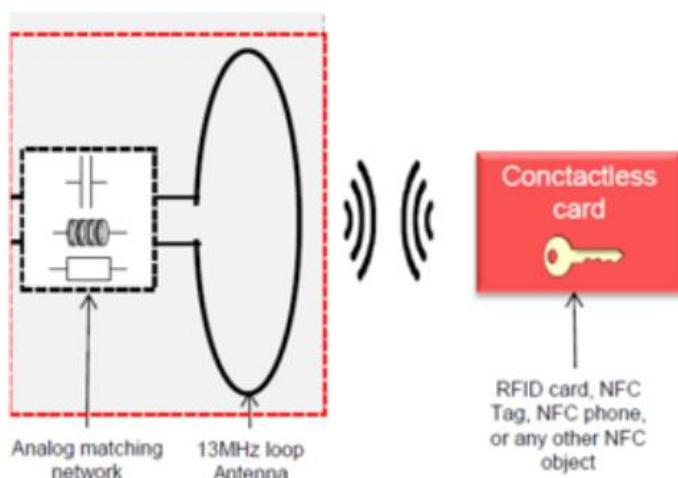
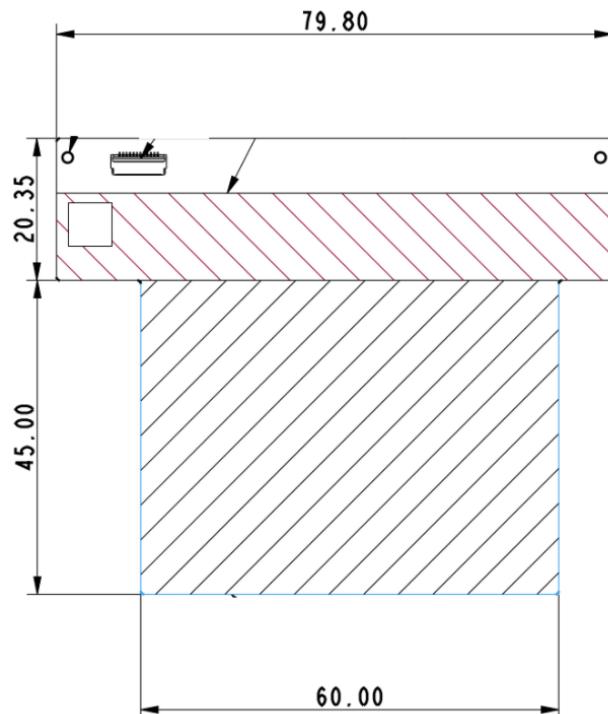
Max Peak field strength: 6.25 dB μ V/m @ 30m

Antenna:

Frequency (MHz)	Antenna Type	Antenna Gain (dBi)
13.56	Coil antenna	0

Antenna Description:

Model	K320-NFC-V01
Transmitter Frequency	13.56Mhz
Receiver Frequency	13.56Mhz
Antenna size	45x60x0.8 mm
Antenna material	PCB FR4



Note:

1. Hopping sequence is pseudorandom.
2. The associated system receiver have an input bandwidth equal to the transmitted signal bandwidth
3. The associated system receiver have the ability to hop in synchronization with the transmitter.
4. The device supports AFH mode.
5. The device supports BLE mode.
6. The frequency hopping system complies with the non-coordination requirement
7. BT&WLAN 2.4G, BT & WLAN 5G, WLAN 2.4G & WLAN 5G can't transmit simultaneously (Declared by client)
8. NFC supports both ISO /IEC 14443A and ISO /IEC 14443B. All lowest and highest data rates as per the standards are supported - 106 kbps, 212 kbps, 424 kbps and 848 kbps, all the modes had been tested, but only the worst data (ISO 14443A 106 kbps) was recorded in the report.

Software Bom List:

Software Name	Software Model	Company name
Android Keyboard (AOSP)	Version 14	Google
Calcuator	Version 14	Google
Chrome	Version 70.0.3538.110	Google
Files	Version 14	Google
Gallery	Version 1.1.40030	Google
PAXSTORE	Version 9.7.0	Shenzhen Zolon Technology Co.,Ltd.
Quickstep	Version 14	Shenzhen Zolon Technology Co.,Ltd.
Settings	Version 14	Google

Note: The Android system can restrict the installation of third-party applications through blacklist and whitelist methods. Before the product leaves the factory, the Kaspersky APP package name will be added to the prohibited installation list to prevent users from installing it.

Statement from the manufacturer:

This device complies with the requirement, Per 15.407 (c) and RSS-247 issue 3 section 6.4(a)states the device shall automatically discontinue transmission in case of either absence of information to transmit or operational failure via software.(Data transmission is always initiated by software, which is then passed down through the MAC, through the digital and analog baseband, and finally to the RF transceiver. Several special packets (ACKs, CTS, PSPoll, etc) are initiated by the MAC. These are the only ways the digital baseband portion will turn on the RF transmitter, which it then turns off at the end of the packet. Therefore, the transmitter will be on only while one of the aforementioned packets are being transmitted.)

Operation Description

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES

FCC ID: 2AV5BK20K21

Pursuant to KDB 594280 D02, RSS 247section 6.4, the overall security measures and systems that ensure that:

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

are described.

The following questions are addressed the description of the software in the operational description for the device and clearly how the device meets the security requirements.

SOFTWARE SECURITY DESCRIPTION		
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	We do not release the firmware on our website for downloading. Our direct host manufacturer (OEM) can

	<p>the different levels of security as appropriate.</p>	<p>request the firmware from us and it will be made available via secure server.</p>
	<p>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?</p>	<p>The configuration file can modify the transmit power and frequency offset; but configuration files can only be modified in the factory. All parameters approved by the FCC are programmed in OTP or in both driver and firmware which would be embedded.</p>
	<p>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.</p>	<p>Verify software through AVB encryption to prevent firmware modification</p>
	<p>4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.</p>	<p>Encryption algorithm combination: SHA256+RSA4096 SHA256 → Hash algorithm (ensuring data integrity). RSA4096 → Asymmetric Encryption Algorithm (providing digital signature or key exchange)</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>The device is client without radar detection function. The client mode is complete independence part in the Wi-Fi & Bluetooth module, so, switching between master or client mode will not affect to the other.</p>
Third-Party Access Control		
	<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>No third Party will have software, or configuration control, to program the device out of compliance of the technical rules under which it has been certified.</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'</p>	<p>This device does not permit third-party software or firmware installation.</p>

	<p>underlying RF parameters are unchanged and how the manufacturer verifies the functionality.</p> <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>For the RF-related software/firmware are built in the OS firmware (NVRAM image). All the image reference above can't not be obtained as raw format. We (the vendor) update the image by a custom specific package (which we call OS package) and also with a custom authorized tool (Term Assist tool). All the packages are tested (normal functionality test for check the firmware is valid and hash5 value check to protect against modification) before release to customers on the official website</p>
USER CONFIGURATION GUIDE	<p>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.</p> <p>a. What parameters are viewable and configurable by different parties?</p> <p>b. What parameters are accessible or modifiable to the professional installer or system integrators?</p> <p>(1). Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?</p> <p>(2). What controls exist that the user cannot operate the device outside its authorization in the U.S.?</p>	<p>There is not any UI to access WIFI setting.</p> <p>None of the RF parameters are viewable or configurable by different parties.</p> <p>There is not any WIFI parameter which is accessible or modifiable to the professional installer.</p> <p>The built in regulatory settings cannot be changed by the end-user.</p> <p>The built in regulatory settings cannot be changed by the end-user.</p>
USER CONFIGURATION GUIDE	<p>c. What parameters are accessible or modifiable by the end-user?</p> <p>(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?</p> <p>(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?</p> <p>d. Is the country code factory set? Can it be changed in the UI?</p>	<p>The end user cannot modify any RF options.</p> <p>The built-in regulatory Settings cannot be changed by the end user.</p> <p>There is a country code regulatory parameter to limit product to operate the device outside its authorization in the U.S.</p> <p>The country code is factory set and cannot be changed in the UI</p>

	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.? e. What are the default parameters when the device is restarted?	The device cannot be changed and only operate in the U.S. At each start up the factory configured country code and antenna gain is read from non-volatile memory
	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.	Not supported
	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?	NA – The device is only a client in 5 GHz operation, and has no user interface to configure the device in a manner that may impact the operational RF parameters.
	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.

The device has no user interface to configure the device in a manner that may impact the operational RF parameters. The device does not support any of the country code configurations or peer-peer mode communications discussed in KDB 594280 Publication D01