WHITE PAPER

Avi Baum
Embedded Connectivity Solutions
Senior Architect and Technology Advisor
Texas Instruments

Texas Instruments

A link to the Internet of Things

IoT made easy with SimpleLink™ Wi-Fi® solutions

Overview

It has been over a decade since the term Internet of Things (IoT) was first coined. Making its way to the center of the stage, it has now become mainstream. All of a sudden, leading companies are adopting the term vigorously into their most advanced products and services. It is trendy and reflects state-of-the-art thinking. However, as the term is more widely used, its interpretations become more diverse. Some would call any connected device an IoT solution, while others will only refer to big data analytics as the IoT aspect of the product.

In this paper we will sort out what is considered the IoT, and define and explore the necessary building blocks of an IoT system, its main virtues and what it takes to build one. We will show that with the help of proper devices, making your device or product IoT enabled is a fairly straightforward task.

What is the IoT?

So, what exactly is the Internet of Things (IoT)? How is it different from the Internet we know and use on a daily basis? Does the fact that it is referred to as the Internet "of Things" stand in contrast to some other Internet, and if not, why is there any distinction to begin with? Why is a postfix needed to designate things in particular?

First, one needs to realize that even basic Internet, the one that we all use on a day-to-day basis, has gone through a great deal of changes over the years. It has gone from being a huge knowledge sharing system to its current state, which is better described as a service-oriented infrastructure. The majority of web traffic nowadays is already non-human and a large share of the content is dynamically created.

The massive explosion of online services, further inspired by the smartphone and handheld revolution, which made these services highly accessible, has created a demand to leverage technology for machine-to-machine (M2M) communication. It has also created a decline in the cost for adding connectivity capabilities into products.

The cloud computing evolution, supported by an increase in storage capacity, has also brought the ability to scale the amount of data that can be stored effectively and affordably. This is yet another angle in enabling machines to generate and collect large amounts of data on a regular basis.

This data has to be processed, analyzed and distilled so that meanigful insights can be extracted and action may be taken based on those insights. The process of making sense out of all this data is also commonly referred to as big data analytics.

Yet, having realized the above, it is still unclear to what extent the Internet-of-people and the Internet-of-machines will blend. Today, the connection is still quite loose. While both share the same infrastructure, the level of interaction between the two is fairly limited. This is, in fact, the essence of the questions introduced at the beginning. Stated differently, it is important to understand how many Internets are there. In our view there will eventually be a

convergence toward one single Internet to serve all. This realization is critical for the immersion of information coming from machines.

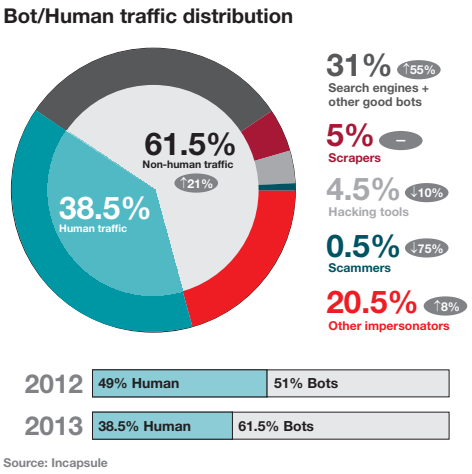

Figure 1. Distribution of Internet traffic sources

The IoT paradigm discussed may be encountered in a wide variety of venues that span across the various activity circles throughout the day using different kinds of devices. In the ***personal*** area network we encounter ***wearable*** devices to enhance our health and wellness. At ***home*** we are surrounded with an ever-growing number of ***appliances***, ***multimedia*** devices and other ***consumer gadgets***. While ***on-the-go***, we use private or public transportation ***vehicles*** and ***infrastructure*** to improve our mobility time utilization. In the ***industrial*** case, ***sensors*** might be introduced for production efficiency, maintenance and failure management. And at a ***metropolitan*** level, smart building management systems and ***infrastructure*** for remote management, on-going maintenance and asset tracking will be observed.

Furthermore, the IoT is not limited to specific types of products. Both high-end technology products and products that are extremely simple may take part in the flow of information either as data providers or consumers. And this is not confined to the boundaries of electronic devices and appliances. It is also reshaping the way traditional products are designed (examples as bizarre as a connected toilet are becoming more common these days).

This framework should be always on; its availability should not rely on Internet availability. While it is true that some functionality will be absent when network connectivity is obstructed, the overall experience, coherence and consistency should be maintained.

Anything.
Anywhere.
Anyone.

Anything

Eventually, any device, appliance or entity will be seamlessly connected to the Internet. Connectivity will not be the main feature of the device, but will extend the device's capabilities.

Anywhere

Any conceived wireless connectivity framework should be abstract enough to run from any location – both geographically and from a network topology perspective. The former refers to Internet-based ubiquity; the latter, refers to the ability to clone the framework into intranet environments where Internet access is limited or undesired. Acknowledging the structure of the Internet beyond the public domain is important to enable the expansion of the IoT paradigm.

Anyone

Currently, not all things are connected to the IoT. But an IoT ecosystem that is easy to use and secure is not that far away. This will make the IoT accessible to anyone. Anyone will be able to connect their product to the Internet, and also customize it with their personal preferences.

The "thing" that matters

Regardless of the interpretation – as the name suggests – an IoT system that follows the approach described above involves things and the Internet. It follows that these things carry some means to connect to the Internet, and most likely in a wireless manner using either Wi-Fi or another wireless technology connected through a gateway to the network router. A wired connection is still a viable option.

There are several fundamental features that a "thing" has to encompass to be a good IoT solution. Among these, the most important features are energy efficiency, security, data handling and simplicity.

Power

Energy distribution and efficiency are becoming more important as awareness in power preservation rises. This is especially true for battery-operated solutions. In order to support the Anything-Anywhere-Anyone vision outlined above, and assuming massive amounts of connected things will be sprouting up; one cannot overlook the importance of power conservation. It will guarantee its scalability. As the number of devices grows, even small amounts of excessive power will be a noticeable waste.

When it comes to power, the challenge is to ensure that adding Internet connectivity does not impose a change to the power supply. In other words, ideally it should fit within the existing power budget headroom. Another challenge directly related to energy management is attributed to the fact that communication introduces inherent overheads. In many typical applications, the amount of information to be transmitted is significantly lower than the total bits over the air.

The trickiest part is to ensure that the eventual outcome yields a positive power balance at the overall system level. For the approach to have merits, the benefit gained by having a connected node needs to exceed the power that was consumed in the process. The inherent nature of the IoT topology, with a large number of nodes also provides an opportunity since a large number of properly managed nodes may result in lower power per node. As shown in Figure 2 on the following page, the higher node density is leveraged to

distribute the power more equally across the nodes. This may in turn reduce the supply capacity of each node and eventually lower the cost and power per node.

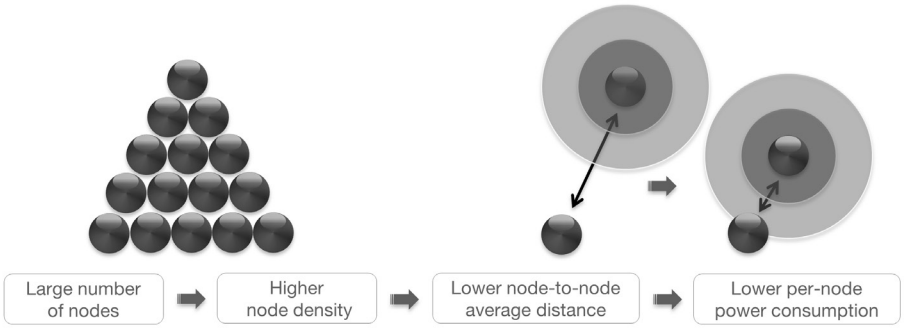

Figure 2. Energy distribution opportunity in IoT setting

Consider for example, a water-boiling system. Assume this system is equipped with a combination of temperature sensors, and a big data analytics system that monitors the actual hot water usage compared to the number of times it was heated. This system can eventually converge to avoid unnecessary heating cycles and save energy that is far more valuable than the power spent on communicating the information among the system components.

Security

Security is always a challenge in data networks. This challenge intensifies in the case of the IoT simply because there are more entry points thereby creating more penetration points. This increased system vulnerability makes the battle for security inevitable. In an IoT solution, threats also take a new level of magnitude since it is not just data that is put at risk. With the IoT the damage potential is much higher (e.g., opening a door remotely, taking a burglar alarm system offline). There will surely be a never-ending fight toward better security. Yet, the presence of multiple nodes also provides redundancy and distributed approaches. In any case, state-of-the-art security schemes are necessary to be ahead of the pack in this regard. More specifically, structures that have been successfully adopted in federal systems and e-commerce are good examples for industry-proven security systems.

Data handling

Massive deployment of endpoints results in higher node density. This requires demand for higher capacity. Furthermore, large quantities of data that are generated create a need for accessible storage. In addition, real network latency introduces a challenge to limited resource systems as shown on Figure 3 on the following page.

Taking these limitations into account when designing the application will help avoid performance issues upfront. While this is mainly cast upon the developer, a properly designed networking engine regulates the traffic thus taking away much of the trouble.

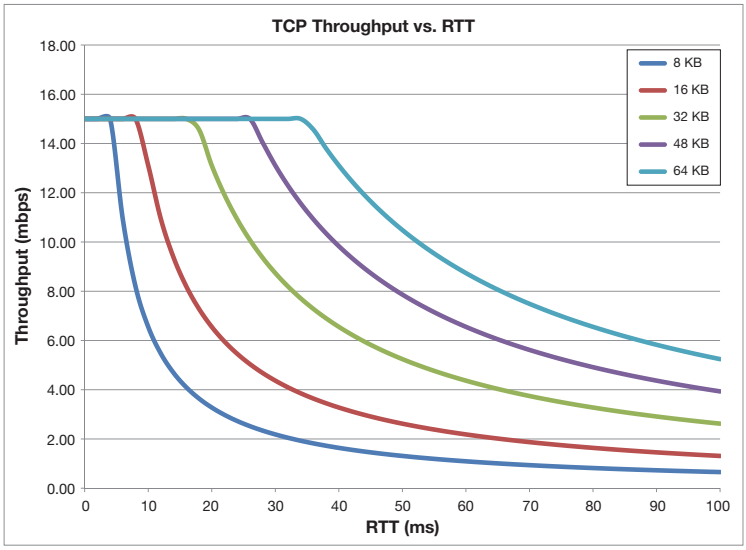

Figure 3. TCP throughput as function of round-trip-time (RTT) for various window sizes

Good design practice includes a proper balance between the number of accesses to the network and the amount of data transferred per access. If possible, aggregating data will improve capacity and achievable throughput. On the other hand, if latency and response time are of the essence, aggregation might not be the right approach.

Simplicity

The simpler it is to add Internet connectivity to products, the more likely it will be adopted. Simplicity is a subjective term and may take various shapes and forms. We refer to it in a holistic manner encompassing all the different stages of the product lifecycle. Understanding the needs and set of expectations of each of the relevant stages along the flow is critical for a successful product. The stages may include, for instance, early evaluation and product assessment, prototyping, field tests, mass production and deployment. In each of these stages, different aspects of the solution require attention in order to achieve maximum simplicity and ease-of-use.

The biggest challenge in this case is to transform subjective measures into objective criteria that can be evaluated and compared. Once this is done, it makes it much easier to evaluate and improve the level of simplicity attained. Examples for such criteria can be the time it takes to introduce a new protocol, the complexity of the code that involves network connectivity, number of bugs or reported issues due to device connectivity, etc.

The IoT players

Now that we've stated the rationale for a single Internet for all, and having realized the main properties of the new nodes to be introduced, let us take a step back and have a wider view of the IoT playground. To do that,

the key players must first be identified. We make a distinction of three clusters of players, users, things and services.

- *Users* are human participants that use services and their own end equipments. They mostly consume information and may inspire actions through profile settings and other decision-making processes.

- *Things* are physical or virtual endpoints representing either a data source, data sink or both. They feed or consume information to and from the Internet. This is also commonly referred to as "the cloud".

- *Services* are information aggregators and may provide tools for data analysis of different kinds. In some cases can be used to carry out actions requested by clients, either users or things.

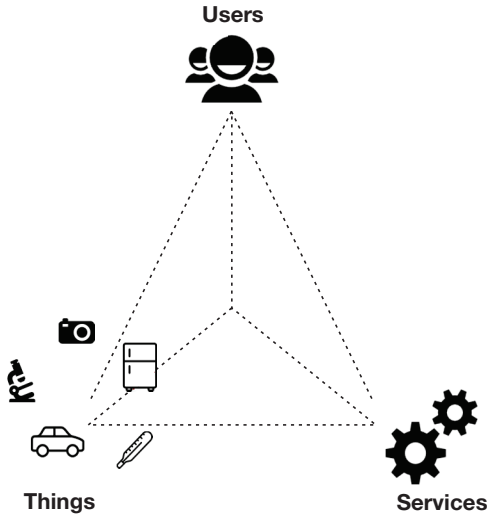

Figure 4. IoT players

Extend. Revamp. Innovate.

It is about time to raise the imminent question… why? What is the big deal with connecting things to the Internet or giving them the ability to connect at all? Why is it an evolutionary act that some consider the beginning of a new era?

To answer that, let us examine a case of an extremely simple device – a light switch. Connecting a light switch allows remote control and monitoring from a larger distance thereby extending the functionality beyond its physical location. This opens up a set of options where the switch is virtually everywhere enabling multiple control points to exist at once.

Additionally, the introduced capability can now overlay other features onto the switch. For example, the switch controls a light that may serve as a feedback path to various activities taking place elsewhere on the network. Each incoming message can generate a short blink; light preferences of the user may be taken into account, etc. These features revamp the definition of a switch, as we know it.

Once such devices are common enough, stable and interoperable, they may become disruptive to already established ecosystems. In the case of the light switch, the fact that it is connected might inspire a new approach to the way houses are built and wired. It implies that there is no longer a need to attach a switch to every light and to make sure every light is routed to predefined physical location. Furthermore, switches could be dynamically mounted around the house and not attached a-priori, they might be avoided altogether or alternatively be reprogrammed to control different lights at will. As farfetched as it may seem, this kind of thinking, seeded by the connected endpoint, will reshape more and more ecosystems in growing number of domains.

Figure 5. Light switch (a) in the traditional way and (b) IoT-enabled

SimpleLink Family. Unlocking the door to the IoT

With the above in mind, along with the knowledge of the growing demand in the IoT, the Texas Instruments (TI) SimpleLink™ family of solutions was born. It is designed exactly for the purpose of addressing the challenges of an IoT node or gateway. The SimpleLink Wi-Fi® CC3100 and CC3200 platforms are equipped with all the needed capabilities described above, thereby allowing customers to explore and innovate for the IoT.

These devices include a Wi-Fi networking engine that incorporates all the required software components up to the application layer. The user is left to focus on their own application, while all the rest is being taken care of by the networking engine. A lot of thought was put into the devices in order to make the process of adding Internet connectivity over Wi-Fi to products extremely easy.

As mentioned, the device comes in two varieties. The **CC3100** Wi-Fi wireless network processor is for use with an external microcontroller (MCU). This leaves the MCU choice to the user. The **CC3200** includes the same networking core as the CC3100 but has the industry's first built-in programmable ARM® Cortex®-M4 MCU allowing development with a single IC.

Ease of use

When it comes to ease of use, the SimpleLink Wi-Fi family is setting a new bar. Starting with the developer, the solution is designed for rapid development cycles. It comes out-of-the-box ready for Internet connectivity and a true IoT experience. An emulation library provided as part of the development kit enables the development of the networking-related aspects of the end product, using a PC regardless of the MCU that will be used in the final product.

A result of a meticulous design, the user is provided with a very slim set of APIs that give access to the variety of capabilities the device has to offer. The APIs are organized into silos to make the navigation extremely intuitive and self-explanatory. Among the silos the developer will find, the socket silo, which represents the interface to the networking layer. BSD socket adherence was selected, owing to its wide usage. This results in an extremely rapid way to make networking code run on the SimpleLink Wi-Fi solutions.

From a vendor perspective, manufacturability is a key aspect of any solution. In the SimpleLink Wi-Fi family's case, because all components are integrated, there is no need for any special production line calibration. This is a burden saved from the vendor. Additionally, the device package is very common and easy to use without imposing any special PCB constraints. The reference design is freely available and provided for the benefit of those who wish to create a discrete layout.

For the end-user, the SimpleLink Wi-Fi family provides on-chip mechanisms for **first-time connection (aka provisioning)** as well as tools for diagnosis and monitoring the device. All these are supported regardless of the content carried by the MCU.

	Care-about	SimpleLink Wi-Fi Family
Developer	Time to get started Time to install SDK	Simple and short out of the box flow SDK is publicly available
	Learn the device specific APIs (SDK)	Standard BSD APIs for networking
	Target platform issues	Evaluation system to decouple networking development
Vendor	PCB complexity	QFN package or module
	Production line testing	No production line requirements
User	Consistent getting started	Encapsulated in the device in the form of predefined mechanism for provisioning
	Consistent troubleshooting	On-chip support for • Ping • HTTP server • mDNS • DNS • TCP/IP • TLS/SSL
	Provisioning method (Initial connection to the network)	Most flexible provisioning options in the market. Supporting: • Access point mode • SmartConfig™ • WPS (PIN and pushbutton methods) • Apple Wireless Accessory Configuration (WAC)

Table 1. SimpleLink Wi-Fi solutions addressing key care-abouts throughout product life cycle

Security

As stated above, security is fundamental, and no real Internet solution can live without it. Nearly every transaction carried out over the Internet today is handled with transport layer security. The network engine of the SimpleLink Wi-Fi solutions encapsulates both the link layer and transport layer capabilities. The user is only required to deliver the information needed in order to establish the secure channel.

At the link layer, this encapsulation translates into a successful network connection on the local network (typically with the AP). At the transport layer, this encapsulation handles all the negotiation with the remote target server so that information can float back and forth securely over the established channel.

Nearly all Internet services today require a secure communication channel, and rightfully so. In many cases, sensitive information is carried across the network. This includes user-specific information, credentials and personal data. Therefore, any device that connects to real-life services needs to integrate a secure transport layer. Taking away the burden from the host platform relieves a great deal of the pain involved in developing a solution that interacts with Internet services.

Low power

For battery-powered products, certain measures can be taken to favor battery life over other performance aspects. In those cases, it is important to provide the system some guidance on the target outcome. In order to avoid exposure of many internal knobs, which will cast a great deal of complexity upon the user, the SimpleLink Wi-Fi devices use a policy-based approach instead.

The policy-based approach provides the ability to guide the system preferences regarding power tradeoffs, while avoiding the need to directly manipulate internal system dials. This approach provides both simplicity and protection. The developer is eventually offered only a limited set of policies to choose from and the rest is done internally. Once a policy is selected, it may be applied with policy-specific information to fine-tune the exact behavior under the selected policy.

A simple sensor node, for example, is more likely to transmit data out and, in some cases, does not need to be responsive. In this case, applying policy that favors immediate return to low-power mode would have benefits in terms of the device's life span. Remote control, on the other hand, would benefit from a low-latency power policy.

Putting it all together with SimpleLink Wi-Fi

Before wrapping up, let's put together an example that shows how all the above comes together to create a simple application that connects securely to an Internet service to retrieve information, and then shuts down to preserve power. For this example let's look at a battery-powered countertop clock with weather station, like the one below. It would be a nice benefit to have the weather (and even the clock itself) automatically connected to the Internet to obtain weather information.

Figure 6. Countertop clock with weather information

Here is the entire SimpleLink CC3100 code that will accomplish the task. It is available in the CC3100 and CC3200 SDKs. This code will go to an Internet service to securely retrieve weather-related information for a given city and then shutdown.


```c
#include <simplelink.h>

#define API         "GET /data/2.5/weather?q=%s&mode=xml&units=imperial HTTP/1.1\r\n
                     Host: api.openweathermap.org\r\nAccept: */*\r\n\r\n"
#define BUFF_SIZE   256

void GetWeatherExample (char *host, int port, char *api, char *city)
{
    unsigned long   ip;
    int             sock;
    SlSockAddrIn_t  addr;
    int             size;
    char            buff[BUFF_SIZE];
    unsigned char   value;

    sl_Start (0,0,0);

    sl_NetAppDnsGetHostByName(host, strlen(host), &ip, SL_AF_INET);

    sock = sl_Socket(SL_AF_INET,SL_SOCK_STREAM, SL_SEC_SOCKET);

    value = SL_SO_SEC_METHOD_SSLV3;
    sl_SetSockOpt(g_SockID, SL_SOL_SOCKET, SL_SO_SECMETHOD, &value, sizeof(value));

    value = SL_SEC_MASK_SSL_RSA_WITH_RC4_128_SHA;
    sl_SetSockOpt(g_SockID, SL_SOL_SOCKET, SL_SO_SECURE_MASK, &value, sizeof(value));

    addr.sin_family         = SL_AF_INET;
    addr.sin_port           = sl_Htons(port);
    addr.sin_addr.s_addr    = sl_Htonl(ip);

    size = sizeof(SlSockAddrIn_t);

    sl_Connect(sock, ( SlSockAddr_t *)&addr, size);

    sprintf(buff, api, city);
    sl_Send(sock, buff, strlen(buff), 0);

    sl_Recv(sock, &buff[0], sizeof(buff), 0);

    /* .. PARSE RESPONSE AND MANIPULATE PER USER NEEDS .. */

    sl_Stop (100);
}
```

To the reader who is not familiar with software development the above might not say much, but one could realize the simplicity of the code in term of its length compared to the task it accomplishes. You can find this exact example in the SimpleLink **CC3100 Software Development Kit (SDK)**. From the perspective of security, note the connection to the server is carried out using a secure transport layer. When considering the power consumption implication, it turns out to be negligible (i.e., not affecting the product life span) if the update period is reasonable. Such a clock, running on four AA batteries will last around two years of continuous operation. Adding a Wi-Fi based connectivity component that updates every 30 minutes, will not violate the 1–2 years estimate.

As a final bonus item, it is worth mentioning the on-chip Web server. It can be used without changing a single line of code to configure the product remotely, thereby offering a new capability.

Summary

The IoT is the next big thing. There is no doubt about it. TI is creating the necessary solutions to help customers create products for the IoT on the endpoint side, today. Thereby enabling its customers to connect more, making dreams a reality. To get a more in-depth exploration of the wide variety of capabilities offered by the SimpleLink Wi-Fi CC3100 and CC3200 platforms, visit: **www.ti.com/simplelinkwifi**.

IoT is too wide to cover in a short whitepaper like this. This is just the tip of the iceberg. Many important concepts of the IoT and the SimpleLink Wi-Fi solution such as security properties and policy management were briefly mentioned. Stay tuned for more information from TI.

IoT is fascinating and there are lots of opportunities to innovate and shape it, and you can easily start today. But, do not take my word for it. You can try it out yourself. Just go to **www.ti.com/iot** to learn more about TI's solutions for the IoT and start exploring the fascinating world of the IoT.

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, enhancements, improvements and other changes to its semiconductor products and services per JESD46, latest issue, and to discontinue any product or service per JESD48, latest issue. Buyers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All semiconductor products (also referred to herein as “components”) are sold subject to TI’s terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its components to the specifications applicable at the time of sale, in accordance with the warranty in TI’s terms and conditions of sale of semiconductor products. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by applicable law, testing of all parameters of each component is not necessarily performed.

TI assumes no liability for applications assistance or the design of Buyers’ products. Buyers are responsible for their products and applications using TI components. To minimize the risks associated with Buyers’ products and applications, Buyers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI components or services are used. Information published by TI regarding third-party products or services does not constitute a license to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of significant portions of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI components or services with statements different from or beyond the parameters stated by TI for that component or service voids all express and any implied warranties for the associated TI component or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Buyer acknowledges and agrees that it is solely responsible for compliance with all legal, regulatory and safety-related requirements concerning its products, and any use of TI components in its applications, notwithstanding any applications-related information or support that may be provided by TI. Buyer represents and agrees that it has all the necessary expertise to create and implement safeguards which anticipate dangerous consequences of failures, monitor failures and their consequences, lessen the likelihood of failures that might cause harm and take appropriate remedial actions. Buyer will fully indemnify TI and its representatives against any damages arising out of the use of any TI components in safety-critical applications.

In some cases, TI components may be promoted specifically to facilitate safety-related applications. With such components, TI’s goal is to help enable customers to design and create their own end-product solutions that meet applicable functional safety standards and requirements. Nonetheless, such components are subject to these terms.

No TI components are authorized for use in FDA Class III (or similar life-critical medical equipment) unless authorized officers of the parties have executed a special agreement specifically governing such use.

Only those TI components which TI has specifically designated as military grade or “enhanced plastic” are designed and intended for use in military/aerospace applications or environments. Buyer acknowledges and agrees that any military or aerospace use of TI components which have ***not*** been so designated is solely at the Buyer's risk, and that Buyer is solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI has specifically designated certain components as meeting ISO/TS16949 requirements, mainly for automotive use. In any case of use of non-designated products, TI will not be responsible for any failure to meet ISO/TS16949.

Products		**Applications**	
Audio	www.ti.com/audio	Automotive and Transportation	www.ti.com/automotive
Amplifiers	amplifier.ti.com	Communications and Telecom	www.ti.com/communications
Data Converters	dataconverter.ti.com	Computers and Peripherals	www.ti.com/computers
DLP® Products	www.dlp.com	Consumer Electronics	www.ti.com/consumer-apps
DSP	dsp.ti.com	Energy and Lighting	www.ti.com/energy
Clocks and Timers	www.ti.com/clocks	Industrial	www.ti.com/industrial
Interface	interface.ti.com	Medical	www.ti.com/medical
Logic	logic.ti.com	Security	www.ti.com/security
Power Mgmt	power.ti.com	Space, Avionics and Defense	www.ti.com/space-avionics-defense
Microcontrollers	microcontroller.ti.com	Video and Imaging	www.ti.com/video
RFID	www.ti-rfid.com		
OMAP Applications Processors	www.ti.com/omap	**TI E2E Community**	e2e.ti.com
Wireless Connectivity	www.ti.com/wirelessconnectivity		

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265