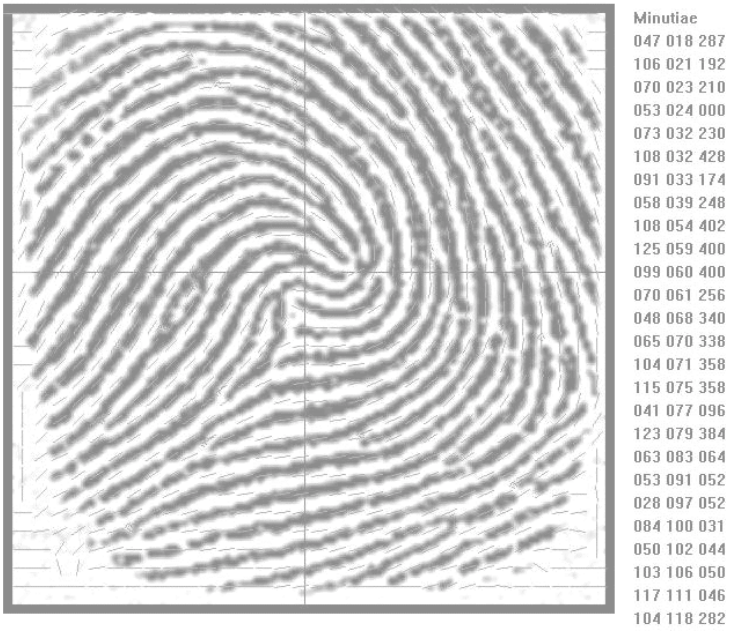
AuthenTec, Inc.
Personal Security for the Real World™

Design Guidelines
For the AuthenTec Sensors



Integrator's Guide

2141 Rev 2.0
09 Feb 01

AuthenTec, Inc.
Post Office Box 2719
Melbourne, Florida 32902-2719
321- 308-1300
www.authentec.com

AuthenTec welcomes your input. We try to make our publications useful, interesting, and informative, and we hope you will take the time to help us improve them. Please send any comments or suggestions by mail or e-mail.

Disclaimer of Warranty

THE SOFTWARE, INCLUDING INSTRUCTIONS FOR ITS USE, IS PROVIDED "AS IS" WITHOUT WARRANTY. AUTHENTEC FURTHER DISCLAIMS ALL IMPLIED WARRANTIES INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR OF FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK ARISING OUT OF THE USE OR PERFORMANCE OF THE SOFTWARE AND DOCUMENTATION REMAINS WITH YOU. IN NO EVENT SHALL AUTHENTEC, ITS AUTHORS, OR ANYONE ELSE INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THE SOFTWARE BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGE FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE OR DOCUMENTATION, EVEN IF AUTHENTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

U.S. Government Restricted Rights

The software and documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraph (c)(1) and (2) of the Commercial Computer Software – Restricted Rights 48 CFR 52.227-19, as applicable. Manufacturer is AuthenTec, Inc., Melbourne, Florida 32901-2719. This Agreement is governed by the laws of the State of Florida.

AuthenTec, Inc.
Post Office Box 2719
Melbourne, Florida 32902-2719
321-308-1300
www.authentec.com
apps@authentec.com

Design Guidelines for the AuthenTec Sensors
2141 Rev 2.0 (09-Feb 01)

Table of Contents

Introduction

This Integrator's Guide offers circuit, PCB, and integration design information that will help in passing standards compliance testing and assure proper performance of AuthenTec sensors. Knowing these design tips when implementing a specific board design can minimize the effort required passing the Electromagnetic Compatibility (EMC) specifications for FCC, CE, VCCI and other such standards. These techniques can reduce or eliminate design iterations needed to bring a product to market.

AuthenTec silicon chip fingerprint sensors have been proven to have superior performance in real world environments when compared with other known fingerprint sensors. Sophisticated chip design techniques have been used to eliminate the effects of external RF signals and other phenomena that might disturb the operation of a sensor. This includes immunity to Electrostatic Discharge (ESD) events.

It is important to note that improper circuit, board layout and module integration surrounding the sensor can affect the proper operation and performance of the sensor. Any given PCB design can affect how well the sensor and its associated circuitry will meet relevant standards. These standards include specifications on RF emissions and immunity to RF and ESD. Careful attention must be paid to the design of the PCB and circuits that interface with the sensor.

Extended Finger-Ring Guidelines

The AuthenTec sensors have been produced with a silver or white finger-ring on the top of the sensor. The finger-ring serves two functions for fingerprint processing. One is to detect the finger and the second is to excite the finger during fingerprint image, retrieval, and optimization. Although there are two functions, the sensor's finger-ring is critical to the proper operation of the AuthenTec system.

The finger-ring can be extended, when appropriate, improving the results for acquisition and recognition of fingerprints. This can often be done by adding a finger-ring extender around the sensor as part of the enclosure. When certain finger conditions are commonplace, i.e. dry fingers, the enhancement of the finger-ring can provide clear and substantial benefits for enrollment percentage and user verification.

The guidelines for designing an "extended finger-ring" are as follows.

- Include the immediate surfaces around the sensor that the finger may touch.
- Material should be electrically conductive, non-corroding and electrically isolated from other conductive surfaces or support structures. An example material to use would be any appropriate base metal (brass or copper) either plated with nickel, or with a gold and alloy mix to aesthetically match the array color. The latter is preferred in the context of human factors, since the overall effect will be to make it look like the whole area (extended finger-ring, sensor finger-ring, and sensor array) is part of the same sensor.

A means for connecting the finger-ring extender to the PCB is required. Connection to the via on the PCB can be accomplished by a 24 gauge stranded wire. (Note: This can be seen in some AuthenTec reference designs as a test point (TP) at the finger-ring node.) The finger-ring node is illustrated in Figure 2.0.

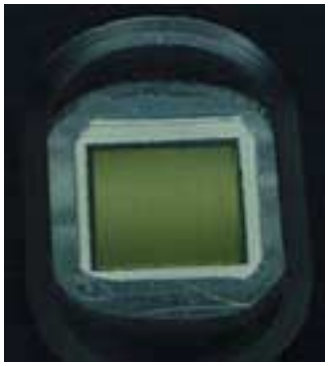
The primary electrical and mechanical property requirements for the extended finger ring are:

- Resistivity less than 0.4 ohm.
- Limit the capacitance presented by the extended finger-ring to acceptable levels where sensor performance is not hindered.
- Life of the metal to solvents and corrosives such as salt from fingers and solvents should be consistent with the sensor.
- Use a material that will remain untarnished and be aesthetically pleasing.
- Solderability of the tab that will connect to the wire which will connect to the PCB - this tab should be where a 24 gauge stranded (or solid if deemed acceptable with handling requirements) insulated wire will be soldered.
- Dimensions of the finger metal should not be greater than a 1.2" by 1.2" plate.

The figures below illustrate two approaches to implementing a finger-ring extender. Figure 1.0 illustrates the standard AuthenTec Technical Kit Evaluation (TEK) module integrated with an extended finger-ring. Figure 2.0 illustrates a prototype of a field installation that was retrofitted with a finger-ring extender.

Figure 1.0 – Collar Based Extended Finger-Ring

Figure 2.0 – Plate Based Finger-Ring Extended



ESD Immunity

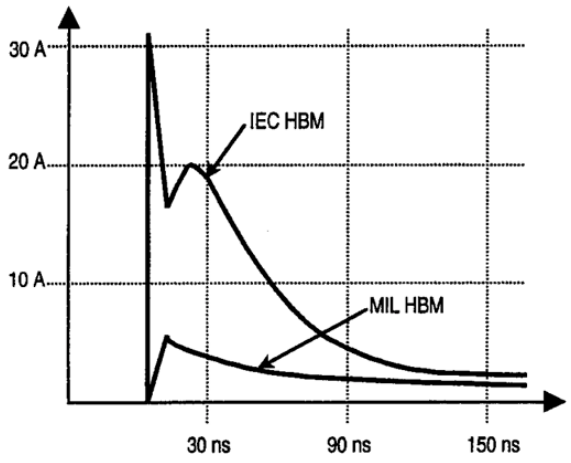
The AuthenTec sensor and surrounding circuitry must provide immunity to ESD events generated by approaching fingers. Unlike conventional integrated circuits that can control ESD events entering the chip through one of the sensor's pins, the silicon chip surface of the AuthenTec sensor must compensate for the finger-to-silicon contact. In standard configurations, the ESD discharge path will be through the finger-ring on the surface of the sensor package. In this configuration some air discharges may enter the chip through random points on the surface of the sensor array. Many of the protection measures for sensor array discharges already exist in the silicon. Additional measures for diverting ESD discharges around the silicon are discussed below.

Comparison of Field Use Criteria versus Test Criteria

The IEC 61000-4-2 Standard calls for resistance and capacitance values in the ESD source that emulate the " human body holding a metallic object such as a key or tool." This " metal discharge situation is… severe to represent all human discharges in the field."

The discharges that the AuthenTec sensors are subjected to in actual practice are far less severe than those stated in the IEC 61000-4-2 Standard. The Standard states, ***If a "metallic object such as a key or tool" were to come in physical contact with the sensor array, severe physical damage may result, rendering the test invalid.*** Normal operation of the device is consistent with other standards that use the Human Body Model (HBM) as well as those that use the U.S. Mil-Spec HBM. In Figure 3.0, the ESD currents generated in the IEC test scenario are far higher than the system is exposed to in normal operation.

Figure 3.0 - IEC 61000-4-2 Human Body Model vs. U.S. Mil-Spec HBM.



ESD Program Background

Since inception, AuthenTec has recognized that silicon-based fingerprint sensor designs must compensate for the ESD in their normal operating environment. AuthenTec's has included techniques and features within its family of sensors to accommodate for exposure to ESD. AuthenTec sensors are protected from ESD with a multidisciplinary approach at all levels of the product from sensor to system. The sensor's internal circuits are designed to tolerate ESD; the surrounding board-level circuitry in the Reference Design provides a mechanism for ESD suppression and event recovery; and the AuthenTec system sensor is packaged so that ESD discharge directly into sensitive circuitry is avoided.

To thoroughly test the sensor's ESD protection measures, AuthenTec has an ongoing program of ESD test and mitigation. Over three hundred sensors have been subjected to both field and controlled conditions tests. In addition, AuthenTec sensors have been used in numerous field trials during the winter in Chicago, Denver, and Washington, D.C. as well as other cities around the world. There have been no failures attributed to ESD. In addition to the continuous ESD performance improvement, the system and its associated Reference Design have been tested in the AuthenTec laboratory and in several certified facilities under standardized conditions to ensure that the system will perform to established criteria under realistic operating conditions. AuthenTec's sensor ESD testing is rigorous, repeatable, comprehensive, and ongoing.

ESD Immunity Strategy

The sensor ESD immunity strategy is based on the premise that the sensor system must meet external interface and host device operating requirements. The sensor system solves this ESD problem from multiple levels of the product design cycle:

- Internal circuits are designed to tolerate ESD.
- Sensor is packaged so that an ESD directly into sensitive circuitry is avoided.
- Surrounding board-level circuitry in the reference design provides a mechanism for ESD suppression and event recovery that is fully transparent to the user.
- Housing can support early discharge of approaching fingers and reduce ESD generated EMI.
- Software of the controlling system is designed to control the power to portions of the sensor to provide ESD immunity.

Sensor Internal Design

The sensors internal design uses ESD tolerant I/O cells and transient suppression device structures on critical power and I/O paths. Two steps provide safe ESD discharge paths: the primary discharge path is by the finger-ring outside of the sensor and the secondary is by guard rings in the event of ESD discharges into the array.

Sensor Packaging

A passivation layer on the sensor's surface protects the pixels. The finger-ring drive acts as the primary ESD discharge. This is the first part of the sensor that a finger will come in contact with during normal operation. When connected to the correct Transient Voltage Suppressors (TVS) and routed as recommended in the Reference Design, the ESD air discharges of +/-8kV will not affect normal operation.

Board Design

The surrounding circuitry in the Reference Design provides specific ESD mitigation features. The layout of the board must control the parasitic capacitance and inductance on nodes and traces to specific components. The recommended component placement reduces ESD impact, as does the careful layout of traces and recommended trace lengths. A TVS is provided to pull ESD currents away from the sensor and nearby circuitry. The Reference Design also includes a current limiter device. The purpose of this device is to provide fail-safe design in the event that software or other higher-level systems fail to recover from an ESD event.

Housing Design

The sensor housing design, as implemented in the AuthenTec TEKs, further mitigates the ESD. The sensor is positioned in the housing to increase the probability of discharging ESD before a finger has contact with the sensor. This is achieved by ensuring that a finger makes adequate contact with the sensor finger-ring. (The addition of a conductive finger guide will further mitigate ESD discharge problems. Making portions of the housing surrounding the sensor conductive may also provide additional protection.)

In addition, the USB-based AuthenTec Reference Design housing uses a ferrite EMI tubular bead on a cable that connects the sensor housing to a computer. This split-ferrite tubular cable bead has an impedance of at least 131Ω at 100MHz. The bead is located nearest the pod and is the most critical component in the housing design. ***There is an extremely high probability that a host computer will be upset from ESD generated EMI and fail without the ferrite bead component specified in the Reference Design.***

System Software

The AuthenTec software controls all higher-level functions of the sensor system and also supports additional ESD immunity. Initially the software only turns on the portion of the sensor that is required to detect a finger. After finger detection, the columns and rows of the sensor are turned on and scanned in sequence for fingerprint data.

One of the most common failure modes during ESD testing is disruption of the host due to ESD-induced ElectroMagnetic Interference (EMI). This disturbance is usually due to the inability of the host to pass the test or the inability of the operating system to resolve the problem.

In the case of the host, the test procedure recommends testing the host system to characterize problems prior to testing the sensor Unit Under Test (UUT). In the case of the operating system, when the USB sensor system is used in conjunction with the Microsoft Windows 98 Operating System, the Reference Design recommends the use of Windows 98 2nd edition or later. This version of the OS has implemented features that provide more effective USB support and is recommended for all USB sensor system customers. These features have also been incorporated in subsequent Microsoft Operating System releases, such as Windows Millennium.

Brief Review of the IEC 61000-4-2 Standard

The IEC 61000-4-2 Standard establishes specific performance criteria for the conduct of ESD testing. The Standard specifies the discharge types (Air or Contact), amplitudes, and polarities that the UUT is subjected to during testing. The data is categorized in four "Levels" which are outlined in Table 1.0.

Table 1.0 - IEC 61000-4-2 Test Levels

Discharge Type	Air Discharge	Air Discharge	Contact Discharge	Contact Discharge
Level 1	+ 2kV	- 2kV	+ 2kV	- 2kV
Level 2	+ 4kV	- 4kV	+ 4kV	- 4kV
Level 3	+ 8kV	- 8kV	+6kV	- 6kV
Level 4	+ 15kV	- 15kV	+8kV	- 8kV

The EN50082-1:1992 Standard also established *Performance Criteria* of A, B, or C to characterize the UUT performance after the application of individual discharges during a test. The latest amendment of EN 61000-4-2:1995, Amendment 1, similarly classifies these three criteria to four levels. They are:

1. Normal performance within the specification limits.
2. Temporary degradation or loss of function or performance that is self-recoverable.
3. Temporary degradation or loss of function or performance that requires operator intervention or system reset.
4. Degradation or loss of function that is not recoverable due to damage of equipment (components), software, or loss of data.

In testing the sensor, AuthenTec has passed Level 3 (± 8kV applied by air discharge) and Performance Criteria 2, "Temporary degradation or loss of function or performance which is self-recoverable." This criterion is sufficient to achieve a CE compliance certification and demonstrate the ESD resilience necessary for the product to operate in its intended environment.

To qualify any design, it should be tested using the applicable ESD standard. The IEC 61000-4-2 ESD Discharge Immunity Standard is recommended to test end-unit IT systems that are undergoing maintenance or normal operation. These units are subjected to ESD discharges to their cases through metallic objects such as screwdrivers. These tests are more stringent than the standard IC industry component-level tests to which Integrated Circuits are tested. ***As mentioned earlier, the application of metallic objects to the sensor array surface will mechanically damage the product. Any further testing would be invalid.*** While the most

stringent component level ESD tests do not exceed ±4kV, the Level 4 (most stringent) IEC 61000-4-2 air discharge is ±15kV. Level 3 (± 8kV Air Discharge) is sufficient to qualify devices for CE marking. Meeting Level 3 of the IEC 61000-4-2 Standard will ensure that the sensor will withstand higher levels of ESD exposure in a normal daily use environment encountered by the device in an end product.

The IEC 61000 Standard calls for resistance (330 Ω) and capacitance (150 pf) values in the ESD source that emulate the "human body holding a metallic object such as a key or tool." The use of this RC network exposes the UUT to 30 amperes of current at 8kV contact. (Industry standards such as ESD STM5.1-1998 or EIA/JESD22-A114-A tests use the standard HBM resistance of 1500 Ω and 150 pf capacitance values in the ESD source RC network. These values typify the levels of exposure expected in a finger touch environments that is normal for sensor system operation. The IEC 61000-4-2 Standard, however, does not allow for any deviation in these values.)

Circuit and Layout Design for ESD Immunity

The AuthenTec circuit designs provide compliance to IEC/EN 1000/61000-4-2 level 3, Criteria 2 at a minimum, which will allow CE marking of products. The circuitry is applicable to both 3.3 VDC and 5.0 VDC applications.

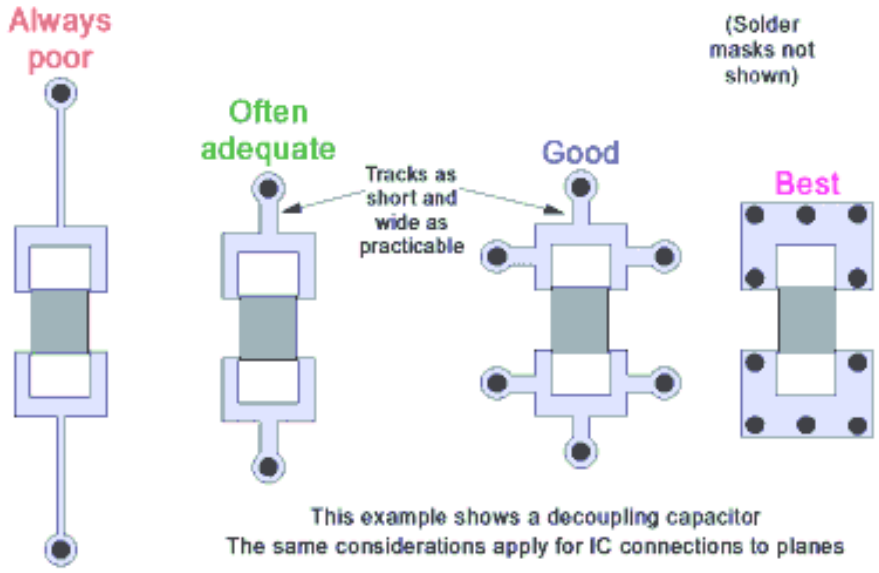
Finger-Ring ESD Suppression

This section provides guidelines on implementing immunity to ESD for the finger-ring on the AuthenTec sensor.

Discharges to Finger-Ring

Circuitry must be carefully routed to handle a 15KV discharge event. A TVS should be directly connected to the finger-ring and routing lines should be as short as possible. This component and its connections should be given the highest priority during routing. In order to insure success, the distance from the finger-ring pin to the TVS pin should be no greater than 5mm or 0.2 inches. There should be no vias between the connection to the finger-ring and the TVS and the trace should be wider to reduce inductance. The parasitic inductance of the trace is the primary concern. During the ESD event a pulse of 30 amps with a 1ns rise time (per the IEC standard) will be on this node. The ground path return for the TVS should have at least two vias to the ground plane to reduce inductance. If the schematic provides a voltage rail connection, two vias should be used to connect to the voltage plane. See Figure 4.0 below, and reference #2.

Figure 4.0 – Low Inductance Connection Techniques



(Note: AuthenTec-authorized components for this application are the SEMTECH SRDA05 and SR05 families. Other components can be evaluated upon request.) The TVS clamps the ESD spike and absorbs the energy from the event. The TVS responds to the fast spike and clamps the voltage under 30 volts if the complete circuit, including ground path, is laid out properly on the PCB. For the TVS absorbing the ESD discharge to the finger-ring, the power rail of the TVS should NOT be connected. The loading effect of the TVS should be less than 15pF. Additional capacitive loading will adversely affect the sensitivity of the sensor's finger detection circuit.

The Printed Wiring Board (PWB) construction and components will support suppression of ESD events that enter via the finger-ring and will minimize transients from propagating into connected equipment or the sensor itself. The finger-ring on the sensor surface is not electrically connected to the rest of the sensor electronics by anything other than the circuitry described. The remaining circuitry discussed below acts to mitigate the ESD pulse on this node from entering the AuthenTec sensor finger-ring drive pin.

Finger Ring Drive (FDRV) Circuit ESD Suppression

This section provides guidelines on implementing immunity to the ESD for the FDRV node signal on the sensor.

This circuit is a series of components that will keep the transient resulting from an ESD event below damaging levels. The circuitry illustrated in Figure 5.0 acts to prevent the ESD from entering the AuthenTec sensor FDRV Pin 59 on the sensor, and pin 106 on the EntréPad™ AES4000 sensor

Figure 5.0 - Finger ring ESD Immunity and FDRV ESD Suppression Circuitry

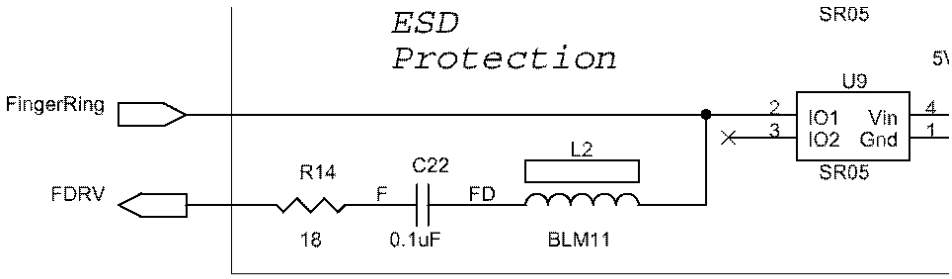
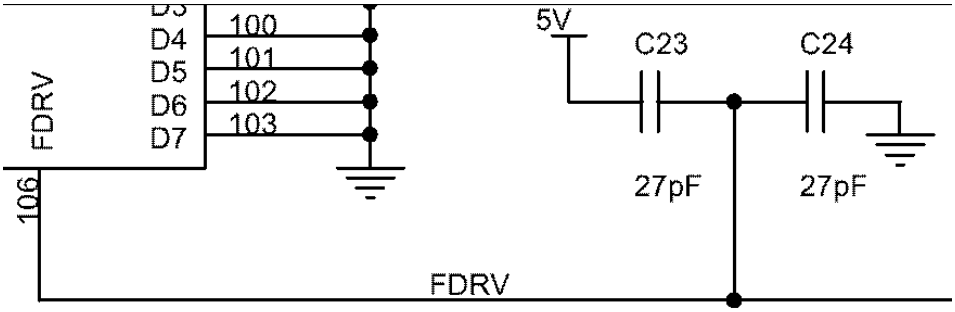


Figure 6.0 - FDRV ESD Suppression Circuitry



The L2, C22, R14, C23, and C24 comprise the ESD suppression circuitry. This series of connections must be routed at least 6mm, or 0.25 inches, away from the finger-ring trace and the pin of the TVS. These traces need to be spaced away from the ground plane by a minimum of the width of the trace on both sides of the traces.

The inductor L2 functions to limit the incident wave and slow down the rise time of the ESD event. The unit is selected to provide high frequency attenuation at 100MHz and 1000MHz. Specifically, values of 1000 ohm @100MHz and a minimum of 100 ohm @ 1000MHz are requirements for this device. DC resistance of L2 is nominally 1 ohm. The placement of L2 should be such that L2 is segregated from the trace coming from the finger-ring. The opposite end of L2 should be placed at least 6mm, or 0.25 inches, from the trace that connects to the finger-ring and the TVS to prevent flashover. The nominal signal that is on this circuit is 1MHz; at this frequency the effect of L2 on the normal circuit operation is negligible.

The capacitor C22 acts to AC couple the signal coming from the FDRV to the finger-ring. This capacitor is needed for normal circuit operation and is not specifically for ESD suppression. The placement of the capacitor should be in line with L2 and R14. Trace lengths should be minimized.

The resistor R14 acts to limit the current and EMI coupled spikes. The value of R14 should not be too high, as finger detection sensitivity will be reduced. The value selected for this resistor can be highly influential in passing the ESD immunity levels required. AuthenTec reference designs presently use 18 ohm for the value of R14. The composition of the resistor should be carbon technology.

Two capacitors, C23 and C24, as shown in Figure 6.0, support improved ESD immunity for the FDRV pin. A value of 27pF on each capacitor provides the recommended capacitance for the finger-detect auto-calibration, yet acts to slow down the rise of the transient resulting from the ESD event by the LPF (low pass filter) made up of the capacitors and R14. Low Equivalent Series Resistance (ESR) capacitors should be used. Low inductance plane connections are required for these capacitors, as shown in Figure 4.0.

Controlled parasitic capacitance routing is required on the FDRV to finger-ring series of connections. Measuring a bare PWB between the FDRV node and ground while shorts are in installed in place of the series components can test this. A value of 15pF has been allocated to board parasitic capacitance. The measured parasitic capacitance should not be greater than this value. For extended finger-ring configurations this should include the connection and the extended finger-ring.

Power Rail ESD Immunity

The power rails should also have connections to a TVS. The power pin of the TVS should be connected to the power plane using a low inductance connection as illustrated in Figure 6.0. This should include the three rails that are normally seen in AuthenTec Reference Designs: 1) power entry rails, 2) Digital Power rails, and 3) Array power rails.

Sensor Array ESD Immunity

These techniques are used to protect the sensor array, which is exposed to a user's finger, from air discharge ESD events. *Contact discharge ESD testing should never be used on the sensor array surface, as this will invariably cause severe mechanical damage regardless of whether the ESD gun is actually discharged.* For applications that require a heartier sensor, contact the AuthenTec or your sales representative.

Current Sense and Cutoff Switch

The current limiter allows a programmable threshold and provides a fail-safe safety function to limit current into the sensor so that it will not heat up beyond a preset limit. The set point resistor sets the current limit for the circuit and should have a 1% tolerance. The formula for the resistance is 1380/Ilimit. Therefore, 5.5K will establish a current limit of 250mA and 4.7K will be approximately 300mA. This current is not the operating current; it is a safety set point. The Reference Design for each sensor will have the specific setting for this protection.

Array Power Switch

The array power Field Effect Transistor (FET) switch provides additional ESD protection by electrically isolating the sensor array from the power supply and allowing the array to be turned off. When an ESD-charged finger is placed on the sensor, the array is powered down, thus supporting ESD immunity. This will allow the ESD event to discharge to the TVS devices and ground, instead of other paths.

ESD Induced EMI

The EMI that emanates from an ESD event can be, and often is, disruptive to nearby electronics. Adequate measures must be taken in the design to provide immunity to this phenomenon. For flat cable and round cable connections to the modules that contain an AuthenTec sensor, this can typically be addressed by filtering the conducted EMI on the cables with ferrite cable beads/clamps. Often, as seen in the industry, these beads or clamps are molded onto the cable.

An impedance of 130 ohm at 100MHz has proven adequate to support CE compliance with a 2-meter USB cable configuration. For embedded applications, where a "ribbon" cable is used, a flat ferrite cable clamp is recommended with the same impedance characteristics as a minimum.

For embedded applications where the sensor resides on the same board as the remaining electronics, the isolation must be accomplished by traditional "board-level EMI isolation" techniques.

EMI Compliance Design Techniques

For additional assists and supports when designing with AuthenTec sensors, the following techniques have been included. These guidelines specifically address EN55022:1998/CISPR 22:1997. Their use will assist in certifying designs to IEC61000-4-3, RF Immunity.

Crystals

When crystals are used in a design, the goal is to minimize the emanations that come from the crystal circuitry. This is important as the AuthenTec sensor uses a crystal or is fed an external clock.

In order to reduce EMI, a common ground plane can be used for the entire board. However, it is also possible to use a continuous localized ground plane for the crystal/clock generator circuit on the component (top) layer of the board. This localized plane can then be connected to the board ground by means of the pin connections of the crystal/clock generator. Placing a localized ground plane under the crystal/clock generator provides an efficient path for RF currents to ground.

All clock traces must be hand routed before any other signal. The clock traces must not intersect each other. Route clock traces on one layer as far as possible. If the clock signals cannot be routed on one layer, ensure that they stay one layer away from either the power or ground plane, as it will cause minimal changes in impedance.

Ensure that a solid ground plane is on the layer adjacent to the clock trace routing layer. Also ensure that there are no discontinuities created by vias.

Do not route other signals below the crystal/clock generator.

Do not use 90° angles when routing clock traces. If possible, use smoothly curving traces.

Use wider traces for VCC, GND and XTAL pins. Wider traces reduce trace inductance.

Board Edge and Ground Planes

The goal is to minimize the emanations that come from the circuitry on the board that includes the AuthenTec sensor. This can be done by routing ground plane over unused areas, around the board edge on both sides of the board and around traces and nodes of all other circuitry. Figure 8.0 illustrates one approach. Notice that there are ground-to-ground vias spaced at regular intervals, approximately 0.2” –0.4”. This will make the ground plane appear as a low uniform impedance when unwanted external and internal signals act upon it.

USB Applications

If the design uses USB to connect a sensor to an application, ESD suppression should also be used on the USB connections. For details, see the USB circuit schematics in the AuthenTec USB based Reference Design Kits (RDK) for the applicable sensor.

Prevention measures, similar to finger-ring suppression, should be followed for the D+ and D- lines. Refer to "*Protecting USB Ports from ESD Damage*" noted in the Reference section of this Guide for further information.

USB Signal Routing

The D+ and D- lines should be routed closely to each other and on the same side of the board wherever possible. Do not separate these lines by more than 0.05 inch.

General PWB and Circuit Guidelines

This section provides general guidelines and best practices for PCB layout. Refer to the Reference section of this Guide for additional information.

Miscellaneous Guidelines

- Avoid running critical signal traces near PCB edges.
- Fill unused portions of the PCB with ground plane.
- Keep the chassis ground trace length-to-width ratio <5:1 to minimize inductance.
- Protect all unprotected-external connections with TVS diodes.

Power Decoupling and Signal Lines

Bypass capacitors should be placed with minimal circuit runs and preferably no vias between power (both analog and digital) and the ground pins at each side of the sensor. Low ESR capacitors should be used. Low inductance connections to ground and power planes should be used as shown in Figure 4.0. Capacitors should be located on each side of the chip where power pins are used.

Power Connections

Analog ground should be connected to the Digital ground, and they should both be the same ground plane. The A/D converter on the chip is not isolated from the power pins.

Signal Connections

All unused pins should be left open.

References

1. *Design Techniques for EMC, Part5: PCB Design and Layout*, Eur Ing Keith Armstrong, C. Eng MIEE MIEEE, as published via the EMC Journal online, http://www.emc-journal.co.uk/archive1/991005.html

2. *Maxim Leads The Way in ESD Protection*, Maxim Engineering Journal, Volume 40, Pages 7-10

3. *Protecting USB Ports from ESD Damage,* SI96-18, Semtech Corporation, http://www.semtech.com

4. SR05 Data sheet, March 18, 1999, Semtech Corporation, http://www.semtech.com

5. *Surging Ideas TVS Diode Application Note, PCB Design Guidelines for ESD Suppression,* SI99-01, Revision 00- February 09, 1999

6. *USB Protection Topology, SI96-18*, Semtech Corporation, http://www.semtech.com

7. *TVS Power Derating vs. Temperature*, SI96-04, Semtech Corporation, http://www.semtech.com