7 Tips for Faster Embedded Wireless Device Certification

Intertek Testing Services
70 Codman Hill Road
Boxborough, MA 01719

icenter@intertek.com 800-WORLDLAB www.intertek.com/wireless

Introduction

The rapid proliferation of wireless technology has not only affected an increase in person to person communications, but also machine to machine communications. Advances in wireless technologies and infrastructure have led to manufacturers of all sorts of consumer and industrial devices to embed wireless communications capabilities in their products. According to the independent wireless analyst firm Berg Insight the number of cellular network connections worldwide used for machine-to-machine communication was 47.7 million in 2008. The company forecasts that the number of machine to machine connections will grow to 187 million in 2014[1].

Machine to machine communications provides value such as faster identification of mechanical and environmental issues that affect a devices performance, reduced need for manual verification, remote monitoring, and operations improvements based on real time feedback.

Some of the growing number of applications for this technology include many non-traditional end devices such as home appliances, medical devices, vending machines, automobiles, industrial equipment, home water and electric meters, and reading devices like Amazon's popular Kindle.

Today manufacturers have a choice between developing devices with "chip on board" solutions or using a module. Both have there challenges and advantages. The purpose of this paper is to provide several helpful tips for those device manufacturers electing to use an embedded module solution.

Both the definition of an embedded device and the application of that device are changing rapidly, creating a new paradigm of certification processes for device manufacturers.

In the past, a conventional wireless device such as a mobile phone would pass through testing and certification based on requirements established by the wireless provider. It was a sometimes difficult process. However, because both sides were accustomed to working together, the steps were relatively straightforward. For a testing and certification expert such as Intertek, the familiarity with the traditional devices manufacturers produce and the service provider's test requirements eased the process.

Today's growing wireless market, however, includes many non-traditional end devices. Those developing these products are not always familiar with the process for testing and certifying their devices that will run on mobile networks.

[1] Berg Insight - The Global Wireless M2M Market

The end result of a successful certification process is the understanding that the product being tested performs well and that the carrier on whose network the application will run feels ready to put the device on line. The end result of an unsuccessfully tested embedded device can range from project failure to stressed relationships with carriers. The added time and expense involved in reworking issues after submission is often many times the cost of effective pretest preparation.

This white paper describes several steps that a embedded device vendor can take prior to submission for formal testing to ensure that the product it has developed will operate correctly on the target network, thus avoiding a last-minute compliance rush.

Start early

Prior to the development of any product, become familiar with the test requirements that will be imposed on your product. Work with a knowledgeable lab such as Intertek to learn what will be expected of your product based on the carrier you wish to deploy with.
To facilitate the embedded device process, a developer should begin testing the device before its design is complete. Besides greatly improving the time-to-market for the device and application, this also ensures that many potential problems are identified and solved before the actual certification process begins. Manufacturers who wait too long to begin testing their products for certification run the risk of problems developing, and slowing or stopping the actual certification process.

One other pre-testing step is also important: make certain that the module on which your device sits is approved for the appropriate carrier's network. Since every device must sit on a module, it is easy to determine from the module vendor that the platform is, in fact compatible and approved for device integration with the specified carrier.

An important point of note is that the latest module might not be the best module for your test. While even an approved module may not have the proper firmware for the software with which you want your device to integrate—and it's important to check that the two jive—you should also make certain that the module has the right level of firmware. Many times modules have old firmware that might be approved by the carrier but is no longer calibrated for that carrier's network. On the other hand, even a module equipped with the latest "state-of-the-art" firmware may not be acceptable because it could be too new for the carrier and hasn't yet been approved as a test vehicle.

The best route to take before offering your device for testing and certification is to ask the carrier what module is recommended and use that recommendation to solicit product from an OEM.

RF connection should be left alone

Out of necessity the RF path must be continued by the device manufacturer from the embedded module to the antenna output of the device. It has been the experience of Intertek technicians that the most direct path and shortest cable length is desired. The module will have an RF connector already in place and our recommendation is to run the input straight from there through a well shielded cable to the antenna port, preferably using a bulkhead connector.

Do not run the RF path through another circuit board or redistribute the signal in any way. The cable provides good shielding—made better when a good quality, well shielded product is used—so it is not advisable to land it on a circuit that would open it up to outside interference.

Other interference issues should also be watched. A cable running too closely to an antenna, power supply or known oscillators can result in an intrusion of radiation energy. Although this only occurs rarely, it's a primary reason to use top quality cable and to be mindful of the path chosen for routing the RF.

Avoid data call issues

The module manufacturer can generally handle a data call with a user name and password already stored in the module. Especially when testing for Verizon Wireless certification, a fixed user name stored in your software will not work. Because Verizon frequently updates its password, you should not use a fixed password when testing on a Verizon network.

Conversely, most carriers prefer fixed passwords so when it comes to data call issues it is best to leave the user name and password up to a module vendor accustomed to working with the carrier in question.

Mobile IP (MIP) versus Simple IP (SIP)

Although it seems counterintuitive, it is important to be sure that the software that controls the module can handle SIP. While Windows dial-up handles everything in SIP, some other software solutions don't and this can lead to trouble during the sting/certification process.

Admittedly SIP is becoming less important in the network and is unlikely to be part of your end design which will be configured to work with MIP. On the other hand, SIP is the fallback for testing and certification and if, for any reason, your MIP product fails, the call will fall back to SIP. If the device and/or module are not configured to handle SIP there will be problems with delays and possible test failures.

Technically, MIP-only devices are allowed in the testing phase; real-world, SIP is a fallback and you should invest the time and money to include it even if you never plan to use it.

Don’t include voice with non-voice applications

Even if you plan to include voice as part of your application at some point in the future and the application is being planned for a voice-enabled device, the wise move is to not include it as part of the certification process if it is not part of the original application.

Adding voice to the process, even if somewhere down the road it will be part of the application, adds unneeded complexity to the lab testing/certification. Even if it doesn't undermine the project as a whole, it will add time and cost to your testing.

Avoid data retry failures

Modules are supposed to contain a throttling algorithm that controls the number of retries a device can make when it fails to connect a data call on the network. Care should be exercised to ensure that the proper algorithm is followed in the event a data call fails to connect. A key area of focus would be the device firmware behavior when a data call fails. Does the firmware cause the module to reset on failure?

Another key area of focus is device design. Due to design constraints, some devices are powered down when not in use in effort to conserve energy. On power up, the intended function is to generate a data call and transfer data on the network. In the event the data call origination is not successful, the device may continue the origination attempt over a fixed period of time. A fixed data retry interval is acceptable in most cases and care should be taken to verify that the fixed interval complies with the carrier test plans.

Keep things simple

The best advice when submitting a wireless embedded product/device/application for testing and certification is to keep the process as simple as possible. Avoid adding any steps (voice, data retry, RF configuration) that can lead to failure and/or the need to remove the product and reconfigure it.

It is also a good idea when working with any major carrier to use a testing facility such as Intertek where the technicians are acquainted with the module OEMs, carriers and many of the procedures being tested. This will help a first time device developer move more calmly through the process and can speed the process for even the most veteran applications developer.

Another advantage to partnering with Intertek is that it can serve as the one-stop-shop for your device, including testing and certification for FCC regulations, safety, network performance, Alltel, CRICKET, Telus, Verizon ODI and SFN/Non Branded, and CCF/CTIA testing.

Conclusion

The rapid growth in the quantity and the diversity of end products being fitted with embedded wireless devices has brought new challenges for the design, testing and certification of these products. In order to access wireless providers' networks, manufacturers must have their products certified. Testing failure, redesign and retesting can lead to costly delays. Embedded applications providers can take steps take prior to submission for formal testing to ensure that the product they have developed will operate correctly on both the device for which it was intended and the network on which that device will run. Starting early, avoiding data call issues, not mixing voice with non-voice applications, keeping things simple and selecting the right lab will reduce the likelihood of delays in certification.

About Intertek

Intertek is the leading provider of quality and safety solutions serving a wide range of industries around the world. From auditing and inspection, to testing, quality assurance and certification, Intertek people are dedicated to adding value to customers' products and processes, supporting their success in the global marketplace. Intertek has the expertise, resources and global reach to support its customers through its network of more than 1,000 laboratories and offices and over 25,000 people in 110 countries around the world.

Intertek's range of testing and certification services for electrical and wireless products provides you with the clearest connection to your market. Our services protect your brand by ensuring satisfactory end user experience and assure the integrity of devices, applications and content across networks. For more information, visit **www.intertek.com**/wireless or call 1-800-WORLDLAB