Testing & Certification of IoT Devices Operating in Unlicensed ISM Bands

Technical Article

Written by Jörg Köpp
Rohde & Schwarz
Munich, Germany

Note:
Originally published at the Wireless Congress in Munich, November 2015
# Table of Contents

1. Abstract .......................................................................................................................... 3
2. Introduction ...................................................................................................................... 4
3. Design for Conformance ............................................................................................... 5
4. The Unlicensed Band Challenge .................................................................................. 7
5. Interference Issues ......................................................................................................... 9
6. Conclusion ...................................................................................................................... 11
7. Literature ....................................................................................................................... 12
1 Abstract

The majority of devices that constitute the Internet of Things (IoT) will use wireless machine-to-machine communications technologies to communicate with each other and with IoT applications in the cloud. Some applications that require global coverage and/or mobility will focus on cellular technologies. But the majority of devices will use wireless technologies that are sharing frequencies in unlicensed bands. Before these wireless devices can go on the air, they must be tested against the applicable regulations, standards and operator-specific requirements. The coexistence of multiple technologies operating on unlicensed bands in one device or in areas with high radio usage like cars or living rooms is of great importance and therefore requires special attention in the design and validation processes. Accordingly, in order to ensure proper functionality, quality and performance throughout the product’s lifetime, it is essential to test the overall communications behavior in all phases of the product life cycle.
2 Introduction

Without the availability of low-cost communications networks and devices, the IoT would not be possible at all. The majority of devices that constitute the IoT will use wireless machine-to-machine communications technologies to communicate with each other and with IoT applications in the cloud. Some applications requiring global coverage and mobility will focus on cellular technologies, especially on LTE-M and NB-IOT in the future. But the majority of devices will use wireless technologies operating in unlicensed frequency bands.

Although most of these technologies have already been used for a long time for all kinds of applications, the effort to design, manufacture and operate communications devices with the desired quality under all the applicable conditions should not be underestimated. Testing is a very powerful tool in all phases of the product lifetime in order to ensure proper functionality, interoperability, performance and quality of experience. This is even more valid in the very cost-sensitive emerging IoT market because the detection of design failures during the certification process or due to bad customer experience can become very costly in the end.

<table>
<thead>
<tr>
<th>Research &amp; development</th>
<th>Design &amp; validation</th>
<th>Pre-compliance &amp; compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital &amp; analog interface debug</td>
<td>RF Parametrics</td>
<td>Standard compliance</td>
</tr>
<tr>
<td>Clock analysis</td>
<td>Co-existence</td>
<td>Regulator compliance</td>
</tr>
<tr>
<td>EMI debug</td>
<td>Functionality</td>
<td>Carrier acceptance</td>
</tr>
<tr>
<td>Power analysis</td>
<td>Performance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Power analysis</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Manufacturing</th>
<th>Deployment &amp; operation</th>
<th>Service &amp; repair</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calibration</td>
<td>Installation</td>
<td>Fault finding</td>
</tr>
<tr>
<td>Verification</td>
<td>Monitoring</td>
<td>Calibration</td>
</tr>
<tr>
<td>Go / NoGo tests</td>
<td>Optimization</td>
<td>Verification</td>
</tr>
</tbody>
</table>

Fig. 2-1: Testing in all phases of the life cycle of Internet of Things devices and networks.
3 Design for Conformance

Generally before any wireless device can go on the air, it must be tested against the applicable standards and regulatory requirements. In some cases, specific requirements of the network operator must be considered. Consideration of such requirements begins even before the conformance tests which are typically performed by a conformance test lab: All requirements must be taken into account and verified starting in the design and integration process.

For example, devices using the IEEE 802.15.4 standard have to fulfill certain RF characteristics and performance requirements to ensure the device delivers the expected performance. Required tests and measurements include the minimum power, transmit power, out-of-band spurious emissions, receiver sensitivity, receiver interference rejection and clear channel assessment functionality, to name just a few examples.

Fig. 3-1: IEEE 802.15.4 spectrum measurements.

In addition, these devices must fulfill requirements defined by international, regional and national regulatory bodies such as the FCC for the United States and ETSI for Europe. Unfortunately, a device designed for global use must fulfill many different regulatory requirements.

First of all, any electrical device has to satisfy the regulatory electromagnetic compatibility (EMC) requirements. For EMC conformance, radiated and conducted emissions tests as well as radiated and conducted immunity tests need to be performed with a well-defined test setup under precisely specified test conditions. Usually, special EMC test systems with specialized test receivers are used for these kind of tests which are typically performed by certified test labs.

Typical EMC issues include unexpected state changes on input pins, corruption of on-chip clock signals, or insufficient decoupling of power lines. Such types of problems should be identified and resolved as early as possible in the design phase. For example, an
oscilloscope that is able to accurately visualize the real-time multi-domain spectrum combined with sensitive near-field probes can be used to identify and diagnose such electromagnetic interference problems.

But there are also specific requirements for devices operating in ISM bands. For example, all data transmission equipment in Europe operating in the 2.4 GHz ISM band using so-called wide band modulation techniques, i.e. WiFi, Zigbee and Bluetooth, has to meet the technical requirements specified in the European Standard: ETSI EN 300 328. This standard essentially describes the technical requirements for two categories of devices: Devices using frequency hopping (FHHS) and devices using wide band modulation (e.g. DSSS or OFDM). The standard also defines test conditions and test procedures to verify the defined technical requirements. The long list of requirements includes maximum RF output power of 20 dBm, power spectral density for wideband modulations of less than 10 dBm, a Tx-sequence duration of less than 10 ms, and a spectrum emission mask for transmitter unwanted emissions in the out-of-band.

Fig. 3-2: Analyzing EMC issues with a near-field probe.
4 The Unlicensed Band Challenge

Quite a few technologies used for M2M communications such as Bluetooth, WiFi 802.11n, Zigbee, Thread and ANT are sharing the 2.4 GHz ISM bands and operate in close proximity to certain LTE bands. The new WiFi standard 802.11ah, Z-Wave and EnOcean are using sub-GHz bands that are likewise used by low-power WAN technologies like Sigfox and Weightless-N. WiFi technologies 802.11n and 802.11ac use the 5 GHz ISM band and in some cases have to share this band with secondary LTE carriers of LTE-U/LAA.

![Fig. 4-1: Examples of wireless communications technologies using unlicensed bands.](image)

The number of devices and technologies using the unlicensed band is increasing every day. As a consequence, more and more devices will share the same spectrum at the same time.

For example, in a smart home scenario several of these technologies in different parallel networks could communicate at the same time. Moreover, devices like gateways use multiple radio technologies, thereby making co-existence a significant concern. Even if all the devices meet the regulatory requirements for operation in the unlicensed bands, each device and radio must expect and be able to deal with interference.

From the conceptual point of view, there are two ways to deal with interference issues: interference avoidance and robustness. For example, WiFi 802.11b in the 2.4 GHz ISM band uses a direct-sequence spread spectrum (DSSS) technology for robustness. The information bits are encoded in an eight-chip symbol using complementary code keying (CCK). To avoid interference with other technologies, WiFi uses a "listen before talk" technique with an exponential back-off timer.

Bluetooth uses an adaptive frequency hopping scheme where devices belonging to a piconet hop synchronously among 79 channels 1600 times per second. The algorithm allows adaptation to the spectrum environment by excluding channels with high interference ("bad channels") from the list of available channels. To improve the robustness, a forward error correction (FEC) mechanism is also used.
Bluetooth Smart is optimized for very low power consumption. It hops between 37 data channels and uses only CRC codes for error correction. Three fixed channels are used as advertising channels which are located in the gap between the non-overlapping WiFi channels in order to avoid interference with WiFi. These advertising channels could be used heavily in the future with large deployments of Bluetooth beacons.

Communications protocols based on IEEE 802.15.4 such as Zigbee and Thread also use a DSSS technology for robustness. Each data symbol representing 4 bits is mapped into a 32-chip sequence. For interference avoidance similar to WiFi, carrier sense multiple access collision avoidance (CSMA-CA) is used along with guaranteed time slots with a very low duty cycle (transmission time of less than 0.1 % of the total time).

<table>
<thead>
<tr>
<th>Technology</th>
<th>Avoidance</th>
<th>Robustness</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11b</td>
<td>Fixed channel</td>
<td>DSSS–CCG</td>
</tr>
<tr>
<td></td>
<td>CSAM-CA</td>
<td></td>
</tr>
<tr>
<td>802.11n</td>
<td>Fixed channel</td>
<td>OFDM</td>
</tr>
<tr>
<td></td>
<td>CSMA_CA</td>
<td></td>
</tr>
<tr>
<td>Bluetooth</td>
<td>Adaptive FHHS (79 channels)</td>
<td></td>
</tr>
<tr>
<td>802.15.4</td>
<td>Fixed channel</td>
<td>DSSS</td>
</tr>
<tr>
<td></td>
<td>CSMA-CA</td>
<td></td>
</tr>
<tr>
<td>ANT+</td>
<td>Adaptive isochronous network</td>
<td></td>
</tr>
<tr>
<td>RMPA</td>
<td>Random phase multiple access</td>
<td></td>
</tr>
</tbody>
</table>

Table 4-1: Interference and robustness techniques.
5 Interference Issues

For example, on the most popular ISM band at 2.4 GHz, different flavors of Bluetooth, WiFi and Zigbee are operating side by side, using the same frequency spectrum, in addition to ANT+, the LPWAN technology RPMA, baby phones and microwave ovens. Of special interest are, for example, home gateways supporting WiFi, Thread and Bluetooth and communicating with a large number of devices in a fully equipped smart home.

Fig. 5-1: Several technologies sharing the 2.4 GHz band collocated on an IoT gateway.

We thus need to investigate how well devices perform under certain RF conditions and especially to verify their co-existence functionality, i.e. how well do the transmitter and receiver perform with a particular radio access technology in the presence of another such technology? One common example involves the case where two radio technologies are implemented in the same device. This is described by the term "in-device co-existence". For example, in the case of a device that supports WiFi and LTE, we are interested in knowing how well these two technologies can co-exist in the device and not cause problems for one other. This effect is specified as the "desensitization". It measures the impact of the cellular radio when transmitting on WiFi reception and visa versa. With a wireless communications tester that supports all relevant technologies in one box, it is easy to perform such types of tests.

Fig. 5-2 shows an example of a device operating on WiFi 802.11n in the 2.4 GHz band and LTE on Band 7. Without the presence of LTE traffic, the WiFi receiver sensitivity on channel 13 is -80 dBm (10 % PER). But with the LTE transmitting on Band 7, which is very close to WiFi channel 13, the receiver sensitivity is only -71 dBm; this is the fault of in-device interference. This kind of measurement can be used to identify design problems or to analyze different interference avoidance strategies.
But sometimes there can be other problems such as hidden interferers, wrong hopping sequences or faulty carrier sensing, thereby resulting in poor performance on some interface. Analyzing such types of problems requires a detailed view of the whole spectrum of interest in realtime over a defined time interval.

A realtime spectrum analyzer is able to calculate one hundred thousand spectra per second by performing a fast Fourier transformation (FFT) in overlapping windows to ensure that even the shortest signals are captured. Based on this spectral data, some useful analysis tools are available. Two of them allow us to view the time and frequency domain on a single screen:

The persistent view creates a spectral histogram by seamlessly superimposing all spectra in a diagram. The pixel color indicates how often a signal occurs at a specific level. Frequently occurring signals are displayed in red and very infrequent signals in blue. If specific signals cease to occur, they disappear from the display when the chosen persistence period has elapsed.

The spectrogram is a way of displaying multiple consecutive spectra vs. time. The power level, which is usually displayed vs. frequency, is displayed vs. frequency and time. Graphically, time and frequency represent the vertical and horizontal axes of the display plane. Each coordinate (frequency f, time t) of the plane is filled with a color representing the power level for the respective frequency and time.
6 Conclusion

These were just some examples of tests that are particularly relevant for devices operating in the unlicensed bands.

All of these tests are essential to connect a device wirelessly to the Internet of Things, but they will not guarantee the desired application performance. Therefore, additional tests should be performed to analyze and optimize the specific performance aspects: RF performance, data and signaling performance such as protocol behavior analysis, as well as end-to-end application performance. Very often this has to go together with analyzing and optimizing power consumption in order to guarantee long battery lifetimes.

Every device needs to be tested during manufacturing, and for some networks testing during installation and operation of the networks is similarly important.

Testing and verification are very important topics in design, integration and manufacturing in order to ensure proper functionality along with high-quality user experience and performance over the product's lifespan.
7 Literature

[1] H. Schmit & Dr. F. Ramian: EVM Measurements for ZigBee Signals in the 2.4 GHz Band. Application Note from Rohde & Schwarz (2014)


Rohde & Schwarz

The Rohde & Schwarz electronics group offers innovative solutions in the following business fields: test and measurement, broadcast and media, secure communications, cybersecurity, radiomonitoring and radiolocation. Founded more than 80 years ago, this independent company has an extensive sales and service network and is present in more than 70 countries.

The electronics group is among the world market leaders in its established business fields. The company is headquartered in Munich, Germany. It also has regional headquarters in Singapore and Columbia, Maryland, USA, to manage its operations in these regions.

Regional contact

Europe, Africa, Middle East
+49 89 4129 12345
customersupport@rohde-schwarz.com

North America
1 888 TEST RSA (1 888 837 87 72)
customer.support@rsa.rohde-schwarz.com

Latin America
+1 410 910 79 88
customersupport.la@rohde-schwarz.com

Asia Pacific
+65 65 13 04 88
customersupport.asia@rohde-schwarz.com

China
+86 800 810 82 28 | +86 400 650 58 96
customersupport.china@rohde-schwarz.com

Sustainable product design

- Environmental compatibility and eco-footprint
- Energy efficiency and low emissions
- Longevity and optimized total cost of ownership

This Technical Article and the supplied programs may only be used subject to the conditions of use set forth in the download area of the Rohde & Schwarz website.

R&S® is a registered trademark of Rohde & Schwarz GmbH & Co. KG; Trade names are trademarks of the owners.

Rohde & Schwarz USA, Inc
6821 Benjamin Franklin Dr | Columbia, MD 21046
Phone 888-837-8772

www.rohde-schwarz.us