White paper

Anritsu envision : ensure

The Benefits of RF Testing for Mission-Critical IoT Designs

Introduction

IoT can be described as the “wild west” of the RF world being that it is a relatively new frontier with a hugely diverse array of technologies, multiple standards from different organizations and not a whole lot of compatibility. Naturally, that brings a new set of challenges for design and manufacturing, particularly in mission-critical IoT applications like health care, factory automation, transportation and utilities.

Although cost is a major factor in many IoT designs, given what’s at stake in mission-critical applications, factors such as data reliability, security and ease of use become far more imperative. This makes it so that the rigorous testing of IoT products is non-negotiable. For example, a failure in meeting RF standards compliance can open the door for regulatory scrutiny, or a downtime in manufacturing operations can cost a company millions of dollars.

This paper briefly covers several mission-critical IoT applications as well as some common RF test methods for IoT and their respective challenges. Finally, next-generation test solutions are presented along with the “hidden” bottom-line benefits that specific test equipment can provide, namely:

- Lowering test and measurement costs
- Shortening the time-to-market (TTM) of IoT products

Risks associated with mission-critical wireless sensor networks

What binds the diverse world of IoT into a common fold is connectivity. A predominant majority of business-critical IoT devices employ some kind of radio connectivity—either short-range wireless links like 4G LTE, Wi-Fi and Bluetooth or long-range low-power wide-area network (LPWAN) technologies such as LoRa, Sigfox and NB-IoT. Mission-critical devices like industrial-grade sensors for industrial IoT (IIoT) and life-saving medical equipment for medical body area networks (MBANs) are exploring the power of connectivity to create the “Internet of Critical Things.” Connectivity services such as these enhance human decision-making in highly dynamic environments that call for another of level of data reliability to prevent the high cost of failure.

According to IHS Markit, industrial applications like building automation, manufacturing control and smart lighting will account for nearly one-half of the new connected devices deployed between 2015 and 2025. While industrial wireless sensor networks (IWSNs) open up a vast repertory of opportunities, there are also risks that come with it. According to Arimo, manufacturers have up to 800 hours of downtime annually with current fieldbus or Ethernet-based industrial links, and the average cost of an automotive plant downtime is $22,000 per minute. The average cost of a downtime incident in industrial automation is $150,000 to $250,000 per hour. Even with quality-of-service (QoS) traffic suppression and slotted protocols for more reliable data transfer, it is difficult to achieve the low bit error rates (BERs) afforded by hardwired connections.

Risks associated with mission-critical wireless sensor networks continued

Oil and gas companies are heavily utilizing LPWANs despite the cost of this infrastructure. This is because tracking flow rate and pressure in the millions of square miles of oil pipelines is not only helpful but can potentially improve operational efficiency and save the environment in the case of a catastrophic failure.

In automotive applications, it is critical that vehicle-to-everything (V2X) on-board units (OBUs) perform adequately when emergency brake, cooperative collision avoidance and automatic notification of crash on road is needed. According to the World Health Organization (WHO), approximately 2,500 people are killed on roads every day—nearly 1 million people each year. The reliability of vehicle WSN is of utmost importance because it has the potential to directly save lives.

These few examples of mission-critical WSNs attempt to make evident the cost in time, money and life of communications failures and downtime. Rigorous testing of sensor nodes and gateways is therefore, not only recommended, but necessary. Critical IoT devices would likely require repetitive testing of both the physical hardware and data transmission in realistic test environments where interference can occur as well as external agitators such as vibration, shock, and moisture ingress.

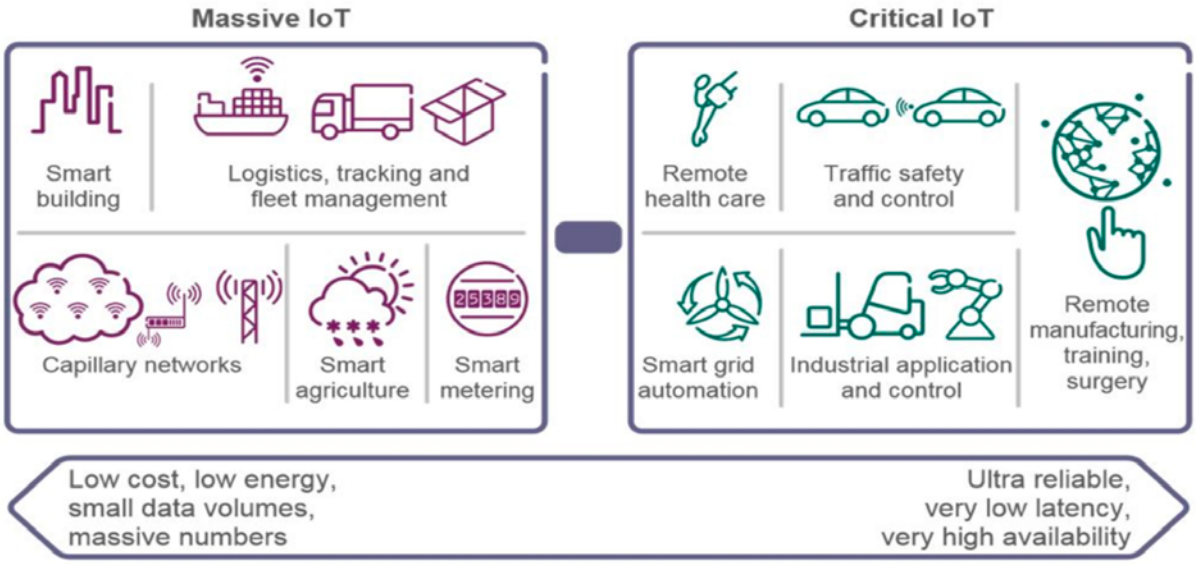

Figure 1: *Mission-critical IoT applications demand new wireless connectivity test and measurement features at lower costs.*
Source: "Cellular Networks for Massive IoT," Ericsson white paper. Jan. 2016.

A landscape of many standards

The challenges of testing a sensor node, gateway or any IoT device is often very specific to the application as the hardware/software varies based upon its requirements. For IWSNs leveraging WirelessHART, ISA 100.11a or some LPWAN standard, data reliability and security are cited to be major concerns over battery life. Automotive applications with Vehicular Ad Hoc Networks (VANETs) utilizing the IEEE 802.11p and IEEE 1609.4 standards would most certainly require extremely high data reliability—or predictable and reliable transmissions—for safety applications. On the other hand, non-safety VANETs would most likely need to be efficient with a high data rate. Smart city applications leveraging LPWANs such as NB-IoT, LTE-M1, Sigfox or LoRa would probably sacrifice throughput for large link distances and battery savings, or act as a fallback backup for areas with low cellular coverage. The emerging IoT standards are meant to address the critical needs of its respective application and, while this often leads to much confusion particularly in the realm of test, this proliferation is necessary to effectively optimize hardware and firmware criterion.

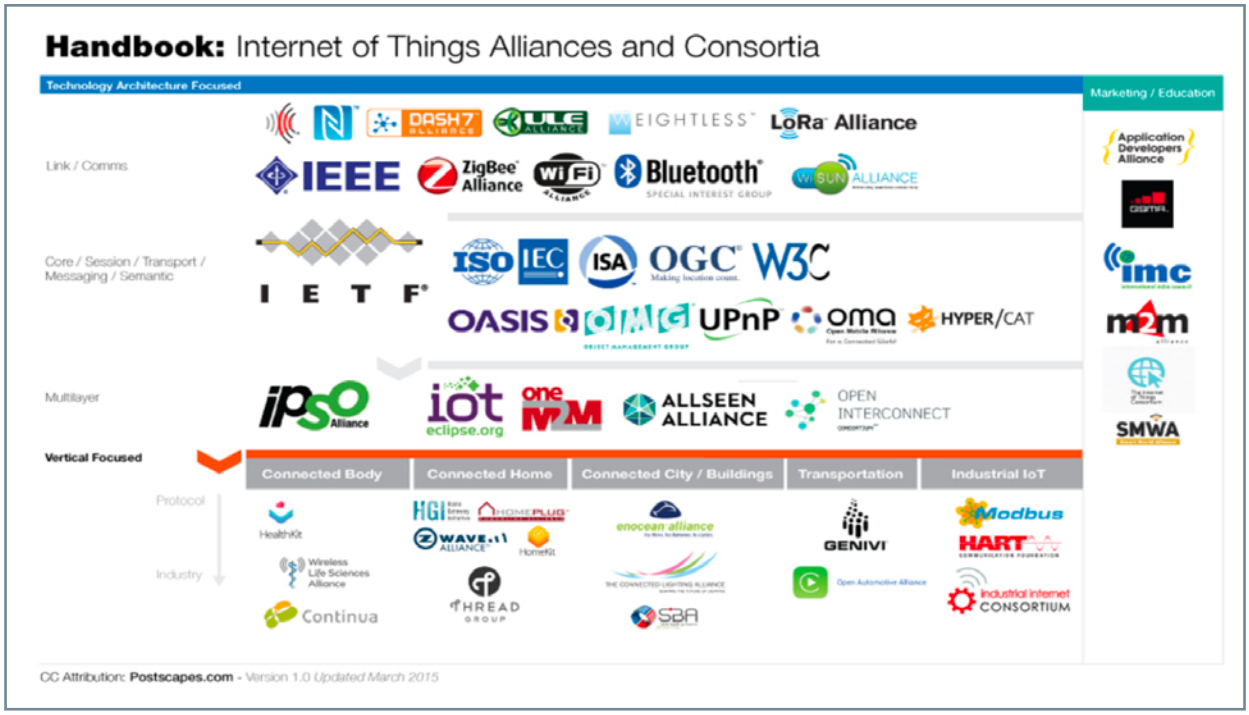

Figure 2: *The proliferation of standards committees can lead to complex testing requirements that are constantly changing.*

A landscape of ever-evolving standards

The landscape of IoT is fraught with standards that are continuously changing. For instance, IEEE standard 802.11, which defines the physical (PHY) and medium access control (MAC) layers for the popular wireless local area network (WLAN), has at least six major releases just within the 2.5-/5-GHz ISM bands. This is evident in Table 1, where significant changes are made not only with the MAC protocols but even with the PHY modulation scheme changing from direct-sequence spread spectrum (DSSS) to orthogonal frequency-division multiplexing (OFDM) and finally to orthogonal frequency-division multiple access (OFDMA) with the most recent 802.11ax release. Many of these releases are, in turn, iteratively improved with their ongoing amendments.

Bluetooth has also had 10 releases from the year 2002, mostly to increase throughput for short-range, indoor connectivity. Both WLAN and Bluetooth are currently the more popular connectivity vehicles for IoT applications, due largely to low cost and high availability. Furthermore, according to Ericsson, the number of short-range IoT devices are expected to exceed the number of mobile phones, so it's likely that these standards will continue to dominate this realm of non-cellular IoT devices.

Standard	Release	Frequency	BW (MHz)	Data Rate (mbps)	Modulation	Max Constellation	Max Range (m)
IEEE 802.11b	1999	2.4 GHz	20	11	DSSS	-	140
IEEE 802.11a	1999	5 GHz	20	54	OFDM	64-QAM	120
IEEE 802.11g	2003	2.4 GHz	20	54	OFDM	64-QAM	140
IEEE 802.11n	2009	2.4/5 GHz	20, 40	600	MIMO-OFDM	64-QAM	250
IEEE 802.11ac	2014	5 GHz	20,40,80,160	6.8	MIMO-OFDM	256-QAM	-
IEEE 802.11ax	2019	2.4/5 GHz	20,40,80,160	10	OFDMA, MIMO-OFDM	1024-QAM	-

Table 1: *Major releases of WLAN IEEE 802.11 standard for the 2.4- and 5-GHz bands.*

A landscape of ever-evolving standards continued

The 3rd Generation Partnership Project (3GPP) is an organization dedicated to standardizing the hardware and protocols particularly around cellular technology. The goal is to ultimately provide an outline so that vendors can begin to release chipsets without having to worry about compatibility issues. **Figure 3** is a depiction of the timeline of some of 3GPP's releases. Naturally, every enhancement in these standards trickles down to a change in testing of the IoT devices. While this might be of no major consequence for a hobbyist or small-scale consumer IoT application, it can be a primary concern for organizations with liability, time and cost concerns.

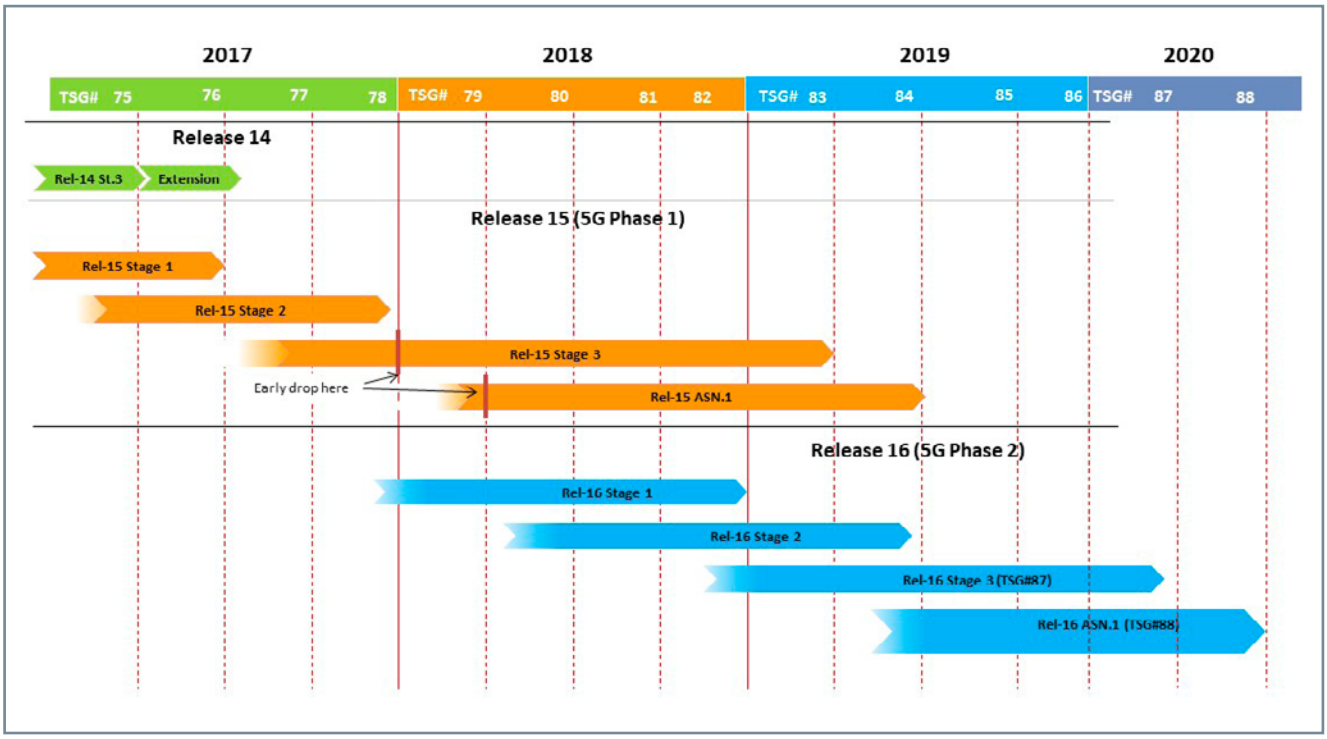

Figure 3: *Timeline of 3GPP standards releases.*
Source: https://www.3gpp.org/specifications/67-releases

Challenges in over-the-air testing

Traditionally, antenna characterizations are performed in an anechoic chamber and radiation patterns are assessed by moving a receiving antenna around the antenna under test (AUT) to obtain a three-dimensional map. These over-the-air (OTA) measurements are straightforward enough with just a small antenna connected to a probe station, but it becomes much more complex to obtain a good isotropic radiation pattern with the unpredictable size, device layout and form factor of IoT devices; they can range from tiny wearables to large in-vehicle WSN. The CTIA released plans for a reverberation chamber for larger devices with dimensions greater than 42 cm where the exact placement of the DUT is not critical (**Figure 4**). This differs greatly from typical antenna characterizations where the DUT is fixed in a very exact position. When properly configured, the chamber provides results for common tests such as total radiated power (TRP) and total isotropic sensitivity (TIS) on par with anechoic chambers. Test equipment manufacturers must then work with OTA chamber vendors that are CTIA-certified to support these varying OTA test environments to keep up with testing the increasingly complex and advanced antenna systems.

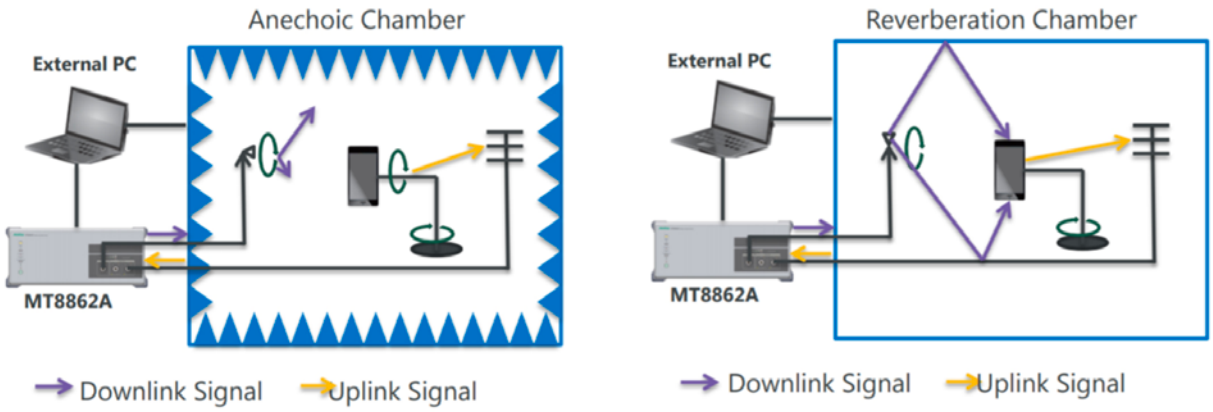

Figure 4: *OTA characterizations for reception power range and receiver sensitivity must be more flexible to shifting physical test setups due to the unpredictable form factors of IoT devices.*

Challenges in testing devices under true operating conditions

End-product verification for IoT devices is of significant importance because the cost of errors only escalate through a project life cycle. As mentioned previously, it is paramount for mission-critical IoT applications as not only do costs compound more significantly but also risks to life and the environment. While thorough product quality assurance (QA) may seem to oppose the rapidly changing world of IoT, that perspective may not be necessarily true so long as a company's production test and QA departments are agile enough to keep up.

Traditionally, manufacturing inspections leverage a specialized test mode that requires a hardwired control line between an end device and the test equipment. This, of course, is not an accurate test of an IoT device under true operating conditions as the effectiveness of the antenna is not taken into consideration. Typical IoT tests for devices operating in the unlicensed bands are performed mainly to minimize the risk of interference. These measurements include device radio emissions and electromagnetic compatibility (EMC). Other basic tests simply make sure that the sensor node or gateway can communicate with each other and transfer data to the cloud in a relatively comfortable, noise-free environment of a lab.

There are multiple factors that can change in the "real-world," including congestion, particularly for technologies utilizing the unlicensed bands such as WLAN, Bluetooth, LoRa and Sigfox. A user's gateway, base station or modem will have to decrypt any incoming message even if the transmission is not meant for it. This increase in capacity will also directly affect the collision rate of messages and thus the packet error rate (PER), especially for asynchronous systems such as LoRa and Sigfox. Another factor includes behavior during mobility for sensor nodes that are not fixed; multipath and fading effects may take on different behaviors in various environments.

An OTA method to track IP data transfer functions and measure throughput in real environments can lead to the discovery of routing issues during the development and early deployment of IoT devices and services. Also, the RF verification of WLAN chipsets, modules and end devices should be carried out when security features are enabled to ensure evaluation under near-to-end user usage conditions. That includes the device's built-in Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) features. Not only are OTA verification measurements more ideal methods to characterize a device, but also access to this type of modular equipment is often necessary as the hardwired connections can lead to cabling and test complexities in changing environments.

Challenges in keeping up with changing standards

Product development teams and their respective test facilities must keep up with the changing standards and updated revisions. Legacy test equipment is normally built for one specific purpose and that would typically suffice in other industries; this is not the case with the IoT industry. Furthermore, firmware OTA upgrades are a major trend in IoT devices being that they minimize maintenance that comes with upgrading and troubleshooting individual nodes. This is a double-edged sword in that it can also change the wireless performance of the device.

Test setups may then need to include equipment built modularly with firmware upgrades to perform necessary measurements. Along the same lines, the test industry has the potential to take lessons from the IoT industry uses of web-based network and application servers. For instance, LoRaWAN network servers can be enabled through The Things Network (TTN), where users can set up and program gateways and nodes readily from their PC with an entire library of support literature.

User-friendly GUIs can also be leveraged on cloud-based servers to lower the barriers for testing and minimize the learning curve associated with upgrading tests to support upgraded devices. It also sidesteps operating system (OS) dependence and eliminates the need to install control software and version matching between the main unit firmware and control software. For instance, to carry out RF measurements defined in the 3GPP TS36.521-1 recommendations for LTE Cat M1 and NB-IoT terminals, one can add specialized software to a radio communication analyzer rather than investing in additional hardware. Another example may include remote-control protocols for control of WLAN-based test equipment via a web browser. This, in turn, lowers the cost that comes with paying for more equipment and paying engineers to learn how to use it.

Challenges in test bench footprint

The setup and takedown of test equipment can waste a significant amount of time unnecessarily. This is usually avoided by allocating a test bench for a specific test and, while this saves time, it comes with the tradeoff of space taken up. Complex wireless technologies directly lead to lengthier calibrations where systems need added splitters, switches and control software. Equipment that can be configured with internal splitters, switches, coaxial interfaces and software interfaces that can communicate with the various wireless connectivity devices and their respective protocols may be more desirable. A single user interface can then validate RF performance of a chipset, module or device in real-world conditions. This can even be extended to where multiple devices are tested simultaneously depending on the component density within the modularly designed equipment. Ready-made measurement software options can be added based on specific application and testing capacity requirements.

Summary

IoT creates huge opportunities for many industries but also an increased risk. Test and measurement can be considered the “sheriff” of the “wild west” that is the IoT, providing a means to develop, produce and test confident designs and well-performing IoT devices. The stakes are high in mission-critical IoT operations, so it’s crucial that designers have confidence in their chipsets, modules, end devices and networks. This is especially true in the RF domain, where environments significantly change once they reach the end users.

This paper has covered the mission-critical IoT landscape and demonstrated how test is heavily intertwined with the quality of mission critical IoT devices and how companies generating products in this realm must keep up with the constantly expanding set of standards and operating conditions in order to maintain a high level of reliability. It has, in turn, described how test solutions can lower overall test costs while increasing production efficiency and speed to market if you know what to look for.

Anritsu’s Solutions

Anritsu’s comprehensive IoT test portfolio integrates unique features designed to make test processes less complicated and more efficient.

Visit **Anritsu’s IoT page** to learn more about the evolution of IoT, technologies and test solutions.

Visit **Anritsu’s 5G-based IoT** page to learn more about specific 5G/IoT applications and test solutions.

Anritsu envision : ensure

Specifications are subject to change without notice.

• United States
Anritsu Company
450 Century Pkwy, Suite 109,
Allen, TX, 75013 U.S.A.
Toll Free: 1-800-267-4878
Phone: +1-972-644-1777
Fax: +1-972-671-1877

• Canada
Anritsu Electronics Ltd.
700 Silver Seven Road, Suite 120,
Kanata, Ontario K2V 1C3, Canada
Phone: +1-613-591-2003
Fax: +1-613-591-1006

• Brazil
Anritsu Electrônica Ltda.
Praça Amadeu Amaral, 27 - 1 Andar
01327-010 - Bela Vista - Sao Paulo - SP - Brazil
Phone: +55-11-3283-2511
Fax: +55-11-3288-6940

• Mexico
Anritsu Company, S.A. de C.V.
Av. Ejército Nacional No. 579 Piso 9, Col. Granada
11520 México, D.F., México
Phone: +52-55-1101-2370
Fax: +52-55-5254-3147

• United Kingdom
Anritsu EMEA Ltd.
200 Capability Green, Luton, Bedfordshire LU1 3LU, U.K.
Phone: +44-1582-433280
Fax: +44-1582-731303

• France
Anritsu S.A.
12 avenue du Québec, Batiment Iris 1-Silic 612,
91140 Villebon-sur-Yvette, France
Phone: +33-1-60-92-15-50
Fax: +33-1-64-46-10-65

• Germany
Anritsu GmbH
Nemetschek Haus, Konrad-Zuse-Platz 1
81829 München, Germany
Phone: +49-89-442308-0
Fax: +49-89-442308-55

• Italy
Anritsu S.r.l.
Via Elio Vittorini 129, 00144 Roma Italy
Phone: +39-06-509-9711
Fax: +39-06-502-2425

• Sweden
Anritsu AB
Kistagången 20B, 164 40 KISTA, Sweden
Phone: +46-8-534-707-00
Fax: +46-8-534-707-30

• Finland
Anritsu AB
Teknobulevardi 3-5, FI-01530 VANTAA, Finland
Phone: +358-20-741-8100
Fax: +358-20-741-8111

• Denmark
Anritsu A/S
Kay Fiskers Plads 9, 2300 Copenhagen S, Denmark
Phone: +45-7211-2200
Fax: +45-7211-2210

• Russia
Anritsu EMEA Ltd.
Representation Office in Russia
Tverskaya str. 16/2, bld. 1, 7th floor.
Moscow, 125009, Russia
Phone: +7-495-363-1694
Fax: +7-495-935-8962

• Spain
Anritsu EMEA Ltd.
Representation Office in Spain
Edificio Cuzco IV, Po. de la Castellana, 141, Pta. 5
28046, Madrid, Spain
Phone: +34-915-726-761
Fax: +34-915-726-621

• United Arab Emirates
Anritsu EMEA Ltd.
Dubai Liaison Office
P O Box 500413 - Dubai Internet City
Al Thuraya Building, Tower 1, Suite 701, 7th floor
Dubai, United Arab Emirates
Phone: +971-4-3670352
Fax: +971-4-3688460

• India
Anritsu India Pvt Ltd.
2nd & 3rd Floor, #837/1, Binnamangla 1st Stage,
Indiranagar, 100ft Road, Bangalore - 560038, India
Phone: +91-80-4058-1300
Fax: +91-80-4058-1301

• Singapore
Anritsu Pte. Ltd.
11 Chang Charn Road, #04-01, Shriro House
Singapore 159640
Phone: +65-6282-2400
Fax: +65-6282-2533

• P. R. China (Shanghai)
Anritsu (China) Co., Ltd.
27th Floor, Tower A,
New Caohejing International Business Center
No. 391 Gui Ping Road Shanghai, Xu Hui Di District,
Shanghai 200233, P.R. China
Phone: +86-21-6237-0898
Fax: +86-21-6237-0899

• P. R. China (Hong Kong)
Anritsu Company Ltd.
Unit 1006-7, 10/F., Greenfield Tower, Concordia Plaza,
No. 1 Science Museum Road, Tsim Sha Tsui East,
Kowloon, Hong Kong, P. R. China
Phone: +852-2301-4980
Fax: +852-2301-3545

• Japan
Anritsu Corporation
8-5, Tamura-cho, Atsugi-shi,
Kanagawa, 243-0016 Japan
Phone: +81-46-296-6509
Fax: +81-46-225-8359

• Korea
Anritsu Corporation, Ltd.
5FL, 235 Pangyoyeok-ro, Bundang-gu, Seongnam-si,
Gyeonggi-do, 13494 Korea
Phone: +82-31-696-7750
Fax: +82-31-696-7751

• Australia
Anritsu Pty Ltd.
Unit 20, 21-35 Ricketts Road,
Mount Waverley, Victoria 3149, Australia
Phone: +61-3-9558-8177
Fax: +61-3-9558-8255

• Taiwan
Anritsu Company Inc.
7F, No. 316, Sec. 1, Neihu Rd., Taipei 114, Taiwan
Phone: +886-2-8751-1816
Fax: +886-2-8751-1817