AN96475

Design Considerations for Electrical Fast Transient Immunity of a CapSense® System

Authors: Shruti Hanumanthaiah, Srinivas NVNS
Associated Project: No
Associated Part Family: All PSoC
Related Application Notes: AN2155, AN78175, AN80994, AN64846, AN85951, AN89056

AN96475 describes best practices for improving the electrical fast transient (EFT) immunity of a CapSense system. This application note discusses failures that can occur in a CapSense system during an EFT test and recommends measures that can improve immunity. This application note focuses on considerations for a CapSense system. For a greater insight into EFT and how it affects microcontrollers in general, see AN80994.

Contents

1 Introduction....2
2 PSoC Resources....3
2.1 PSoC Creator....3
3 What Is EFT?....4
4 Failure Modes....5
4.1 Device Reset when CapSense Sensors Are Touched....6
4.2 Sensor False Trigger and Unresponsiveness to Touches....6
4.3 Communication Failure....8
5 Performance Criteria....8
6 Troubleshooting, Design Considerations, and Mitigation Techniques....8
6.1 Target Board Design Considerations....9
6.2 Firmware Techniques....15
7 Summary....18
8 References....19
Worldwide Sales and Design Support....21

Safety Notice



EFT testing involves hazardous voltages.

Electrical safety principles must be duly followed.

Consult a certified safety technician.

1 Introduction

This application note discusses the effects of electrical fast transients (EFT) in a CapSense system and recommends hardware and firmware techniques to mitigate them. It also explains a set of guidelines that a designer can use to build a CapSense system that is immune to such transients.

International standards related to EFT provide guidance to the product designer on the testing methodologies for compliance. The fast transient immunity requirements for electronic products are defined in IEC 61000-4-4 (for EFT) by the International Electrotechnical Commission (IEC).

The section, What Is EFT?, describes EFT in brief and refers to the application note AN80994 – Design Considerations for Electrical Fast Transient (EFT) Immunity. AN80994 describes best practices for improving the EFT immunity in embedded system designs.

Fast transients can have varied effects on CapSense systems including improper touch recognition and system reset; the next section, Failure Modes, talks about these effects.

CapSense based systems are used in harsh environments such as home appliances and industrial environments. Therefore, it is vital for the design engineer to start a regime of mitigation in parallel with the system design.

The Troubleshooting, Design Considerations, and Mitigation Techniques section presents tips on debugging and lists some possible methods to improve EFT immunity of a failing system. It also describes how a system design engineer can pre-empt EFT-related issues by considering certain design-time principles specifically for a CapSense system. This application note mainly focuses on considerations for a CapSense board design. It also provides firmware techniques that can be incorporated to improve a CapSense system's immunity. Design considerations for general embedded systems including some important design considerations at the system level and power supply are covered in the application note AN80994 – Design Considerations for Electrical Fast Transient (EFT) Immunity.

This application note assumes that you are familiar with PSoC and the PSoC Creator IDE. If you are new to PSoC, introductions can be found in:

- AN54181 - Getting Started with PSoC 3
- AN79953 - Getting Started with PSoC 4
- AN77759 - Getting Started with PSoC 5LP

If you are new to PSoC Creator, see the PSoC Creator home page.

This application note also assumes that you are familiar with CapSense concepts. If you are new to these concepts, see AN64846 - Getting Started with CapSense.

Finally, this application note assumes that you are familiar with basic PCB design techniques. If you are new to this, see:

- AN61290 - PSoC 3 and PSoC 5LP Hardware Design Considerations
- AN88619 - PSoC 4 Hardware Design Considerations

2 PSoC Resources

Cypress provides a wealth of data at www.cypress.com to help you to select the right PSoC device for your design, and quickly and effectively integrate the device into your design. For a comprehensive list of resources, see KBA86521, How to Design with PSoC 3, PSoC 4, and PSoC 5LP. The following is an abbreviated list for PSoC 4:

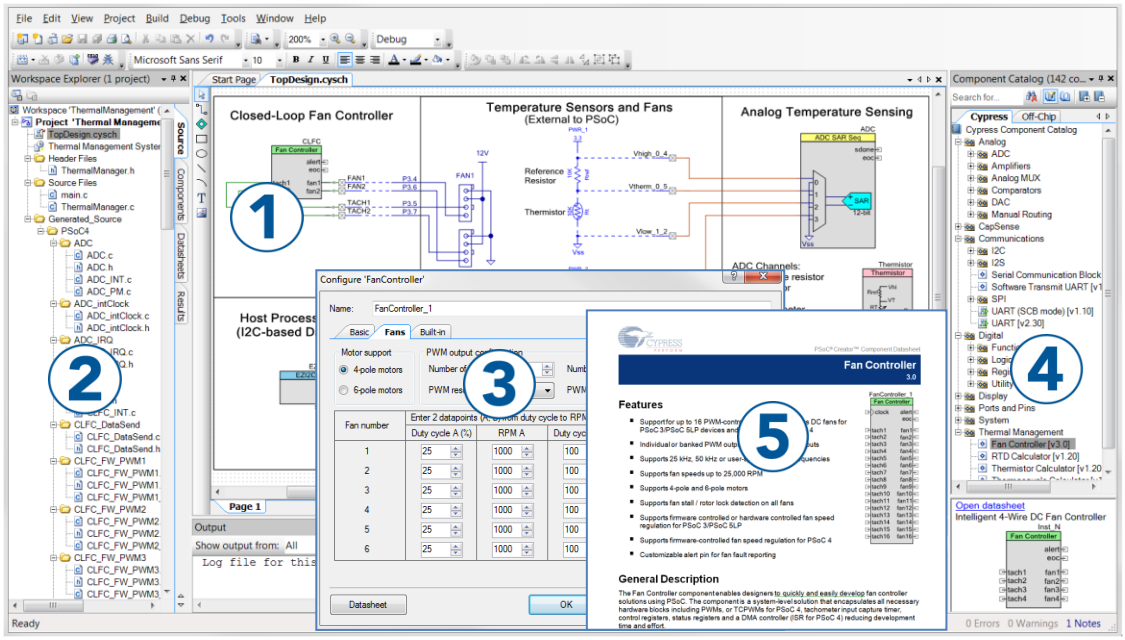
- **Overview:** PSoC Portfolio, PSoC Roadmap
- **Product Selectors:** PSoC 1, PSoC 3, PSoC 4, or PSoC 5LP. In addition, PSoC Creator includes a device selection tool.
- **Datasheets** describe and provide electrical specifications for the PSoC 4 device family
- **CapSense Design Guide:** Learn how to design capacitive touch-sensing applications with the PSoC 4 family of devices.
- **Application Notes and Code Examples** cover a broad range of topics, from basic to advanced level. Many of the application notes include code examples.
- **Technical Reference Manuals (TRM)** provide detailed descriptions of the architecture and registers in each PSoC 4 device family.
- **Development Kits:**
  - CY8CKIT-040, CY8CKIT-041, CY8CKIT-042, CY8CKIT-042-BLE, CY8CKIT-044, and CY8CKIT-046 PSoC 4 Kits are easy-to-use and inexpensive development platforms. These kits include connectors for Arduino™ compatible shields and Digilent® Pmod™ daughter cards.
  - CY8CKIT-049 is a very-low-cost prototyping platform for sampling PSoC 4 devices.
  - CY8CKIT-001 is a common development platform for all PSoC family devices.
- The MiniProg3 device provides an interface for flash programming and debug.

2.1 PSoC Creator

PSoC Creator is a free Windows-based Integrated Design Environment (IDE). It enables concurrent hardware and firmware design of systems based on PSoC 3, PSoC 4, and PSoC 5LP. See Figure 1 – with PSoC Creator, you can:

1. Drag and drop Components to build your hardware system design in the main design workspace
2. Co-design your application firmware with the PSoC hardware
3. Configure Components using configuration tools
4. Explore the library of 100+ Components
5. Review Component datasheets

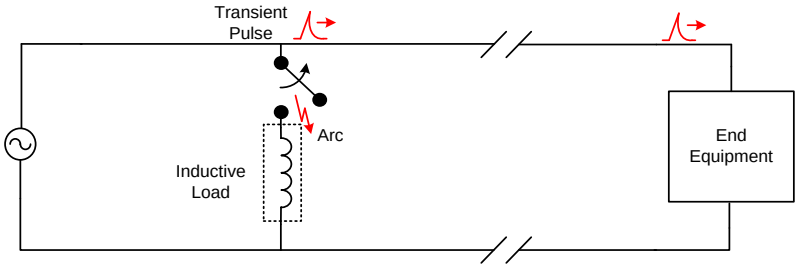
Figure 1. PSoC Creator Features



3 What Is EFT?

Inductive loads such as relays, switch contactors, or heavy-duty motors when de-energized produce bursts of narrow high-frequency transients on the power distribution system – these are called fast transients. Fast transients have a rise time/dwell time in the order of nanoseconds and can have amplitudes in kV. These fast transients can also be produced when the utility provider switches in or out the power factor correction equipment. A common cause of power line transients is the sparking that occurs whenever an AC power cord is plugged in, equipment is switched off, or circuit breakers are opened or closed. Figure 2 shows how transients are generated and coupled to end equipment over power lines.

Figure 2. Generation and Coupling of Transient Noise to End Equipment



The IEC 61000-4-4 specification defines the test voltage waveform that is intended to simulate the transients created by the switching of inductive loads on AC power lines. The specification also defines the requirements for immunity to repetitive fast transients and the necessary test methods for systems.

The EFT waveform, as defined by the IEC 61000-4-4 standard, is intended to be used by manufacturers to test the performance of equipment when subjected to fast transients. Equipment manufacturers that have designed a CapSense-based system use the IEC standard to test the performance of the device, CapSense sensors, and the system as a whole. See AN80994 for details on the test pulse waveform, its characteristics, test levels, and test procedure.

Primarily, the testing involves injecting EFT pulses into the equipment's AC power supply lines. The EFT waveform can also be injected into the signal and control lines, and power earth connections to simulate the coupling of transient noise onto these lines. The pulse waveform has a high amplitude (0.5 – 4 kV), short rise time, high repetition rate, and low energy content. IEC 61000-4-4 also defines four standard test levels and one special level based on the amplitude of the pulse waveform. The peak voltage increases as the test level increases. Table 1 summarizes the peak voltage of the pulse.

Table 1. IEC 61000-4-4 Test Levels

Level	Power Supply Terminal		I/O Signals/Data Terminals	
	Peak Voltage (kV)	Repetition Rate (kHz)	Peak Voltage (kV)	Repetition Rate (kHz)
1	0.5	5 or 100	0.25	5 or 100
2	1	5 or 100	0.5	5 or 100
3	2	5 or 100	1.0	5 or 100
4	4	5 or 100	2.0	5 or 100
X*	Special	Special	Special	Special

Note 1: Use of 5-kHz repetition rates is typical; however, 100 kHz is closer to a real world scenario.

Note 2: The terminals to be tested have to be determined by the manufacturer.

* "X" is a special level. This level must be specified in the equipment specification.

Although there are international standards that specify the requirements for the transient immunity performance with respect to a specific class of equipment, CapSense system manufacturers often define the requirements for their system. The manufacturers generally go for a level higher than that specified by the international standards for the specific class of equipment to ensure robustness of the system.

4 Failure Modes

Transient-induced noise conductively couples to the end equipment via the AC power cord, DC power, and signal/control lines. If proper filtering is not used in the equipment, the noise can propagate to different PCBs, including the board that constitutes the CapSense system.

As described in AN80994, transient-induced noise is both common-mode and differential-mode.

Transient-induced noise is likely to interfere with signals in a system. In a broad classification, the following blocks, pins, and signals are most influenced by transient-induced noise: power and ground signals, reset circuits, clock/oscillator signals, edge-sensitive triggers, high-frequency digital signals, analog signals, communication blocks such as I2C, SPI, UART, CPU, and flash/RAM.

When transient-induced noise affects one or more of these blocks, the following types of system failures can occur:

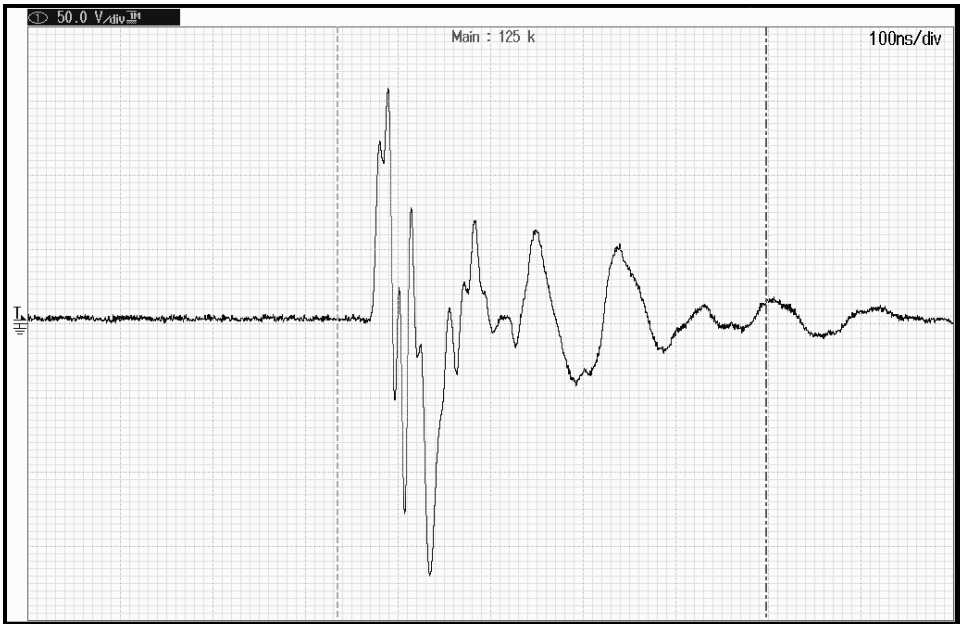
- Device reset
- Device latch-up. Latch-up may require a power cycle to resolve.
- Corruption of analog and digital signals
- Communication failure
- Memory corruption

Specifically in a CapSense system, the following types of failures can occur:

- Device reset when CapSense sensors are touched
- False triggering of CapSense sensors including sensors stuck in ON condition
- CapSense sensors not responding to touch

Figure 3 shows the waveform on the supply line measured at the output of an AC-DC converter without load when the EFT test signal is injected into the converter. As can be seen, the peak voltage is ~350 V. When there is load such as a controller circuit on the output of the AC-DC converter, the characteristics of the noise seen by the device might vary depending on the filters and decoupling network at the supply inputs of the controller.

Figure 3. Transient Noise Waveform on Supply Line Measured at the Output of an AC-DC Converter (Without Load)

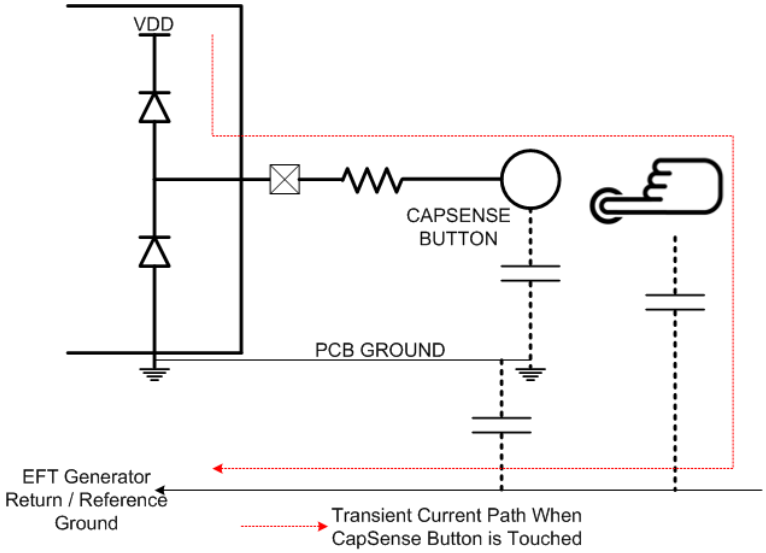


AN80994 covers the details of failures that occur in a general embedded system. The following subsections provide details of failures that can occur in a CapSense system.

4.1 Device Reset when CapSense Sensors Are Touched

When a user touches a sensor, and if the added finger capacitance is proportional (high enough) to the sensor capacitance, the touch would create a low-impedance return path for the transient current back to the EFT generator. The transient-induced noise triggers the ESD clamp circuits on the sensor I/O so that the effective supply voltage seen by the device dips, triggering a brown-out reset. Figure 4 shows the representation of the current path during EFT testing.

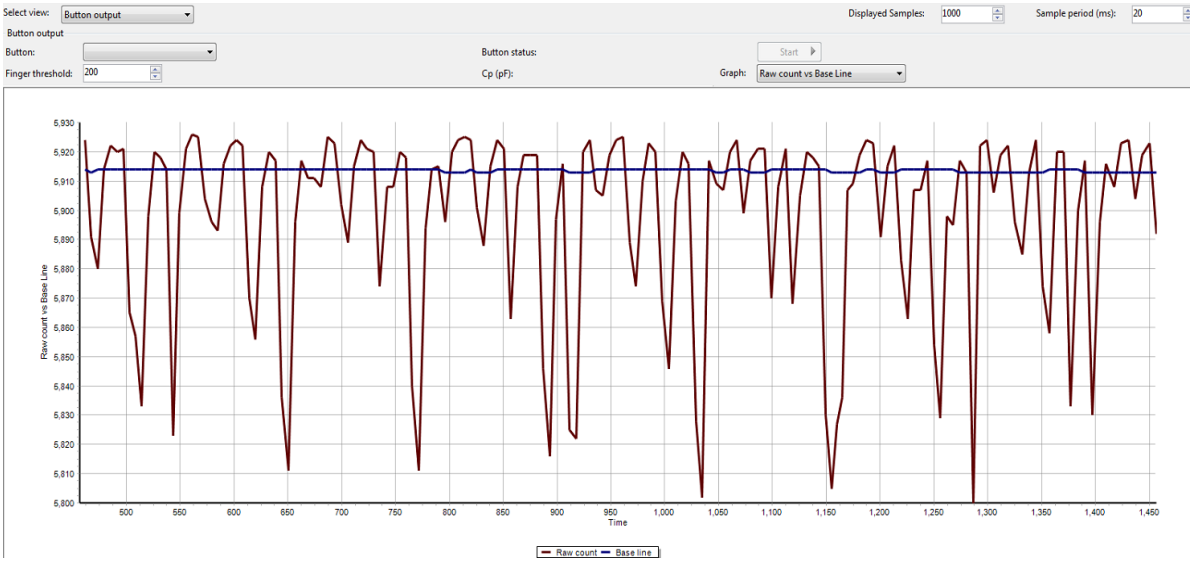
Figure 4. Transient Current Path when Sensor Is Touched During EFT Testing



4.2 Sensor False Trigger and Unresponsiveness to Touches

Transient-induced noise can cause noise in rawcounts such as positive or negative spikes or shift in rawcounts. The noise can cause sensors to false-trigger or not respond to valid touches. For example, positive spikes can cause sensor false-trigger, while negative spikes can cause sensor unresponsiveness to valid touches. Figure 5 is a graph showing the rawcounts of a sensor. The negative spikes in rawcounts may cause sensors not to respond to touches as the rise in rawcounts caused by finger touch may be compensated by the negative spikes. Therefore, the difference counts may not cross the finger threshold.

Figure 5. Variation in Rawcounts During EFT Testing



The CapSense block can completely malfunction due to transient-induced noise. For instance, rawcounts can become zero during the noise injection and return to a normal value when the noise is removed, as shown in Figure 8. C_{MOD} charge and discharge cycles can become abnormal, as shown in Figure 7 and return to normal when the noise is removed, as shown in Figure 6 .

Figure 6. Normal Waveform on CMOD Pin (Representative Image)

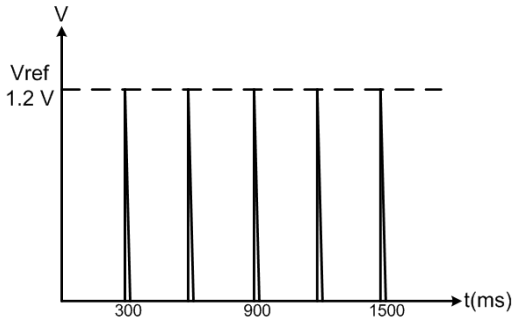


Figure 7. Waveform on CMOD Pin During an EFT Test (Representative Image)

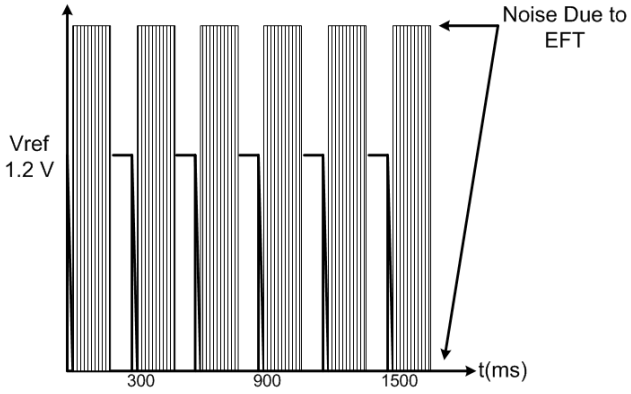
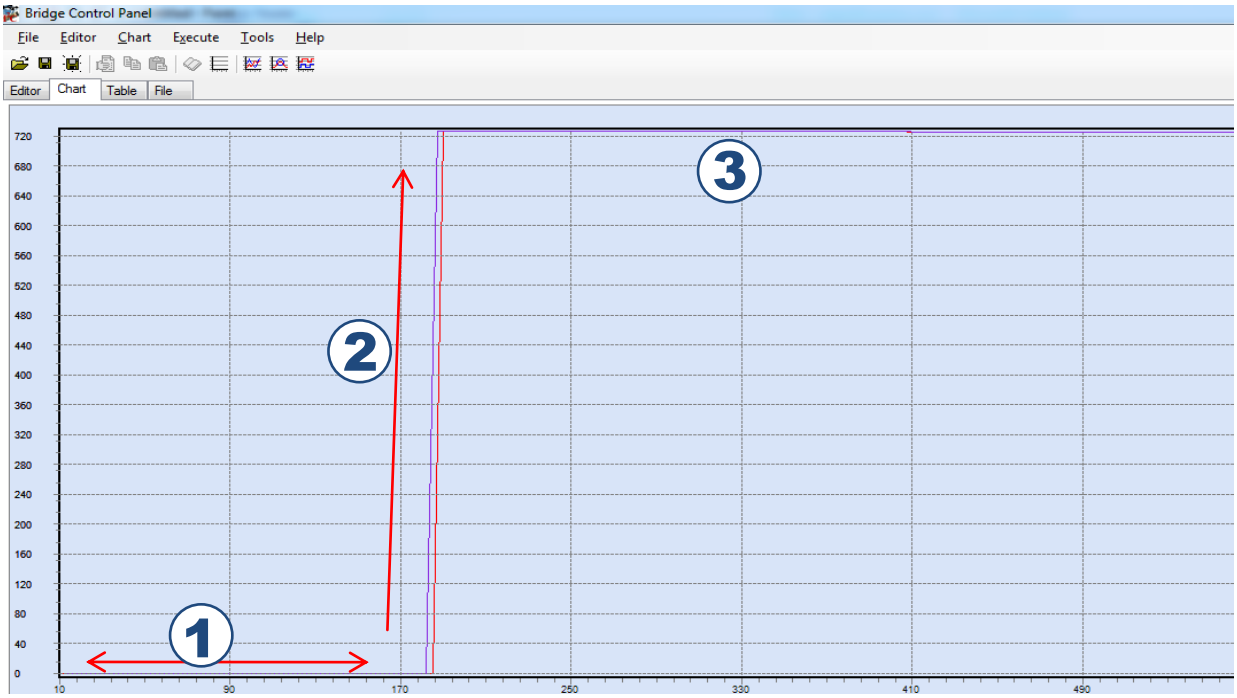


Figure 8. Rawcounts and Baseline Behavior with Transient-Induced Noise



1. Rawcounts (blue line) and baseline (pink line) are zero during EFT test.
2. Rawcounts and baseline recover after the completion of the test.
3. Rawcounts and baseline remain stable at their original values after the EFT test is complete.

4.3 Communication Failure

I2C and UART are the commonly used communication protocols in a CapSense system. Communication can fail due to any of the following reasons:

- malfunctioning of the communication block in the controller
- clock stretch or glitch on clock lines
- loss of signal integrity
- malfunctioning transceiver
- interface malfunction

When the communication fails due to any of these reasons, either the communication is completely lost or the host might read corrupted data. If the host reads corrupted data, such as wrong CapSense sensor status, the host may act on the wrong data leading to system malfunction.

5 Performance Criteria

The loss of functionality or degradation of performance of a CapSense system, relative to the performance as defined by its specifications, per IEC 61000-4-4, can be categorized as listed in Table 2.

Table 2. Performance Criteria

Criteria	Description
Performance Criteria A	Normal performance after the EFT test is within limits as specified by the manufacturer.
Performance Criteria B	Temporary loss of function or degradation of the performance during the EFT test; the controller recovers to its normal performance without any intervention after the test.
Performance Criteria C	Temporary loss of function or degradation of the performance during the EFT test; the controller recovers to its normal performance with intervention after the test.
Performance Criteria D	Loss of function or degradation of the performance during the EFT test; the controller does not recover owing to damage.

Most CapSense system manufacturers design their equipment to perform according to criteria A.

6 Troubleshooting, Design Considerations, and Mitigation Techniques

Effective troubleshooting of problems due to transient-induced noise is non-trivial even though it is often overlooked as part of system compliance testing and bring-up. In a CapSense system, the sequence of troubleshooting steps is:

1. Detect if there is a reset and determine the cause of the reset.
2. Check if there is any false triggering of sensors or if sensors do not respond.
3. Look for any communication failures, which could be a complete loss of communication or data corruption.

For details on finding out the type of reset, see AN80994.

Techniques to mitigate the effects of transient noise include the following:

1. Reflecting the transient energy back to the source by providing a least-impedance return path
2. Dissipating the transient energy before it propagates to sensitive circuits
3. Designing firmware/software that is immune to transient-induced noise

The areas in which the mitigation techniques can be applied can be divided as follows:

- System-level considerations
- Power supply design considerations
- Target board design considerations
- Firmware techniques

This application note covers target board design considerations and firmware techniques for a CapSense system. For a general embedded microcontroller-based system, the mitigation techniques in the areas mentioned above are covered in AN80994.

6.1 Target Board Design Considerations

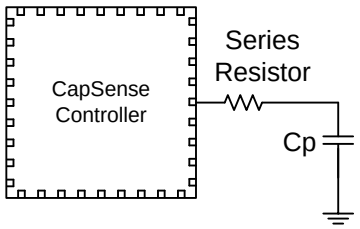
6.1.1 Schematics

Use the following general considerations at schematic level:

1. Use supply line filters including bypass capacitors, bulk capacitors, decoupling capacitors, TVS diodes, LC filters, and common mode chokes.
2. Protect communication lines by using filter components such as pull-up resistors, series resistors, and capacitors on I2C/SPI lines. Use an isolated level translator for UART communication.
3. Protect the reset, interrupt, and other critical control inputs from transients by adding a capacitor or RC network.
4. Protect I/O lines using bidirectional TVS diodes and RC filter. Terminate unused I/Os using typically a 10-kΩ series resistor.
5. Place series resistors on CapSense sensors (see Figure 9).

   The series resistor value must be chosen such that the sensors get charged and discharged completely for every switching clock pulse. The typical recommended series resistor value for CapSense sensors is 560 Ω. If the device resets due to a human finger touching the sensors, increase the impedance on the path by increasing the series resistor value to about 2 kΩ or 3 kΩ depending on the sensor parasitic capacitance and the switching clock set in firmware.

Figure 9. Series Resistor on CapSense Sensor



How to Select Series Resistor

As resistors provide a voltage drop, small values in series are more practical in applications. The resistor's end-to-end capacitance limits its impedance. For example, a 1-MΩ resistor at DC is not the same at 100 MHz. To improve transient immunity, use carbon or metal oxide resistors because they provide a low value of parasitic capacitance and inductance, and can withstand short pulse overloads.

Some typical resistor types are the following:

- Surface mount technology (SMT) and thin-film resistors are good for high-frequency response but not for transient protection. They are composed of a thin metal layer (thickness of tens of nanometers), which limits the device's ability to withstand the EFT energy. In addition, EFT voltage tends to arc across SMT.
- Metal-film resistors are suitable for high-power-density or high-accuracy circuits but not for transient protection.
- Wire-wound resistors are suitable for high-power handling circuits but not for circuits sensitive to high-frequency due to their large inductance. Also, they are not available in surface mount form (without molding), making them unsuitable for applications with size and weight limitations.

- Foil-based resistors offer the best precision and stability and can better withstand EFT than thin-film and thick-film resistors. Their main disadvantage is a limit on the maximum value of approximately 150 kΩ.

Getting a system EFT test qualified might be an iterative process. It is recommended that you have footprints for the filter components on board and start the EFT tests with minimal components such as bypass and decoupling capacitors populated on the board. To improve the immunity further, you can try using filters such as LC, common-mode chokes, TVS diodes, and ferrite beads sequentially or combine more than one. Use bulk capacitors when the power supply design is not very good and you expect the output of the power supply to have ripples.

6.1.2 PCB Layout

You need to keep in mind two basic principles before designing a PCB for good transient immunity.

The first is that currents should be returned to their source as locally and compactly as possible, that is, through the smallest possible and least-impedance path. This applies to both transient noise and desired signal current.

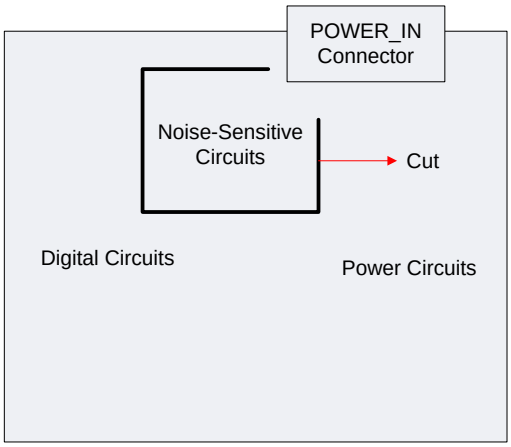
The second is that a system should have only one reference plane. A reference plane, often a ground plane, is placed adjacent to a signal layer in a PCB for return currents to flow. Having two reference planes causes signal integrity issues, which can be amplified by transient noise. More than one reference plane also creates a dipole antenna that radiates energy. A single reference plane is not achieved if the reference planes and the connections of the reference planes do not have low impedance.

Finally, to reiterate a point mentioned in the previous section, it is recommended that you design filters into the PCB. For initial testing, have a provision to bypass these filters.

For a CapSense system:

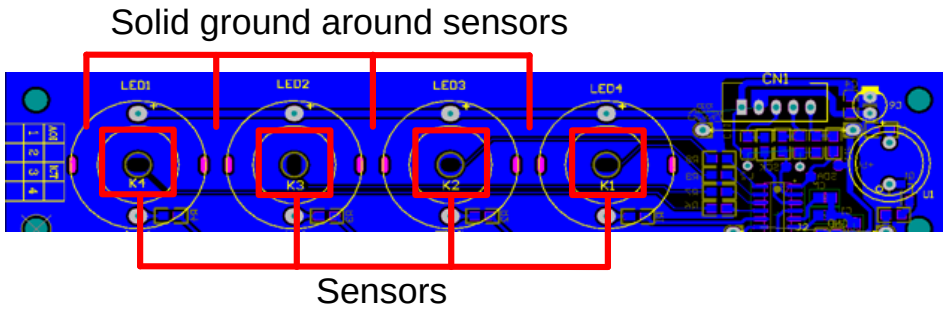
1. Isolate or provide physical separation between CapSense components and their signals from noisy subsystems such as transformers. A CapSense system in general is sensitive to external noise.
2. Isolate the CapSense system such that the sensor currents and the CMOD capacitor current flow back to their source in the shortest possible path. This ensures that the desired current does not take an unnecessarily long path and get subjected to radiated or conducted noise on the way.
3. Keep CapSense sensor traces away from I/O lines including communication lines that might be vulnerable to transient-induced noise.
4. Keep the sensor traces short. Long traces are susceptible to noise and can also become carriers of noise.
5. Separating analog and digital ground might be required with devices (such as PSoC) that have provision for separate ground pins, if there are noisy digital signals. The CapSense block typically operates on an analog ground.
6. Stitch the analog and digital grounds appropriately such that there is only one reference plane. The other method of isolating the two grounds is to cut a notch in the ground plane where you want to separate the ground reference of sensitive signals from the ground reference of noisy signals, as shown in Figure 10:

Figure 10. Ground Plane Cut Example



7. Connect hatch patterns of ground on different layers with as many vias as possible that are placed equidistant from each other to reduce the inductance.
8. For a two-layer board, follow the CapSense layout guidelines for ground and sensor scheme. For a single-layer board, if the board is small and the sensor traces are short, have solid ground pour throughout the board, even around the sensors. Make sure that the parasitic capacitance does not exceed the maximum. See Figure 11.

Figure 11. Single-Layer Board Design



6.1.3 Example PCB Design in Two Layers

The following PCB design is an example of a CapSense board design for improved EFT immunity. Figure 12 and Figure 13 show the top and bottom layers of a two-layer CapSense board designed with PSoC 4200M. The board supports nine buttons and has nine corresponding LEDs.

Figure 12. Top Layer

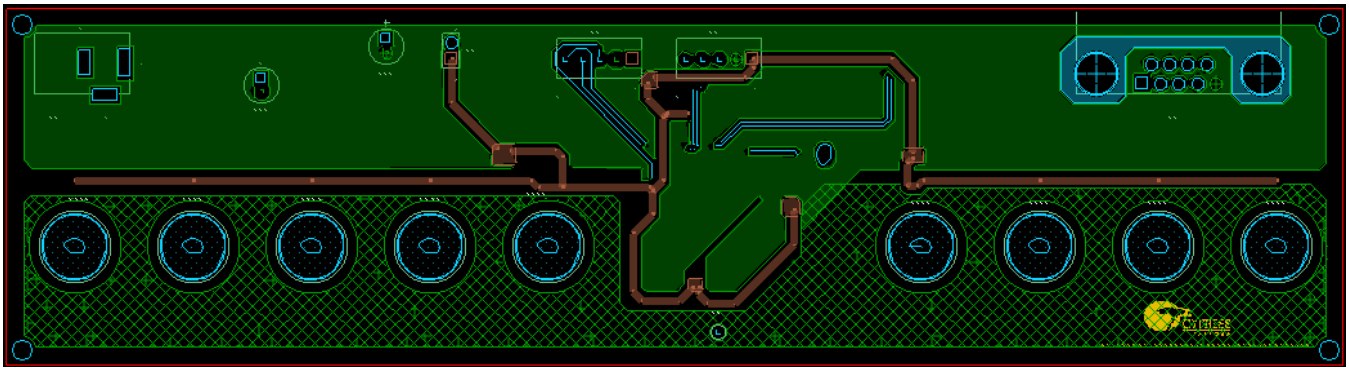
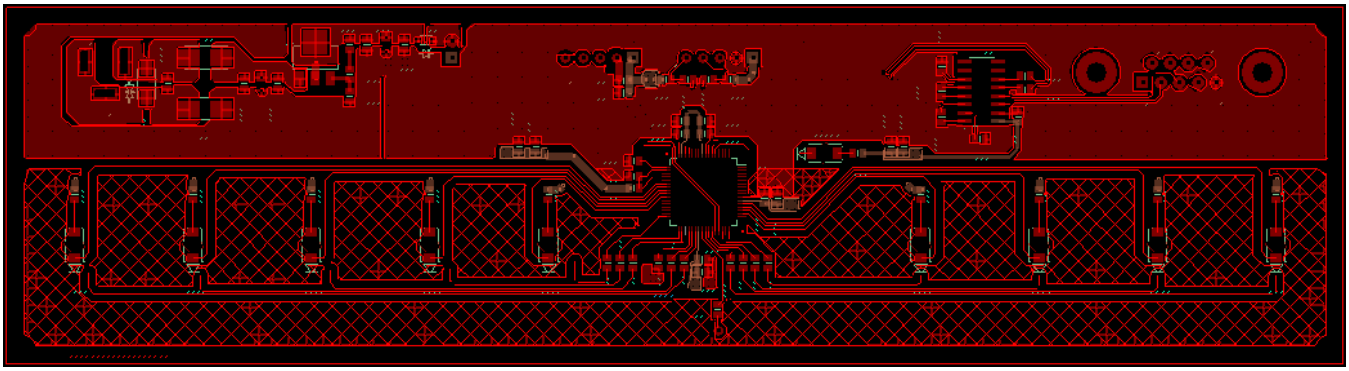


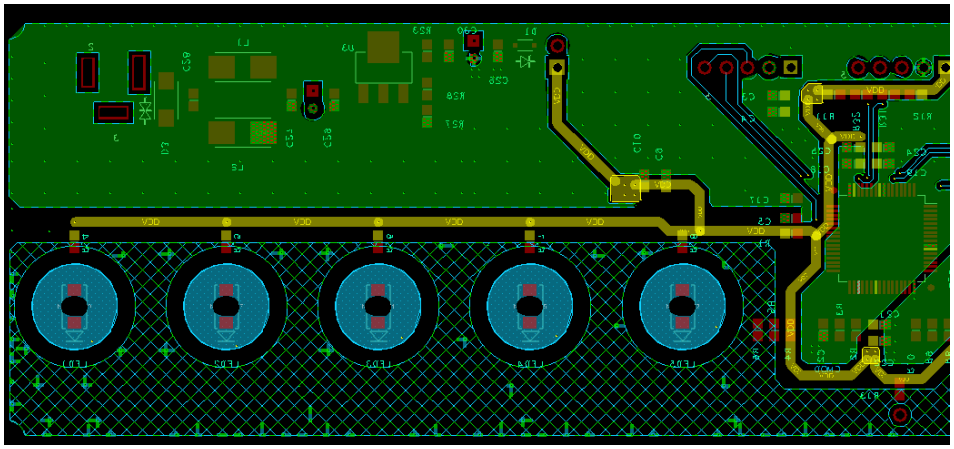
Figure 13. Bottom Layer



Some salient features of the board layout are as follows:

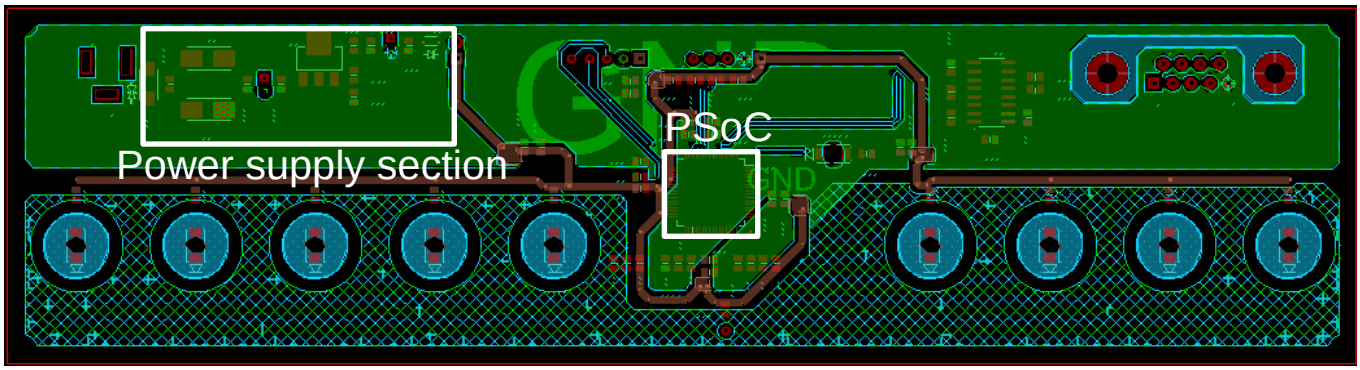
1. The thick 50-mil VDD trace running from the power supply to the PSoC device (see Figure 14) helps minimize resistive drops for DC currents, yet at the same time maintains a finite impedance for high-frequency AC signals/noise.

Figure 14. Thick VDD Supply Trace (Highlighted in Yellow)



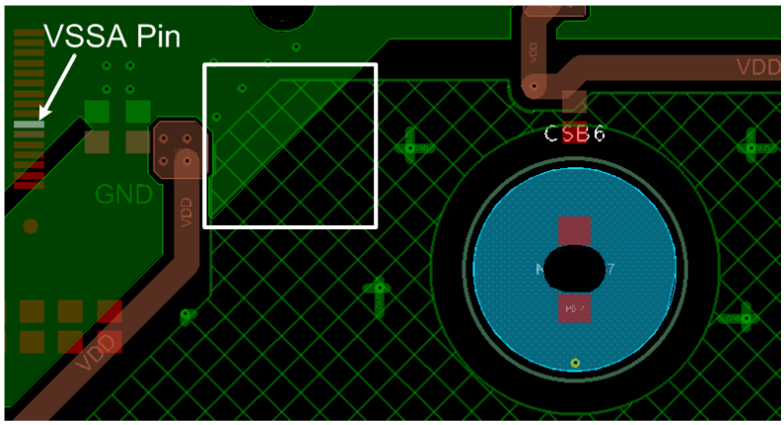
2. The solid ground pour from the power supply to the PSoC device and to the rest of the circuit (Figure 15) helps maintain a stable reference voltage for all circuits. It also provides a low-impedance path for the noise to return to the source.

Figure 15. Solid Ground Plane - Top Layer



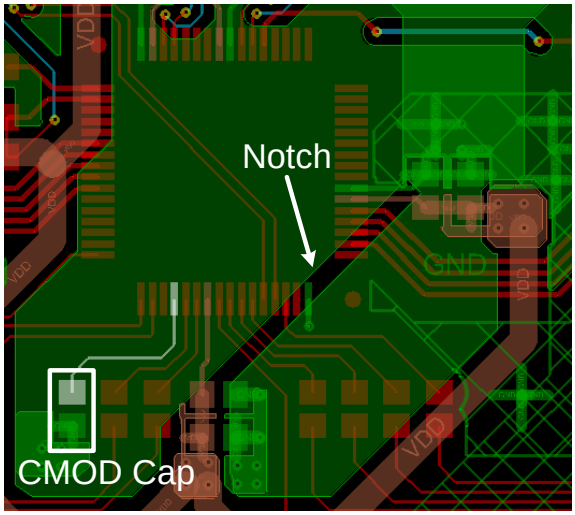
3. Hatch ground around the sensors is the ground reference for sensors. It is separated from the solid ground and joins the VSSA pin near the PSoC device as shown in Figure 16.

Figure 16. Hatched Ground Pattern and Solid Ground Pattern



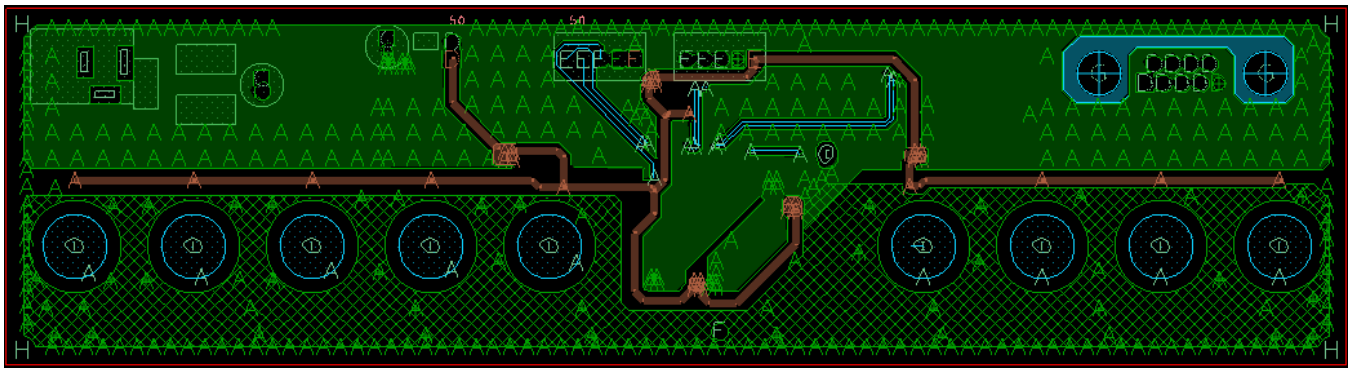
4. The current through the CMOD capacitor finds the shortest return path to the source (that is, the, PSoC device). The notch cut in the ground plane forces the CMOD current to return to its source in the shortest path (see Figure 17).

Figure 17. Notch in Ground Forces Switching CMOD Capacitor Current via Least-Impedance Path



5. Hatched and solid ground patterns on the top and bottom layer are stitched with many vias placed uniformly to reduce the impedance, as shown in Figure 18.

Figure 18. Ground Plane Stitching to Reduce Impedance – Character “A” on the Layout Depicts a Via



6. Power supply filters are placed at the entry of the supply (see Figure 19 and Figure 20).

Figure 19. Schematic of Power Supply and Associated Filters

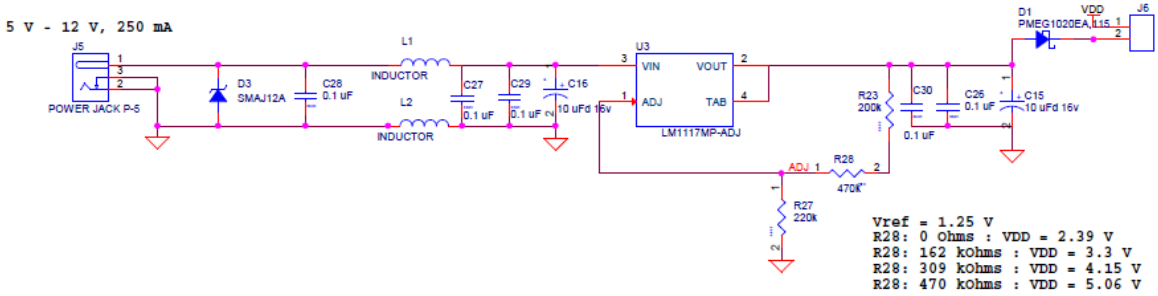
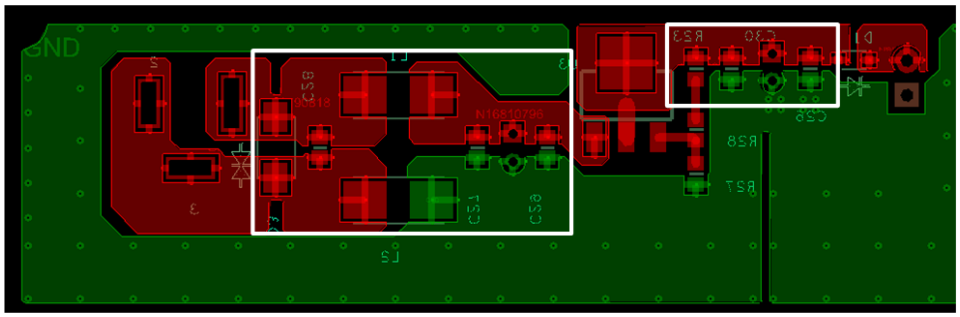
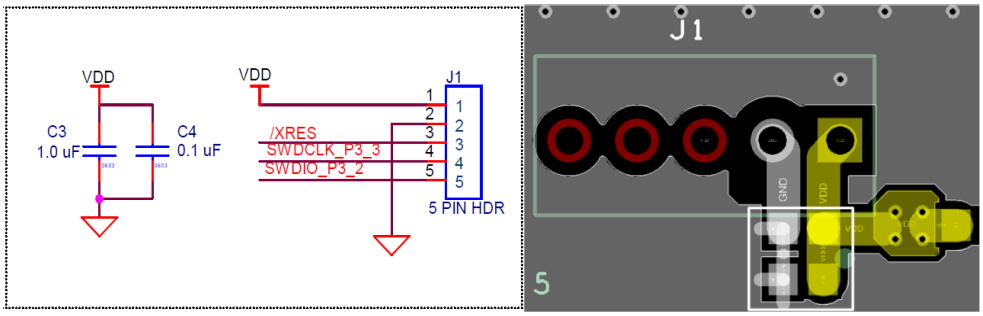


Figure 20. Layout of Power Supply on Bottom Layer and Associated Filters (Highlighted in White Box)



7. Bypass capacitors are placed on the supply lines of the programming header. This will be helpful if the programming header is used to power the board during EFT tests (see Figure 21).

Figure 21. Programming Header Supply Filters – Schematic and Layout



6.2 Firmware Techniques

A properly designed firmware can go a long way in eliminating or minimizing errors caused by transients. Firmware should be designed in such a way that if a transient upsets the program, it does not lock up, but recovers gracefully.

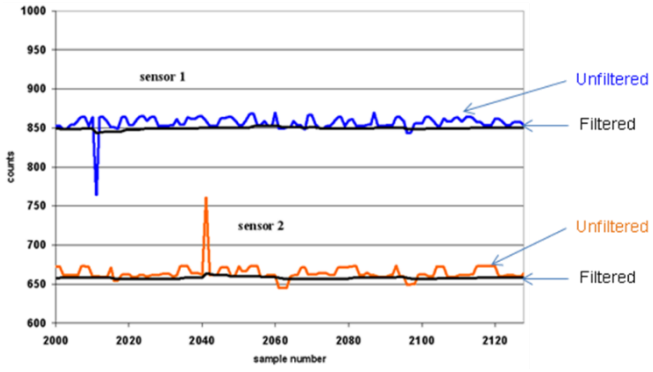
CapSense-specific firmware techniques involve event-based filters that are defined based on the noise pattern. This application note briefly describes the firmware techniques that can avoid the false triggering and unresponsiveness of sensors.

1. Median filter

   Positive and negative spikes are the most common type of noise seen in rawcounts due to transient-induced noise. The median filter is the first line of defense. Median filters eliminate noise spikes as shown in Figure 22. In a median filter, a buffer of size 'N' stores the N most recent samples of the input. The median is then computed using a two-step process. First, the buffer values are sorted from the smallest to the largest; then, the middle value is selected from the ordered list. The buffer is scanned for the median with each update of the buffer. Implement a median filter of buffer size N corresponding to the width of the noise spike. Select the buffer size 'N' based on the number of samples the spikes would last, as shown in the equation below. Assuming that the width of finger touch response is larger than that of spikes, median filters with appropriate buffer size do not eliminate any valid finger touch responses.

   $$N = (Number\ of\ samples\ of\ spikes * 2) + 1$$

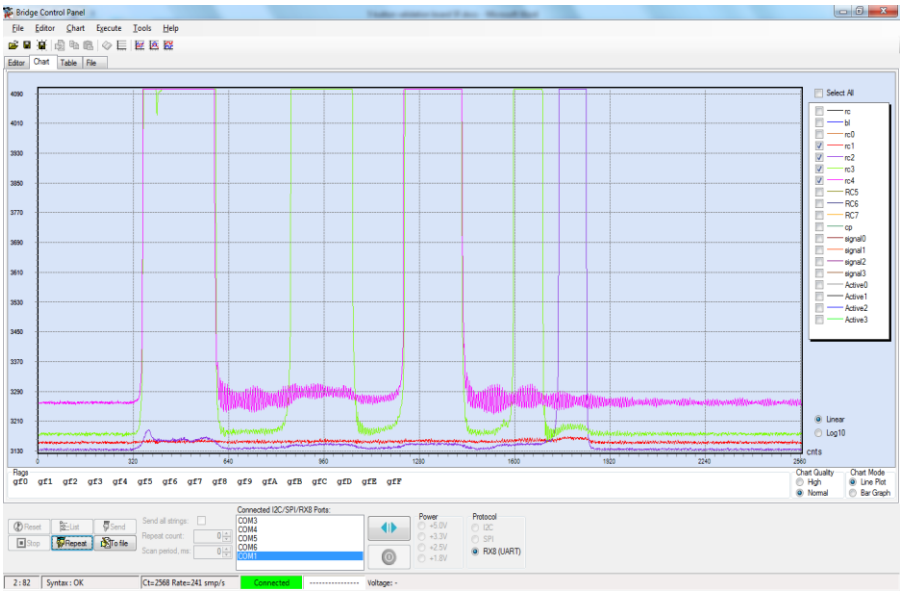
Figure 22. Median Filter Response – Showing Unfiltered and Filtered Rawcounts



2. Negative edge debounce

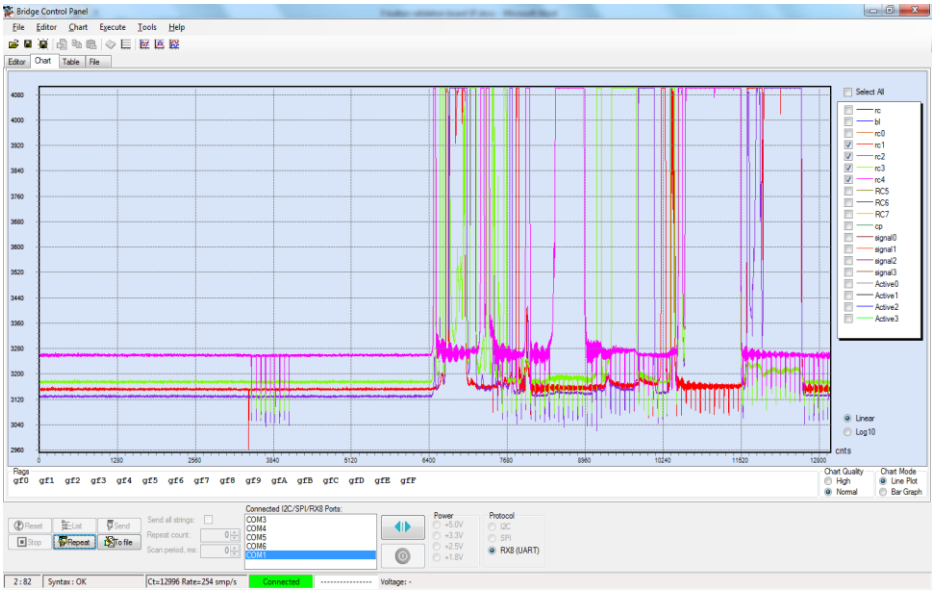
With transient-induced noise, there will be negative spikes in rawcounts when sensors are touched (see Figure 24); these spikes can turn OFF the sensors inadvertently when the sensors are still touched. Implement negative-edge debounce similar to positive-edge debounce to avoid false sensor-deactivation. Figure 23 and Figure 24 show graphs of rawcounts of four sensors. Figure 23 shows graph of rawcounts in which rawcounts go up with sensor touch and there are no negative spikes when sensors are touched in the absence of transient-induced noise.

Figure 23. Without Transient-Induced Noise, No Spikes in Rawcounts when the Sensor Is Touched



However, in Figure 24, in the presence of transient-induced noise, there are huge negative spikes in rawcounts. With these negative spikes, when a sensor is touched, the sensors might turn OFF as the negative spikes may pull the rawcounts down below the finger threshold.

Figure 24. With Transient-Induced Noise, Spikes in Rawcounts when Sensor Is Touched



3. Low baseline reset (LBR)

   Baseline can reset to a lower value of rawcounts when there is a negative spike in rawcounts, as shown in Figure 25. This baseline reset can falsely trigger the sensor when the rawcounts recover. The baseline resets only after the spike lasts for more than the LBR value. The LBR value in the CapSense Component must be set based on the width of negative noise spikes (see Figure 26) such that there are no false triggers or a baseline "stuck" condition. Sometimes, negative spikes might last for more than 255 samples. However, the CapSense Component limits the value of LBR to 255.

   Implement LBR in the application firmware by using a firmware counter for wide negative noise spikes that last for more than 255 samples.

Figure 25. Dip in Rawcounts(Y Axis) Causing Baseline to Fall with LBR = 10 and Noise Spike Width = 20

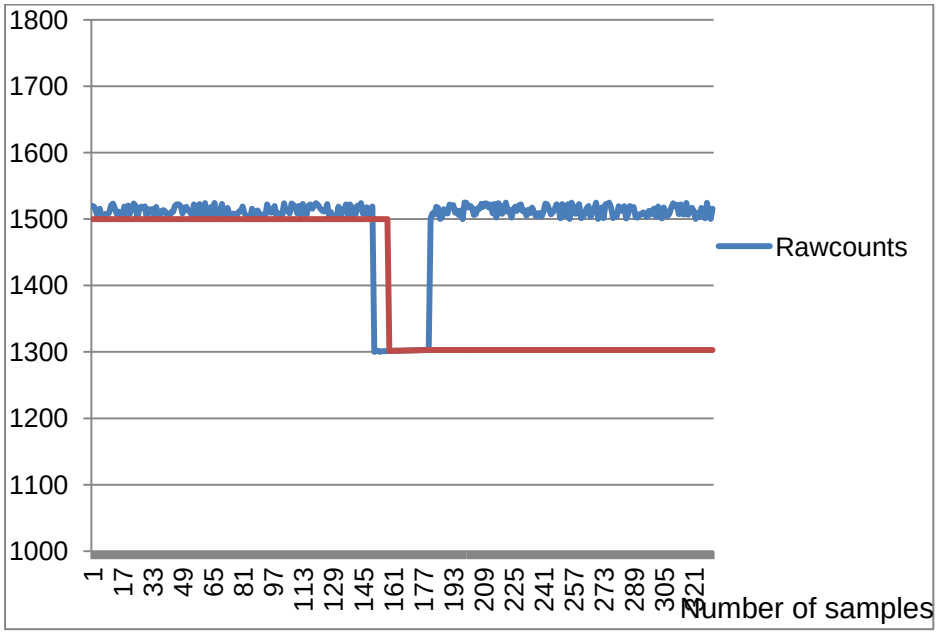
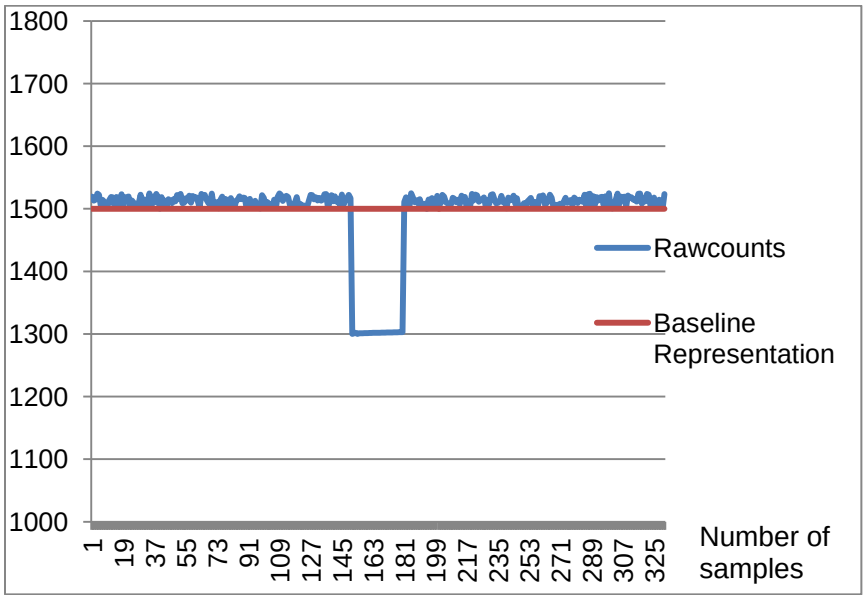


Figure 26. Dip in Rawcounts (Y Axis) Not Causing Baseline to Fall with LBR = 30 and Noise Spike Width = 20

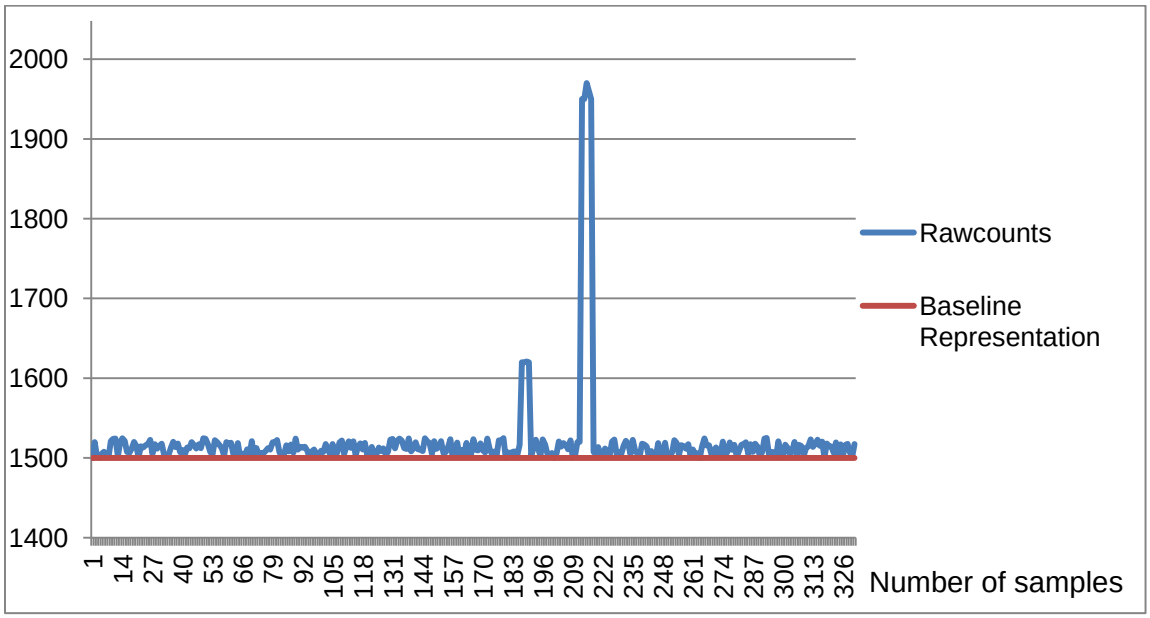


In these figures, the noise spike lasts for about 20 samples. With an LBR value of 10, the baseline would follow rawcounts; once the rawcounts recover, the baseline gets stuck leading to a false trigger. With LBR =30, the baseline would not follow rawcounts when there is spike of 20 samples; thus false triggering is prevented.

4. Upper signal cut-off

   Positive spikes in rawcounts due to transient-induced noise (see Figure 27) can cross the finger threshold, which can lead to sensor false-triggers. Implement an upper cut-off on the signal to avoid false triggers due to positive spikes. Any signal above the upper cut-off must be treated as noise, and this signal must not trigger the sensors.

Figure 27. Rawcounts with Noise in Positive Direction



5. Time-based Autoreset

   When a sensor is stuck in the ON condition, the Autoreset feature can recover the sensor from the stuck condition. A sensor is considered to be stuck in ON condition if the sensor is ON for more than the time which the user is expected to touch the sensor for. There are applications where the user is expected to touch sensors for a long time (such as up to 10 seconds). In such a scenario, a sensor is considered to be stuck in ON condition if the sensor is ON continuously for more than 10 seconds. Autoreset resets the baseline to the current rawcount value if the sensor is ON for a specific time and thus turns OFF the sensor. Implement a time-based Autoreset in the application firmware based on the number of sensor scan samples. Time-based Autoreset will provide control and good granularity at the Autoreset time, which varies from application to application.

6. Dynamic debounce adjustment – advanced technique

   Debounce indicates the number of samples for which the difference count of a sensor should be above the finger threshold for the sensor to be reported ON. A small value of debounce may be insufficient, and positive spikes can falsely trigger the sensors. A large value may slow down the response to a finger touch. The debounce value can be dynamically adjusted in firmware by tracking the number of samples for which the positive spikes last and by distinguishing the spikes from the finger-touch signal using the upper finger threshold.

7. Manual thresholds

   Use manual thresholds instead of automatic thresholds. This will allow flexibility in setting values for various threshold parameters such as finger threshold, noise threshold, negative noise threshold, and low-baseline reset based on the noise in an application.

7 Summary

This application note provides design guidelines and techniques to boost the EFT immunity of a CapSense system. It also explains the failure modes of a CapSense controller.

About the Authors

Name: Shruti Hanumanthaiah

Title: Applications Engineer

Background: Shruti is an applications engineer with a background in electronics and communication. She is working on CapSense applications using PSoC.

Name: Srinivas NVNS

Title: Applications Engineer

Background: Srinivas is an electrical engineer with a background in power electronics, control systems, and embedded firmware. He is working on power applications using PSoC.

8 References

- IEC EN 61000-4-2 – Electrostatic discharge immunity test.[1]
- IEC EN 61000-4-4 – Electrical fast transient/burst immunity test. [1]
- Mark I. Montrose, *EMC and the Printed Circuit Board: Design, Theory, and Layout Made Simple,* Wiley-IEEE Press, 1998).
- Mark I. Montrose and Edward M. Nakauchi, *Testing for EMC Compliance: Approaches and Techniques* (Wiley-IEEE Press, 2004).
- Henry W. Ott, *Electromagnetic Compatibility Engineering* (John Wiley & Sons, 20 September 2011)
- Vishay, “Engineering Note ILB, ILBB Ferrite Beads, Electro-Magnetic Interference and Electro-Magnetic Compatibility (EMI/EMC),” www.vishay.com/docs/34097/ferritenote.pdf
- AN57821 - PSoC 3, PSoC 4, and PSoC 5LP Mixed Signal Circuit Board Layout Considerations
- AN80994 - Design Considerations for Electrical Fast Transient (EFT) Immunity
- AN54181 - Getting Started with PSoC 3
- AN79953 - Getting Started with PSoC 4
- AN77759 - Getting Started with PSoC 5LP
- AN64846 - Getting Started with CapSense
- AN61290 - PSoC 3 and PSoC 5LP Hardware Design Considerations
- AN88619 - PSoC 4 Hardware Design Considerations

1 This standard is not available for free. However, you can purchase a copy at www.iec.ch.

Document History

Document Title: AN96475 - Design Considerations for Electrical Fast Transient Immunity of a CapSense® System

Document Number: 001-96475

Revision	ECN	Orig. of Change	Submission Date	Description of Change
**	5137853	SSHH, SNVN	02/22/2016	New application note
*A	5709495	AESATP12	04/26/2017	Updated logo and copyright.

Worldwide Sales and Design Support

Cypress maintains a worldwide network of offices, solution centers, manufacturer's representatives, and distributors. To find the office closest to you, visit us at Cypress Locations.

Products

ARM® Cortex® Microcontrollers	cypress.com/arm
Automotive	cypress.com/automotive
Clocks & Buffers	cypress.com/clocks
Interface	cypress.com/interface
Internet of Things	cypress.com/iot
Memory	cypress.com/memory
Microcontrollers	cypress.com/mcu
PSoC	cypress.com/psoc
Power Management ICs	cypress.com/pmic
Touch Sensing	cypress.com/touch
USB Controllers	cypress.com/usb
Wireless Connectivity	cypress.com/wireless

PSoC® Solutions

PSoC 1 | PSoC 3 | PSoC 4 | PSoC 5LP | PSoC 6

Cypress Developer Community

Forums | WICED IOT Forums | Projects | Videos | Blogs | Training | Components

Technical Support

cypress.com/support

All other trademarks or registered trademarks referenced herein are the property of their respective owners.

Cypress Semiconductor
198 Champion Court
San Jose, CA 95134-1709

© Cypress Semiconductor Corporation, 2016-2017. This document is the property of Cypress Semiconductor Corporation and its subsidiaries, including Spansion LLC ("Cypress"). This document, including any software or firmware included or referenced in this document ("Software"), is owned by Cypress under the intellectual property laws and treaties of the United States and other countries worldwide. Cypress reserves all rights under such laws and treaties and does not, except as specifically stated in this paragraph, grant any license under its patents, copyrights, trademarks, or other intellectual property rights. If the Software is not accompanied by a license agreement and you do not otherwise have a written agreement with Cypress governing the use of the Software, then Cypress hereby grants you a personal, non-exclusive, nontransferable license (without the right to sublicense) (1) under its copyright rights in the Software (a) for Software provided in source code form, to modify and reproduce the Software solely for use with Cypress hardware products, only internally within your organization, and (b) to distribute the Software in binary code form externally to end users (either directly or indirectly through resellers and distributors), solely for use on Cypress hardware product units, and (2) under those claims of Cypress's patents that are infringed by the Software (as provided by Cypress, unmodified) to make, use, distribute, and import the Software solely for use with Cypress hardware products. Any other use, reproduction, modification, translation, or compilation of the Software is prohibited.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CYPRESS MAKES NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THIS DOCUMENT OR ANY SOFTWARE OR ACCOMPANYING HARDWARE, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. To the extent permitted by applicable law, Cypress reserves the right to make changes to this document without further notice. Cypress does not assume any liability arising out of the application or use of any product or circuit described in this document. Any information provided in this document, including any sample design information or programming code, is provided only for reference purposes. It is the responsibility of the user of this document to properly design, program, and test the functionality and safety of any application made of this information and any resulting product. Cypress products are not designed, intended, or authorized for use as critical components in systems designed or intended for the operation of weapons, weapons systems, nuclear installations, life-support devices or systems, other medical devices or systems (including resuscitation equipment and surgical implants), pollution control or hazardous substances management, or other uses where the failure of the device or system could cause personal injury, death, or property damage ("Unintended Uses"). A critical component is any component of a device or system whose failure to perform can be reasonably expected to cause the failure of the device or system, or to affect its safety or effectiveness. Cypress is not liable, in whole or in part, and you shall and hereby do release Cypress from any claim, damage, or other liability arising from or related to all Unintended Uses of Cypress products. You shall indemnify and hold Cypress harmless from and against all claims, costs, damages, and other liabilities, including claims for personal injury or death, arising from or related to any Unintended Uses of Cypress products.

Cypress, the Cypress logo, Spansion, the Spansion logo, and combinations thereof, WICED, PSoC, CapSense, EZ-USB, F-RAM, and Traveo are trademarks or registered trademarks of Cypress in the United States and other countries. For a more complete list of Cypress trademarks, visit cypress.com. Other names and brands may be claimed as property of their respective owners.