COMPLIANCE DESIGN & CERTIFICATION FOR IOT CELLULAR APPLICATIONS

What your product design team needs to know about compliance design and certification for IoT cellular applications

In this whitepaper, we explore the compliance design and certification requirements involved when integrating cellular capabilities into your product. Often, design teams are focused on meeting the product's functional requirements and end up with a product that works great, but can't be sold commercially due to cellular certification and compliance testing issues. This can result in costly delays for your organization. To get you to market faster, Digi's team of experienced engineers has been working with companies for years from idea concept through product launch to ensure your product has the right design to pass the required cellular compliance tests. This whitepaper will cover key areas of compliance design along with a discussion on the hardware and firmware aspects impacting the overall product design.

Introduction

The advent of new cellular module products combined with better Internet of Things (IoT) support from cellular carriers are making it easier and less expensive than ever before to design cellular data connections into new IoT applications. Compliance and regulatory issues sometimes trip up designers as evidenced by the number of projects for products that "work, but need approvals" that our customers bring to our design services company.

Common Issues We Encounter

- Spurious RF emissions in excess of FCC or other national body requirements
- Sensitivity below the required level for cell carrier approval for use on their network
- Transmit power out of range for cell carrier or PTCRB approval
- Noise in the transmit signal beyond limits specified by the carrier or PTCRB
- Multiple radio interference issues (in “converged devices”) for PTCRB approval
- Connection retry interval requirements not met, so the device tries too soon or too often to reconnect to the network
- Over-the-air provisioning support requirements for initial network enrollment
- Exceeding specific absorption rate (SAR) requirements for body-worn transmitters

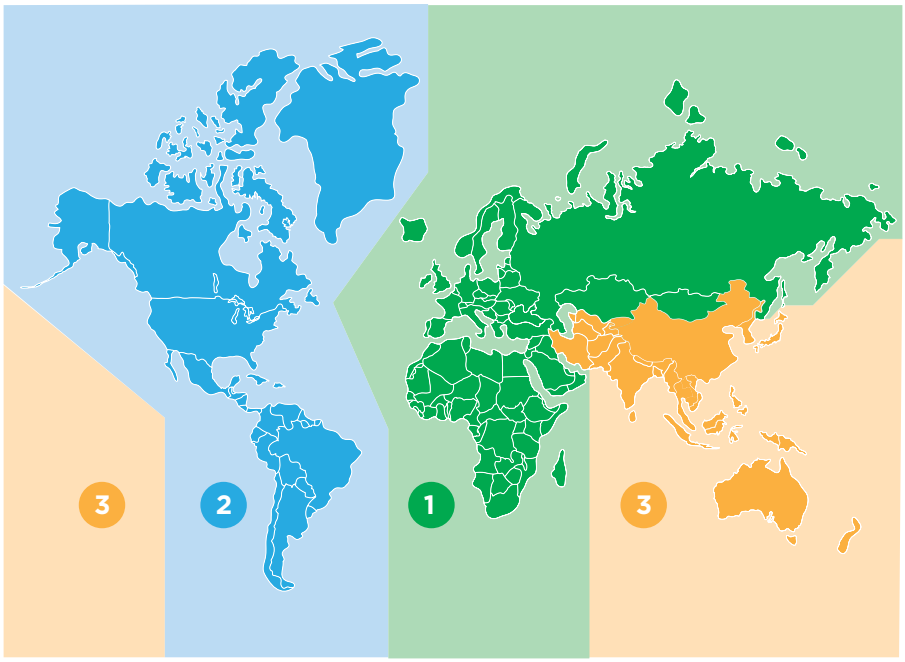
In this whitepaper, we’ll examine some of the unique compliance design issues that need to be controlled in a cellular-based embedded technology design, along with ways to control them before you miss your product launch window. Our experience spans:

- Automotive monitoring and tracking for behavior-based insurance monitoring, car sharing, tracking for high-risk auto loans and remote automobile diagnostics
- Remote asset tracking for commercial and consumer applications
- Home automation, security and energy consumption technology
- Medical device monitoring
- Industrial systems
- Consumer electronics
- Defense and aerospace systems

IoT and Cellular

Let's begin by first providing some context to our domain of interest, the IoT terminal device. As defined above, there is a large variety of applications that deploy IoT technologies. The aforementioned list of technologies is to be considered a few of the more popular IoT technologies of the last 10–15 years.

Because all leading manufacturer's, pursuant of the global marketplace, have to be cognizant of the standards governing technical regions identified by the ITU (International Telecommunications Union), we must examine the ITU. Every global region has cellular guidelines that require compliance requirements specific to a region and/or country. Please reference the following map.



ITU Regions

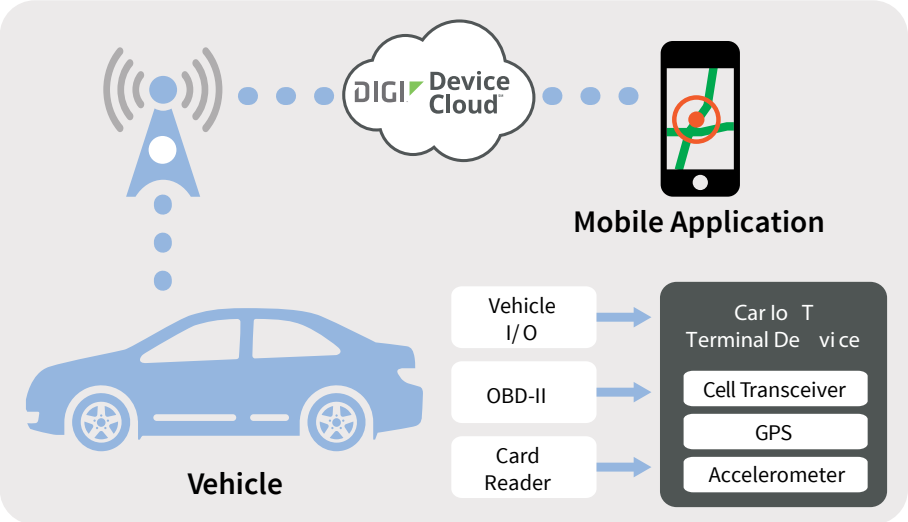
This strongly suggests that there are quite a few exceptions to the regional approach to cellular compliance. This is because there are countries within regions that have unique laws that govern the use of cellular technologies.

Considering the rate of the migration of new cellular technologies, coupled with the instability and infrequent longevity of foreign governments, it is not uncommon for manufacturers to pursue international cellular markets that lack cellular infrastructure and, therefore, compliance guidelines. As a result, it is wise for manufacturers to ensure they consistently monitor cellular global standards.

For the sake of capturing the intent of this whitepaper, we will confine our subject matter to IoT, as per the cellular-to-automobile application.

In the diagram below, the IoT terminal device interfaces the communication devices that are specific to a network within a connected car through the automobile's OBD-II (Onboard Diagnostic- Revision II) diagnostic system, horn, locks and door sensors, as well as sensing the car's environment using GPS (Global Positioning System), temperature sensors and an accelerometer.

The OBD-II (Onboard Diagnostic- Revision II) references what was formally called an ECM (Electronic Control Module). This module receives remote vehicle sensor inputs from all major subsystems on a vehicle. The ECM calculates those inputs then sends output signals back to the various subsystems. The process enables the OBD-II system to provide the vehicle owner or repair technician access to the status of the various vehicle subsystems. This is commonly performed by the use of a standardized digital communications port to provide real-time data in addition to a standardized series of diagnostic trouble codes, or DTCs, which allow one to rapidly identify and remedy malfunctions within the vehicle.



The IoT terminal device is embedded within the car to provide monitoring and control capabilities for functions such as vehicle location, movement and orientation, vehicle operating and performance data (OBD-II) and even detecting if the car doors are open or closed. Control functions that can be performed remotely consist of items like

locking/unlocking the doors or activating the horn.

While IoT terminal devices may use communication channels other than cellular, cellular connectivity is increasingly common for a number of reasons. Consider the following trends:

- Cellular module hardware costs continue to decrease
- Cellular connection costs (data plans) continue to fall, especially for low-data IoT applications
- Tools to efficiently administer a private network of cellular-connected IoT devices are now available from most carriers
- The complexity to design in the current generation of cellular modules has been greatly reduced.

When you combine these trends with the expectations of a new generation of consumers you should not be surprised to find major network connectivity changes. For example, in many US markets, new home automation and security system installations are almost exclusively cellular-based, as cellular service has replaced landlines in over 40% of US households.

Compliance Design

The effort needed to comply with the applicable regulations is often overlooked in the planning for a cellular-enabled IoT device design. Product design teams naturally focus on the functional requirements for the application and sometimes end up with a product that works great, but can't be sold commercially. As reported by a leading cellular certification lab, "80% of all new cellular designs fail certification the first time." While the requirements vary by application and by region, the types of compliance testing that apply to cellular-enabled IoT devices may include:

- FCC Part 15, Subpart C for Intentional Radiators
- FCC Part 22/24 Cellular Transmitter Certification
- PTCRB Certification
- PTCRB Converged Devices Certification
- Wireless Carrier Compliance Testing

80%

of all new cellular designs fail certification the first time.

PTCRB testing and carrier compliance testing are the most common roadblocks for designs that use a board- mounted module or socketed cell module. While these types of designs may eliminate some testing (e.g., FCC Part 22/24 Cellular Transmitter Certification if compliant with the module FCC grant), such designs often require

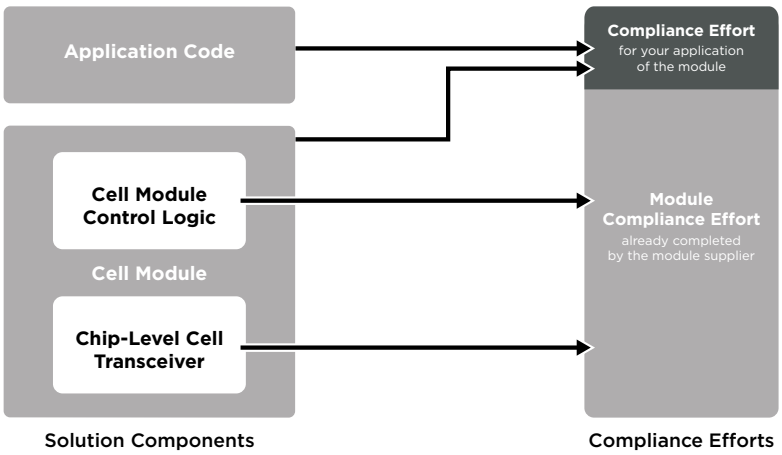
wireless carrier compliance testing by an approved authority. Below, we will cover these requirements in more detail, but the most commonly overlooked hardware design items include antenna efficiency and electro- magnetic interference (EMI) requirement compliance. On the firmware side of the design effort, frequently overlooked support includes cellular module firmware update support, controlled data connection retry intervals and over-the-air (OTA) provisioning support.

The embedded resources required for a particular cellular-enabled IoT terminal device application vary widely and can range from a powerful application processor running Linux to a 32-bit microprocessor running a real-time operating system, to even an 8-bit microcontroller with no operating system. Even though the platforms vary widely, the compliance design demands for this entire range of terminal devices are quite similar.

Hardware Design

Often, a hardware design can operate reasonably well as a prototype, but have no commercial value because it fails even a minor compliance requirement. Depending on the time and expense required to correct any hardware design shortcomings detected during compliance testing, these failures can have catastrophic results for the commercial success of a new product. Careful attention is required up front for the hardware design requirements for cellular products. Module selection, the antenna solution and EMI management are the key areas of concern.

Compliance Efforts for a Cell Module Solution



Module Selection

Designing for compliance starts with choosing the right module from the right vendor. This choice must consider the tradeoffs between cellular technology, cost, vendor support for your design team, power consumption, geographic regions supported and support for future carrier network changes. Except for the very highest volume applications, the use of a module makes more sense than doing a chip-level design. The cost to execute a cell module-based design is much reduced compared to a chip-level design and the compliance costs can be reduced by up to 95% (i.e., the compliance costs for a module-based design can be 1/20th the costs of a chip-level design). Typical module PTCRB certification costs are $30k and up, but even at that reduced level, the compliance requirements and the corresponding demand on the design team remains quite significant.

Antenna Solutions

Compliance success demands that the antenna solution be designed into the system at the beginning of the project. Often, styling or mechanical constraints compromises and these need to be optimized early on. The device size enclosure will commonly affect the RF performance. In addition, elements like the LCD, battery and PCB ground plane significantly affect antenna performance. Early attention to the complex field exposure limits (SAR) is required to understand when a device will be used within 20cm of the body and can pay big dividends when it comes time to obtain device approval.

During certification, compliance with Total Isotropic Sensitivity (TIS) and Total Radiated Power (TRP) is a key requirement and is dependent on transmission line, antenna and EMI performance. These over-the-air (OTA) measurements give a good indication of the real-world wireless performance of your device. The entire product design impacts these critical measures, including the enclosure, PCB assembly and the product's effective ground plane. The ground plane of the PCB is an especially important part of the antenna system, as it directly affects the antenna impedance and radiation efficiency. Specifying an off-the-shelf chip antenna can simplify the design of an antenna solution, but antenna datasheets show performance only for one very specific physical and ground plane arrangement. They do not show performance for the arrangement of your specific product. Pre-testing is required before submitting for final certification testing to reduce costs and delays associated with approval lab failures.

Finally, ensuring the antenna's impedance is properly matched is a key contributor to compliance success. Most cellular antennas

have multiple resonances, meaning they are much more difficult to match than single-band, narrow band antennas (e.g., 2.4GHz Wi-Fi). Be sure your team uses a vector network analyzer to fully understand antenna performance before pursuing certification testing. Starting with the correct antenna design at the beginning of the project will ensure you have the right antenna placement and ground plane size that will yield a certifiable and marketable product.

Electro-Magnetic Interference (EMI)

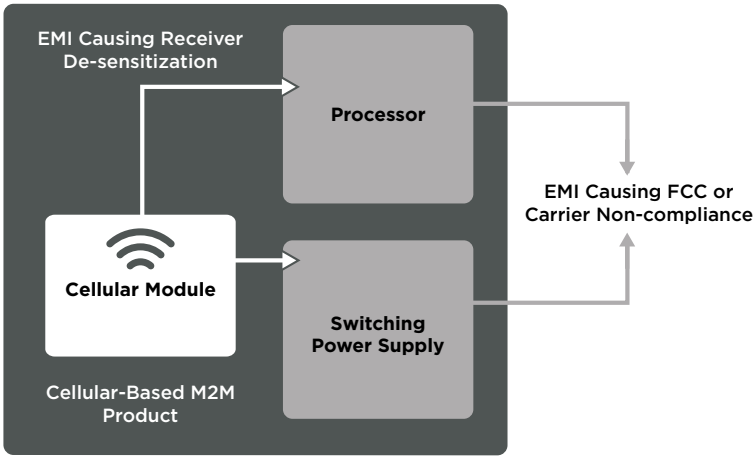
The management of unintended RF radiation is just as important to product compliance as the handling of the product's intended RF radiation. Many assume that passing FCC 15.1b unintentional radiator requirements for spurious emissions is the only EMI concern, but radiated spurious emissions (RSE) limits for PTCRB turn out to be even more stringent than the FCC requirements. A product's EMI must be minimized to prevent self- quieting or desensitization of the cellular receiver that can cause TIS requirement failures. RSE compliance is equally important, and it is very common for improperly designed analog or digital circuitry on the host PCB to generate and radiate harmonics of the cellular fundamental frequency and cause RSE failures during PTCRB or FCC certifications.

Many design aspects contribute to successful EMI management, but key points to manage include:

- PCB stack-up (number and order of layers)
- Ground plane design
- Component placement
- Placement Trace routing
- Proximity of power and high speed digital to RF traces and antennas
- RF decoupling capacitors
- Power supply layout
- Location and filtering of inputs and outputs

Electro-Magnetic Interference (EMI) Design Considerations

When a design incorporates multiple radios (e.g., cellular, Wi-Fi, Bluetooth, etc.) and antennas are located within 20cm of each other, it is described as having co-located radios. These designs require even more care because the intended transmissions from one radio become EMI for another radio as well as exacerbate radiated spurious emissions. Careful antenna placement, special filtering and even specific application firmware functions may be required to meet the additional performance, regulatory and carrier requirements of co-located radio designs.



EMI Impacts

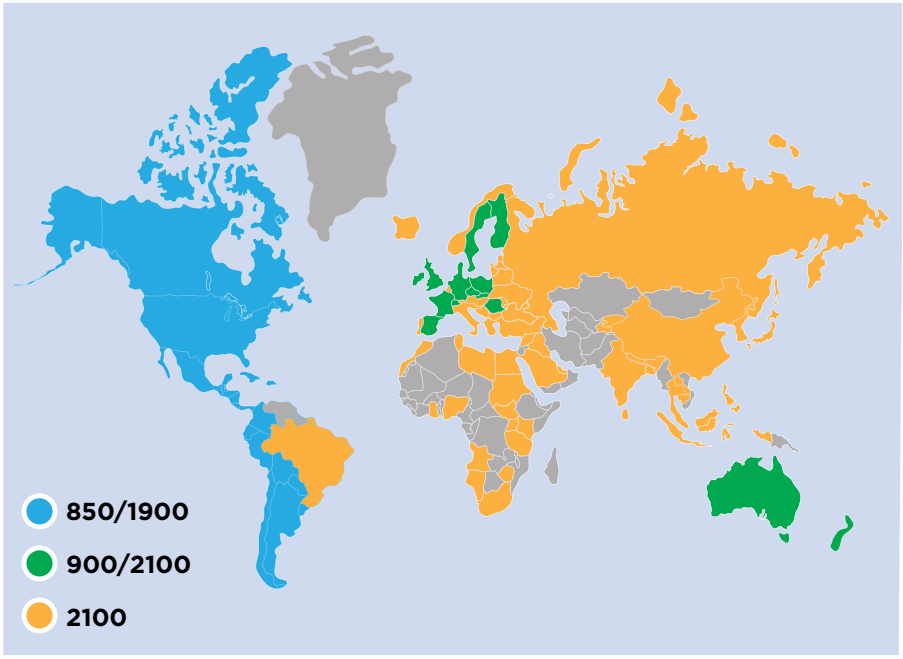
In addition to the obvious concerns of adequate supply power and managing for the possibility of limited battery power, power supply design has a major impact on EMI. Consider that the instantaneous current draw for a GSM cell module can be as high as 2 amps and the potential impact of power supply design on a device's compliance testing becomes clear. For efficiency with such high currents, switching mode regulators are popular for cellular designs; however, such switching power supplies are inherently noisy and can desensitize cellular receivers, commonly causing TIS failures during testing. Layout and filtering of power supplies is a critical element to control when designing for EMI compliance.

The following five cellular technologies are the most reconized and acceptable thus far, globally: These frequencies dominate the global market, considering they can be employed by any telco device that supports 2G GSM or 3G UMTS, and therefore can be used nearly everywhere in the world:

GSM Global System for Mobile Communication	Frequency	Band
	850 MHz	V
	900 MHz	VIII
	1800 MHz	III
	1900 MHz	II
	2100 Mz	I

Examples of non-standard frequencies include 450 MHz, 800 MHz and 1700 MHz.

Europe	2G	900 and 1800 MHz
	3G	900 and 2100 MHz
Americas	2G & 3G	850 and 1900 MHz
Global	3G	2100 MHz



Worldwide GSM/UMTS Networks

Deployments by region (UMTS-FDD)

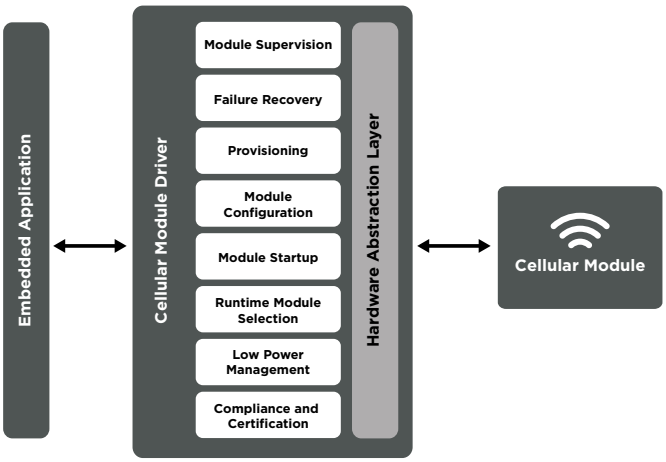
Frequency Band	Common Name	North America	Latin America	Europe	Asia	Africa	Oceania
2100	IMT	No	Aruba (SetarNV), Brazil, Costa Rica	Yes	Yes	Yes	Yes
1900	PCS A-F	Yes	Yes	No	No	No	No
1800	DCS	No	No	Nov	China (China Unicom) (Spectrum allocated, but no deployments)	No	No
1700	AWS A-F	USA (T-Mobile US, Cincinnati Bell, i wireless), Canada (Eastlink, Mobilicity, Vidéotron, Wind Mobile)	Chile (VTR, Nextel), Colombia (TIGO,Movistar), Uruguay (Ancel), Perú (Movistar, Nextel)	No	No	No	No
850	CLR	Yes	Yes	No	Hong Kong (SmarTone), Israel (Cellcom, Pelephone), Philippines (SMART), Thailand (CAT, DTAC, True Move)	No	Australia (Telstra,VHA), New Zealand (Spark NZ)
800		No	No	No	replaced by band 19	No	No
2600	IMT-E	No	No	No	No	No	No
900	E-GSM / U-900	No	Dominican Republic (Orange Dominicana), Paraguay (VOX), Venezuela (Digitel GSM)	Yes	Hong Kong (CSL, 3), Israel (Orange), Japan (SoftBank Mobile), Malaysia (Maxis), Philippines (Globe), Singapore (M1, SingTel, StarHub), Thailand (AIS), Kuwait (Wataniya)	South Africa (Cell C)	Australia (Optus,VHA), New Zealand (2degrees, Vodafone NZ)
1700		No	No	No	Japan (EMOBILE, NTT docomo)	No	No
1700	EAWS A-G	No	No	No	No	No	No
1500	LPDC	No	No	No	Japan (SoftBank Mobile)	No	No
700	LSMH A/B/C	USA, Canada	No	No	No	No	No
		No					
700	USMH C	USA, Canada	No	No	No	No	No
		No					
700	USMH D	USA, Canada	No	No	No	No	No
		No					
700	LSMH B/C	initially: USA, Canada	No	No	No	No	No
		later: Reserved					
800		No	No	No	Japan (NTT docomo)	No	No
800	EUDD	No	No	No	No	No	No
1500	UPDC	No	No	No	Japan (No)	No	No
3500		No	No	No	No	No	No
1900	EPCS A-G	USA (No)	No	No	No	No	No
850	ECLR	USA (No)	No	No	No	No	No

Firmware Design

When developing firmware for a cellular-enabled IoT device, a number of functional areas demand attention:

- Module supervision
- Failure recovery
- Provisioning module
- Configuration
- Module startup
- Runtime module selection
- Low power management
- Compliance and certification

Compliance and certification are listed last here, but product design teams need to bear in mind that products that don't comply with the required approvals (e.g., carrier acceptance testing, PTCRB or FCC) cannot be taken to market. Development teams are encouraged to work on compliance design requirements early in the design process not only to reduce costs, but also to allow for more robust design solutions and eventually to reduce your overall time to market.



Firmware Functions for Cellular Module Support

Q: "If I design with a module, doesn't that take care of compliance issues?"

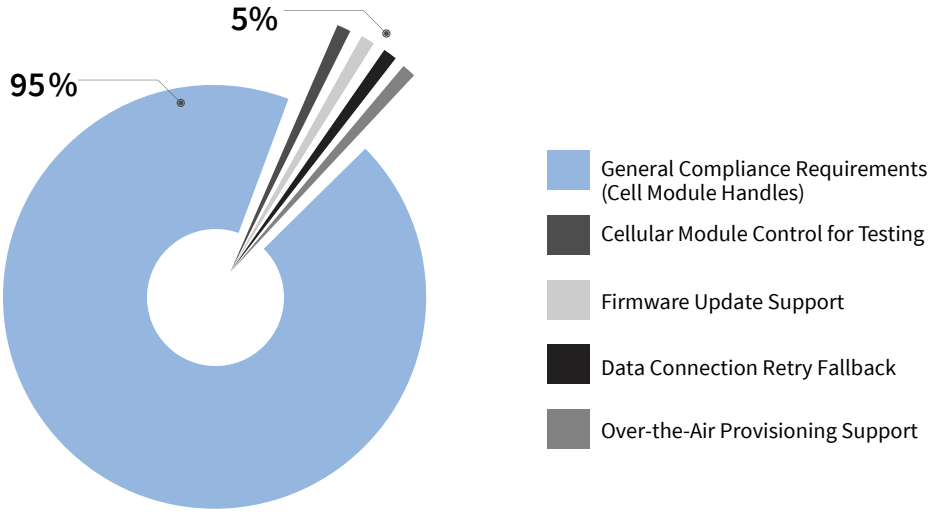
A: Selecting a cell module design that is certified for your geographic market and for use with the cell carrier networks does dramatically reduce your design responsibility for compliance. The cost of compliance for a module-based design could be as little as 5% of the cost of a full chip-level design. But ignoring that 5% will almost certainly prevent approval of your new cellular-enabled product for sale.

Q: "So what's in that 5%?"

A: While the firmware that is already designed into your selected cell module takes care of most of the compliance aspects of your design, there are several areas where your application remains responsible:

- Cellular module control for testing
- Firmware update support
- Data connection retry fallback
- Over-the-air provisioning support

These areas aren't complex to implement as long as the requirements to accommodate them are anticipated early in the design.



General Compliance Requirements

When you use a cellular module in your solution, it has been pre-certified to meet the vast majority of the network carrier's requirements. You don't need to worry about things like power level selection, preferred roaming list management and network registration sequence. Thousands of requirements are already handled, but there are a few that your firmware must support before it can be used on the network.

Cellular Module Control for Testing

One of the first and most important requirements is that your application allows test technicians to directly access the command channel for the cellular module, to allow test commands to be entered. While in this mode, your application must not be attempting any other control of the module. Availability of this pass- through mode is a critical requirement for completing approvals testing.

Firmware Update Support

Most carriers require cell modules to be able to accept new firmware images that are pushed from the network side. These updates, while infrequent, may occur at any time and obviously will affect the availability of the cell module during the update process. Your application must detect when the cell module enters a network-initiated firmware update and not interfere with the process. For example, an application that detects a cell module to be unexpectedly unavailable (such as happens during a firmware update cycle) may reset the cell module to try to restore it. Clearly, a reset operation during a firmware update session can have catastrophic results for the cell module.

Data Connection Retry Fallback

When a cellular data connection is observed to fail, the impulse is to have your application code immediately attempt to reconnect it. But if the failure is on the network side, a large number of terminal devices may be affected. If they all attempt reconnection at the same time, it may trigger a new network failure, a process that may then be repeated endlessly. Some carriers require repeated reconnection attempts to implement an increasing retry period as the number of attempts proceeds. Be sure to check the specific requirements of your carrier, the selected cellular module and your application to ensure that you meet these requirements.

Over-the-Air Provisioning Support

Provisioning with a network confirms a cellular module's authority to use the network. Especially on CDMA networks, this generally requires application support. And the process is complicated by the fact that the carrier's procedures may assume a user-mediated cellular device (e.g., a cell phone), where substantial display, input and human interpretation capabilities are available. For IoT applications, the process must be automated, accommodate limited device capabilities, and recover from

Development teams are encouraged to work on compliance design requirements early in the design process not only to reduce costs, but also to allow for more robust design solutions and eventually reduce your overall time to market.

unexpected failures during the initial provisioning attempt. Such operations are a key requirement that will be tested during carrier approval of your design, and your application must implement these features, or at least not interfere with the cellular module's implementation of these features.

The four key firmware issues that cause problems for new IoT terminal device designs are listed above, but of course, your carrier, cellular module or application may demand additional firmware design attention for full compliance. Consult with your carrier, the manufacturer of your cellular module and with design services firms experienced in this area to be sure you're not surprised by compliance requirements that depend on your application firmware.

Resources for IoT Cellular Development

Few organizations are expected to be experts in managing compliance risks for embedded systems that use cellular modules. Having the right partner on your side, though, can make all the difference. Digi Wireless Design Services will work with you from design to product launch using our proprietary and proven methodology to ensure that your product will pass the required FCC and carrier certifications. With a state-of-the-art RF lab, dedicated team of cellular engineers and a library of proven IP, we have the tools and resources to get your product to market the first time.

Summary

Cellular communication is increasingly common in terminal devices used in IoT systems; while cellular module solutions ease the basic design effort, the effort to meet governmental and industry regulations for cellular IoT devices is often overlooked in project plans. As a result, cellular compliance often trips up designers at the last minute, with one leading lab reporting an 80% first-test failure rate. Module selection, antenna selection and EMI control are the key hardware design functions supporting compliance success for cellular-enabled M2M devices. On the firmware side, manual cellular module control for testing, firmware update support, data connection retry fallback and over-the-air provisioning support are the key functions supporting compliance. Digi can greatly help you reduce compliance risks and expedite the approval of your products to market.

About Digi

Digi International (NASDAQ:DGII) is the M2M solutions expert, combining products and services as end-to-end solutions to drive business efficiencies. Digi provides the industry's broadest range of wireless products, a cloud platform for device management, and development services to help customers get to market fast with wireless devices and applications. Digi's entire solution set is tailored to allow any device to communicate with any application, anywhere in the world.

Key Takeaways:

- ✔ Cellular communication is common in terminal devices used in IoT systems.
- ✔ The effort to comply with applicable regulations for cellular IoT devices is often overlooked in project plans.
- ✔ Cellular compliance often trips up product designs late in the design process (80% first-test failure rate).
- ✔ Using cellular modules, rather than chip solutions, can reduce compliance costs by 95%, but failure to control the last 5% is a roadblock to your product receiving certification to get to market.
- ✔ Module selection, antenna selection and EMI control are the key hardware design functions supporting compliance.
- ✔ Manual cellular module control for testing, firmware update support, data connection retry fallback and over-the-air provisioning support are the key firmware functions supporting compliance.

Contact a Digi expert and get started today

PH: 877-912-3444
www.digi.com

Digi International
Worldwide HQ
11001 Bren Road East
Minnetonka, MN 55343

Digi International - France
+33-1-55-61-98-98

Digi International - Japan
+81-3-5428-0261

Digi International - Singapore
+65-6213-5380

Digi International - China
+86-21-5049-2199

DIGI™

/digi.international @DigiDotCom /digi-international

© Copyright 2015 Digi International Inc. All rights reserved. 91003069 A1 4/15

While every reasonable effort has been made to ensure that this information is accurate, complete and up-to-date, all information is provided "AS IS" without warranty of any kind. We disclaim liability for any reliance on this information. All registered trademarks or trademarks are property of their respective owners.