Design Techniques for EMC
Part 6 - ESD, electromechanical devices, power factor correction, voltage fluctuations, supply dips and dropouts

By Eur Ing Keith Armstrong C.Eng MIEE MIEEE, Cherry Clough Consultants

This is the **sixth** and final article in this series on basic good-practice electromagnetic compatibility (EMC) techniques in electronic design, published during 2006-8. It is intended for designers of electronic modules, products and equipment, but to avoid having to write modules/products/equipment throughout – everything that is sold as the result of a design process will be called a 'product' here.

This series is an update of the series first published in the UK EMC Journal in 1999 [1], and includes basic good EMC practices relevant for electronic, printed-circuit-board (PCB) and mechanical designers in all applications areas (household, commercial, entertainment, industrial, medical and healthcare, automotive, railway, marine, aerospace, military, etc.). Safety risks caused by electromagnetic interference (EMI) are not covered here; see [2] for more on this issue.

These articles deal with the practical issues of what EMC techniques should generally be used and how they should generally be applied. Why they are needed or why they work is not covered (or, at least, not covered in any theoretical depth) – but they are well understood academically and well proven over decades of practice. A good understanding of the basics of EMC is a great benefit in helping to prevent under- or over-engineering, but goes beyond the scope of these articles.

The techniques covered in these six articles will be:

1) Circuit design (digital, analogue, switch-mode, communications), and choosing components
2) Cables and connectors
3) Filtering and suppressing transients
4) Shielding (screening)
5) PCB layout (including transmission lines)
6) **ESD, electromechanical devices, power factor correction, voltage fluctuations, immunity to power quality issues**

Many textbooks and articles have been written about all of the above topics, so this magazine article format can do no more than introduce the various issues and point to the most important of the basic good-practice EMC design techniques. References are provided for further study and more in-depth EMC design techniques.

Table of contents for this article

6. Part 6 – ESD, electromechanical devices, power factor correction, voltage fluctuations, immunity to power quality issues

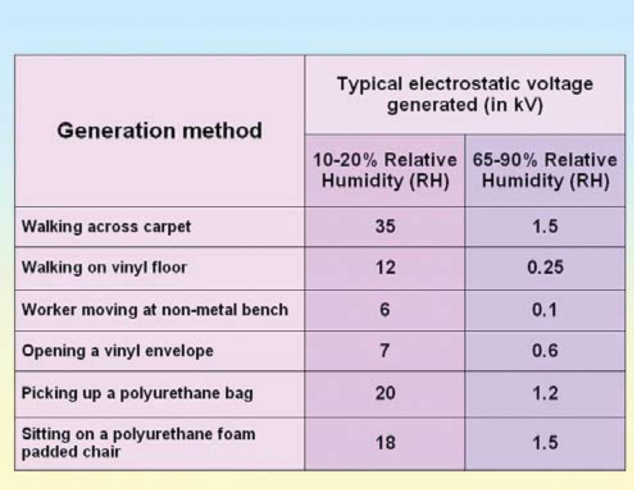
6.1 Electrostatic Discharge (ESD)

6.1.1 ESD threats

Normal commercial and industrial ESD tests employ the IEC/EN 61000-4-2 basic test method that attempts to simulate 'personnel discharges' from people's fingers. We have all experienced such discharges when the humidity of the air is low, when touching a metal object such as a door handle. Ordinary people do not generally notice ESD events from their fingers that are less than about ±3kV, and ESD events that make people hop about and complain loudly are generally in excess of ±15kV.

Figure 6A gives some examples of the electrostatic voltages that can be generated on a human body just by moving around in a typical building and doing ordinary things, for various values of the relative humidity of the air, from [3]. The mechanism by which this and most other terrestrial electrostatic charges are generated is called tribocharging, but this is not the article to discuss that phenomenon.

The IEC/EN 61000-4-2 test method uses an ESD 'gun' that discharges a 150pF capacitor through a 330Ω resistor to create ESD events up to ±8kV at up to ±30A, with risetimes between 0.7 and 1ns. The high dV/dt and dI/dt of these ESD events ensure that they have significant EM energy at frequencies beyond 1GHz. The test method is described in [4] (page 184), Chapter 43 of [5], Part 3 of [6] (which also describes some low-cost alternatives), and in the guide to EN 61000-4-2 in [7].



Generation method	Typical electrostatic voltage generated (in kV)	
	10-20% Relative Humidity (RH)	65-90% Relative Humidity (RH)
Walking across carpet	35	1.5
Walking on vinyl floor	12	0.25
Worker moving at non-metal bench	6	0.1
Opening a vinyl envelope	7	0.6
Picking up a polyurethane bag	20	1.2
Sitting on a polyurethane foam padded chair	18	1.5

Figure 6A Examples of personnel electrostatic charging

Figure 6B sketches the basic circuit elements of an IEC/EN 61000-4-2 ESD gun, which can be fitted with two types of discharge tip: a round one that simulates a human finger and is used for creating discharges in the air, and a pointed tip used for discharging by direct contact with conductive surfaces or objects.

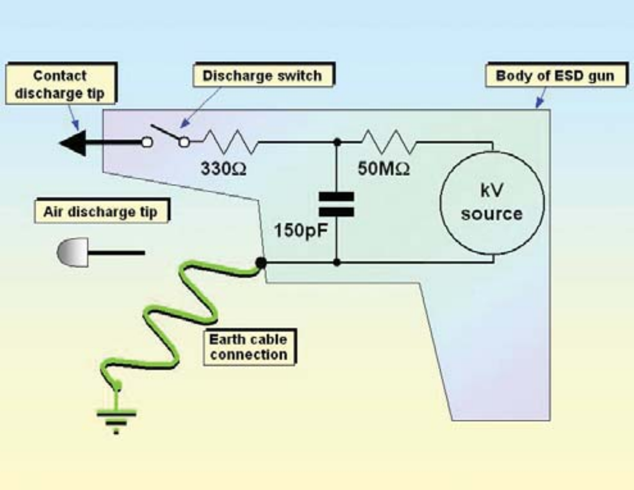


Figure 6B Overview of an IEC/EN 61000-4-2 'ESD Gun'

Figure 6C shows an example of a commercially available ESD gun, that has plug-in modules for various discharge waveshapes, including that specified in IEC/EN 61000-4-2 (see Figure 6F).

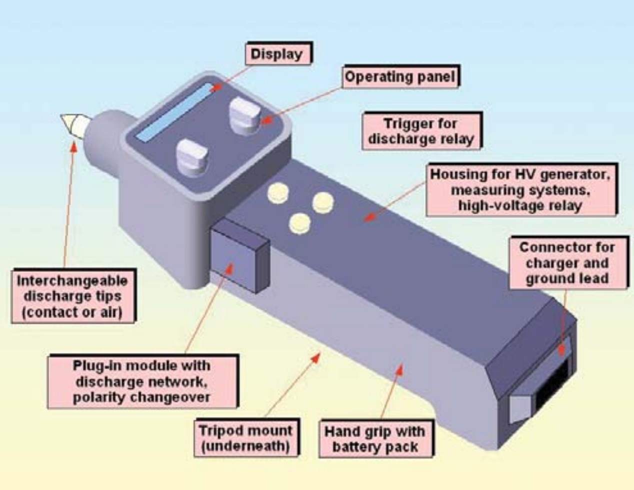

Display
Operating panel
Trigger for discharge relay
Housing for HV generator, measuring systems, high-voltage relay
Connector for charger and ground lead
Interchangeable discharge tips (contact or air)
Plug-in module with discharge network, polarity changeover
Tripod mount (underneath)
Hand grip with battery pack

Figure 6C Example of a KeyTek MiniZap®

Figure 6D shows that testing to IEC/EN 61000-4-2 simulates three different kinds of 'personnel ESD' events, and can also cause 'secondary arcing' to occur – effectively ESD events within the product's structure. The 'near-fields' from an ESD test can be kV/m at 1m from a discharge, and kA/m within 100mm of a discharge – these are very intense fields indeed.

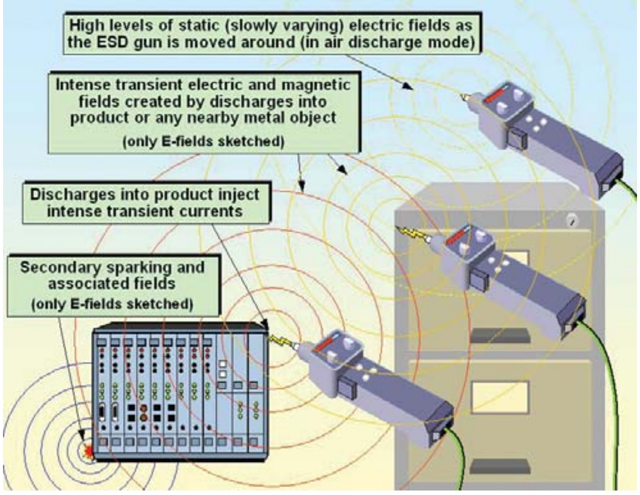
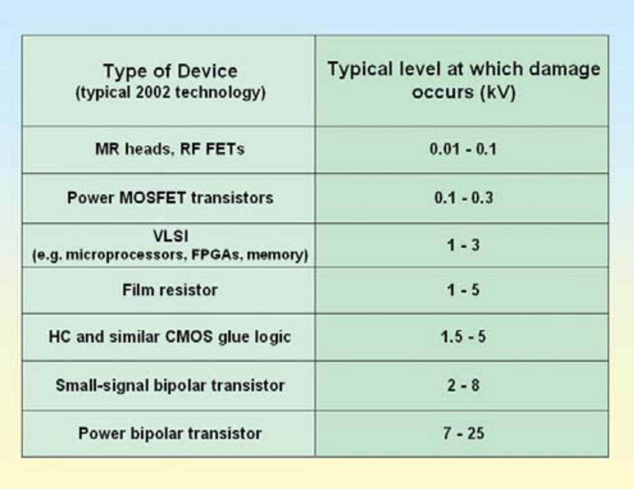

High levels of static (slowly varying) electric fields as the ESD gun is moved around (in air discharge mode)
Intense transient electric and magnetic fields created by discharges into product or any nearby metal object
(only E-fields sketched)
Discharges into product inject intense transient currents
Secondary sparking and associated fields
(only E-fields sketched)

Figure 6D Various EM phenomena associated with ESD testing

The automotive industry uses the ESD test method ISO 10605 instead of IEC/EN 61000-4-2, and tests up to ±25kV with products powered, and when unpowered to simulate handling during shipping and installation [8].

These ESD tests inject sufficient voltage and current into products to permanently damage ICs and transistors, and even some passive components, see Figure 6E. And the intense electric (E) and magnetic (H) fields they create can couple transient noises into nearby circuits and disrupt signals, causing errors and often creating big problems for software.



Type of Device (typical 2002 technology)	Typical level at which damage occurs (kV)
MR heads, RF FETs	0.01 - 0.1
Power MOSFET transistors	0.1 - 0.3
VLSI (e.g. microprocessors, FPGAs, memory)	1 - 3
Film resistor	1 - 5
HC and similar CMOS glue logic	1.5 - 5
Small-signal bipolar transistor	2 - 8
Power bipolar transistor	7 - 25

Figure 6E Examples of ESD damage levels for devices

The damage levels in Figure 6E are based on tests in 2002 on unassembled devices (so ignores any protection provided by their circuits and enclosures) using the semiconductor manufacturing industry's 'human body model' – which discharges a 100pF capacitor through a 1.5kΩ resistor, generating a peak current of ±2A with a risetime of between 5 and 20ns. Modern (2007) microprocessors, memory devices and glue logic use insulating layers that are a great deal smaller than their 2002 ancestors, and probably have damage levels around 100V – reducing all the time as silicon feature size continues to reduces according to Moore's law [26].

Figure 6F shows the waveform of the discharge current that is specified when calibrating an ESD gun to IEC/EN 61000-4-2, and it also shows the sort of waveform that can obtain in real life due to radio-frequency (RF) resonances in the product being tested. Resonances can extend the ns transient of an ESD spark into a complex electromagnetic event that lasts for tens of µs.

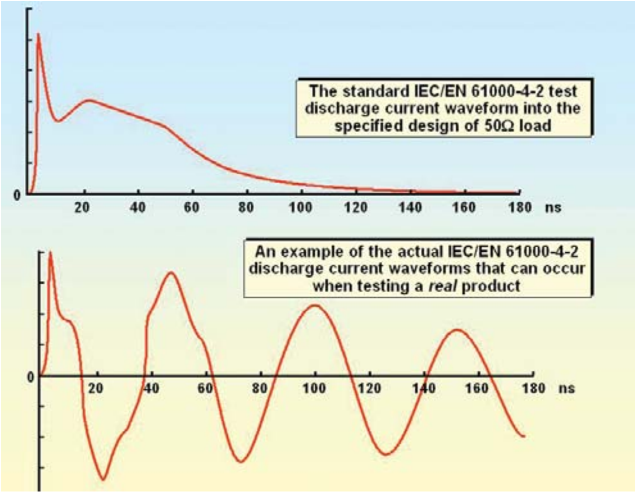


Figure 6F Examples of ESD waveforms

There are concerns [9] that the IEC/EN 61000-4-2 tests do not simulate real-life personnel ESD events well-enough to prove that products incorporating modern microprocessors and memory chips will be reliable in real life. [9] also claims that the standard does not specify the design of the ESD gun well enough to prevent significant differences when testing a given real product with different manufacturers' guns. This is also discussed in the guide to EN 61000-4-2 in [7].

But in real-life applications, ESD events can originate from a wide variety of sources other than people's fingers, as sketched in Figure 6G. These sources can have much higher values of capacitance than 150pF, and/or much higher voltages (up to ±40kV has been seen) or risetimes as low as 10ps.

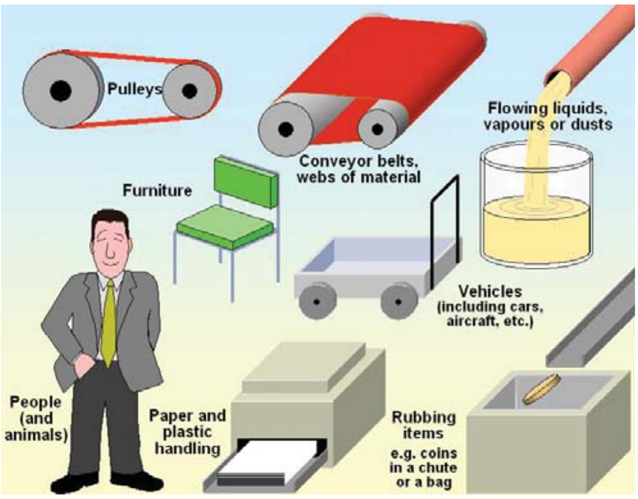

Pulleys
Conveyor belts, webs of material
Flowing liquids, vapours or dusts
Furniture
Vehicles (including cars, aircraft, etc.)
People (and animals)
Paper and plastic handling
Rubbing items
e.g. coins in a chute or a bag

Figure 6G Examples of some ESD sources

It may seem odd that, as indicated in Figure 6G, fluid flow can cause ESD – but many serious incidents and accidents in the petroleum and other industries have occurred due to this very problem (see No. 458 in [12]), and it is also implicated in the crash of TWA 800 from an explosion caused by sparking in one of its fuel tanks. Spacecraft can suffer from very high levels of ESD due to charging of insulated parts by the solar wind, and by charged particles from outer space. And aircraft (fixed and rotary wing) can become charged up to very high levels due their passage through the air, especially during certain weather conditions (see No's 22, 23, 294, 295 and 431 in [12]). Motor vehicles can also become highly charged (see No. 366 in [12]).

Products that pass ESD tests in a laboratory can fail in the field due to more aggressive ESD events in their operational environments. Very high voltages and very low risetimes do not generally go together. High-voltage events tend to have a risetime of 1ns or longer, whereas low-voltage events (such as caused by jingling coins in a plastic bag, see [10]) can have risetimes as low as 10ps – with a spectrum of energy that extends well beyond 10GHz. The measurement of ESD risetimes is limited by the availability of suitable instrumentation, and it seems that as oscilloscopes get faster, we discover that real-life ESD events can be faster than we previously thought.

For more background on ESD and the forms it can take visit [10] and [11]. 21 examples of real-life ESD problems are described in [12]. An interesting example is the ESD caused by the rotors of AC motors running in nylon or other insulating bearings. Few designers would expect the little motor embedded within their product to be an ESD source, but the E- and H-fields created when its rotor discharges across its bearing to its frame can easily upset microprocessors and cause software to malfunction or crash.

6.1.2 Prevent ESD by preventing electrostatic charge from building up

This is generally a system or installation design technique, but it is used in all semiconductor manufacturing areas, and widely used in electronic assembly areas, so products intended for use in such environments can benefit and may not need to pass any ESD tests.

There are two basic methods: one is to make sure that all the materials used are dissipative (i.e. have a resistance between 10^6 and 10^9 Ω/square), and are connected to the ground reference, so that electrostatic charges decay quicker than they are generated and high voltages cannot build up. Some materials are made dissipative by coating them with appropriate materials (e.g. antistatic spray for carpets and furnishings). But many coatings only function as intended in atmospheres with a certain minimum relative humidity – so humidity control becomes a necessary feature of the heating, ventilating and air-conditioning system of the area.

The other method is to make the air itself conductive by using high-voltage needles to create alternating batches of negative and positive ions in a fan-blown air-stream. Ionised air is conductive, and alternating negative and positive ionisation results in air that is neutrally charged on average and so does not cause electrostatic charges to accumulate. Blowing the ionised, conductive air around the area to be protected causes any static charges on products, furniture or people to dissipate. In fact, a neutrally ionised air stream is the one sure way to remove charge from the surface of an insulator without having to wipe all over it with a grounded conductive brush or cloth.

The above techniques can also be used *within* products, to improve their reliability by discharging rotating belts, pulleys, motors with nylon bearings and the like so that they don't give rise to internal sparks that could upset their electronics. Dissipative materials can be used, such as conductive rubber (instead of insulating rubber) for drive belts, conductive plastics for wheels and pulleys, etc.

Insulating parts that move, including consumables such as the paper in a photocopier or printer, can also be discharged with grounded conductive brushes, often made of stainless steel or carbon fibre for longevity. Also, neutrally ionised air streams can be blown inside equipment to prevent the build-up of static charges.

6.1.3 Prevent the discharge from happening with insulation

When a product has to cope with external ESD from people or other sources, a very powerful design technique is insulation. We use plastic enclosures, membrane keyboards, plastic knobs, switch caps and control shafts, etc. to prevent the injection of the intense discharge currents into the product – in effect we simply do not permit the charged person or object to discharge into our product.

Figure 6D shows that this technique still leaves the product exposed to the slowly varying electrostatic fields and the intense E and H-fields from nearby discharges. Slowly varying fields are generally only of concern for very high impedance circuits (typically >1MΩ), and both these and the intense fields can be dealt with by techniques described in 6.1.8: for example a product might use all the techniques described in the earlier parts of this series [13] [14] [15] [16] and [17] – and then have insulation applied all over as well, to prevent direct ESD.

Typical plastics have a breakdown voltage through their thickness of about 40kV/mm, which can be a problem for membrane type control panels in extreme ESD environments if we want to use 'clicky' tactile buttons. To get a good button-clicking experience we need to a top plastic layer of about 0.5mm that will insulate up to about 20kV, if we have to use thicker layers it will ruin the feel of the button.

Membrane panels can employ a metal shielding layer immediately below their top layer of insulation, as described in 4.3.13 in [16]. This should intercept any discharges that manage to penetrate the top insulating layer, but to be effective it must be connected to the product's RF Reference, which in a shielded enclosure will be the enclosure shield itself [16], and in an unshielded enclosure will be the PCB's 0V plane [17] [18].

4.3.13 in [6] says that the shield layer should RF-bond to the metal enclosure all around its perimeter. This not the normal method used by membrane panels manufacturers, who generally use a 'shield grounding' trace in the flexi-ribbon cable that connects the panel's switch traces to the PCB. This is effectively a 'pigtail', like the bad-practice method of terminating cable shields discussed in 2.6.6 of [14], and it allows stray RF coupling into the membrane panel's conductors. If we do not use a metal shield within our insulating enclosure, for example as discussed in 4.7.7 of [16], we might need to filter the membrane panel's interconnections as described in [15] or ESD-suppress them as described 6.1.5 below.

Capacitive sensing techniques will work through almost any practical thickness of plastic, glass or ceramics and so can be made to withstand any ESD voltages, but they provide no tactile feedback at all. Using a remote control, such as a wireless remote, allows us to locate the human interface in a more benign ESD environment.

Air and vacuum are the biggest problems when using insulation to prevent actual discharges from occurring to the product. Enclosures must have seams and joints to make it possible to assemble them, and these create gaps in the insulation, and the gaps contain air. Air has a breakdown voltage of only about 1kV/mm, less if humidity is high. In space the gaps are filled with vacuum, which also has a breakdown voltage of about 1kV/mm but does not suffer from variations due to weather.

The resulting problem is shown in Figure 6H – we need very large air gaps between conductors and places that could be touched by people or other ESD sources, to be sure they don't break down and allow a discharge into the product.

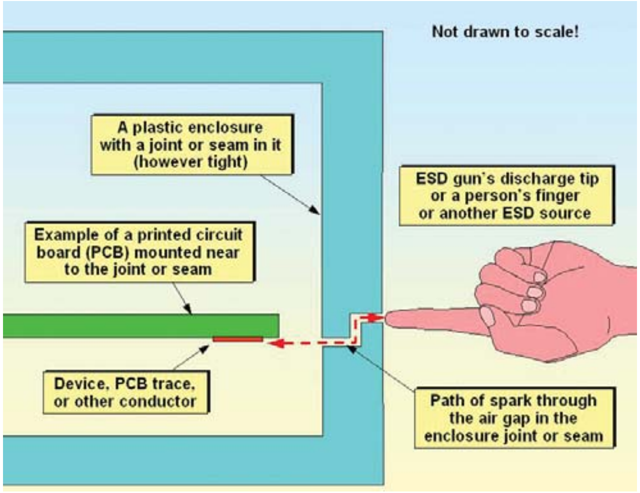

Not drawn to scale!
A plastic enclosure with a joint or seam in it (however tight)
ESD gun's discharge tip or a person's finger or another ESD source
Example of a printed circuit board (PCB) mounted near to the joint or seam
Device, PCB trace, or other conductor
Path of spark through the air gap in the enclosure joint or seam

Figure 6H ESD penetrating a seam in a plastic enclosure

To withstand ±8kV we need *at least* an 8mm air-gap, and *at least* 25mm for ±25kV, taking into account the reduced breakdown voltage with increased humidity (unless the product is intended to work in a vacuum instead). Another issue is that all practical insulating surfaces are coated with dirt, damp, greasy fingerprints, possibly even mould, so discharges will find the surface of an insulator to be an easier path than even the air. It is not uncommon during ESD testing to see a spark from an 8kV discharge wriggle around on a painted metal surface for several tens of millimetres, tracking through the dirt and other contamination before finding a microscopic pinhole that allows it to reach the metal surface underneath.

So the best approach to insulating surfaces is to assume they are conductors and not take them into account at all in the total length of the air gap. Figure 6J shows how the air gap in Figure 6H can be increased, and also introduces the 'guard ring' PCB technique and the possible need to use shielding for very sensitive devices or traces.

People have been using perimeter guard rings on PCBs for decades, but because of the prevalence of the 'single-point grounding' myth, they thought it best to use a long trace around the PCB perimeter, connected to the 'chassis ground' – or whatever – at one point. As [14] shows, all they were really doing was creating resonant structures that were very effective antennas at certain frequencies. These take the broadband energy in the ESD discharge and re-radiate it as a very intense field at their resonant frequency, possibly replacing one type of ESD failure with another.

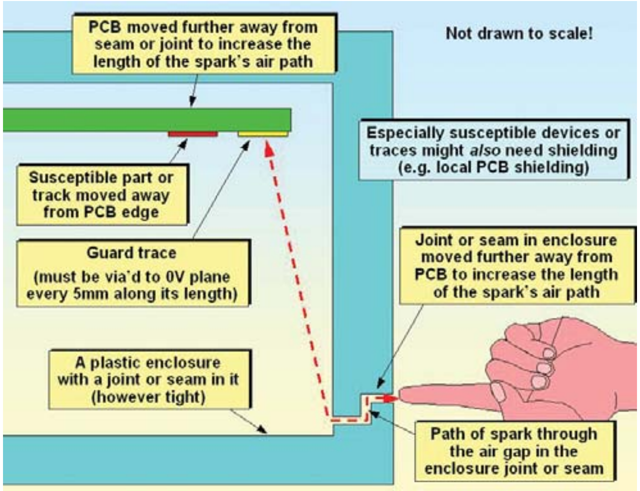

PCB moved further away from seam or joint to increase the length of the spark's air path
Not drawn to scale!
Especially susceptible devices or traces might *also* need shielding (e.g. local PCB shielding)
Susceptible part or track moved away from PCB edge
Guard trace (must be via'd to 0V plane every 5mm along its length)
Joint or seam in enclosure moved further away from PCB to increase the length of the spark's air path
A plastic enclosure with a joint or seam in it (however tight)
Path of spark through the air gap in the enclosure joint or seam

Figure 6J Solutions to the problem of ESD penetrating seams in plastic enclosures

Another possibility is that because the inductance of such a guard ring was so high, when it received a discharge its voltage could rise so high that it then caused a secondary discharge to the devices and traces it was supposed to be protecting.

The *only way* to implement an effective guard trace for ESD (or for any RF purpose above a few MHz) is to start with an RF Reference plane layer that maintains a very low impedance up to the highest frequency of concern for ESD (in excess of 1GHz) – and then connect the guard trace to the plane with via holes whose spacing is much smaller than the wavelength of the highest frequency. The effect of the dielectric constant of the PCB on the wavelength must be taken into account [17] [18].

The previous part of this series [17] only describes basic EMC techniques for PCBs, so for the details of implementing perimeter (or other) guard traces that are effective for RF and/or ESD, see [18].

An alternative approach to the problem of joints and seams in insulating enclosures is simply to fill them up with insulator, such as a (gas-tight) rubber gasket, silicone or epoxy sealant. The sealant approach is very acceptable for joints and seams that should never need to be opened during the life of the product (e.g. around the edges of a display), and the rubber gasket approach can be practical where access is required.

Beware of the temptation to try to make a totally sealed product. It is more difficult than it seems, and there have been many attempts that ended up with excessive amounts of condensation sloshing around inside, causing rapid corrosion.

Controls and displays are weak points in any ESD scheme, because they must somehow connect between the protected circuitry and the world inhabited by charged-up people and other ESD threats. Plus, of course, the charged-up people keep insisting on pointing at things on displays and touching the controls. (Cable and antenna connections are also weak points, and these are discussed in 6.1.5.)

LED and filament lamp indicators can use surface-mounted devices with plastic light guides to communicate their light to the human interface, as shown in Figure 6K. The light guides can be cheaply made from injection mouldings that snap into the enclosure and align with the LEDs or lamps on the PCB. This method is very low-cost, but it is important that any seams or joints between the light guides and the enclosure's insulating surface are friction-welded, glued or sealed so that sparks cannot track along contamination on the light guide's surface and get into the PCB.

Another technique is to present the LEDs or lamps at apertures in the enclosure, but cover them with a glued-on plastic overlay, generally the one carrying the control panel markings, that has transparent areas over the displays.

A problem with glued plastic layers, that also afflicts membrane panels, is the uniformity of the glue layer. Any missing glue, or imperfect bonding with the insulating enclosure surface, will create an air-gap that will allow sparks to slip under the overlay or between the laminated layers in the membrane panel and inject discharge currents into indicator devices, or into printed traces in membrane panels.

Where glue uniformity and quality cannot be guaranteed, make sure the edges of the plastic layer extend a very long way beyond the vulnerable components or traces. For 8kV ESD, 20mm would not be excessive. Or else seal them with silicone or other insulation as shown in Figure 6K.

For rotary shafts for switches, potentiometers and encoders, toggle switches, and similar manual controls, plastic knobs, shafts and toggles are recommended. For many years now, equipment has been so miniaturised that their control knobs are so small that discharges from operator's fingers can easily track across their surfaces and into any metal shafts they are mounted on – thereby penetrating the insulating enclosure and damaging some vital device or scrambling its software. So plastic shafts should be used, as shown in Figure 6K.

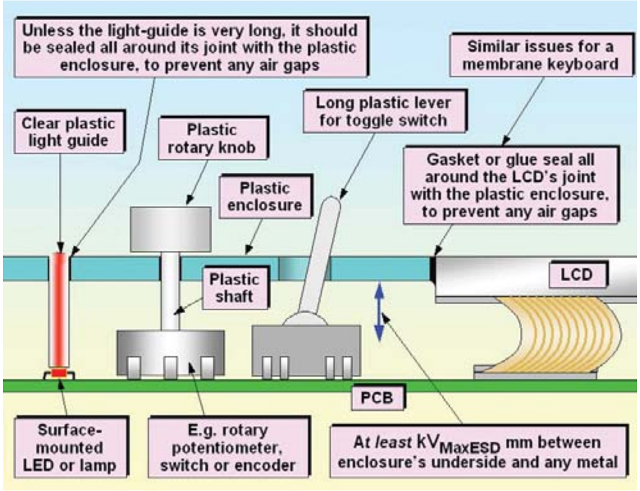

Unless the light-guide is very long, it should be sealed all around its joint with the plastic enclosure, to prevent any air gaps
Similar issues for a membrane keyboard
Long plastic lever for toggle switch
Clear plastic light guide
Plastic rotary knob
Gasket or glue seal all around the LCD's joint with the plastic enclosure, to prevent any air gaps
Plastic enclosure
LCD
Plastic shaft
PCB
Surface-mounted LED or lamp
E.g. rotary potentiometer, switch or encoder
At least kV_{MaxESD} mm between enclosure's underside and any metal

Figure 6K Indicators, displays and controls penetrating plastic enclosures

Figure 6K also shows that the assembly of LCD panels and graphics displays should avoid exposing their edges to ESD events. This is where a good mounting bezel with a rubber gasket, or a silicone or other type of sealant (that could also be used to hold the display in place, simplifying assembly) can be very useful. The fixed windscreens in almost all models of motorcars introduced since 1990 are an example of appropriate assembly techniques. Older vehicles used to have all sorts of bezel contraptions to hold them in place, and it was not unusual for them to leak (allow water to penetrate the enclosure) – but these days they simply glue them in, and incidences of water penetration are rare.

6.1.4 Control the discharge with shielding

Shielding is an alternative ESD suppression method to insulation (see 6.1.3). It allows the discharge to occur to the product, but then seeks to control it so that it doesn't upset any of the product's electronics. Shielding techniques were discussed in Part 4 of this series [16], and at first sight it might seem that all we need to do is design our shielding to be effective enough at a high-enough frequency.

For normal ESD testing, with risetimes close of 0.7ns or longer, we can assume the highest frequency of concern ($1/\pi t_r$) is about 500MHz, but real ESD events are much faster than this, at 0.3ns or less [9] and so we should assume 1GHz or more instead.

But the very high intensities associated with ESD events (tens of amps with sub-ns risetime, E-fields of kV/m, H-fields of kA/m) significantly increase the demands on our shielding, In fact, designing shielding for ESD is rather like designing it for military or aerospace purposes, where we can be dealing with kV/m E-fields at 1GHz or more from nearby radars, so in this section we need to discuss how to apply the techniques described in [16] to the ESD situation.

Clearly, with such high levels of E and H near-fields, the shielding effectiveness (SE) required at the highest frequency of concern will be higher than what is usually required to cope with the normal domestic, commercial and industrial environments (typically tested at 3V/m or 10V/m, although achieving immunity to the close proximity of cellphones, walkie-talkies or GPRS-enabled computing devices can require testing at 60V/m or more).

Because of the very high levels of ESD current flowing around the outer skin of a shielded enclosure, any gaps or apertures that make these surface currents divert from their natural paths become very intense sources of secondary E and H-fields. So it is very important to locate sensitive devices, PCB traces and conductors *very far away* from even tiny gaps or joints in the shield. Figure 4R in [16] shows the general principle, but much more than its 40dB of SE might be required.

The voltages developed across a gap or aperture in a shield, due to their diversion of the flow of the ESD currents, can be so high that they break down the air (or vacuum, in the case of spacecraft) at that point and spark across the gap. This is known as *secondary arcing* and, as might be expected, where it occurs it can cause very great problems. It can even occur *inside* products whose external shielding provisions are not as good as they should be, generally playing havoc with their electronics.

Secondary arcs are often small faint blue things that are hard to see even when right in front of your eyes, but more often than not they are hidden within a metal seam, or inside or on the bottom surface of the product being tested and so even less visible, as sketched in Figure 6L. When secondary arcing is suspected, for example when the ESD gun is applied to the top of the product, but the microprocessor that resets (and its reset lines) are located near the bottom, a powerful diagnostic technique is to do ESD testing in the dark.

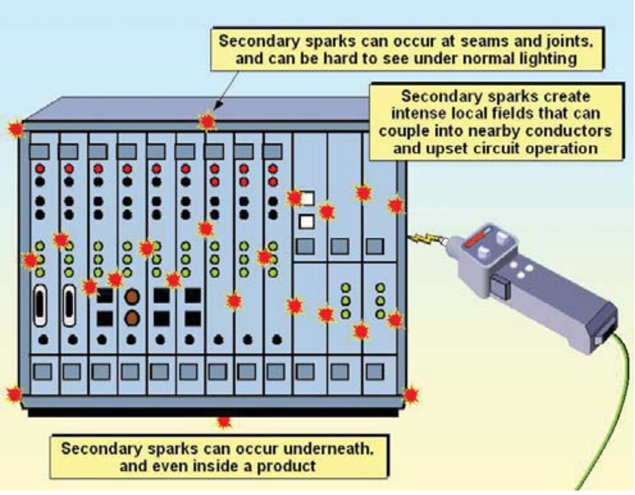

Secondary sparks can occur at seams and joints, and can be hard to see under normal lighting
Secondary sparks create intense local fields that can couple into nearby conductors and upset circuit operation
Secondary sparks can occur underneath, and even inside a product

Figure 6L Sketch of some secondary arcing possibilities

It is of course inadvisable to do ESD testing in total darkness, because we need to see what we are doing well enough to:

a) Apply the ESD gun to the correct point on the product, and in the specified manner

b) Not accidentally discharge the gun to ourselves (painful, but not damaging to people. Where one's health depends on implanted or portable electronic medical devices such as pacemakers or defibrillators, you should not be anywhere near an ESD test anyway.)

So close the blinds and/or turn the lights down quite a lot, and wait a few minutes for your eyes to get accustomed to the gloom. People can see quite well by moonlight, which has one-millionth the luminous intensity of sunlight, so given time our eyes adapt to gloom very well.

The tester has to watch where the ESD gun is applied and has a limited ability to monitor other areas of the product, so spotting any secondary arcing can be made much easier if someone else looks closely at different parts of the product during the tests. It can also help to reorient the product, for example lying it on its side to see its underside. Detecting internal secondaries can require more radical techniques.

Indicators, controls and displays are weak points for ESD when relying on shielding, just as they are for the insulation techniques discussed in 6.1.3. The insulation-based techniques sketched in Figure 6K (plastic light guides, knobs, shafts and toggles, etc.) are effective with metal enclosures too, but the apertures they create in the shield might cause problems for nearby sensitive devices when discharges occur to the metal surface, or when shielding for frequencies above 300MHz. Figure 6M shows some alternative techniques that prevent the creation of apertures in the shield.

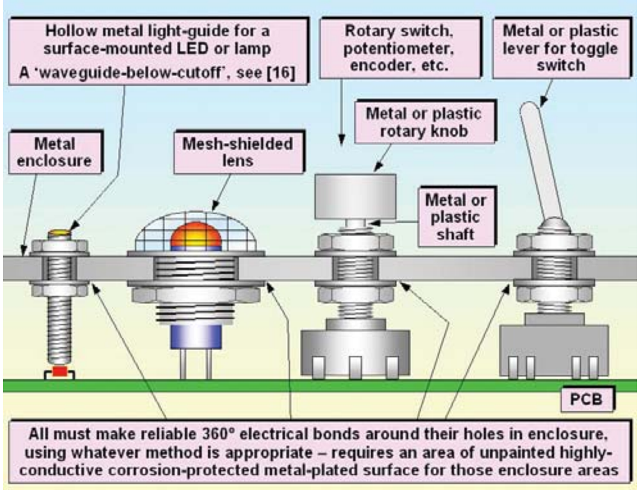

Hollow metal light-guide for a surface-mounted LED or lamp
A 'waveguide-below-cutoff', see [16]
Rotary switch, potentiometer, encoder, etc.
Metal or plastic lever for toggle switch
Metal or plastic rotary knob
Metal enclosure
Mesh-shielded lens
Metal or plastic shaft
PCB
All must make reliable 360° electrical bonds around their holes in enclosure, using whatever method is appropriate – requires an area of unpainted highly-conductive corrosion-protected metal-plated surface for those enclosure areas

Figure 6M Indicators, displays and controls penetrating shielded enclosures

Figure 6M does not show how to deal with panel-type displays or membrane keyboards. Displays need to be treated using one of the techniques described in [16] (e.g. Figure 4AH). Membrane keyboards should RF-bond their metal backing plates, and/or any internal shielding layers to the shield all around their perimeter, using conductive gaskets, see 4.3.13 in [16]. Care should be taken to prevent discharges into their edges or backs.

It is often assumed that a Faraday Cage (i.e. an effective shielded enclosure) always prevents any external voltages from creating voltage differences within it. Whilst this is true for established DC voltages (as Michael Faraday found, when sitting inside his eponymous cage holding a gold-leaf electroscope) – and also true for continuous RF for enclosures with no apertures made of a metal with at least 10 skin-depths at the frequency concerned. But it is not true for transient voltage fluctuations such as ESD.

When a discharge is applied to a shielded enclosure, at first the transferred charge spreads all over the outer skin of the metal shield, and in the short-term whilst current is still flowing, it is confined to the outer surfaces by skin effect. Once the currents have equalised the voltage all over the outer skin of the shield (which they do at the speed of light, so it would only take about 1ns for a small enclosure) they stop flowing, and the charge then becomes static – an electrostatic voltage on the outside of the metal enclosure.

Over the next few ns the charge diffuses through the thickness of the metal shield material until it appears on its inner surface. The rate of diffusion depends on the relative permeability of the metal – the higher it is, the smaller the skin depth and the slower the rate of diffusion.

Inside any metal enclosure there are hundreds or thousands of stray capacitances between the shield material and each device (in fact, each pin of each device), PCB traces and other conductors – and they are all different. When the charge appears on the inner surfaces of the shield, it charges up these stray capacitances, and during this process they carry charging currents (sometimes called displacement currents). These transient charging currents will of course be injected into the devices, PCB traces and other conductors that they are 'strays' to. Figure 6N shows the general idea, but really needs an animated sequence to better show the sequence of events.

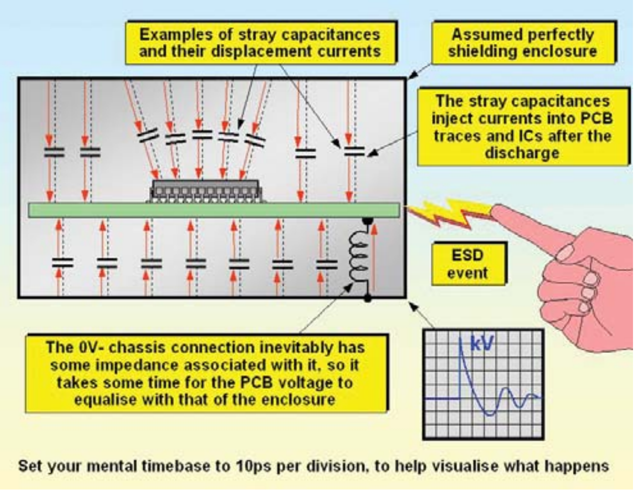

Examples of stray capacitances and their displacement currents
Assumed perfectly shielding enclosure
The stray capacitances inject currents into PCB traces and ICs after the discharge
ESD event
The 0V- chassis connection inevitably has some impedance associated with it, so it takes some time for the PCB voltage to equalise with that of the enclosure
kV
Set your mental timebase to 10ps per division, to help visualise what happens

Figure 6N Effects of a discharge to a shielded enclosure

Eventually the 0V-chassis connection (if there is one) will carry currents that equalise the static voltages throughout the interior of the product. If there is no intentional connection, equalisation will happen more slowly due to ionisation of the air in the product. The transient currents in the stray capacitances are different for each device pin, PCB trace or other conductor, and so they cause transient voltage differences between different parts of the circuits. These transient differential-mode voltages can upset the operation of circuits, and reset or crashed microprocessors are a common consequence.

Note that a wired connection between the enclosure shield and a safety earth or other external 'ground' has no effect over the process described above. The length (and hence inductance) of the earthing/grounding wire or strap is simply too great for it to carry the charge away from the outer surface of the shield before it has time to diffuse inside. However, direct metal-to-metal bonding at multiple points around the perimeter of a metal enclosure, to a large metal surface (e.g. the metal hull of a ship or metal fuselage of an aircraft) should allow the surface charge to 'drain away' fast enough to have *some* effect.

One solution to this ESD problem is to create a high-quality 0V plane on the PCB, as described briefly in [17] and in detail in Chapter 4 of [18]. Then 'RF bond' this plane to the shield with multiple low-impedance (at 1GHz) bonds – described briefly in [17] and in detail in Chapter 3 of [18].

Another solution is to use filtering and shielding techniques on the PCB, at least over the most sensitive components. These techniques are described briefly in section 5.3 of [17] and in detail in Chapter 2 of [18], from which Figure 6P is taken, and PCB shielding-cans can be quite low-cost. It may be necessary to apply the 0V planes and RF bonding at the same time as the PCB-level filtering and shielding.

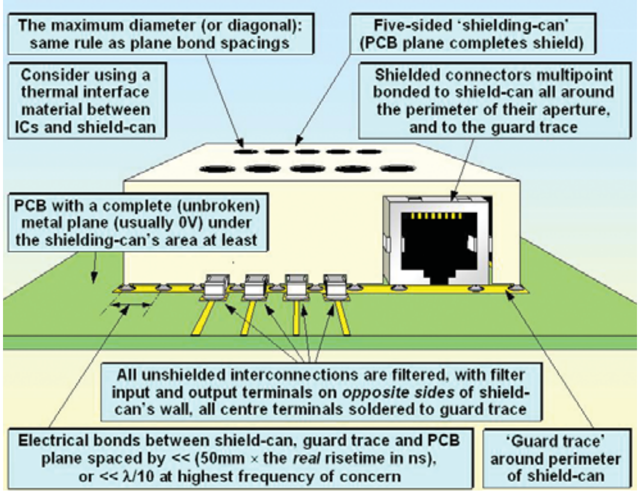

The maximum diameter (or diagonal): same rule as plane bond spacings
Five-sided 'shielding-can' (PCB plane completes shield)
Consider using a thermal interface material between ICs and shield-can
Shielded connectors multipoint bonded to shield-can all around the perimeter of their aperture, and to the guard trace
PCB with a complete (unbroken) metal plane (usually 0V) under the shielding-can's area at least
All unshielded interconnections are filtered, with filter input and output terminals on *opposite sides* of shield-can's wall, all centre terminals soldered to guard trace
Electrical bonds between shield-can, guard trace and PCB plane spaced by << (50mm × the *real* risetime in ns), or << λ/10 at highest frequency of concern
'Guard trace' around perimeter of shield-can

Figure 6P Overview of PCB-level filtering and shielding techniques

6.1.5 Protecting signal, data, control or power conductors

Discharges into semiconductors can be fatal for them, so if it is not possible to protect conductors with the methods described in 6.1.2 - 6.1.4 above, and if we really have no choice but to expose conductors to ESD discharges, for example the antennas on portable radio receivers, we need to apply appropriate suppression or filtering techniques to them.

This is especially a problem for the pins of connectors, which are exposed to ESD discharges from:

- Personnel discharges (e.g. people fingers)
- Plugging in other equipment (equipment with two-core mains leads are not earthed, so could be charged up to kV)
- Charged-up cables (dragging a cable over the floor can cause all of its conductors to take on an electrostatic charge at several kV)
- Discharges from a variety of other sources

A solution for passing tests to IEC/EN 61000-4-2, which attempts to simulate personnel ESD, is to use small metal-shrouded connectors with their shroud directly connected to the product's RF Reference (its shielding, or PCB 0V plane if unshielded). Appropriate connectors include D-types, USB, Firewire, RJ45, etc. If the 8mm diameter 'air discharge' tip was used for such tests it would most likely discharge to the metal shroud, sparing the connector pins. But in any case there is a clause in IEC/EN 61000-4-2 that mandates using the pointed 'contact discharge' tip, and only applying it to the metal shrouds of such connectors.

Although this is an appropriate technique for personnel discharge, it doesn't deal with the remaining three bullet points above. It allows a product to pass the ESD tests as part of declaring compliance with the EMC Directive, but it doesn't necessarily mean that the product is protected against all the ESD events it will experience in real life.

(Some manufacturers place all their connectors on the rear of their product, so they can state that they are not "accessible to persons during normal use" to take advantage of a clause in IEC/EN 61000-4-2 that removes the requirement to do *any ESD tests at all* on those connectors. I'm sure I don't need to say why I don't recommend that approach!)

For signal conductors that could be exposed to any types of ESD discharges, current-limiting, transient suppression, or filtering techniques will almost always be needed to protect their circuits from upset and damage to their devices. Some DC power conductors may also need similar protection, although if they are well decoupled (see [17] and Chapter 5 of [18]) this should be sufficient.

As far as I am aware, almost all ICs are fitted with ESD protection diodes that shunt overvoltages and undervoltages to their DC power rails, and those that are not have bold warnings of this fact on their data sheets. But because of the commercial pressures to make devices cheaper, hence use smaller silicon die, these diodes have never been very large or powerful and they are becoming progressively smaller and less powerful. We can help these diodes do their job by putting impedances in series with the conductors that are suffering from the ESD event (e.g. connector pins), as shown in Figure 6Q.

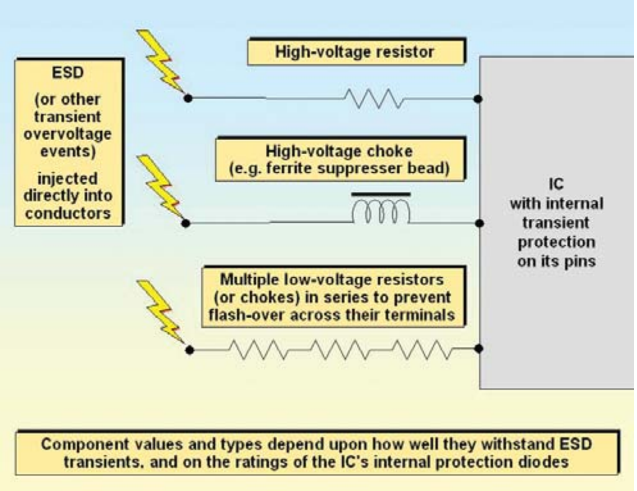

ESD
(or other transient overvoltage events)
injected directly into conductors
High-voltage resistor
High-voltage choke (e.g. ferrite suppresser bead)
Multiple low-voltage resistors (or chokes) in series to prevent flash-over across their terminals
IC with internal transient protection on its pins
Component values and types depend upon how well they withstand ESD transients, and on the ratings of the IC's internal protection diodes

Figure 6Q Adding impedance in signal lines to limit discharge current

As Figure 6Q shows, the resistors or soft-ferrite chokes used must be rated to withstand the full ESD voltage. If ordinary 0805 or similar types are used, *at least* ten (possibly twenty) will be required in series, otherwise their terminals will spark-over – defeating their purpose of limiting discharge currents. When many resistors are used in series, they must not be placed close to each other on the PCB, otherwise the ESD might flash-over between different resistors or track across the inevitable surface contamination on the PCB.

The values of the resistors or chokes are chosen to limit the worst-case discharge current to one that the IC's own protection diodes can handle, the data for which should be provided on the data sheet. All such designs should be proven by assiduous testing, not just a few discharges. And some ESD testing should also be done in the near-dark, to reveal any 'sneak' discharges on the PCB. Where contamination by dust or condensation is likely, test in the dark with foreseeable contamination simulated.

Unfortunately, the values of impedance required may be so high that high-data-rate signals suffer from degraded signal quality (e.g. collapsed eye-pattern). Also, many types of individual semiconductors are unprotected against overvoltages and some are especially susceptible, so just adding series impedance isn't going to work for them.

Filtering or suppression techniques must provide at least 40dB of attenuation (e.g. reduce 8kV to 80V) and possibly as much as 70dB (e.g. from 24kV to 8V) for transients with risetimes of 0.7ns (ideally 0.2ns) – equivalent to a frequency of 460MHz (ideally 1.6GHz). They will not be able to achieve this very high performance without an RF Reference that provides a very low impedance up to the highest frequency of concern. Suitable RF References will either be a metal plane in the PCB (see [17] and Chapter 4 of [18]) or the wall of a shielded enclosure that has a good SE at the highest frequency of concern (see [16]). Figure 6R shows two general techniques: a TVS device, and transient-rated diodes.

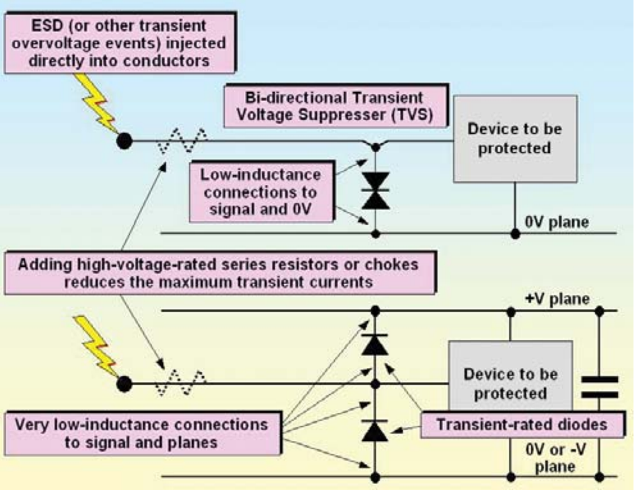

ESD (or other transient overvoltage events) injected directly into conductors
Bi-directional Transient Voltage Suppresser (TVS)
Device to be protected
Low-inductance connections to signal and 0V
0V plane
Adding high-voltage-rated series resistors or chokes reduces the maximum transient currents
+V plane
Device to be protected
Very low-inductance connections to signal and planes
Transient-rated diodes
0V or -V plane

Figure 6R Adding transient voltage protection

The basic principles of transient overvoltage protection were covered in the final sections of [15], for low-frequency surges. TVS devices are generally avalanche diodes, which seem to be increasingly referred to as SADs (silicon avalanche diodes) – the fastest-operating type of transient protection device. Surface-mounted metal-oxide-varistors (MOVs, sometimes called VDRs) should be fast enough to suppress ESD with 0.7ns risetimes, but might not be quick enough where risetimes of 0.5ns or less could occur.

Transient-rated diodes usually come in pairs in SOT-23 packages or similar, and are specified exclusively for transient suppression applications, not for use as ordinary diodes. Sometimes the level of ESD exposure makes it necessary to use high-voltage-rated impedances in series with TVSs or transient diodes, in which case all the high-voltage issues discussed earlier apply to the resistors or chokes.

Many TVS devices have too large a self-capacitance for high-frequency or high-data-rate signals, although low-capacitance versions, some as low as 1pF, are becoming increasingly available – spurred by the rapid increase in high-speed interconnections such as USB2 and Firewire. Transient diodes are reverse-biased in normal operation and so have a low capacitance, which makes them suitable for high-speed signals, as long as the discharge currents are not too high. When using transient diodes, the DC power rail they connect to should be a plane with very low impedance at the highest frequency of concern, just like the RF Reference plane.

A problem with reverse-biased transient diodes is that their leakage currents double with every 10°C rise in temperature, making them difficult to use in high-temperature applications, or on sensitive high-impedance DC-coupled circuits. Many other exotic solutions are possible, for example using an isolated-gate FET (IGFET) arranged so that an incoming overvoltage turns it on and temporarily shorts the trace to the RF Reference.

The placement of the components on a PCB, and the routing of their traces, is vital if the required transient attenuation is to be achieved, and Figure 6S sketches the details, for a TVS. The same layout rules apply to transient-rated diodes as well.

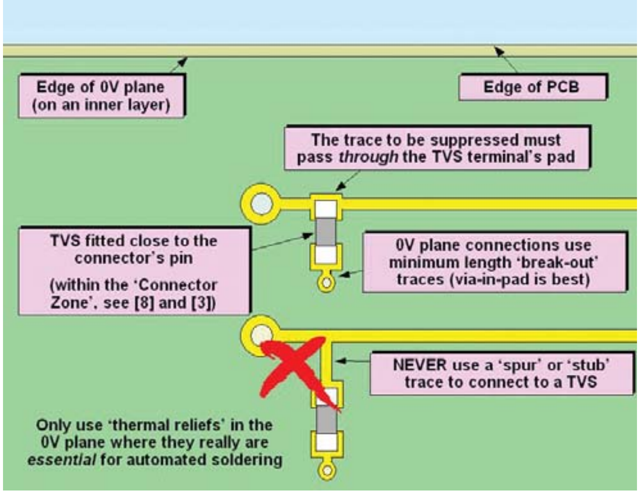

Edge of 0V plane (on an inner layer)
Edge of PCB
The trace to be suppressed must pass *through* the TVS terminal's pad
TVS fitted close to the connector's pin
(within the 'Connector Zone', see [8] and [3])
0V plane connections use minimum length 'break-out' traces (via-in-pad is best)
NEVER use a 'spur' or 'stub' trace to connect to a TVS
Only use 'thermal reliefs' in the 0V plane where they really are *essential* for automated soldering

Figure 6 SPCB layout issues for transient voltage protection

An IEC/EN 61000-4-2 ESD test at 8kV can generate a dI/dt in excess of 43A/ns. A 1mm wide trace just 1mm long, routed over an RF Reference plane layer, will have a self-inductance somewhere between 0.3 and 0.6nH (depending on its height above the plane) [18]. At 43A/ns the peak voltage drop along the 1mm trace will therefore be between 13 and 26V. So the short trace shown connecting the TVS to the via hole in Figure 6Q could limit the efficacy of the transient suppression.

The via hole to the reference plane shown on Figure 6S also has self-inductance. On a two-layer 1.6mm thick board the length of the via hole carrying TVS current will be 1.6mm, giving it a self-inductance of 1.6nH. 43A/ns in such a via hole would drop 70V peak. The TVS device itself will also have internal series resistance and self-inductance, which will also add more peak volts.

The faster risetimes or higher voltages possible with some types of real-world ESD events could double or even triple the above estimates. Clearly it is possible for the PCB layout itself to degrade the performance of the TVS or transient diodes by so much that even if they had zero clamping voltage (which of course they do not) the ICs would still be exposed to quite high peak voltages, just from the self inductances of very short traces, via holes and the transient suppression devices themselves.

However, as long as these voltages are not *too* high, the internal transient protection devices in the ICs themselves should cope with them.

The very best suppression devices are three-terminal types, like the three terminal filter components discussed in [15]. To get the best performance from them, they should be used with at least two parallel vias to their Reference plane, arranged symmetrically around the device and very close to it. Also, the PCB dielectric between the Reference plane layer and the layer on which the suppression device is mounted should be as thin as is practical, say 0.15mm or less. Such precautions are not yet generally necessary, but perhaps they will become more common in future as devices explore silicon processes at 45nm and smaller.

[15] covered the basic principles of filtering, and the above descriptions of the issues associated with ESD suppression using a TVS also apply to the high-voltage-rated series resistors (or chokes) and shunt capacitors when using filtering instead. Where the signals are very slow, some manufacturers just use a large capacitor on its own, with no series impedance, to act as a capacitive voltage divider with the capacitance of the ESD gun, by charge redistribution.

For example, if the ESD gun had a 150pF capacitor charged to 15kV, using a 150pF shunt capacitor to protect an IC's pin would result in 7.5kV at the IC's pin, 1.5nF would give about 1.5kV, 15nF would give 150V and 150nF would give 15V. These are idealised calculations – as shown above the self inductances of even short PCB traces and via holes could easily add tens of peak volts to these values, and there is also the issue of the behaviour of the capacitor with such transient charging currents.

Ceramic capacitors are the only suitable types, with COG or NPO being the best. A typical surface-mounted capacitor might have an internal series resistance of 10mΩ and a series inductance of 1nH, generating an additional peak voltage of 43V with a current risetime of 43A/ns.

The voltage ratings for any series resistors or chokes are the peak ESD voltage itself. Because kV can leap large distances through air or vacuum, their location on the PCB and proximity of them and their traces to other devices and their traces is very important. The voltage rating for the capacitors in any voltage dividers or filters is set by charge redistribution. The value of capacitor or 'clamping voltage' of a TVS should, of course, be less than the level that damages the IC it protects, taking into account the additional transient voltages caused by the self-inductances of shunt components, traces and via holes, and itself. The TVS's capacitance is set by the circuit impedance and data rate; and its peak current rating by the magnitude of ESD event (taking into account any current limiting by high-voltage-rated series resistors or chokes).

6.1.6 'Earth lift' problems for interconnected items of equipment

The above discussions have only considered the ESD protection of a single product, on its own, but when two or more products are interconnected (e.g. by power, signal, control or data cables), 'earth lift' adds a new type of ESD problem.

As Figure 6T shows, when an ESD event injects current into a chassis or enclosure (either directly or via a shunt suppresser like a TVS, transient diode or capacitor), the chassis (etc.) suffers an 'earth lift' transient as the discharge current flows in the very high inductance of the earth-bonding network.

As mentioned before, self-inductance of ordinary conductors is so high that earthing using wires or even braid straps has little/no effect on the peak transient voltage attained by the chassis of the product suffering the discharge. In fact, the peak voltage attained will be almost the same as it would be for an unearthed product, for example one that was battery powered, or 'double-insulated' from the mains power and so powered by a two-core mains lead with no safety earthing conductor.

The peak transient voltage of a product can be determined by charge redistribution between the ESD source's capacitance and the space-charge capacitance of the product. We can calculate the capacitance of the product very approximately as:

$$C = 4\cdot\pi\cdot 8.85\left(\frac{1}{a}-\frac{1}{b}\right) \quad \text{pF}$$

where:

a = the radius of the sphere representing the product, and…
b = the distance of the product from the nearest floor or wall or ceiling that is either made of masonry or has substantial metal in it (e.g. a suspended ceiling)

For the value of 'a' I suggest using half of the average of the two longest product dimensions, e.g. width and length, solely on the basis that it feels about right. Obviously, we do not expect to get a very accurate assessment using the above formula, and this carries across into the accuracy we can expect of the peak transient voltage we would calculate by charge redistribution. Accurate calculations of peak transient voltage can be achieved using modern computer simulation techniques, which can also determine the capacitance of the ESD source.

The earth-lift voltage is common to all of the conductors in an interconnecting cable, so it is a common-mode (CM) ESD transient, which just means that it can damage a number of input and output devices simultaneously.

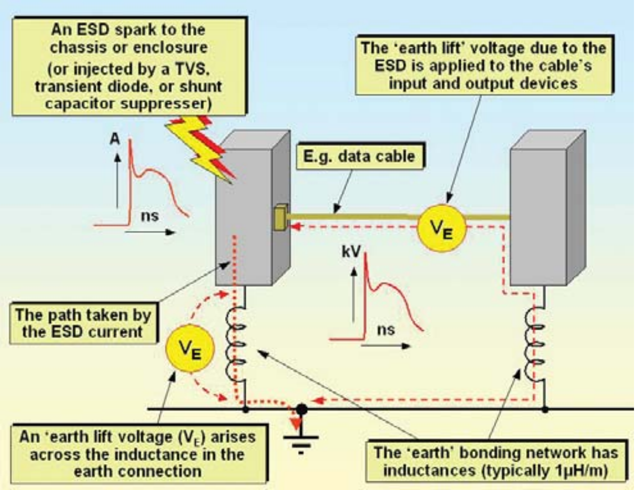

An ESD spark to the chassis or enclosure (or injected by a TVS, transient diode, or shunt capacitor suppresser)
The 'earth lift' voltage due to the ESD is applied to the cable's input and output devices
A
ns
E.g. data cable
V_E
kV
ns
The path taken by the ESD current
V_E
An 'earth lift voltage (V_E) arises across the inductance in the earth connection
The 'earth' bonding network has inductances (typically 1µH/m)

Figure 6T PCB layout issues for transient voltage protection

For protection, either prevent the ESD from happening in the first place using the techniques described in 6.1.2 or 6.1.3, or reduce the impedance of the products' local earthing network to negligible amounts by direct metal-to-metal bonding each of the interconnected products to the same sheet of metal, at multiple points around their perimeters. Such brute-force 'earth bonding' can be quite straightforward in a ship, aircraft, offshore oil platform or other structure made solely from large metal sheets.

Also, using well-shielded cables and connectors to interconnect the products, each cable shield 360° bonded to the frame/ chassis/shield etc. of the product at *both* ends as described in [14], will reduce the earth-lift voltage; although I am not sure whether this method on its own always guarantees freedom from earth-lift problems.

If all of the above methods are impractical, or inadequate, we are left with applying circuit techniques to the input and output devices: either galvanic isolation or suppression with TVSs, transient diodes, filters or just capacitors, as discussed in 6.1.5. Since earth-lift is a CM phenomenon, a CM choke may be just as effective, if not more so, than individual chokes in series with each of the conductors in the interconnecting cables. PCB-mounting CM choke components are available, but are probably not rated to withstand ESD voltages.

Figure 6U shows a few of the very wide variety of cable-mounted CM chokes that are available for round and flat cables. Whilst these do not generally offer as high values of impedance as the board-mounted types, they have very good high-voltage performance, limited only by the insulation of the cable they are used on.

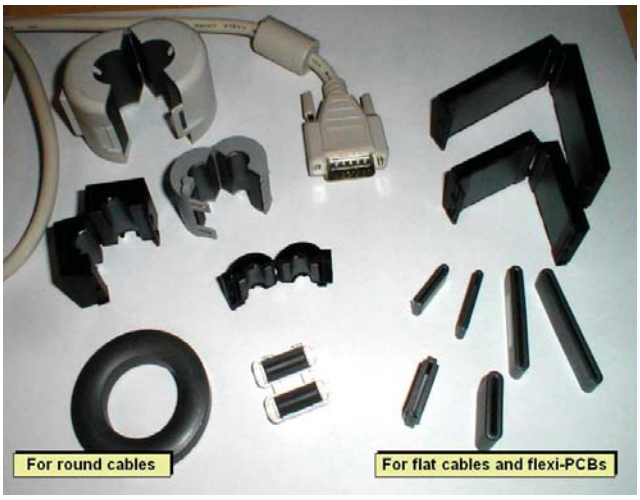


Figure 6U Examples of cable-mounted CM chokes

Galvanic isolation is by far the most robust technique, and can use transformers (e.g. pulse transformers in Ethernet, microphone transformers in professional audio), optical isolators, fibre-optics, wireless, infra-red, free-space modulated lasers, and other techniques. But the vast majority of transformers and optical isolators are not rated for kV isolation and will spark-over when subjected to ESD test voltages.

Transformers can be designed and made with appropriate ratings, usually to special order. 10kV-rated optoisolators have been available from some suppliers for many years, essentially just an emitter and receiver spaced 20-30mm apart by a light guide. It is difficult to obtain such devices that will also handle high-rate digital data, for which fibre-optics and free-space lasers will generally be required. Fibre-optics are generally preferred for EMC reasons anyway, see [14].

6.1.7 Protecting data and signals from errors

Transient suppression devices such as TVSs, transient diodes and shunt capacitors only prevent actual damage to devices, they don't prevent signal corruption. But after a typical ESD test, if the operating state of the product has altered, or any data has been lost, the result is a failure. So it is not sufficient to simply prevent device damage, we have to maintain signal integrity too.

Hardware and/or software design is generally needed to discriminate between ESD events and valid signals. Keyboard strokes, button presses and slow signals, control or data are all easy to distinguish from ESD events using simple techniques, because the ESD events are so brief.

For example, a very quick 'jab' at a momentary contact switch might last as little as 25ms, which is at least 10,000 times longer than almost any ESD event, including the decay of any product resonances it excites. So a simple resistor-capacitor low-pass filter, or a couple of lines of keyboard polling software that checks whether the data is still valid after a few ms, is often perfectly adequate.

But high-speed data uses signals with risetimes and/or durations that might not be so very different from ESD events, making simple discrimination schemes unreliable. High-speed analogue signals should use high-quality shielding (see [14]) and digital data can too. Alternatively, convert all signals into digital data and employ error-detecting or error-correcting protocols.

Any digital engineer can design error detecting/correcting communications protocols, but the temptation to do so should be *resisted at all costs*! It is not at all easy to get a robust product unless you are an expert *in this type of design*. As Figure 6F shows, even a single very short ESD event can cause surprising EM phenomena whose amplitudes, frequencies and durations are hard to predict, and some ESD events are neither single nor short.

But ESD is not the only type of transient that a data communication link needs to be protected from. Fast transient bursts have hardly been mentioned in this series, because they are generally dealt with quite adequately by techniques already described (making allowances for their frequency range and amplitude), but our error detecting or correcting protocol needs to cope with these long bursts of noise too. In real life, fast transient bursts can last for several hundred ms, sometimes for several seconds, especially in high-power industries or near high-voltage distribution switchyards.

We can easily purchase ICs and/or software that have enjoyed the benefit of experts with aggregate experiences of hundreds of man-years *solely* in protecting data in communications links. So we should always buy these, as they will be much more cost-effective than anything we might think we can do ourselves, no matter how clever we are.

Ethernet and CAN bus are but two examples of robust datacommunications, but they are not perfect – in extreme EM environments the data rate of Ethernet can drop to zero, and so can the CAN bus, due to a small oversight in the CAN bus standard [19]. More sophisticated protocols exist, one highly respected example being that used by the real-time MIL-STD-1553 bus, of which commercialised versions are now available.

6.1.8 Use all the other EM design techniques too...

The EM engineering techniques described in the earlier parts of this series [13] [14] [15] [16] [17], as well as those in [18], control E, H and EM-fields and so can be used to improve immunity to E- and H-fields from ESD events. Sometimes the techniques were described with examples of reducing emissions, and sometimes of improving immunity, but any technique that attenuates fields and/or conducted noise is equally effective for either purpose.

The fields from ESD events within a few metres can be very strong, making it necessary to take more care over the EM design, going into finer detail (e.g. using λ/100 gaps in seams instead of λ/10). Other sources of advice on good ESD design include [4] and [5].

6.1.9 Software techniques

Software is easily corrupted by transient voltages due to ESD, leading to a variety of possible errors, malfunctions and crashes. Where the hardware techniques in this series do not provide sufficient immunity to transient or short-term events such as ESD, or are too impractical or too costly, appropriate software programming techniques can be a huge help – and of course they generally add no cost in manufacture.

This series has described hardware techniques only, because this is where my experience and skills lie. I dare not write about software, because my ignorance in that area would soon be revealed, so instead I refer the reader to people who *do* understand software techniques for EMC, especially [20] [21] [22] [23] [24] [25], section 12.2.5 of [4], and Chapter 37 of [5].

Of course, software techniques cannot work if the devices the software runs on are damaged from ESD or other EM disturbances (e.g. surges). However, the use of multiple redundant processor 'channels' with voting and other operations on their independent outputs can be used to detect faulty digital processors, whether the errors are transient or permanent due to damage.

But it important to note that redundant hardware channels are often all exposed to the same EM disturbance in (almost) the same way at (almost) the same time, for example an E or H-field from a nearby ESD or lightning ground stroke, or an overvoltage surge on their common mains power supply.

So if all of the channels use the same technology and construction, they can all fail in the same way at the same time. This is a bad thing and is known as a 'common-cause' failure. It is best dealt with by using:

- Diversity of design (e.g. different types of microprocessor, different software languages, different PCB layouts, different designs of power converters, etc.), plus…
- Diversity of location and cable routing (e.g. not placing all the channels in the same cabinet, not routing all the cable sin the same trunking, etc.), plus…
- Diversity of power supply (e.g. more than one independent mains supply, battery backup, etc.).

For very high-reliability systems, such as those that control weapons, financial institutions, national security and safety-critical applications such as fly-by-wire passenger aircraft, a great deal of care needs to be taken with ensuring diversity of design. It can even require the different software programmes for the diverse channels to be written to different requirement specifications produced by different teams of people who have never shared the same university courses or employers.

6.2 to 6.6 will appear in Issue 75

6.7 References

[1] Keith Armstrong, "*Design Techniques for EMC*", UK EMC Journal, a 6-part series published bi-monthly over the period February – December 1999. An improved version of this original series is available from the "Publications & Downloads" page at www.cherryclough.com.

[2] The Institution of Engineering and Technology (IET, was the Institution of Electrical Engineers, IEE), Professional Network on Functional Safety, "*EMC and Functional Safety Resource List*", from the "Publications & Downloads" page at www.cherryclough.com.

[3] Anita Woogara, "*Study to Predict the Electromagnetic Interference for a Typical House in 2010*", 17 September 1999, Radiocommunications Agency Report reference MDC001D002-1.0. This Agency has now been absorbed into Ofcom, and at the time of writing this report is available via the 'static' legacy section of the Ofcom website, at: http://www.ofcom.org.uk/static/archive/ra/topics/research/topics.htm.

[4] Tim Williams, "*EMC for Product Designers, 4th Edition*", Newnes, December 2006, ISBN: 0-7506- 8170-5, www.newnespress.com.

[5] John R Barnes, "*Robust Electronic Design Reference Book, Volume I*", Kluwer Academic Publishers, 2004, ISBN: 1-4020-7737-8, www.wkap.com.

[6] Tim Williams and Keith Armstrong, "*EMC Testing*", a series in seven parts published in the EMC & Compliance Journal 2001-2, available from the 'Publications & Downloads' page at www.cherryclough.com.

[7] Guides on the IEC/EN 61000 series test standards mentioned in this article have been written by Keith Armstrong with the assistance of Tim Williams, and published by REO (UK) Ltd, and are available from www.reo.co.uk/guides. In addition to describing the compliance test methods, they discuss how and where the EM disturbances arise, what they effect, and how to adapt the immunity test methods to real-life EM environments to reduce warranty costs and also improve confidence in really complying with the EMC Directive's Protection Requirements.

[8] Martin O'Hara, "*Electrostatic Discharge Testing for Automotive Applications*", EMC-UK 2007 Conference, Newbury Racecourse, 16-17 October 2007.

[9] "*Characterization of Human Metal ESD Reference Discharge Event and Correlation of Generator Parameters to Failure Levels — Part I: Reference Event*" and "*— Part II: Correlation of Generator Parameters to Failure Levels*" by K Wang, D Pommerneke, R Chundru, T Van Doren, F P Centola, and J S Huang, IEEE Transactions on EMC Vol. 46 No. 4 November 2004, pages 498-511.

[10] Doug Smith, "*Unusual Forms of ESD and Their Effects*", Conformity 2001, page 203, www.conformity.com. This article originally appeared in the 1999 EOS/ESD Symposium Handbook, and can be downloaded from http://www.emcesd.com.

[11] Doug Smith's website, from which numerous very interesting articles on real-life ESD can be downloaded, is: http://emcesd.com.

[12] "*The First 500 Banana Skins*", Nutwood UK Ltd, 2007. This very interesting book costs about £10 plus post & packaging from pam@nutwood.eu.com or via http://www.compliance-club.com.

[13] Keith Armstrong, "*Design Techniques for EMC, Part 0 – Introduction, and Part 1 – Circuit Design and Choice of Components*", The EMC Journal, January 2006 pp 29-41, plus March 2006 pp 30-37, available from http://www.compliance-club.com.

[14]Keith Armstrong, "*Design Techniques for EMC, Part 2 – Cables and Connectors*", The EMC Journal, Issues 64 and 65, May and July 2006, from the EMC Journal archives at www.compliance-club.com.

[15]Keith Armstrong, "*Design Techniques for EMC, Part 3 – Filtering and Suppressing Transients*", The EMC Journal, Issues 66-68, September and November 2006, and January 2007, from the EMC Journal archives at www.compliance-club.com.

[16]Keith Armstrong, "*Design Techniques for EMC, Part 4 – Shielding*", The EMC Journal, Issues 69-71, March, May and July 2007, from the EMC Journal archives at www.compliance-club.com.

[17]Keith Armstrong, "*Design Techniques for EMC, Part 5 – PCBs*", The EMC Journal, Issues 72 and 73, September and November 2007, from the EMC Journal archives at www.compliance-club.com.

[18]Keith Armstrong, "*EMC for Printed Circuit Boards, Basic and Advanced Design and Layout Techniques, 1st Edition*", Armstrong/ Nutwood, January 2007, ISBN: 978-0-9555118-1-3 (softback perfect bound) or 978-0-9555118-0-6. For a contents list visit www.cherryclough.com. To order, email pam@nutwood.co.uk.

[19]Brian Kirk, "*Using software protocols to mask CAN bus insecurities*", IEE Colloquium on "*Electromagnetic Compatibility of Software*", 12th November 1998, IEE Colloquium digest reference No. 98/471.

[20]John R Barnes, "*Designing Electronic Systems for ESD Immunity*", Conformity, Vol.8 No.1, February 2003, pp 18-27, download from http://www.conformity.com/0302designing.pdf

[21]John R Barnes, "*Designing Electronic Equipment for ESD Immunity, Part* I", Printed Circuit Design, Vol. 18 no. 7, July 2001, pp. 18-26, http://www.dbicorporation.com/esd-art1.htm, and: "*Designing Electronic Equipment for ESD Immunity, Part II*", Printed Circuit Design, Nov. 2001, http://www.dbicorporation.com/esd-art2.htm.

[22]Dr D. Coulson, "*Software Tips for Immunity in Microcontroller System Designs*", Approval magazine, Mar/April 1998, pages 16-18.

[23]Dr D. Coulson, "*EMC – Software Hardening of Microcontroller Based Systems*", Electronic Engineering, March 1999 pages 12-15.

[24]IEE Colloquium, "*Electromagnetic Compatibility of Software*", 12th November 1998, IEE Colloquium digest reference No. 98/471.

[25]Dr D R Coulson, "*EMC-Hardening Microprocessor-Based Systems*", IEE Colloquium: "*Achieving Electromagnetic Compatibility: Accident or Design*", Wednesday 16th April 1997, Colloquium Digest reference No. 97/110.

Note: IEE colloquium digests cost around £20 each (+ p&p if you are outside the UK) from IEE Publications Sales, Stevenage, UK, phone: +44 (0)1438 313 311, fax: +44 (0)1438 76 55 26, sales@theiet.org. They might not keep digests before a certain date, in which case contact the IET Library on +44 (0)20 7344 5449, fax +44 (0)20 344 8467, libdesk@theiet.org.uk.

[26]Moore's Law, see http://en.wikipedia.org/wiki/Moore's_law

6.8 Acknowledgements

I am very grateful to the following people for suggesting a number of corrections, modifications and additions to the first series published in 1999 [1]: Feng Chen, Kevin Ellis, Neil Helsby, Alan Keenan, Mike Langrish, Tom Liszka, Tom Sato, and John Woodgate.

Eur Ing Keith Armstrong CEng MIEE MIEEE
Partner, Cherry Clough Consultants,
www.cherryclough.com, Member EMCIA
Phone: +44 (0)1785 660 247, Fax: +44 (0)1785 660 247,
keith.armstrong@cherryclough.com;
www.cherryclough.com