

Designing Electronic Systems For ESD Immunity

Here's A Comprehensive Checklist To Ensure That Your System Is Properly Protected

This article describes over 140 different ways to make your electronic equipment and electronic products immune to electrostatic discharge (ESD). Many of these techniques can also improve your system's electromagnetic compatibility (EMC), electromagnetic interference (EMI), and overall robustness.

An ESD arc is an intense noise source with significant energy from 1MHz to 500MHz. This energy penetrates your system by every means possible, coupling into cables and printed circuit boards (PCBs), and may cause system upsets, lock-ups or unwanted resets, as well as lost data and risk of permanent damage.

The key to effective immunity against ESD is to begin early in development, following conservative design practices and providing "wobble room" in areas where you may need to tweak your design. ESD testing throughout development can also help you to find and fix weak spots as you go.

Specifically, we defend against ESD by reducing the coupling into your system, and by making the system immune to transients through use of any or all of the following methods:

- Plastic enclosures, air space and insulation.

- Metal enclosures and shielding.
- Grounding and bonding.
- Power distribution, bypassing and decoupling.
- PCB design and mounting.
- Cable design and routing.
- Filters and transient suppressors.
- Robust components.
- Robust circuit design.
- Watchdog timers.
- Software.
- ESD testing to find and fix weak spots.

Plastic Enclosures, Air Space And Insulation

Plastic enclosures, air space, and insulation prevent ESD arcs to a system (direct ESD):

1. For $\geq 20\text{kV}$ breakdown voltage, keep $\geq 20\text{mm}$ air-path length between electronics and:
 - Any points that users can touch- including ventilating/mounting holes and seams.
 - Any ungrounded metal parts that users can touch- including controls, indicators, and fasteners.
2. Recess PCBs and cables in the enclosure, or use tongue-in-groove or shiplap seams.
3. Cover unused connectors.

John R. Barnes
dBi Corporation

4. Choose switches and controls with plastic shafts, or put plastic knobs (without metal setscrews) on metal shafts.
5. Cover LEDs and indicators with insulating overlays, tape, caps or lightpipes.
6. Keep traces on membrane keyboards $\geq 12\text{mm}$ inside the border, seal the circuitry layers, or add a plastic bezel.
7. Keep traces on tactile rubber keypads in tight, and extend the rubber top layer.
8. Round corners and edges on heatsinks and metal parts that are close to ventilating/mounting holes and seams.

Metal Enclosures And Shielding

Metal enclosures and shielding intercept ESD arcs and their electric, magnetic and electromagnetic fields, also protecting your system from external arcs (indirect ESD):

9. Provide for $\geq 20\text{kV}$ breakdown voltage between ungrounded enclosures and electronics, and $\geq 1.5\text{kV}$ breakdown voltage ($\geq 2.2\text{mm}$ air-path length) between

- grounded enclosures/shields and electronics.
10. Design plastic enclosures to accommodate shields made of:
 - Sheet metal
 - Mylar/copper or Mylar/aluminum laminate
 - Thermoformed metal mesh, metallized fiber mat, or metallized fabric
 - Silver, copper or nickel paint
 - Electroless plating
 - Zinc arc spray
 - Vacuum metallization
 - Highly-conductive fillers in the plastic (require special inserts to make contact)
 11. Aim for ≤ 1 ohm/square resistance, using low resistivity metals (see Table 1).
 12. Choose compatible materials for shields, fasteners, and gaskets to minimize corrosion (see Table 1):
 - EMFs within 0.75V (0.25V for salt-spray environments) for surfaces that will be in contact
 - Surface area of anodic part(s) larger than cathodic part(s)
 13. Overlap seams in shields by ≥ 5 times the gap.
 14. Bond seams in shields at least every 20mm (0.8") with welds, dimples, fasteners, fingerstock, or conductive gaskets.
 15. Don't nick, crack, or thin shields- make gentle bends and rounded corners.
 16. Make holes ≤ 20 mm (0.8") diameter and slots ≤ 20 mm (0.8") long; space openings apart by their largest dimension; use many small openings instead of one/a few big ones.
 17. If a control/indicator requires a larger opening, put a secondary shield between it and the electronics.
 18. For grounded equipment, connect shields to chassis ground at the connector entry point.
 19. For ungrounded equipment, connect shields to circuit common near switches and controls.
 20. Put a secondary shield parallel and close to susceptible electronics, connected to chassis ground/circuit common at the cable connection point.
 21. Put cable entry points near the center of conductive panels.
 22. Use alodine, iridite or chromate coatings on aluminum, and conductive chromate coatings on steel.
 23. Mask or scrape off anodizing and paint from seams, joints and connectors.
 24. Don't depend on hinges or screws for bonding. Force clean metal surfaces into direct contact.
 25. Put a ground plane next to a double-
-

sided card, connected to ground on the card at close intervals.

- 26. Bond displays with a shielding coating to the enclosure, around the entire periphery.

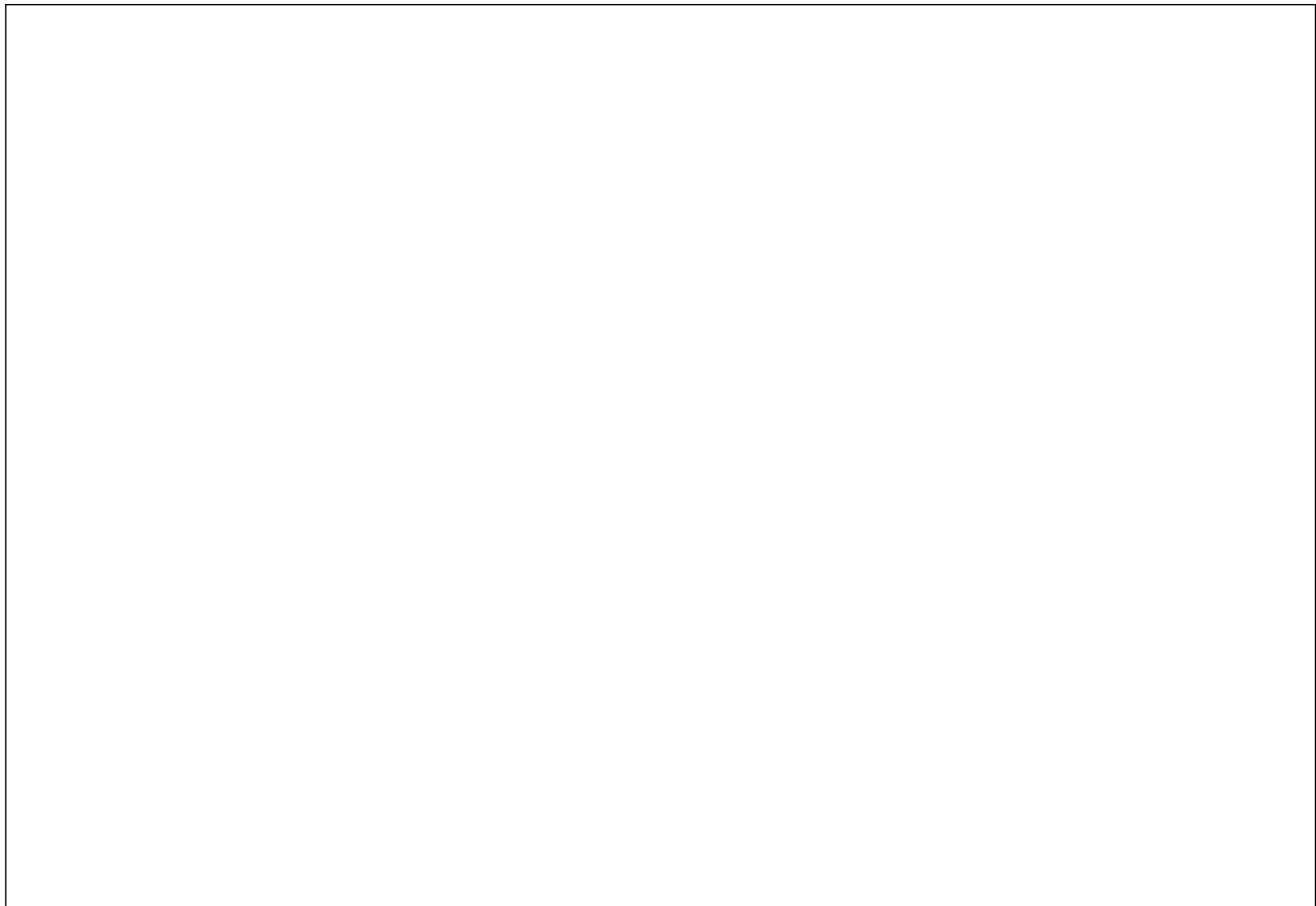
Grounding And Bonding

Current from an ESD arc follows every available conductive path from the point of contact. Bonding minimizes the voltage drops along these current paths, while grounding drains off the charge:

- 27. Keep the ESD current density and the current-path impedances as low as possible by using multipoint grounds where you want the current to flow, and single-point grounds where you don't.
- 28. Weld, braze, sweat or swage metal parts that don't need to come apart.
- 29. Bond metal pieces that must come apart by:

- Direct metal-to-metal contact between clean surfaces, held tightly together.
 - Direct contact between metal surfaces with thin conductive coatings, held tightly together.
 - Dimples or outside-star washers (to pierce paint/grease/insulating films) compressed between the metal surfaces.
- 30. Protect bonds from moisture.
 - 31. Put multiple bonding straps or jumpers across hinges.
 - 32. Position bonding straps or jumpers away from PCBs and cables.
 - 33. Use solid bonding straps ≥ 5 mm wide where possible, braided bonding straps and stranded bonding jumpers where you must.
 - 34. Choose compatible materials for bonding straps/jumpers and fasteners (see Rule 12).
 - 35. Make bonding straps short and wide, with width $\geq 1/5$ the length

- and preferably $\geq 1/3$ the length.
- 36. Make gaskets ≥ 5 mm wide.
- 37. Bring chassis ground to within 40mm (1.6") of each cable entry point.
- 38. Connect chassis ground to metal pieces of the enclosure, connector housings, switch housings, and control shafts (via grounding fingers or conductive bushings).
- 39. Connect the grounds on all the boards inside an enclosure with multiple conductors.
- 40. Connect chassis ground to circuit common with a ferrite bead.
- 41. Encircle a membrane keyboard/rubber keypad with a wide chassis-ground guard ring, connected to the metal enclosure all around the periphery, or at least at all four corners- don't connect this guard ring directly to circuit common.



Power Distribution, Bypassing And Decoupling

Power distribution networks are prime targets for inductive coupling from ESD:

42. Use multilayer PCBs with paired power/ground planes.
43. Use tightly-interwoven power/ground grids on double-sided PCBs:
 - Route power traces next to ground traces.
 - Connect vertical and horizontal traces/infill with vias wherever possible.
 - Keep power/ground grids $\leq 60\text{mm}$ (2.4") on a side, and preferably $\leq 13\text{mm}$ (0.5") on a side.
44. Provide plenty of ceramic bypassing/decoupling capacitors on PCBs, close to their circuits/connectors.
45. Tightly twist power wires and their returns together.
46. Put a ferrite bead in each power line where it enters a PCB.

Metal	Electromotive Force (EMF), volts	Resistivity, nano ohm-meters
Magnesium	(anodic, corrodes) +2.37V	42
Magnesium alloys	————	50 - 175
Aluminum	+1.66V	27
Zinc	+0.76V	60
Galvanized steel	————	100 - 197
Aluminum alloys	————	27 - 86
Chromium	+0.74V	132
Cadmium	+0.40V	73
Mild steel	+0.44V	100 - 197
Iron	+0.44V	101
Tin-lead solder	————	145 - 195
Stainless steel	————	560 - 780
Lead	+0.13V	206
Tin	+0.14V	126
Nickel	+0.25V	69
Brass	————	61 - 110
Beryllium copper	————	29 - 115
Copper	-0.34V	17
Bronze	————	91 - 212
Monel	————	510 - 614
Silver solder	————	22 - 172
Titanium alloys	————	482 - 1700
Silver	-0.80V	16
Titanium	+1.63V	540
Gold	-1.50V (cathodic, passive)	22

Table 1: Galvanic Series (in order of decreasing EMF)

47. Put a ceramic 1kV capacitor, metal-oxide varistor (MOV), or transient suppressor between each power pin in a connector and chassis ground.

PCB Design And Mounting

Intelligent PCB layout is our best weapon against ESD, and can incorporate most of the techniques described in this article:

48. Design any protection circuits that you might need into your original layout ("wiggle room"). You can leave these components unpopulated or replaced by 0-ohm resistors if they aren't needed:
 - Put the protection circuit at the connector (preferred), or $\leq 25\text{mm}$ (1") from the receiver/driver.
 - Position the components to minimize parasitic capacitance, mutual inductance, and the wiring common to the input and output of the protection circuit.
 - Use short and wide traces (see Rule 35) to chassis ground/circuit common.
 - Route signal and ground to the protection circuit, then to the receiver/driver.
49. Make provisions for changing the grounding scheme, especially circuit common to chassis ground connections:
 - Run chassis ground along PCB edges that have connectors to the outside world; use wide traces in all layers, tied together by vias about every 13mm (0.5").
 - Connect chassis ground to the connector housings and to any mounting holes on these edges. Use topside and bottomside pads without soldermask, put vias around the mounting holes, and don't get solder on these pads during assembly. Screws with built-in Belleville washers connect the pads to tabs/metal standoffs on the chassis/shield.
 - Make provisions for isolating/connecting other mounting holes to chassis ground- isolated pads with 0-ohm resistors to circuit common, choice of plastic or metal standoffs, etc.
 - Separate circuit common/power from chassis ground by an identical 0.64mm (0.025") wide moat in all layers.
 - Connect circuit common to chassis ground by ground ties (1.27mm (0.050") wide traces on the top and bottom layers) paralleled by pads for ferrite beads/capacitors at mounting holes and every 100mm (4") along the moat.
50. Put a circuit-common guard ring around the rest of the PCB:
 - $\geq 2.5\text{mm}$ (0.1") wide in every layer you can, stitched together by vias about every 13mm (0.5").
 - Keep signal traces $\geq 0.5\text{mm}$ (0.020") inside this guard ring.
51. Use multilayer PCBs with paired power/ground planes- they have 1-10% of the common-impedance and inductive coupling of equivalent double-sided PCBs:
 - Put each signal layer next to a ground/power layer.
 - Use a "submerged trace" scheme; top and bottom layers

have components and short traces, completely surrounded by ground; otherwise the signal/power wiring is on the inner layers, essentially encased in a Faraday cage.

52. Put all connectors on one edge if you can.
 53. Put input/output circuits close to their connectors.
 54. Put ESD-susceptible circuits at the center of the PCB.
 55. Keep circuits compact.
 56. Put vias solid into power/ground planes.
 57. Make all signal traces as short as possible.
 58. Parallel signal traces that can get direct ESD hits, and signal traces $\geq 300\text{mm}$ (12") long, by ground traces.
 59. Keep resets, interrupts, and edge-triggered signals away from:
 - The edges of the PCB.
 - Unprotected input/output signals.
 60. Where permitted, fill in unused areas with ground, with layers tied together by vias at least every 60mm (2.4")- patches exceeding 25mm x 6mm (1" x 0.25") should have at least two connections to ground at opposite ends.
 61. If accidental slots in power/ground planes are longer than 8mm (0.3"), stitch the sides together with traces.
65. If you can't reach chassis ground, connect a cable shield to circuit common with a 1-10nF 1kV capacitor or an anti-parallel pair of diodes.
 66. Choose compatible materials for mating connectors, connector backshells, and cable shields (see Rule 12).
 67. Minimize loop area inside cables by providing one ground wire per 1-5 signal wires; use S-G-S-S-G-S-G-S for flat cables.
 68. If a cable has spare wires:
 - Connect them to circuit common at both ends.
 - Connect them to ground/power/signal wires at both ends.
 - Clip them short, so they are completely enclosed by the shield.
 69. Prefer coaxial cable, or twisted pair with at least 4 twists in the shortest wavelength of concern, to round cable or flat cable.
 70. Choose cable shields:
 - $\geq 0.025\text{mm}$ (0.001") thick.
 - Prefer foil or foil-and-braid shields to braid shields, with metal-to-metal contact at the overlap.
 - $\geq 85\%$ optical coverage for braid shields.
 71. Choose connectors with dimpled contacts between the mating connector shells, and between the connector shells and backshells.
 72. Fit ferrite sleeves on cables so that they encircle everything except the shield or shield drain wire(s).
76. Cascade low-pass filters (frequencies of f, $30*f$, $1000*f$, etc.) if needed. Filters are usually effective only up to 100-1000 times their design frequency.
 77. Follow power-line filters with high-frequency ESD filters.
 78. Configure protection circuits as:
 - A blocking device.
 - Shunt device(s) to chassis ground/circuit common.
 - An L-network, with a blocking device and shunt device(s) to chassis ground/circuit common.
 - A pi-network, with shunt device(s) to chassis ground, a blocking device, and shunt device(s) to circuit common.
 79. Connect blocking devices to ESD sources and low-impedance drivers/receivers:
 - $\leq 100\text{k}$ resistors for CMOS inputs.
 - $\leq 50\text{-ohm}$ resistors for bipolar inputs.
 - Ferrite beads if low resistance is important. They provide 50-500 ohms impedance from 10-1000MHz.
 80. Connect shunt devices to high-impedance drivers/receivers:
 - 100-1000pF capacitors to chassis ground.
 - 10-100pF capacitors to circuit common.
 - Clamps to chassis ground/circuit common.
 - Crowbars to chassis ground/circuit common.
 - Keep leads very short- 1nH/mm lead inductance slows down turn-on.
 - Connectors are available with built-in capacitor arrays, ferrite sleeves, and MOV arrays.
 81. Limit transients to a safe voltage with clamps that turn on in $\leq 1\text{ns}$:
 - Reverse-biased diodes to power and ground, with a 100-200nF bypass capacitor nearby.
 - MOVs, multilayer varistors (MLVs), and multifunction capacitors (MFCs)- 0.5 ns turn on.

Cable Design And Routing

ESD can arc to the connectors on cables, while indirect ESD can couple into cables through induction or radiation:

62. Keep cables short.
63. Keep internal cables $\geq 50\text{mm}$ (2.0") from slots, seams, and bonding straps/jumpers, routed over continuous metal.
64. Terminate cable shields to the outside of the metal enclosure/shield, preferably with 360-degree bonds- short and wide connections (see Rule 35) may suffice, but keep unshielded sections of the cable $\leq 40\text{mm}$ (1.6") long.

Filters And Transient Suppressors

Filters and transient suppressors block ESD-induced voltages, and shunt ESD-induced currents elsewhere:

Determine the maximum capacitance you can put on the signal lines.

74. Put filters on resets, interrupts, and edge-triggered signals.
75. Put filters/transient suppressors on off-board receivers, and on off-board drivers for cables that can get direct ESD hits- including signals that go through opto-isolators.

- Zener diodes and avalanche diodes- 0.05 ns turn on; can put a standard diode in series to reduce the capacitance.
 - Limited by their maximum power dissipation.
82. Short out transients with crowbars that turn on in $\leq 1\text{ns}$ - trigger level must exceed the maximum signal level, and hold current must exceed the maximum loop current.
 83. Choose components to withstand ESD voltages and currents:
 - Thick-film and carbon composition resistors.
 - Shunt capacitors that may take direct ESD hits should be rated $\geq 1\text{kV}$, or be large enough to absorb $2.3\mu\text{C}$ without exceeding their voltage rating if they aren't protected by transient suppressors.
 84. Provide for the same protective circuitry on all the signals going through a connector, to keep common-mode noise from becoming differential-mode noise- running all the wires through a common-mode choke works well.

Robust Components

Choose robust active components to keep ESD transients from affecting the circuitry:

85. Choose active components that:
 - Are just fast and sensitive enough to do the job.
 - Have enough noise margin that small series resistors on their inputs and outputs will not affect them.
 - Have high noise/noise-energy immunity.
 - Have good ESD immunity (see Table 2)- upset usually takes about 10% of the damage-threshold voltage.
 - Have differential inputs and outputs.
 - Can read back all internal registers.
 - Are immune to latch-up.
86. Don't push components close to their design limits.

87. Test proposed substitute/second-source active components. They may have poorer immunity to ESD upset.
88. Prefer processors with fixed interrupt vectors over ones that read the interrupt address from memory.
89. Avoid programmable input/output chips. A configuration change can completely change their function.
90. Beware of chips with "one-way" instructions- ones that can be reversed only by hardware reset.

Robust Circuit Design

Design circuits such that noise ESD-induced transients cannot cause long-term effects, including upsets, unwanted resets, lock-ups, or lost data:

91. Tie unused inputs/bi-directional pins high or low through resistors.
92. Avoid edge-triggered logic; latch data with strobes instead of clock edges.
93. Do not connect resets, interrupts, or other edge-triggered signals to long cables.
94. Do not use circuits that can enter an endless wait/disabled state:
 - Halted.
 - Waiting.
 - Deadlocked.
 - Low-power mode.
 - I/O idle mode.
 - I/O invalid mode.
95. Give software control of peripheral chip resets.
96. Design peripheral circuits using "hold" or "ready" such that a reset will restore normal operation.
97. Give software a way to hardware reset the entire system, as a last-ditch recovery technique.
98. Make sure that ESD transients won't trigger power monitors.
99. Check parity/framing on data whenever you can.
100. Use differential signals wherever you can.
101. Isolate signals coming from the outside world with opto-isolators or transformers.

Watchdog Timers

Watchdog timers are circuits that monitor a "heartbeat" generated by the software- this heartbeat stops if the system hangs or the software "gets lost" because of ESD, whereupon the watchdog timer resets and restarts the system:

102. Connect the watchdog timer to master reset to force a cold start (all data lost on restart), or to a non-maskable interrupt (NMI) to force a warm start (some data retained on restart).
103. Use an edge-triggered input, so that the software must toggle the input to reset the watchdog timer.
104. Make sure that software cannot stop the watchdog timer once it has been started.
105. Design the software to periodically reset the watchdog timer. This code should be in as few places as possible, and preferably just one spot in the main loop.

Technology	ESD Damage Threshold (Volts)
MOSFET's	10 - 200V
Recording Heads	10 - 800V
VMOS	30 - 1800V
NMOS	60 - 500V
GaAsFET's	60 - 2000V
EPROMs	100 - 500V
Laser Diodes	100 - 1700V
JFETs	140 - 7000V
SAW devices	150 - 500V
CMOS	150 - 3000V
Op Amps	190 - 2500V
PIN Diodes	200 - 1000V
DRAMs	200 - 3000V
Schottky Diodes	300 - 2500V
Film Resistors	300 - 3000V
Bipolar Transistors	300 - 7000V
SCRs	500 - 1000V
ECL	500 - 2000V
Schottky TTL	500 - 2500V

Table 2: Immunity to ESD Damage

106. Design the software to run software and hardware sanity checks, including confirming that the watchdog timer is running, before resetting it.
107. Choose a period long enough to prevent timeouts when the system is operating correctly, even during rare events, but short enough to prevent danger if the system hangs and must be restarted.
108. Use a tight timeout during software testing to ensure that the watchdog timer won't time out during normal operation.
109. Provide a hardware method to disable the watchdog timer (disconnect it from reset/NMI) for product development, ESD testing, and servicing.
- Software**
- It takes a lot of work, but software can be designed to find and correct errors before they become dangerous, including errors caused by random transients like ESD:
110. Validate inputs from humans, other software modules, and hardware as soon as you receive them (and recheck them just before use), by checking:
- Type
 - Range
 - Framing
 - Parity/checksum/cyclic-redundancy check (CRC)/Error-correcting code (ECC)
111. Acknowledge correct data and return an error code for incorrect data.
112. Retransmit data if you don't receive an acknowledgement.
113. Read critical hardware inputs three times, several microseconds apart, and verify that they match before using them.
114. Use serial protocols that ignore a single high in a long string of lows, and vice versa.
115. If a peripheral uses an index register to access internal registers, set the index register just before doing critical reads/writes.
116. Don't let out-of-domain inputs affect program flow.
117. Check pointers, indexes, and index registers against the bounds of data structures, arrays, stacks and heaps before using them.
118. Check the count before entering a delay loop.
119. Immediately exit with an error if you find that the count is outside its legal range while executing a loop.
120. Point all unused interrupt vectors to an error handler.
121. Log abnormal events for later analysis.
122. Store critical data in multiple locations. Periodically crosscheck these locations and fix mismatched data.
123. Break large tables into fixed-length records, each with a checksum.
124. Protect blocks of data with parity bits/checksums/CRCs/ECCs.
125. Put redundant data (pointers, counts, type/status identifiers) into data structures for easy checking and repair.
126. Keep a copy of all output states in memory, and periodically:
- Reread control and selection inputs.
 - Refresh configuration registers and output ports.
 - Check memory, and correct errors.
 - Re-enable interrupts.
127. To regain control if the program counter "gets lost", put recovery code between routines, at the end of data tables, and in unused memory, with:
- A group of NOPs (as long as the longest instruction that the processor can execute) followed by a software interrupt, call, or jump to an error handler.
 - Two absolute jumps/calls to an error handler, located such that the data bytes match the opcode.
128. Do sanity checks before exiting a routine. Verify:
- A token that was written before calling the routine.
 - Checkpoint flags that are set at critical points in the routine.
 - A flow-check counter that is incremented in the routine.
 - The stack pointer is in a valid range.
 - The return address is to a code segment, and a CALL instruction precedes the return address.
129. Make sure that the error detection/warm-boot process is fast enough to find and correct errors before the system becomes dangerous.
130. Put a multibyte flag filled with mixed 1s and 0s in each volatile RAM as a power-loss indicator.
131. Try to restore the last correct state after an error. If this is unknown, go to a safe state, then notify the user and any attached units.
- ESD Testing**
- ESD testing points out weak spots that we have overlooked:
132. To work on the hardware's ESD immunity, run a specially-compiled version of the software:
- With the software ESD-immunity features disabled.
 - That continuously exercises all functions of the system without operator intervention.
 - That uses a LED/beeper/status display to warn that an error occurred.
133. Have product designers attend or help with the ESD testing.
134. Begin with indirect ESD tests, harden the system to that desired ESD-immunity level, and only then start running direct ESD tests.
135. Start testing at 2kV, and work up in 2kV steps until you see failures or have exceeded your desired ESD-immunity voltage by 1-2kV:
- Find target points with the ESD gun in continuous/fast-repetition mode using the air-discharge tip. Mark these points with chalk or water-soluble marker.
 - Test target points at both polarities before increasing the voltage.

- Zap each target point ≥ 50 times at a given voltage.
 - Zap at \leq one pulse per second. Slow down if the system uses error detection/recovery and needs to fully recover after an error, or if the system consistently passes the first few times you hit a target point, then consistently fails (you may be charging up something with a high-resistance discharge path).
 - Keep run/fail maps which show the voltage/polarity at which each target point fails.
136. Check supposedly identical ports early in testing to see if one of them is more sensitive than the rest. Then, concentrate your testing on this port.
137. Test the system in both operating and installation configurations, and at all customer-accessible points, including any service areas that the user may access.
138. If you have multiple sources for critical chips (microprocessors, and chips driving/receiving off-board signals) hand-pick the chips for your ESD-test system from the leading chip vendors.
139. If only a few spots seem to be vulnerable, turn out the lights and zap the system to try to see the discharge path.
140. Identify vulnerable cables by disconnecting the cable, or clamping a snap-on ferrite onto the cable next to the connector, and rerunning that section of the test.
141. If just one area is failing, try testing another unit:
- Similar symptoms at similar voltages/polarities indicate a design problem.
 - Different symptoms indicate a contact/bonding problem, cable position, or a marginal component (maybe damaged by the ESD testing).
142. Mock up shields/gaskets/bonding straps from aluminum foil and copper tape.
143. If a certain failure seems to come and go, check the seams and bonds near the target point.
144. If you install an ESD fix, but it doesn't seem to affect the ESD immunity, leave it in place until you have attained the system's desired ESD immunity. Then you can remove the ESD fixes one-by-one to determine which one(s) are effective.
145. Test software defenses with an emulator. Make random changes (one at a time) to registers, stack-pointers, the program counter, and data in memory, then watch what the system does.
146. Save your test system for comparison, in case field problems arise or production units show a sudden drop in ESD immunity.

Electronic engineers, PCB layout folks, mechanical engineers, and programmers must all cooperate to develop equipment and products with good ESD immunity. This is much easier when ESD immunity is considered throughout the design process, instead of treated as an afterthought. ■

About The Author

John R. Barnes is a NARTE Certified EMC and ESD Engineer and president of dB Corporation, an EMC/EMI/ESD testing laboratory. He can be reached at jrbarnes@iglou.com. The full bibliography of over 1500 sources for this article can be downloaded from the company's web site at www.dbcorporation.com/esd-anno.htm.