Processing solutions for biometric systems

Arun Mani
Marketing Team

Mark Nadeski
Marketing Manager

Texas Instruments

Introduction

Biometrics authentication is the process of extracting measurable biological or behavioral characteristics for the purpose of uniquely identifying or authenticating an individual. This is a rapidly growing market driven in large part by concerns for countries to strengthen their national security. Ideally large-scale biometrics security solutions would consist of a unified biometrics solution, but the vastly different computational requirements for different biometric technologies and applications makes this quite difficult.

This document describes the various biometric authentication systems and the key elements of these systems that determine their computational requirements. This paper then discusses the wide mix of processing solutions from Texas Instruments and how these processors form a scalable platform to build a variety of biometrics solutions.

Biometric behaviors

While there are innumerous biological and behavioral traits that can uniquely identify an individual, the most commonly used characteristics are fingerprint, iris, face, voice, vein, signature and hand geometry. A biometric system captures these characteristics and converts them into digital form where an algorithm can be used to make an identification or verification decision. Figure 1 shows the percentage of biometric systems on the market associated with each of the major biometric characteristics.

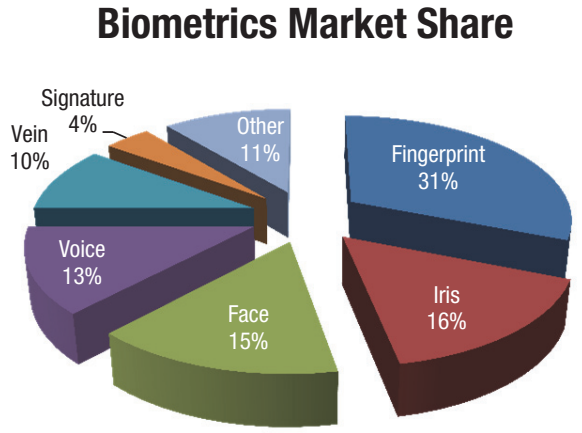

Figure 1: Biometrics market share by system type

Fingerprint: Human fingerprints are made of ridges and valleys. The pattern formed by the ridges and valleys are unique to every person. In order to map out the pattern, the biometric system traces points through the ridges identifying minutiae points like the splits in the ridges, empty spaces and joining or crossing of ridges. The number of reference points required to uniquely identify a person varies from 12 to 17 points. This low number of reference points makes fingerprint systems the most popular modality of biometric systems. Less points to extract and analyze translates to relatively low processing requirements and a lower overall cost compared to other biometric systems. But the fingerprint systems have a few shortcomings. Complexity is added for a fingerprint system to take into account cuts, dirt, wear and tear that may be present on a finger. Also, it turns out that it can be difficult to distinguish between a real finger and a picture of a finger. Another added complexity is that a small percentage of the population either does not have any minutiae or has less minutiae than average, making authentication via a fingerprint system for these individuals more problematic. While

these issues constantly plague fingerprint systems, the systems remain widely used around the world.

Iris: The iris is the elastic, pigmented, connective tissue that controls the pupil. The iris pattern is unique for a person and is stable throughout a person's life. An iris biometric system scans and analyzes about 200 points to authenticate a person. As a result, these systems are extremely accurate. The scanning process takes place anywhere from three to 10 inches from the body making this process non-intrusive. This identification process is not affected by the lens, contacts or surgery. Relative to a fingerprint system, the processing power of an iris system needs to be approximately 10× faster in order to produce results in the same timeframe. This extra processing power increases the cost of the iris systems. Unlike fingerprint systems, iris recognition requires cooperation from the identified subject, which can sometimes be difficult to achieve, especially if trying to identify a hostile subject.

Face: Human faces have multiple features that can be used to uniquely identify an individual. Examples of these facial characteristics are the distance between the eyes and the width of the nose. There are about 80 such features termed as nodal points that can be extracted and analyzed. The greatest benefits of facial biometric systems are the ability to capture the features from a far distance without the subject becoming aware of the system. This benefit also comes with increased challenges. Outside of a controlled environment, it becomes very difficult to match faces that are not posed, illuminated or showing expression in a standardized way. Once conditions start to deviate from the ideal, system accuracy drops significantly. Simple things like dim lighting, wearing a hat or other means to obscure an image of the face and motion blur all add complications and reduce accuracy. Controlled systems have much higher accuracy ratings, but can still be fooled if subjects alter their facial features using prosthetics or other means.

Voice: Identifying subjects using their voice prints is one of the oldest and most often used processes of identification. The voice systems are very similar to the fingerprint system. They are easy and affordable to implement, but they also have many short comings. The voice print of a subject can change dramatically because of external factors like environment and health. Voice prints might also change over time and might need constant update of the subject's voice samples.

Vein: A person's palm has a broad and complicated vascular pattern which can be used to uniquely identify a subject. Vein patterns are extremely secure as they lie under the skin and are difficult to replicate. Due to the complexity of the vein patterns, the processing power requirements of the vein systems are high compared with other biometric systems.

Modes of operation of the biometric systems

The biometric system can be operated in two modes: enrollment and authentication modes. In the enrollment mode, the biometric system converts the person's biometric characteristics into a digital template and stores this in a storage system. Figure 2 shows the typical enrollment mode for a biometric system.

In the authentication mode, the biometric system can be used for a verification process or an

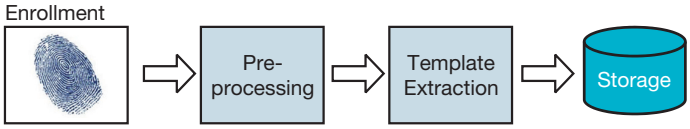

Figure 2: Enrollment process for biometrics systems

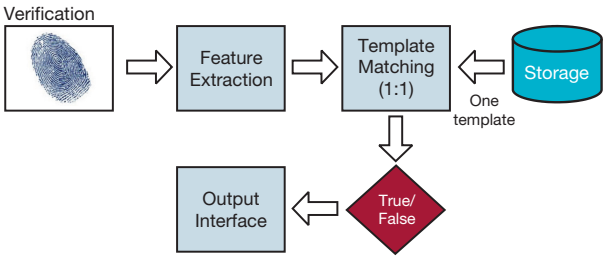

Figure 3: Biometrics verification process

identification process. During the verification process, the biometric system validates a person's identity by comparing the recorded characteristics with his or her own template. This verification is known as one to one. This process is shown in Figure 3.

During the identification process, the system identifies the user by comparing the recorded characteristics with all the users in the database. This identification is known as one to many. The process is shown in Figure 4.

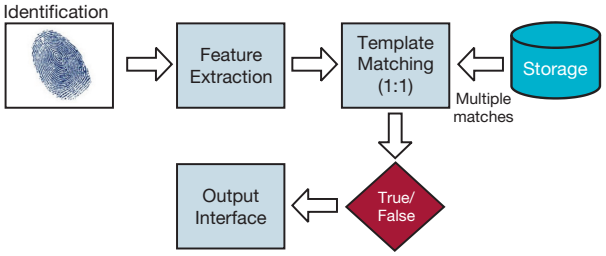

Figure 4: Biometrics identification process

Types of biometric systems

Most of the biometric systems can be classified into either a stand-alone system or a client-server system.

Stand-alone biometric system:

The stand-alone (also known as a biometric terminal) system incorporates both the enrollment and the authentication process. Figure 5 illustrates the biometric terminal system. The biometric features that are extracted (templates) during the enrollment phase are encrypted and stored in a secure internal memory. During the authentication process, these templates are retrieved, decrypted and matched with the features of the individual who is attempting authentication. Based on the matching algorithm the decision of accepting or rejecting the match is conveyed to the user.

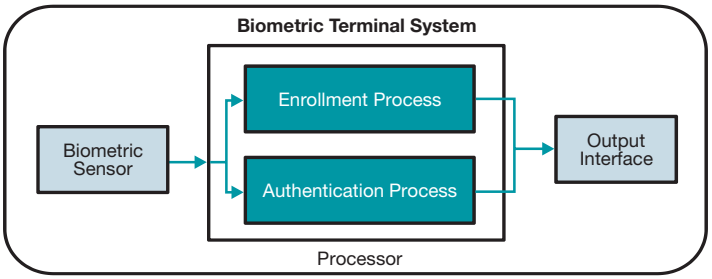

Figure 5: Biometrics terminal

Client-server biometric system:

Client-server systems are deployed to manage the authentication process for a large population set. As shown in Figure 6 on the following page, the client station will be very similar to the terminal system except that the template will be stored and matched in the remote server station. The client station extracts the template, encrypts and compresses the data. This compressed data is securely transferred to the server. During the enrollment process, the server stores the encrypted data. During the authentication process, the individual's biometric features are extracted and digitized into the template. This template is then decompressed, decrypted and compared with the already stored template and the matching decision is securely transmitted to the client station.

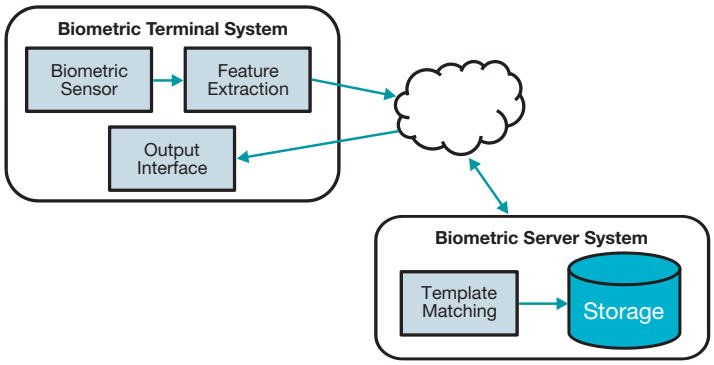

Figure 6. Biometrics client server system

The terminal systems and the client stations used to be restricted to bulky desktop computers due to the speed and processing requirements of the biometric process. But the requirements for mobile biometric systems have increased as more and more applications in markets like banking, law enforcement and military required rugged security systems that can work in remote and/or unfriendly terrains. Even more recently, the integration of a fingerprint scanner in smart phones have further increased consumer awareness of mobile biometric systems. These changes have paved the way for embedded biometric terminals and client stations.

Due to the advancement in embedded processors, these embedded systems have not only become mobile but they also have sufficient processing power to execute both the enrollment and authentication processes. Further, these embedded processors provide sufficient security features that are ideal to provide secure access to buildings, secure access to industrial systems and efficient management of human resources.

The server stations themselves currently remain predominantly rack servers or FPGAs to satisfy significant computation requirements, but the power efficiency and scalability of embedded multicore processors make them attractive substitutes for next-generation biometric server stations.

Hardware elements of the biometric systems

Irrespective of the type of biometric system, systems can be subdivided into four basic elements: sensing, processing, storage and interface for access.

Sensing element: Sensing elements are how inputs are gathered for a biometrics system. They are responsible for either collecting the biometric characteristics of the person during the time of enrollment or verifying one's identity during the time of access. The biometric features captured through these sensing elements are sent to the processing elements.

Processing element: Processing elements extract useful information from the signals captured by the sensing element. The processing elements can construct a template out of the information extracted. They can also compare this template against either a specific template or a collection of templates to verify or identify a person. In the case of the stand-alone system, both the template extraction and matching process will be implemented in the terminal. In the case of client-server systems, the template extraction process will be executed in the client station, while the matching process will be executed in the server station.

Storage element: The main purpose of the storage element is to store the processed template that can be recalled to match during the authentication process. For most identification solutions (1:N), the storage element would be a random access memory (RAM) or Flash erasable programmable read-only memory (EPROM) or some form of memory IC. In a few cases, the storage element could be a data server. In the case of verification (1:1), a removable storage like a contact or

contactless smart card can be used. The storage unit will be part of the server station in case of the client-server system.

Interface element: Once the processor element completes the specified application, the decision of the biometric application needs to be conveyed to the user. The interface element is used for this purpose. The interface element can be an RS-232 serial interface or a high-bandwidth USB interface. Alternatively this element might be a network medium like Ethernet, wireless or *Bluetooth*® interfaces. In case of the client-server station, the data transfer to and from the server station requires a fast and secure interface like Ethernet.

Software elements of the biometric systems

The efficiency of the biometric system not only depends on the hardware elements used, but also by the software modules of the system. The software can be classified into six elements.

Encode element: The purpose of this element is to encode or compress the data collected by the sensing elements based on the systems requirements.

Enhancement element: The encoded data needs to be enhanced to improve the captures minutiae. Some of the enhancement processes used are filtering, edge correction, edge enhancement and similar analytics-based algorithms.

Normalization element: The enhanced minutiae need to be normalized to produce more standardized data that is independent to the type of sensing element used.

Template generation element: Normalized data produced can be used to extract the template information. This element forms the core of the application and it depends on the biometric modality used. As the complexity increases, the capabilities of the processor must also increase.

Matching element: The matching element is responsible for the authentication process. The matching process can be intensive for an identification application (1:N) or rather simple for a verification application (1:1).

Storage element: During the enrollment process, the template generated will be sent to storage. Due to increased security requirements, it is often critical to encrypt the template before storage. This encryption process is performed by the storage element. Additionally, this element is also responsible to decrypt the templates before the matching element performs the authentication process.

The keystone of the biometric system

From the previous two sections, we can clearly see the importance of the processing elements to the biometric system. The key attributes that can help to evaluate the processing elements are:

1. Speed
2. Flexibility
3. Power usage
4. Scalability

Speed

As different modalities have different computation requirements, the processing power of the systems varies. Irrespective of the biometric system and their computation intensity, the user expects these systems to have a very fast response time. The fast response time relates directly to the computation

requirement of the system which correlates to the clock speed of the processing element.

Flexibility

As many biometric system manufacturers are now offering systems with multiple modalities, the processing elements of these systems need to be flexible. This means that not only the processing elements should be fast enough and able to handle the processing requirements for multiple modalities, but they must also be compatible with multiple connectivity interfaces to accommodate different biometric sensors.

Power usage

As the mobile biometric systems continue to gain traction, power-efficient processor elements that can perform more computationally with a smaller power footprint are becoming essential for biometric systems.

Scalability

The security requirements for the applications targeted by the biometric systems have increased multifold in the last few years. In order to provide robust security capabilities, most of the biometric system manufacturers are integrating multiple biometric technologies. This means the processing elements should be capable to execute multiple algorithms on the fly.

Given the requirements of speed, flexibility, low power and scalability, embedded processors are gaining a lot of interest among the biometric system manufacturers. In particular, the portfolio of embedded processors from Texas Instruments (TI) is proving to be a very good fit for satisfying the processing requirements of biometrics systems.

The rest of this paper discusses the key features of TI's high-performance ARM® and DSP processors that make them an ideal processing solution for biometric systems.

TI's high-performance ARM and DSP processors for biometrics systems

TI's ARM and DSP portfolio offers a wide variety of processors with a rich set of attributes that make them ideal for biometric systems. The key attributes that align with the processing requirements discussed above are:

1. Multiple connectivity options to sensing elements (Flexibility)
2. Multiple connectivity options to the interface elements (Flexibility)
3. High processing performance (Speed)
4. Easy access to the storage elements (Speed)
5. Ability to secure the templates (Security)
6. Scalable software infrastructure to enable easy migration from one authentication process to another (Scalability)
7. High performance per Watt (Power usage)

The processors in TI's portfolio that can fulfill these basic set of requirements are shown in Figure 7 on the following page. (Note: This figure only shows TI products that are publicly known and available at the time of this paper's publishing. Please contact your local TI representative or visit **www.ti.com** to learn about all of TI's processors available for the biometrics space.)

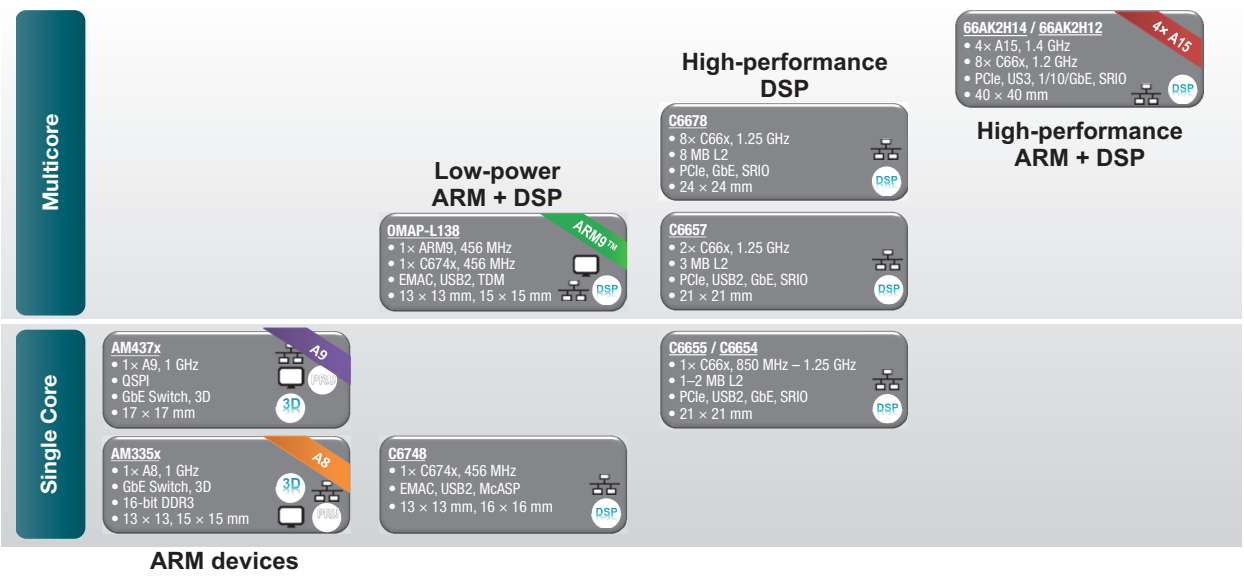

Figure 7: Texas Instruments' processing solutions for biometric systems

The processors shown on the left-half of Figure 7 are ideal for biometrics terminal or client stations. The important devices to consider here are the Sitara™ **AM335x** family of devices based on the **ARM Cortex®-A8**, the Sitara **AM437x** family of devices based on the **ARM Cortex-A9**, the low-power **C6748 DSP** and the low-power DSP + ARM Cortex-A9 device the **OMAP-L138** processor.

The processors shown towards the top are ideal for the server stations. Important devices here are the **C6678** multicore DSP and the **66AK2H12** and **66AK2H14** SoCs, which are high-performance multicore DSP + multicore ARM Cortex-A15 devices.

More information on each of these devices, including data sheets and block diagrams, is available at **www.ti.com**. But irrespective of terminal or server applications, it is important to explain how these processors satisfy the basic requirements.

Multiple connectivity options to sensing elements: Each of these processors has multiple interfaces like SPI, I^2C and USB to connect to a wide variety of sensing elements. Additionally the Sitara AM437x devices also have a video input port and the 66AK2xx devices have high-bandwidth network interfaces that can help bring in data from multiple terminals.

Multiple connectivity options to the interface elements: Each of these processors provides multiple options to display the results or share the data through a network. While all of them have multiple USB interfaces that can be used to connect to output devices like display panels, most of them have a built-in display subsystem to allow easy connectivity to display systems. All of TI's processors also provide network interfaces to connect and share the data across multiple systems.

Sufficient processing power: The selection of the processing element depends on the biometric modality used in the biometric systems and there is quite a range of processing required depending on the modality. For example, fingerprint systems can operate efficiently on a 300-MHz version of a Sitara AM335x processor. While the iris system requires

a 1-GHz DSP like that on a C6748 DSP to handle the image-processing algorithms efficiently and quickly. The processing power is also determined by the mode of operation. In an identification mode, a stand-alone system might require matching the capture template to a significantly large database. In these cases, a 1-GHz version of a Sitara AM335x processor or a C6748 DSP will be ideal to quickly deliver an accurate result. In the case of a client-server system, the identification process will take a long time to compare with millions of stored templates. In these scenarios a high-performance hybrid processor like the 66AK2H12 SoC will be able to divide the database into multiple sections and perform the comparisons in parallel in individual DSP cores.

Easy access to the storage elements: TI's processors also have built-in volatile memory with error correcting code (ECC) to guarantee data integrity. These processors also provide interfaces like NAND, NOR, SATA, etc., to connect to external memory devices.

Ability to secure the templates: As data needs to be sent to the external storage device or shared through the network, it is critical for the processors to have encryption features to provide secure storage and transfer of data to and from the processor. TI's processors have crypto accelerator units that can encrypt data using algorithms like AES, SHA/ MD5, DES and 3DES. In addition, the TI processors can also be operated in a secure boot mode where the system is completely secured even from the device start to protect the consumer's intellectual property.

Scalable software infrastructure to enable easy migration from one authentication process to another: In order to help the user to implement multiple authentication processes, it is important to have strong software collateral that not only provides easy access to resources within a device, but also provides flexibility to move from one device to another. TI's software development kit (SDK) provides highly modular software drivers that are light weight and easy to integrate with the user's applications. In addition, the SDK also provides a simple-to-use open-source framework model for debug. The SDKs for different processors are also aligned to make the transition from one device to another easy. The software provides a strong suite of image- and signal-processing libraries that can help the users to efficiently build comparison algorithms. In addition, it also provides various standard multicore development suites that can be used to port existing multicore-based biometric systems on to the high-performance processors like 66AK2Hx processors.

High performance per Watt: A key strength of TI's portfolio of embedded processors is the ability to deliver high processing performance at low power levels. The OMAP-L138 processor and C6674x DSP product lines have power consumption that ranges from 8 mW in standby mode to 400 mW total power, making them ideal for the smallest of biometric systems. At the higher end, TI's C667x and 66AK2Hx devices are powered by TI's C66x DSP core, the industry's fastest floating- and fixed-point DSP core which delivers up to 16 GFLOPS and 32 GMACS while consuming only10 mW/MHz.

Conclusion

The biometric authentication market is growing rapidly with the increased need for more processing and portability. There are many different types of biometrics that can be used for authentication and a flexible system is needed that can handle multiple of these biometric modalities. To create a unified platform of biometric systems, a scalable line of power-efficient, flexible processors with multiple connectivity options is required. TI's broad processing portfolio of ARM and DSP-based processors is an ideal fit for biometrics with solutions spanning from low to high end.

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