Application Report
SLAA932–December 2019

MSP430™ System-Level ESD Troubleshooting Guide

Lixin Chen
Maggie (Qun) Zhang

MSP430 Applications
MSP430 Quality

ABSTRACT

System-level electrostatic discharge (ESD) immunity, as one part of electromagnetic compatibility (EMC), has become more and more important in our daily lives with most electrical products. The MSP430™ microcontroller (MCU) portfolio offers a wide variety of 16-bit MCUs with ultra-low-power and integrated analog and digital peripherals for sensing and measurement applications. This application report introduces the concepts of system-level ESD immunity tests, troubleshooting guidelines, and a failure analysis procedure when encountering system-level ESD problems with MSP430 devices.

Contents

List of Figures

List of Tables

Trademarks

1 Overview of System-Level ESD and EMC Test Standards

Electrostatic discharge (ESD) is the transient static electricity flow between two objects with different electrical potentials when they come into contact or close enough.

ESD is one example of electromagnetic interference (EMI), which is the generic term describing a situation in which an electrical disturbance generated by a certain electronic or electrical equipment causes an undesirable response in another equipment. Electromagnetic compatibility (EMC) is just the opposite; it is the discipline of analyzing and preventing or fixing interference problems.

IEC 61000-4-x standards define the test and measurement techniques for EMC immunity tests of electronic equipment. The most common test standards follow:

- IEC 61000-4-2: System-level ESD immunity test
- IEC 61000-4-3: Radiated radio-frequency, electromagnetic field immunity test
- IEC 61000-4-4: Electrical fast transient/burst immunity test
- IEC 61000-4-5: Surge immunity test
- IEC 61000-4-6: Conducted RF immunity test
- IEC 61000-4-8,9,10: Magnetic field immunity test
- IEC 61000-4-11, and -12 to -35: additional tests

IEC 61000-4-2 is an International Electrotechnical Commission (IEC) immunity standard on system-level ESD. It defines the typical discharge current waveforms, test levels, test setup, and test procedure. For quick reference of ESD waveform, test levels, and test bench setup, see *IEC 61000-4-2, IEC 61000-4-4 and IEC 61000-4-5 tests for TI's protection devices*. For more detailed description about the system-level ESD test, see the IEC 61000-4-2 standard.

Many products specify the system-level ESD immunity requirement for end customers and define which levels are needed to comply with IEC 61000-4-2 standard. To achieve the system-level ESD immunity performance and pass the IEC 61000-4-2 tests, system designers need to follow specific guidelines during development. To understand the difference between component-level and system-level ESD, and for detailed guidelines related to MSP430 MCUs, see *MSP430 System-Level ESD Considerations*.

2 System-Level ESD Failure Scenarios

A product designed with an MSP430 microcontroller (MCU) uses firmware programmed in the MSP430 MCU to work with power supply circuits, external components (for example, sensors and parallel or serial communication devices) and electrical actuators that are connected to the MSP430 MCU. When there is system-level ESD failure in the system, the failure scenarios will be diverse and depend on the system design and the noise immunity performance of the components. The following behaviors are examples of ESD failures:

- System reset when ESD applies and resume after the ESD
- System reset and cannot resume after the ESD
- LCD display failed (can be restored or cannot be restored after ESD test)
- Serial communication failed – UART, I^2C, or SPI
- System hang-up
- Abnormal power consumption
- Memory corruption
- ADC sampling incorrect, Speaker or buzzer noise
- Device damage

System-level ESD failure can be caused by normal operations such as lighting, occasional zap when reaching for a door knob, cable plug, BGM (blood glucose meter) test strip plug, and more. So the system-level ESD test is widely used to evaluate the ESD immunity performance for most products before mass production.

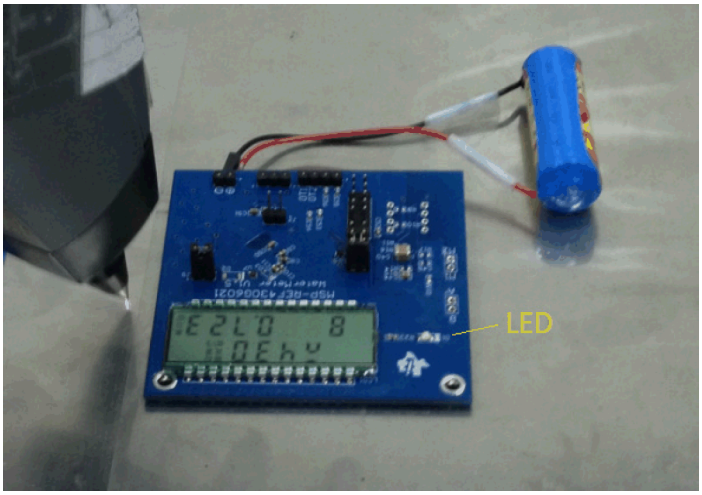


Figure 1. System-Level ESD Failure Example

Figure 1 shows an example of the system-level ESD test that failed on a water meter MCU board. The green LED blinks several times after power on and turns off. When ESD simulator discharges onto the metal plate of the test platform, the LED blinks again which means the water meter board resets, showing that the test failed.

ESD failure scenarios can be summarized in two categories:

- Soft failure
  - A failure that can be corrected in the system
  - A failure requiring intervention to resume (for example, reboot, power cycle, or a hardware reset)
- Physical failure
  - Catastrophic failures that cause permanent damage. The board will work abnormally.
  - Latent defects that cause partially degraded performance. The board can still work functionally but life cycle will be impacted.

The debug and troubleshooting of soft failure scenarios are discussed in Section 3 from system application point of view. Regarding the physical failure scenarios, a failure analysis process can be applied which is discussed in Section 4.

3 System-Level ESD Soft Failure Troubleshooting Guidelines

System-level ESD tests are normally executed at the post-design phase or the pilot run stage of the product development. When finding system-level ESD test failed cases, designers and testers need to address the root cause and provide solutions to fix the test failed issue in a critical situation. In this section, the recommended troubleshooting methodology and guidelines are discussed for MSP430 system-level ESD failures. The typical procedure for troubleshooting follows:

1. Reproduce the failed case reliably.
2. Analyze the root cause from mechanical construction, hardware, software, and silicon.
3. Identify the root cause and find solution.
4. Try one or more software workarounds to improve and fix the issue.
5. Try one or more hardware or mechanical workarounds to improve and fix the issue.

3.1 Reproducibility of the Failure Case

In a system-level ESD test, an electric discharge is generated by an ESD simulator, which should be calibrated. The equipment under test (EUT) is placed on the test platform, which is set up following the IEC 61000-4-2 standard.

For debug of a system-level ESD failure cases, the first step is to reproduce the failure scenario reliably. Then the workaround can be verified under the same test condition. However, the reproducibility is normally poor due to variance in the test results. There are several factors that affect the test result including the ESD simulator brand, temperature and humidity, EUT grounding status, EUT working status, and conductors around the test platform. To achieve a highly successful reproducibility ratio, it is recommended to keep following items:

- Perform the test following the IEC 61000-4-2 standard with a calibrated ESD simulator and a qualified test platform.
- Use the same ESD simulator.
- Grounding of the EUT should be same.
- Temperature and humidity should be similar.
- EUTs run the same firmware.

To avoid an exception case, it is better to test two more EUTs to confirm that the failure case is consistent in the batch of products.

A system-level ESD test is not the only method to reproduce the failure scenarios. Some other operation such as cable plug or test strip plug can also be used for this purpose.

Some failure cases can be hard to reproduce when the system runs into abnormal situation randomly during the ESD test. Generally, a power cycle will recover the system but it is hard to reproduce the failure in the short term. For this kind of case, see the discussion in Section 3.3.

3.2 Software Debug Guidelines

MSP430 devices implement some self-diagnostic features such as reset source reporting in the SYSRSTIV register and oscillator fault detection. There are also some simple workarounds that can be implemented to address the root cause.

3.2.1 Reset Source Identification

An unexpected reset is a one of the failure scenarios in ESD tests of MCU systems. For this case, it is better to find the reset source before implementing any improvement approach. In some MSP430 devices (MSP430F5x, MSP430F6x, MSP430FG6x, MSP430FR5x, MSP430FR6x, MSP430FR4x, and MSP430FR2x), there is a good feature to identify the reset source: the reset source can be read from the interrupt vector register SYSRSTIV after reset. The SYSRSTIV value indicates the interrupt events. The value definition can be found in the device specific data sheet. Table 1 is an example from the MSP430FR235x data sheet.

Table 1. Example of SYSRSTIV Register Description

INTERRUPT VECTOR REGISTER	ADDRESS	INTERRUPT EVENT	VALUE	PRIORITY
SYSRSTIV, System Reset	015Eh	No interrupt pending	00h	
		Brownout (BOR)	02h	Highest
		RSTIFG $\overline{\text{RST}}$/NMI (BOR)	04h	
		PMMSWBOR software BOR (BOR)	06h	
		LPMx.5 wake up (BOR)	08h	
		Security violation (BOR)	0Ah	
		Reserved	0Ch	
		SVSHIFG SVSH event (BOR)	0Eh	
		Reserved	10h	
		Reserved	12h	
		PMMSWPOR software POR (POR)	14h	
		WDTIFG watchdog time-out (PUC)	16h	
		WDTPW password violation (PUC)	18h	
		FRCTLPW password violation (PUC)	1Ah	
		Uncorrectable FRAM bit error detection	1Ch	
		Peripheral area fetch (PUC)	1Eh	
		PMMPW PMM password violation (PUC)	20h	
		Reserved	22h	
		FLL unlock (PUC)	24h	
		Reserved	26h to 3Eh	Lowest

Software can read the SYSRSTIV register at beginning of the user code to identify the reset source. An LED connected on a GPIO can be programmed to blink with different patterns to indicate different reset sources. For system-level ESD, normally SYSRSTIV can be used to check reset source of power, I/O, the reset pin, watchdog, clock, and memory. For example, if SYSRSTIV readout value is 0x04, the reset source was the $\overline{\text{RST}}$/NMI pin.

3.2.2 Oscillator Fault Detection

Oscillator failure is another failure scenario for MCU system-level ESD tests. During ESD test execution, noise will interfere into the crystal oscillation circuits from conductors on the board or from the air. If the oscillation is weak between the crystal and the MCU oscillator pins, the clock will fail during the ESD tests. If the crystal clock sources a DCO+FLL reference clock and the MCLK/SMCLK source is set to the DCO clock, the ESD test may impact the oscillator behavior and may cause the MCLK/SMCLK clock to fail. Then the system will run with unexpected behavior for CPU or peripherals.

How to know if the ESD failed case is related to the external crystal? The following check points are recommended for reference:

1. Switch the MCLK/SMCLK clock source from external crystal to internal oscillator and perform the ESD test again.
2. Monitor the crystal fault registers. The corresponding oscillator-fault interrupts can also be enabled to check oscillator failures. The register name is different in different MSP430 devices. Some examples include OFIFG, LFXT1OF, XT2OF, LFXTOFFG, HFXTOFFG, and XT1OFFG. See the oscillator-fault logic section in the family user's guide for details.
3. Use external oscillator to feed into the XIN pin and the crystal oscillator is configured to bypass mode.

Software can blink an LED or send a message through a communication interface to indicate the cause of the failure.

3.2.3 Software Workaround

If the reset source is identified, the corresponding solution can be checked. Normally, a software workaround is preferred because it is faster than a hardware workaround, which requests longer time for test. MSP430 MCUs provide some features for software workaround trial.

1. The $\overline{\text{RST}}$/NMI pin can be configured to NMI mode.

   If the reset source is the $\overline{\text{RST}}$/NMI pin, configure the $\overline{\text{RST}}$/NMI pin to NMI functionality to see if there is any improvement for the ESD test.

2. The glitch filter can be configured on I^2C and UART signals in the eUSCI_B and eUSCI_A modules through the UCBxCTLW1 and UCAxCTLW1 registers.

   This feature may be a workaround if the ESD failure scenario involves the I^2C or UART communication and the root cause is a glitch on the communication lines. Table 2 is an example for the deglitch time settings from the MSP430FR604x data sheet.

Table 2. Example of eUSCI (UART Mode) Glitch Filter Setting

PARAMETER		TEST CONDITIONS	V_{CC}	MIN	TYP	MAX	UNIT
t_t	UART receive deglitch time[1]	UCGLITx = 0	2.2 V, 3.0 V	5		30	ns
		UCGLITx = 1		20		90	
		UCGLITx = 2		35		160	
		UCGLITx = 3		50		220	

(1) Pulses on the UART receive input (UCxRX) shorter than the UART receive deglitch time are suppressed. Thus the selected deglitch time can limit the maximum useable baud rate. To ensure that pulses are correctly recognized, their duration should exceed the maximum specification of the deglitch time.

3. Critical register and memory write protection should be enabled.

   Memory write protection should be enabled when building the code. In MSP430 devices, there are passwords to protect critical registers (memory controller, PMM, Watchdog, BSL, JTAG) from unintended access. Some password violations trigger a PUC reset that can be read from the SYSRSTIV register after reset.

   In MSP430FR5x and MSP430FR6x devices, the Memory Protection Unit (MPU) module can protect against accidental writes to designated read-only memory segments or execution of code from a constant memory segment.

   In MSP430FR2x and MSP430FR4x devices, the PFWP and DFWP bits in the SYSCFG0 register can protect against any unintended memory writes to user program memory section or information memory section.

   In system-level ESD tests, memory protection enabled can help to avoid failures related to memory corruption. It is recommended to check if the setting is correct for the memory write protection before the ESD tests. See *MSP430 FRAM Technology – How To and Best Practices* for more details about how to use the MPU in the Code Composer Studio™ IDE and the IAR Embedded Workbench® IDE.

4. The CRC module and memory controller built-in access error detection can be used for the memory integrity analysis.

   Many MSP430 devices have integrated cyclic redundancy check (CRC) module. This module can be used to check if the memory (RAM, flash or FRAM) has been unintendedly changed by system-level ESD tests.

   In MSP430Fxx devices, the flash memory controller has the ACCCIFG register to indicate whether an access violation occurs. In MSP430FRxx devices, the FRAM controller has the CBDIFG and UBDIFG registers to indicate if there is correctable error or uncorrectable bit error detected. See the device family user's guide for details.

5. Peripherals registers can be tested.

   The following are examples of tests. The LCD frequency can be changed for a new trial if the LCD fails. The oscillator drive strength can be increased for a trial if the failure is related to crystal. GPIO drive strength can be checked if the failure is related to the GPIO output. Serial communication speed can be reduced if the failure is related to the UART, SPI, or I^2C.

6. If the clock is impacted during the ESD test to cause the failure case, the following methods can be tried to see if there is any improvement.
   a. Check the clock source. If the clock source is a crystal clock, switch the clock source to an internal clock source.
   b. Change the frequency setting of the clock.
   c. Enable the oscillator modulation mode.

Software workarounds may not be effective every time. If the system still cannot pass the ESD tests, hardware debug, troubleshooting, and workarounds need to be considered.

3.3 Hardware Troubleshooting Guidelines

Normally, hardware troubleshooting take more time than the software method because the EUT enclosure, mechanical, cable connection, or board layout may need to be changed. It is better to have an efficient software simulation tools to do the system-level ESD simulation and then use Signal Integrity/Power Integrity (SI/PI) simulation to address the board weak points before the board fabrication. Then the potential EMC issue can be avoided in the design phase.

The ESD simulation tool is also very helpful when debugging the ESD test failures. But the ESD simulation is not very easy to implement because accurate modeling setup is relatively difficult and the simulation tools are normally expensive. So in most cases, hardware troubleshooting and workaround are required.

Generally, the system-level ESD issue troubleshooting is conducted from two respects.

- Path control for noise transmission

  Guide the noise to transmit to GND quickly without passing the critical sensitive components.
- Improve the noise filter performance

  Try to filter the noise in noise transmission path.

It is recommended to start the system review from these two aspects. The following are hardware debug examples recommended for trial.

1. Review the enclosure mechanical construction around the PCB. Try to reduce the ESD leakage possibility. Check if there is good grounding for the metal on the enclosure. If there is floating metal on the enclosure close to the PCB, try to move the PCB or sensitive components far away from the metal. Cable entry is another important point to review. See *MSP430 System-Level ESD Considerations* for design guidelines including enclosure grounding, openings, and cable entry.
2. Review the PCB layout. Check the ESD noise transmission path from the discharge point. Place critical components far away from the path. Try to reduce the transmission path resistance, or change the path by board layout rework. Adding isolation is also a path control option. Signal return path is very important, especially for the sensitive signals. See *MSP430 System-Level ESD Considerations* for more PCB design guidelines.
3. If the root cause of the failure is as related to the crystal clock, try to increase the crystal circuit robustness by checking the load capacitance match, crystal circuit layout and drive strength setting. See *MSP430 32-kHz Crystal Oscillators* and *MSP430 System-Level ESD Considerations* for more details about the crystal circuit design.
4. Use recommended reset circuit for better reset pin protection

   The reset pin and test pin signals are important for SBW communication. Keep these two signal traces as short as possible in board layout. In addition, from the MSP430 data sheets and the *MSP430 Hardware Tools User's Guide*, the parallel capacitor on the reset trace should be less than 2.2 nF or 1.1 nF. When a large noise occurs on the reset pin, the capacitor may not be enough to filter. To improve this, the circuit in Figure 2 is recommended to increase the filter capability for the noise on the reset pin.

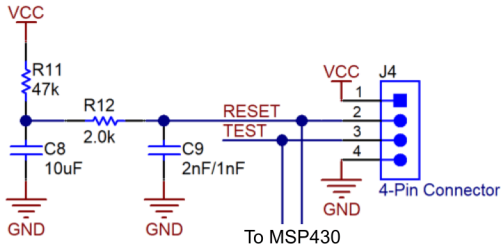


Figure 2. Recommended SBW Circuit for MSP430 MCUs

In the Figure 2, a 10-µF or larger capacitor can be used for C8. Resistor R12 works as isolation for the capacitors C8 and C9. With this circuit, JTAG and SBW can work well and the noise filter capability of the reset signal path is also improved.

5. Add a pulldown resistor on the TEST pin

   The TEST pin has built-in pulldown resistor to confirm it is in low logic during firmware execution. Normally, the built-in pulldown resistor is weak. Add an external smaller pulldown resistor to see if the ESD failure is related to a TEST pin logic error.

6. Add a series resistor and parallel capacitor in long signal traces to reduce the EMI impact

   The values of the series resistor and parallel capacitor to add depend on the signal speed and drive strength. Normally, the value should not be big so that the signals are not impacted too much. If the ESD failure is related to the LCD, this method can be tried.

7. Increase the decoupling capacitor value or add TVS for power traces

   If the power trace is a weak point for the ESD test from the reset source check introduced in Section 3.2, increase the decoupling capacitor value for trial. A capacitor bigger than 22 µF can be tested. Power TVS can also be added for the test.

   If there are multiple boards in the system and the power is transmitted on an internal cable, add a decoupling capacitor on the power pin at the receiving connector side.

8. Add TVS on signal traces connected to an external interface

   For signals connected to external interface, it is important to have ESD protection. A signal TVS can be used for this purpose. Serial resistors can also be an option. In addition to TVS, more ESD suppression devices can be used. See *MSP430 System-Level ESD Considerations* for more details.

9. Add shielding to isolate EMI impact over the air

   If the EMI noise from the air interferes with the EUT, add GND shielding between the EMI source and the EUT to isolate them.

10. Add GND shielding on cables connected between boards especially for flat cables.

11. Use the latest revision MCU material

    Usually newer version silicon have more reliable system-level ESD performance.

12. Use failure analysis process

    Some system-level ESD failures are hard to reproduce. Normally, a power cycle will recover the system and it is hard to reproduce it in short term. The MCU may have abnormal electrical behavior such as higher power consumption and big voltage drop. For this case, it is mostly like a latch-up issue occurs at some pins or modules of the silicon, and a failure analysis procedure for troubleshooting is discussed in Section 4.

Sometimes, several workarounds can work together to fix the issue.

3.4 Real Case for Troubleshooting a System-Level ESD Issue

In the post design phase of the meter product shown in Figure 3, it was reported that system-level ESD test cannot pass the defined standard level air-discharge at 15 kV. The meter product with MSP430 device always reset during the ESD test. This was indicated by the LED panel initializing.

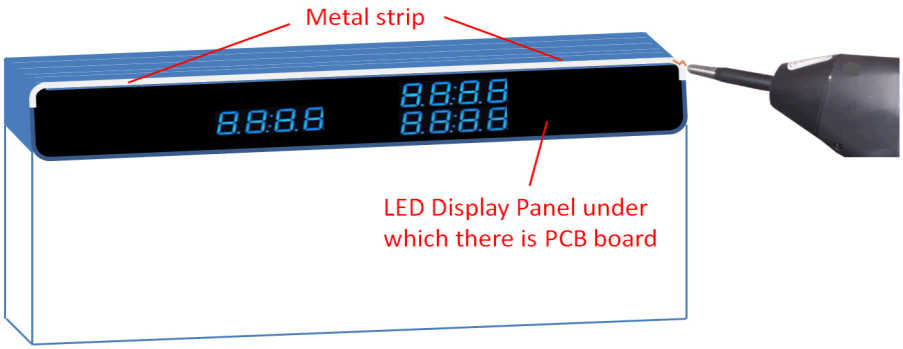


Figure 3. System-Level ESD Real Test Case – Metal Strip on the Enclosure

The following steps were conducted to resolve the issue.

1. Reproduce the failure case reliably

   There was a long metal strip around the upper edge of the LED panel of enclosure. When the ESD simulator discharged directly on the metal strip, the system reset.

2. Read the SYSRSTIV register

   The value was 0x02 for most times and 0x04 for several times. That means the ESD test failure is mainly caused by a BOR on the MCU, and the reset pin circuit also needed to be checked. So a voltage drop on the power was the root cause of the issue.

3. Review mechanical construction and layout

   It was found that the metal strip is floating because the metal was just a thin film on the long plastic strip. The MCU board was under the front panel. The plastic strip thickness is 2 to 3 mm. The PCB upper side was close to the strip where there were lots of long GPIO signal traces parallel with the strip. And the SBW 4-pin connector was in this area. The PCB is a two layers design and the GND return path was not good. There were no high speed signals on the board.

4. Tried software workarounds but failed

   Set $\overline{\text{RST}}$/NMI pin to NMI mode in the firmware and did the system-level ESD test again. But it still failed.

5. Tried hardware workarounds but failed.

   Use the recommended RESET circuit; cut off the RESET and TEST traces on the board; increased the decoupling capacitor and add TVS on MCU power input; added glue around upper side of the enclosure to improve the isolation between internal board and external metal strip; improve the GND return path.

6. Tried to move the board 20 mm away from the metal strip (manually change the mechanical installation).

   The ESD test was passed. That proved the distance between the board and the metal strip is the critical root cause. But the mechanical design was fixed and it would take long time for the mechanical rebuilt. So the customer would not like to change the mechanical design.

7. Changed the MCU to new revision silicon (keep the original mechanical installation)

   ESD test pass level was better. The failure of the ESD air-discharge level improved from 11 kV to 13.5 kV.

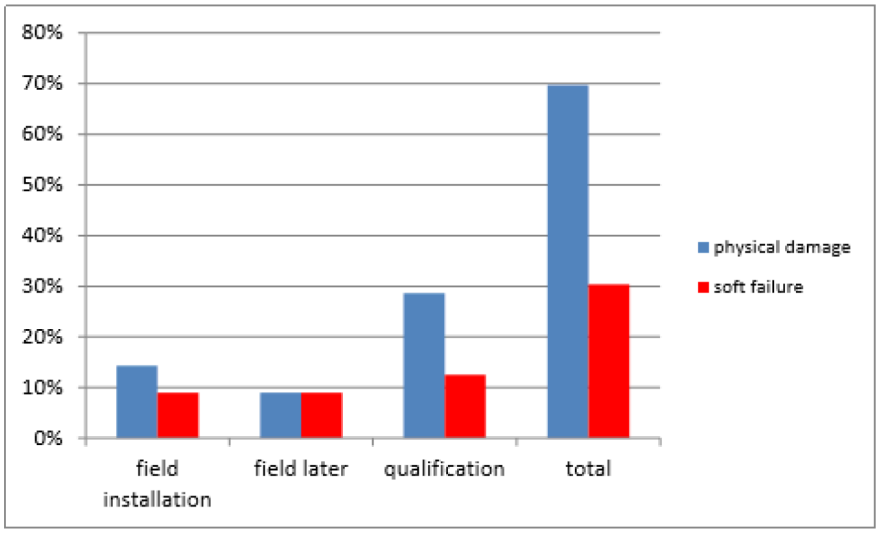
Recommended solution:

- Change the MCU to a newer version of the silicon.
- Improve the layout and build a new board for test
  - Move the SBW 4-pin connector to the back side of the PCB so that the reset and test signal traces can be far away from the metal strip.
  - Use the recommended reset circuit.
  - Optimize the layout to place the parallel GPIO long signal traces far away from the metal strip.
  - Increase the decoupling capacitor value for DVCC.
  - Add power TVS at LDO output for the MCU.

Test result after applying the recommended solution: ESD test passed 15-kV air discharge with 100% pass rate at 3 boards.

4 System-Level ESD Failure Analysis Procedure

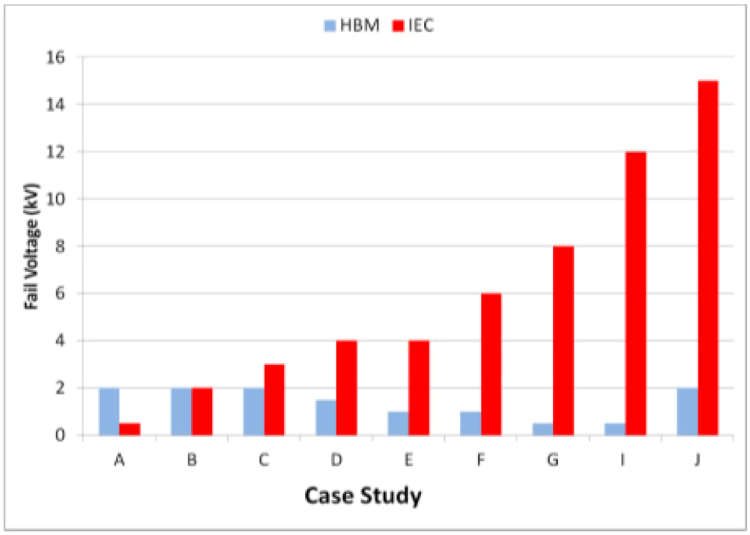
As mentioned in Section 2, system-level ESD can result into two failure categories: 1) physical damage and 2) soft failure. Reference [5] studied 58 system-level ESD cases, which covered the full range from system qualification, to field installation and field failure after installation. Figure 4 shows the two failure types seen from these 58 system-level ESD cases.



NOTE: From Reference [5]

Figure 4. Types of Failures and When Failure Occurred of System-Level ESD

Furthermore, the system-level ESD stress and application were totally different from component ESD (HBM and CDM), so there is no correlation between both modes in the real cases. Figure 5 shows the failure level comparison between system-level ESD and component HBM ESD mode. So analysis focusing on the real system or application can help with system-level ESD troubleshooting and problem solving.



NOTE: From Reference [5]

Figure 5. Component HBM and System-Level ESD Fail Level Comparison

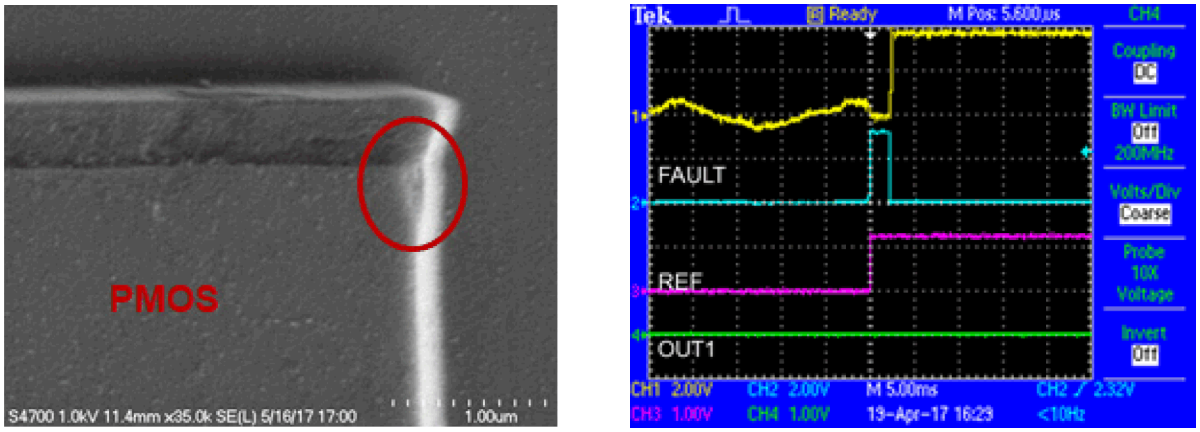
When encountering system-level ESD or EMC problem, the fail analysis plays a unique role to localize the failure location and identify the failure trigger source by utilizing some special equipment. The analysis finding can support to work out a solution and to build a robust system against the ESD in the application environment.

4.1 Failure Analysis Role and Procedure

Failure analysis has structural steps to support root cause determination and identification. Figure 6 presented a typical failure analysis procedure. This is indeed not an automatic process. Normally the different types of failures (ESD, EOS, functional, or parametric) dictate the diverse and logical paths for the analysis to be successful.

Figure 6. Failure Analysis Procedure

Failure analysis is a good tool to disclose if there was physical damage caused by the system-level ESD. This damage can present as an abnormal electrical signal detected by, or example, ATE or bench test. Figure 7 shows an example of PMOS damage by a system-level ESD test that caused abnormal output. Because the power of the ESD strike is not enough to cause a large damage area on silicon die, it can be difficult to visualize small damage on die, like the tiny damage of the PMOS case. It may apply more efficient to use failure isolation techniques (for example, IR, LSM, EMMI, or probing) and sample preparation methods (for example, backside analysis or FIB) to limit the analysis time consumed.



(a) ESD strike at PMOS of OUT1 circuit (b) No signal on OUT1

Figure 7. Images of System-Level ESD Failure Case

Regarding soft failures caused by system-level ESD, the silicon die of the impacted MCU might not present physical damage. Hot spot analysis as a failure analysis technique can complement the methods of troubleshooting discussed in Section 3. The hot spot analysis technique uses microthermography to inspect the excessive heating area on die. Excessive heating normally indicates unexpected current flow as the soft failure mode of system-level ESD. The difficulty of the hot spot analysis is how to stabilize the failure phenomenon when processing the analysis procedure. One real case of soft failure by system-level ESD was studied in Section 4.2 by hot spot analysis technique.

4.2 Real Case Scenario of System-Level ESD Failure Analysis

A line failure for a meter application was reported. The failed meter experienced a problem with "low-battery" indication soon after battery insertion. The problem would go away if the meter lost power or was power cycled. This means the failed meter did not encounter physical damage. So the failure phenomenon was indicated as a soft failure.

Board-level analysis on the failed meter found that the core MCU was drawing an extra 20-mA current through V_{CC}, which was an unexpected behavior. Ideally the high amount of current can only occur by two reasons: I/Os being driven out at high current, or latch-up trigger on the MCU. During the debugging, the I/Os were isolated on the failed meter, while still can detect the 20-mA current on the MCU. So the possible latch-up on MCU was suspected which needed to be analyzed.

After reviewing the schematic, the meter system has a direct-battery power supply, shown in Figure 8. No ordinary way for improperly voltages could generate extra current on MCU. The system-level ESD event could be the possible source to trigger the latch-up and lead to the unexpected 20-mA current on MCU. The failure analysis was then done on the MCU to identify which pin or pins had the extra current flow. Hot-spot analysis is the most appropriate method for this the failure signature.

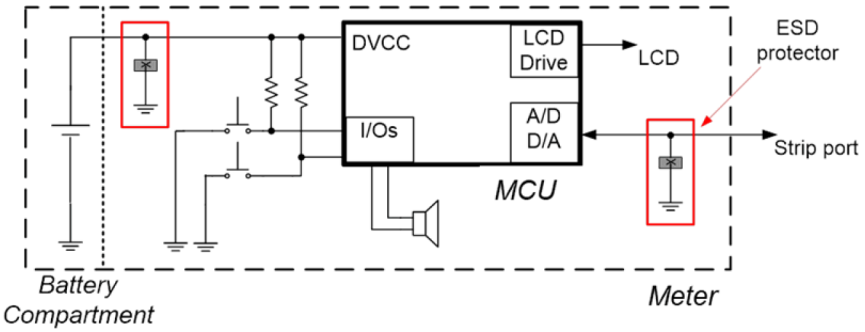
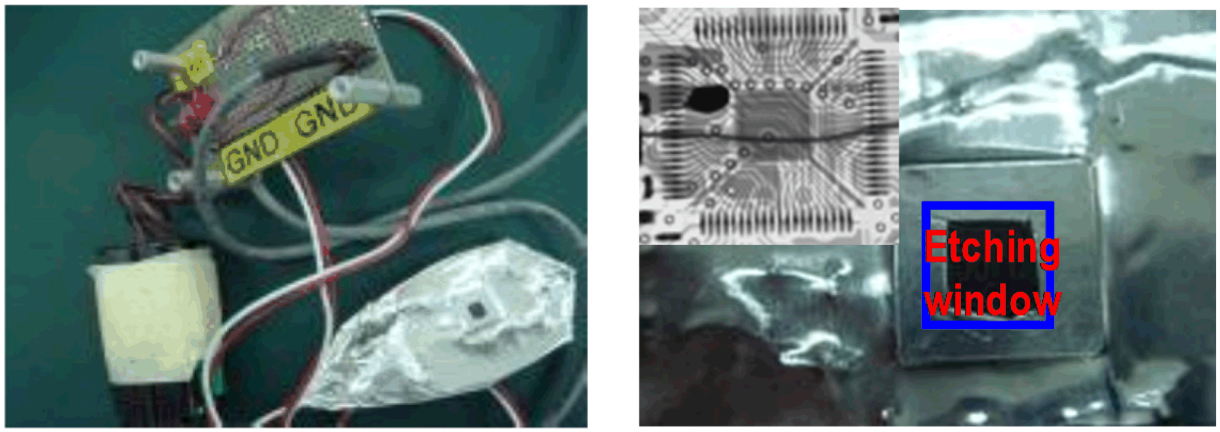


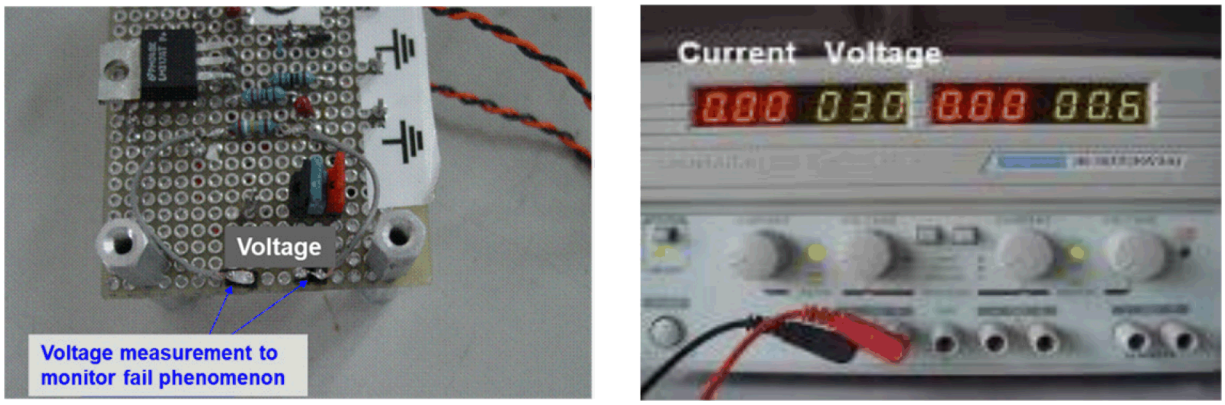
Figure 8. Typical Schematic Showing Meter Power Supply Structure

A special battery fixture was designed to supply the failed meter with continuous power. This avoided failure recovery due to the meter losing power. This test needed sample preparation to expose the die from its package of the powering MCU, showed in Figure 9. During each analysis step, the test also needed to monitor the extra current to the MCU to see if the failure persisted or recovered. The voltage at the specific locations to the failed meter was measured, which indicated the MCU had unexpected current. Figure 10 shows the test board connected between meter board and power supply.



(a) MCU enwrapped with acid-free tape (b) Defined etching window of the package

Figure 9. Photos Showing Sample Preparation



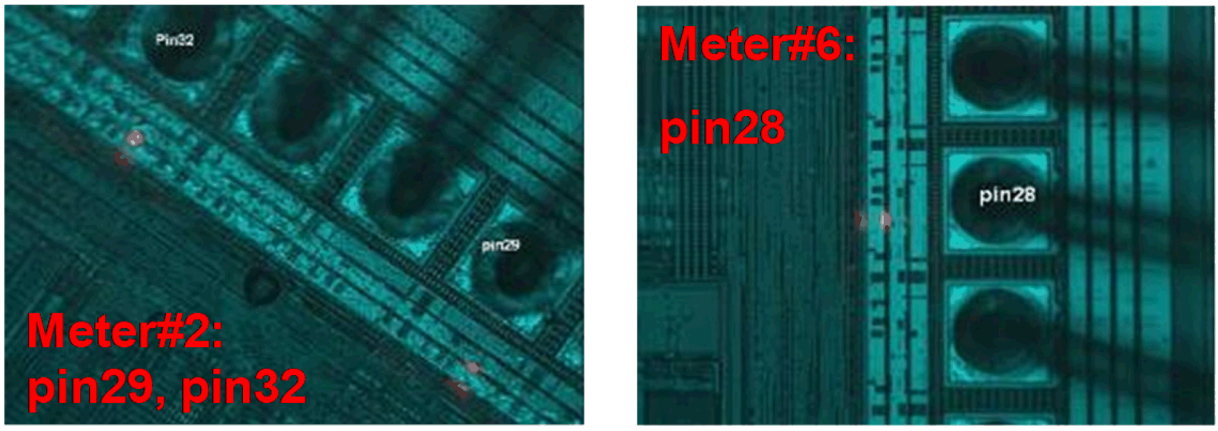
(a) Powering meter through test board (b) Meter powering monitor

Figure 10. Photos Showing Meter Continuously Powering During Hot Spot Analysis

Six failed meters were analyzed, and meter 1 was selected to trial the sample preparation and handling with lesson learn for improper handling. The remaining five failed meters (meter 2 to meter 6) were successfully prepared to expose the MCU die for the hot spot analysis. Figure 11 shows the typical hot spot images. The emission hot spots were observed at the MCU LCD pins of failed meters (see Table 3).

Table 3. Hot Spot Pins on MCU of Failure Meters

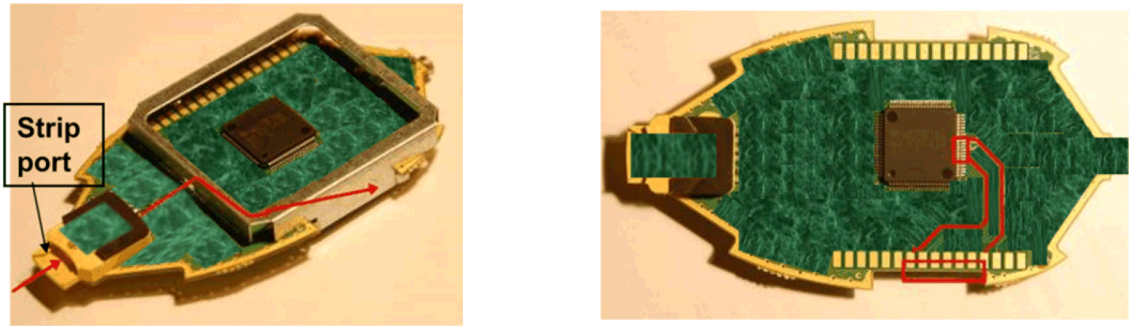
Failed Meter	Hot Spot LCD Pin
2	Pin 29 and pin 32
3	Pin 28
4	Pin 30
5	Pin 27
6	Pin 28



(a) Image of meter 2 (b) Image of meter 6

Figure 11. Emission Hot Spot Images of MCU Die

Further reviewing the meter board, it was apparent that a system-level ESD strike could be traveling from the strip port and causing MCU latch-up as shown in Figure 12. We found a large metal bracket in the meter board as shown in Figure 12(a). The bracket was clipped on the board but not soldered with possible weak grounding. And the tolerance between the LCD pads and the bracket was also found to be smaller than recommended, and shown in Figure 12(b). So the ESD protectors on the board could allow ESD from the strip port to jump to the bracket, then jump to the LCD pads, and finally travel to the MCU to trigger the latch-up and lead to the meter failure of "low-battery" at line.



(a) Photo showing ESD traveling from strip port to metal bracket on meter board

(b) Photo showing connection between metal bracket on meter board and LCD driver pins of MCU

Figure 12. Photos of System-Level ESD Strike Route

Based on the failure scenario of the analysis, the following solution was proposed:

1. Replaced the weak ESD protectors with diode-clamp protectors on the board.
2. Improved the grounding of the LCD bracket on the board.
3. Improved the tolerance between the bracket and the LCD pads on the board.

This case shows how to identify the problem through the hot spot analysis technique. The analysis also supports building a more robust system against system-level ESD for the application, which can be used in system-level ESD troubleshooting and problem solving.

5 References

1. IEC 61000-4-x Tests for TI's Protection Devices
2. MSP430™ System-Level ESD Considerations
3. Electrostatic Discharge (ESD)
4. Causes of the ESD immunity testing problems in the IEC 61000-4-2 standard (https://iopscience.iop.org/article/10.1088/1742-6596/418/1/012049/pdf)
5. White Paper 3, System Level ESD, Part II: Implementation of Effective ESD Robust Designs, Mar. 2019 (http://www.esdindustrycouncil.org/ic/en/documents/36-white-paper-3-system-level-esd-part-ii-effective-esd-robust-designs)
6. MSP430™ FRAM Technology – How To and Best Practices
7. MSP430™ 32-kHz Crystal Oscillators
8. MSP430™ Hardware Tools User's Guide

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

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