Immunity requirements related to design choices

Tim Williams
Elmac Services
www.elmac.co.uk

Introduction

RF emissions design limitations and requirements are normally set by legislation, although there is often a need to prevent mutual interference with wireless receivers on-board or nearby. But immunity requirements are harder to pin down. In the EU the EMC and R&TTE Directives require "adequate" immunity. In other jurisdictions, with few exceptions, there are no legal immunity requirements. However some sectors, for instance military, automotive and railway equipment, do have particular specifications. In these cases the spec is normally set by the customer rather than by legislation and there is the opportunity for negotiation on a technical basis. In some other instances, such as electricity meters or alarm systems, there is an industry standard which mandates immunity and regardless of legislation, a product which doesn't meet it cannot be sold.

But this still leaves many sectors and applications where it is up to the manufacturer to define an adequate level of immunity. Any product will be placed into an environment in which each of its various interfaces is subjected to a range of electromagnetic stresses (Figure 1). How should the level of immunity be decided, and what do these decisions then mean for the design of the product?

Figure 1   The electromagnetic stress demons surround every electronic product

There are various aspects of the question which can be addressed systematically. Many are covered by EMC standards. These include:

- the phenomena to be guarded against

- the levels of applied stress for each phenomenon, and the ports to which it is applied

- the performance criterion to be applied, and the operating mode(s) to be verified, in each case

These headings form the basis for a test plan, which can and should be laid down at an early stage of a new design. But they should also guide the design team in their choice of mitigation techniques. This article looks at the way design choices can be married to the immunity requirements: the critical question for designers is always, how much EMC mitigation is enough? We can partition the problem, on the basis of phenomena, into continuous stresses (application of criterion A in the generic standards) and transient stresses (criterion B), with a mention also of low frequency immunity issues.
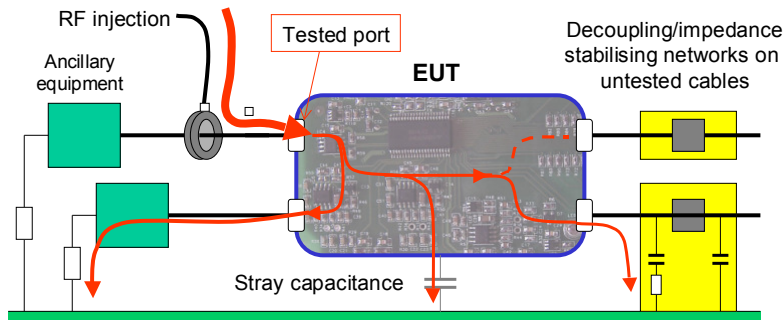
Continuous phenomena: conducted and radiated RF

As a general rule, and one that is subject to exceptions, digital circuits are less susceptible to continuous RF while analogue circuits are more so. There are quite a few designers of purely digital circuits who treat the RF immunity tests with disdain, because they've never seen a failure. But analogue designers are (or should be) far more familiar with RF susceptibilities and always need to take design precautions. These are principally of two sorts, mirroring the two routes of coupling: via connected cables, and directly with the circuit.

Cable coupling: interface protection

The standard cable-coupled RF immunity test of IEC 61000-4-6 requires an injected level, typically of 3V or 10V open circuit voltage from a source impedance of 150Ω, in common mode into each interface to be tested. The test frequency range is 150kHz – 80MHz, with a possible extension up to 230MHz; from the design point of view, you can assume that cable-coupled RF must be anticipated certainly up to this higher frequency [1]. The real RF environment is quite well represented by this requirement. MF (300kHz-3MHz) and HF (3MHz-30MHz) interference levels of several volts are relatively rare, but possible if a product is located near a broadcast or amateur-band transmitter and connected to a long cable. Above 30MHz, sources are more likely to be mobile transmitters in the neighbourhood, but these can quite easily create common-mode cable voltages of a few volts if they are within a few metres. Military products, mounted on the same platform (aircraft, ship or vehicle) as HF transmitters can see substantially higher levels; the DEF STAN 59-411 DCS02 test for instance can inject 115dBμA (560mA, or 56V in a 100Ω system) over 10 – 100MHz for safety critical aircraft equipment.
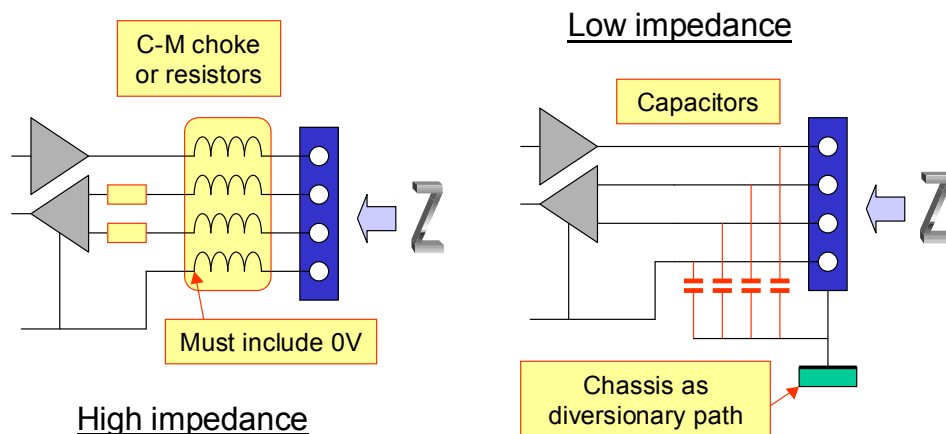
These tests mean that every cable interface needs *RF common mode filtering or screening*, effective up to at least 200MHz and perhaps beyond. This is not just on interfaces that will be tested; even untested interfaces will see some level of common mode RF current, as Figure 2 makes plain. Plus of course, in the radiated case, all connected cables are subjected to the stress. The current injected into any one interface must flow back to its source through some common mode path, and this will typically include every other connected cable. The path(s) taken by the disturbance will be determined by the various ratios of common mode impedances both within and outside the product. Only if the product's chassis is well grounded, and if every tested interface is well filtered to this chassis, can untested interfaces be ignored.

Figure 2   Injected RF passes from the tested port through other ports to ground
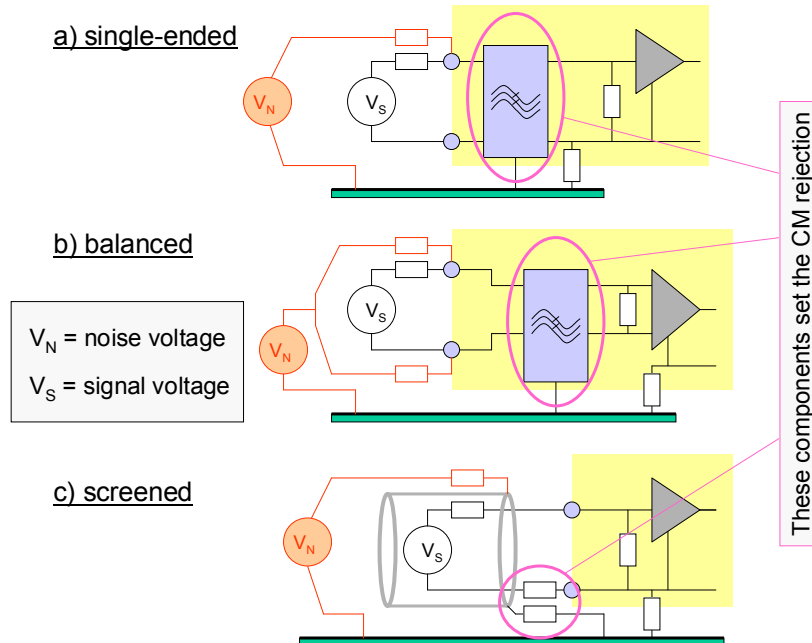
The choice of filtering or screening the cable interfaces depends on how much control you can exert over the connected cables, what signals they carry, and the cost constraints on the product. Generally it is preferable to rely on filtering alone, because screened cables are more expensive and require greater effort on the part of the installer; they also need a proper ground structure for the screen connection. But the advantage of a screen is that, when correctly implemented, it can attenuate interference by several tens of dB more than a simple filter can achieve, especially important if the interference is in the same frequency range as the wanted signal. Video and wideband data circuits fall into this category.

The *RF common mode filter* can be configured to be high impedance or low impedance. Low impedance implies capacitive filtering to chassis; high impedance means a common mode choke (Figure 3). One technique will reduce current flow and leave a high common mode voltage at the interface, but without this voltage affecting the circuit. The other technique diverts current into a harmless route and leaves a low common mode voltage at the interface, but only as long as the diversionary route is itself low impedance. A combination of both is of course possible, and necessary if the attenuation of a single stage is inadequate. The choice depends firstly on the possibility of implementation (for instance, parallel capacitors are ruled out for high-speed interfaces) and then on the native impedance of the unfiltered interface – a high-impedance input will not benefit much from a series choke, while a low-impedance input won't be helped much by capacitance. The choice is also affected by whether or not a particular interface expects to see EFT/Burst transients (see later), as a simple choke at the interface may not be able to cope with high voltage bursts applied directly in series with it.

Figure 3   High versus low common mode impedance

To a first order, the applied stress level sets the required common mode rejection for the input filtering, compared to the level of the wanted signal (see Figure 4). For instance, if a video channel can cope with 30mV before in-band interference becomes obtrusive, then a rejection of 40dB against 3V is needed. But classical video connections are generally single-ended rather than differential, and single-ended filtering can't separate in-band interference from the signal. Hence *screening* is usually required, and then the screening attenuation is dominated by the transfer impedance at the shield connection to chassis.

Figure 4   Equivalent circuit of voltage injection at inputs

On the other hand, balanced interfaces such as for data communications can use effective in-band common mode filtering; and low-frequency single ended interfaces for audio or transducers can be effectively filtered against RF from150kHz upwards.

Imperfections tend to upset the neat equivalent circuits shown in Figure 4: component imbalance, resonances, and inadequate layout. The last of these will affect either the ground path or the effectiveness of the filter components, or both. Too much inductance in the ground connection will limit the attenuation of any capacitive filtering, and too much coupling across a common mode choke will limit its impedance. Resonances can be related to layout imperfections, self-resonance in filter components or spurious frequency responses in operational circuits. Sometimes they can be modelled into the equivalent circuit if the causal parameters are known, but especially at higher frequencies they can be impossible to anticipate. However, it is rare for such unintentional resonances to have a high Q, and this means that their impact on the circuit's RF response is moderate. In many cases their effect can be mitigated by designing an extra 20dB into the interface protection, over what is required according to the simple equivalent circuit.

For balanced circuits, the filter components can influence the common-to-differential mode conversion. Common mode RF attenuation becomes increasingly effective as the frequency rises, but at the lower frequencies, there is the threat of conversion of the common mode disturbance into a differential mode input, which of course cannot be rejected by the input amplifier.

If the entire circuit is perfectly balanced, then this conversion does not occur. But actually maintaining balance requires that every component in one half of the circuit

exactly mirrors that in the other: not only its intended value but also the values of its unwanted parasitics. This is not easy to achieve. In the common mode choke, the construction of the windings will cause a small degree of imbalance in the inductance of each half and in the stray capacitance associated with each half, figures which are never quoted in the data for such parts. But if discrete components are used for the capacitors, their tolerances are usually the dominant source of imbalance: depending on their construction, COG ceramic capacitors are typically ±5% or ±10%, while X7R can easily be ±20%. Some capacitor types, intended specifically as I/O filters, have tolerances as wide as +50% –20%. If you are designing a capacitor filter for a balanced circuit, be sure to evaluate the effect of worst case tolerances on the common-to-differential mode conversion across the frequency range.
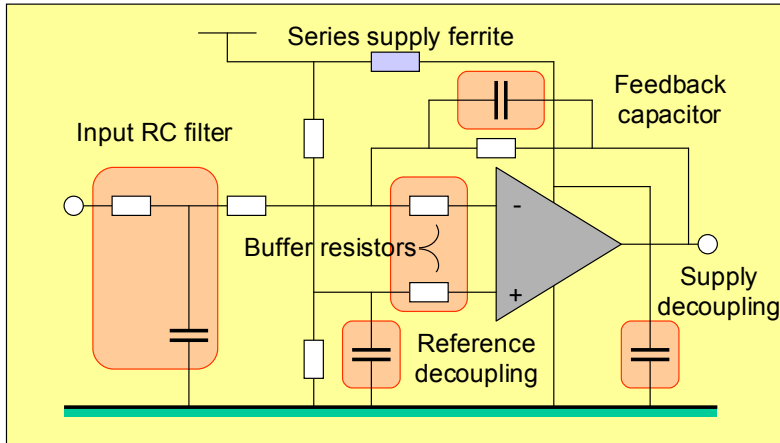
Radiated coupling: circuit design, layout and shielding

Radiated RF interference couples principally via connected cables up to frequencies of the order of 200MHz, when cable lengths are closer to quarter-wavelength multiples than are the structural components of the product, including its PCBs. But a quarter wavelength at 250MHz is 30cm, and so for typical product sizes RF coupling becomes more efficient with structures than with cables above this frequency. RF coupling directly with internal structures cannot be dealt with by interface filtering. So for these frequencies, mitigation techniques must concentrate on

- Good PCB and internal layout

- Bandwidth limiting at the circuit level

- Shielding, either of the whole unit or subsections of it

Standard *PCB layout* principles to control RF emissions are also good for immunity: foremost among these is the ground plane [2][3]. But we are not so much concerned with tracks carrying intentional HF currents, as those which carry low-level broadband signals that will be affected by the directly induced disturbance. The protection afforded by the ground plane must be extended to these.
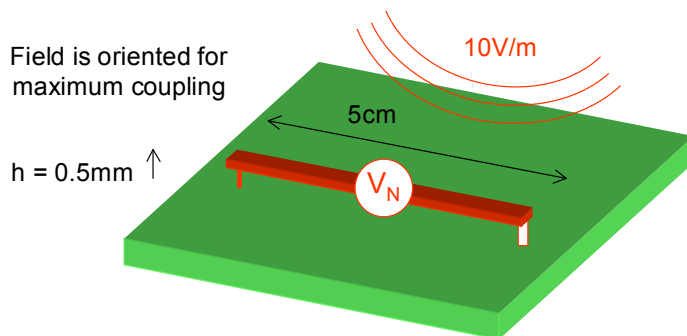
Bandwidth limiting is a simple but vital technique for any low frequency analogue circuit (Figure 5). Many analogue amplifiers will respond to RF, especially if it is applied across their input pins, well beyond their intended operating frequency [4]. It's therefore necessary to make sure that such RF doesn't appear anywhere in the circuit where it could create a non-linear response, as Figure 5 shows; RC filters and series buffer resistors are a standard technique for this, as is decoupling of power supplies and reference voltages using both series and parallel components. The time constants of the filters should be chosen to have no effect on the signal circuit but to adequately attenuate the unwanted interference; a simple RC filter shows a 20dB/decade increasing attenuation above its corner frequency of $1/2\pi RC$, so for instance a 220Ω + 10nF network will have little effect below 70kHz but give better than 40dB above 7 MHz (although parasitic L in series with the C, and C across the R, will kick in and limit the attenuation at higher frequencies).

Figure 5   Circuit methods for bandwidth limitation

As with cable coupling, an estimate of induced RF in known sensitive parts of an unshielded circuit can be made from a knowledge of simple antenna structures and applied stress levels, so that the required degree of filtering can be predicted to an order of magnitude. And also as with cable coupling, resonances in the structures, and parasitics and undetected layout mistakes, will limit the effectiveness of such predictions.

Faraday's law can be invoked to give an order of magnitude estimate of voltage induced into a circuit of a particular area. So for instance, take a 5cm long track placed 0.5mm above a continuous ground plane as might be found on a standard four-layer board (Figure 6). We have to make the initial assumption that the impinging field is a plane wave with the free-space impedance of 377 ohms. Then a 10V/m field has a magnetic component of $(10/377) = 27$mA/m or $34 \cdot 10^{-9}$ Tesla (1A/m $\equiv 4\pi \cdot 10^{-7}$ T in non-magnetic media).

Figure 6   RF voltages induced into a circuit by direct coupling

Faraday's law states that the induced voltage

$$V \quad = \quad -A \cdot dB/dt$$

where A is the loop area in m^2 and B is the magnetic flux density in Tesla.

dB/dt is frequency dependent and can be given by $2\pi F \cdot B$ for a sinusoidal signal (F in Hz). So to take the above geometry and incoming field at two different frequencies, say 50MHz and 600MHz, we have an induced interference voltage (ignoring the minus sign) assuming maximum coupling of

$$V_{50MHz} \quad = \quad 25 \cdot 10^{-6} \cdot 2\pi \cdot 50 \cdot 10^{6} \cdot 34 \cdot 10^{-9} \quad = \quad 0.267mV$$

$$V_{600MHz} \quad = \quad 25 \cdot 10^{-6} \cdot 2\pi \cdot 600 \cdot 10^{6} \cdot 34 \cdot 10^{-9} \quad = \quad 3.2mV$$

This calculation ignores the electric field coupling, which is acceptable for low impedance circuits and small structures, and it also becomes invalid for higher frequencies where the structure dimensions are significant with respect to a quarter wavelength: in FR4 fibreglass with a relative permittivity of 4.5, a quarter wavelength at 600MHz is $3 \cdot 10^8/(600 \cdot 10^6 \cdot 4 \cdot \sqrt{4.5}) = 11.8$cm. Even so, it demonstrates why it is that digital circuits on surface-mount multilayer boards are rarely affected by RF interference at the commercial field strength levels – a few millivolts is neither here nor there to a digital signal, though it could be to a low-level ADC or audio or video amplifier.

Shielding should really be a method of last resort, when filtering and layout control are inadequate or unavailable. This is often not so much because of direct coupling to PCBs, as because internal wiring between PCBs has not been sufficiently protected. Such wiring should in best practice be treated as the PCB tracks themselves, and provided with a ground plane structure – double sided flexi connectors are a quite simple way of doing this. Alternatively, treat each internal board-to-board connection as if it were external, and implement filtering for VHF and above on interfaces to these connections. Small ferrite chips and low value three-terminal capacitors are good for this purpose.

High levels of RF stress (30V/m and above) as are found in military or automotive applications, and/or analogue circuits that are sensitive at the sub-millivolt level, normally mandate shielding. Important design issues for shielding are mostly mechanical and centre around minimising apertures in the shield. The larger the maximum aperture dimension, the less effective the shield becomes; and whatever you do, such apertures (for instance ventilation slots) should not be placed anywhere near sensitive circuits, either components or tracks.

RF immunity of digital circuits

Generally, digital circuits are more robust against RF interference than analogue, as mentioned above. When RF susceptibilities do happen, they can be divided into two types – timing effects, and spurious transitions (Figure 7).

As an increasing RF induced disturbance is superimposed on a digital signal the first effect that occurs is that the intentional signal transitions are modulated by the interference and timing jitter occurs. Therefore, a digital design that is not critically dependent on timing accuracy will be more immune than one in which timing has been "tuned" for maximum performance.

Beyond this, higher levels of interference will push the node voltage to a point at which spurious transitions occur. Maximum susceptibility will be when the interference is in-phase at the same frequency as any ringing on the intentional transitions. The unwanted transitions are likely to propagate through the digital network causing corruption of data transfer and swift failure of the digital program. The exact point at which this happens will be a function both of coincidence in timing and the levels induced in particular nodes; trying to detect and deal with the problem on a node-by-node basis will usually be unrewarding, and so it is necessary to implement good layout practice in all the active parts of the digital circuit. At the same time, good signal integrity design – proper decoupling, 0V impedance control, transmission line routing and matching – will improve immunity, since signal nodes with marginal integrity will be inherently more affected by induced superimposed RF.
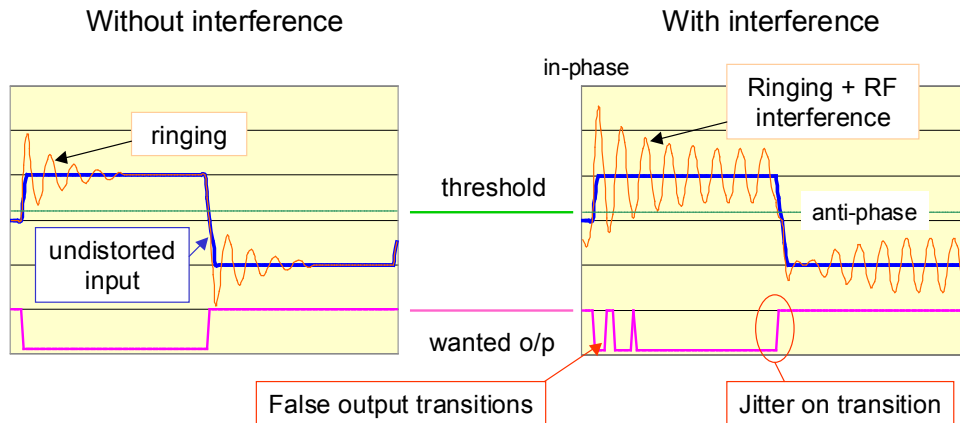
Figure 7   RF interference effects on digital signals

Transient phenomena: ESD, burst and surge

By contrast with the above discussion, transient immunity is more of a problem for digital than analogue circuits. Nanosecond-period spikes occur in the same time frame as a digital clock cycle and can therefore corrupt a single data transfer, resulting in complete failure of the program. In an analogue application, the same disturbance may be completely ignored by the signal circuit simply because it can't respond fast enough. On the other hand, bursts of short duration pulses lasting for milliseconds may still have enough energy to disturb or overload some analogue functions, particularly if their bandwidth is not sufficiently limited. And in either case, surge transients may cause not only disruption but actual circuit damage.

Electrostatic discharge

It is common for ESD to be a problem for most digital designs. There are two diametrically opposed techniques for dealing with the ESD threat:
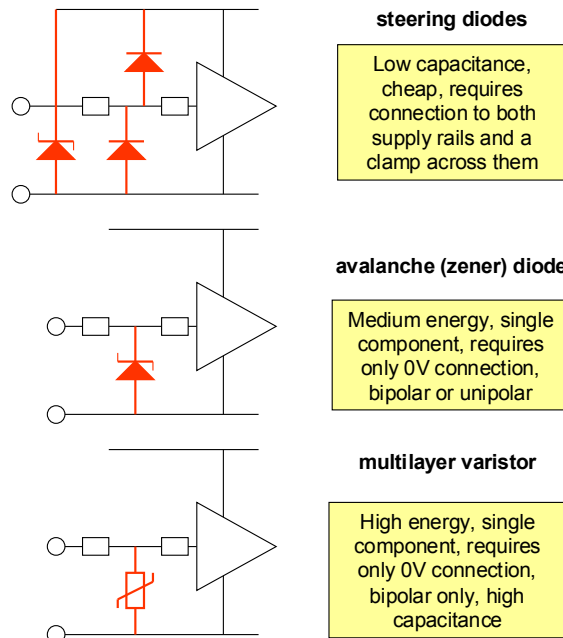
- Accept that an ESD strike will occur to any exposed metalwork, and divert it away from the operating circuit;

- Design the housing of the product to avoid an ESD strike altogether.

In both cases, it is necessary to ensure that the circuit can cope with radiated ESD transients due to nearby events, which means that any potentially susceptible circuit node is protected by good layout and if necessary by filtering. Any edge-triggered circuit is potentially affected by the ESD; the leading edge of the waveform can reach several amps in less than a nanosecond, meaning that the rise time is 10^9–10^{10} amps/second. Interrupts, and particularly resets should be treated as critical. Layout of the track which carries the signal should ensure that it is protected by a continuous ground plane. Where the signal connects to an input pin, such as the RESET of any processor, it would be sensible to include an RC filter, with a time constant of 100-500ns: a series 1k resistor and a 100pF capacitor between the sensitive pin and its nearest 0V pin is fine.

Power supply decoupling must not be ignored; it's not just an emissions requirement. Transient variations in the power rail voltage can cause functional corruption, and an ESD pulse can create such a variation. Decoupling, with the same HF principles as for emissions, is essential to prevent such variations.

ESD-specific interface protection should only be mandatory if strikes directly to connector pins are intended or likely in the real environment. However, as with RF, ESD current can flow out through interfaces as a result of strikes elsewhere on the product (see Figure 2). Some protection of such interfaces is therefore advisable. There are various types of protection device which should be selected on the basis of application: fast data communications interfaces such as USB or LVDS will need low capacitance devices, while power supplies can cope with much higher capacitance and leakage.

steering diodes

Low capacitance, cheap, requires connection to both supply rails and a clamp across them

avalanche (zener) diode

Medium energy, single component, requires only 0V connection, bipolar or unipolar

multilayer varistor

High energy, single component, requires only 0V connection, bipolar only, high capacitance

Figure 8   ESD interface protection options

Remember that the same interface will also potentially be subjected to volts of continuous RF, and the ESD protection scheme should be integrated with the RF protection. In the simplest case, this means that RF filtering capacitance can be paralleled with a zener-type breakdown device to prevent overvoltage on this capacitance. Unfortunately, such protection diodes can rectify the applied RF and may in fact make RF immunity worse. Therefore the RF filter attenuation should be designed with the intention of keeping voltages across these diodes below their threshold of non-linearity.

The actual voltage that will appear across the interface will not be anything like the full ESD voltage: it will be attenuated by a complex circuit of impedance dividers involving the capacitance and series impedance of the source, the capacitance of the interface filtering, and the various series impedances between the source and the ground return path. With a full knowledge of these impedances it would be possible to model the voltage and current waveforms at critical points, but diagnostic and confidence testing is quicker, cheaper and usually more reliable.

Enclosure design has to respect the ability of the ESD strike to find its own path. Apertures and discontinuities represent inductance and hence a high impedance to the current; but conversely, short-distance gaps can be bridged by a high voltage arc. Designing a plastic case to avoid discharges involves ensuring that there are no creepage paths from the outside to any conductive points inside. Any floating metalwork (including unconnected copper on the PCB) can acquire a high static charge due to ESD events, which may then create internal discharges; all such metallic parts should be connected, typically to chassis or to 0V.
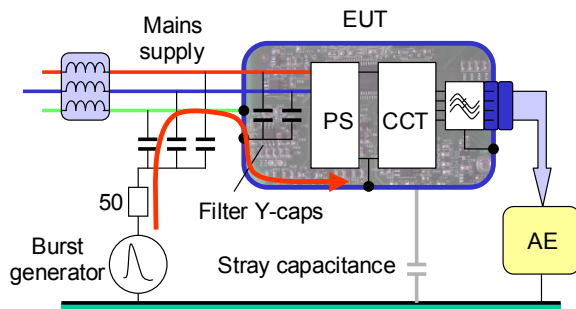
Electrical fast transient bursts

EFT bursts are easily dealt with if capacitive filtering to a solid chassis metalwork is available for all tested interfaces. Typical EFT/B failures are due to an inadequate or unavailable interface ground reference. The most recent second edition of IEC 61000-4-4 applies the burst always in common mode with respect to the test set-up ground plane; the first edition didn't make this clear, and so some testers would apply the burst separately to mains L, N and E individually. Particularly with power supply susceptibilities, this could cause different failure mechanisms compared to the straight common mode application.

Using the second edition, mains EFT/B transients will be applied to any protective earth (PE) terminal in parallel with live and neutral, so a path must be provided back to the outside world which doesn't involve the circuit. The PE will typically be connected to chassis metalwork which will therefore be carrying the full burst voltage. Not much burst energy will appear between the chassis and the circuit, but it will stress any unprotected (filtered or screened) interfaces, and stray capacitance from the circuit to the outside test ground plane will also play a part (Figure 9). This means that circuit-level transient protection is as important for EFT/B as it is for ESD, and the same techniques are useful for both.

High frequency filtering capacitors at some point before any active circuitry are always needed to cope with both EFT/B and RF interference on the power supply. For signal interfaces, the chosen method of protection (high impedance choke versus low impedance capacitors) will depend on whether the protection components are able to tolerate the expected applied levels. The typical residential-environment level of 500V can usually be blocked by a choke circuit, but higher industrial levels of 1kV will need a more robust approach, involving parallel capacitance, protection diodes or isolation.
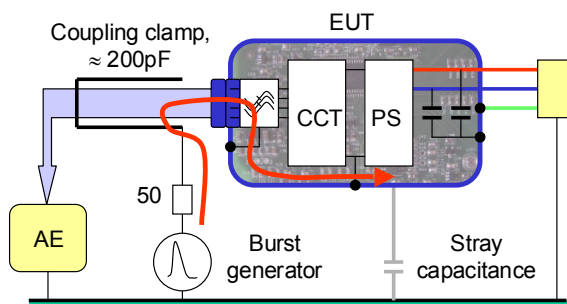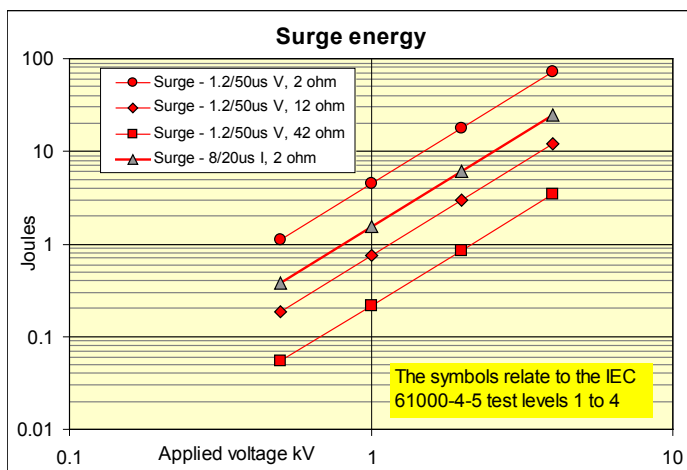

Figure 9   Equivalent circuits for EFT/B application according to IEC 61000-4-4

Surge

Surge protection is principally a matter of ensuring that the high voltage applied (from a low source impedance) during a surge event is prevented from damaging active circuitry at the power supply or signal interfaces. This can be achieved either by designing an interface to tolerate a high voltage – using over-rated components, series resistors and steering diodes, or transformer or opto-isolation – or by clamping the surge voltage itself to a tolerable level. Over-rating may be feasible if the surge voltage is no more than 500V, but gets rapidly impractical for surges in excess of 1kV, which may be applied in common mode or differentially. If it is employed, not just the component ratings but also the creepage and clearance distances across PCB tracks and other conductors that may be exposed to the full voltage must be investigated and adequately controlled.

Surge clamping is an effective technique but requires the clamp devices to be correctly positioned and matched to the expected surge energy and voltage. The common IEC 61000-4-5 test has a predictable energy (Figure 10), but designing only for this doesn't guarantee protection under all real-life conditions, and some over-specification is advisable. The most important design criterion for the surge protection device is that the voltage developed across it by the peak surge current is still less than can be withstood by the downstream circuitry. This can easily be twice the rated voltage of the device, which is typically quoted at 1mA (all devices have published curves which show the voltage-current profile); which is to say that for instance a 39V part, to adequately protect a 24V ±25% supply, demands a downstream voltage withstand of at least 80V and preferably 100V. Then the size of the protection device is determined by the maximum energy that can be deposited in it by a surge of a given waveshape and voltage from a given source impedance. The IEC 61000-4-5 surge comes from a source impedance of 2, 12 or 42 ohms depending on whether it is applied across mains L-N, mains LN-E, or signal lines.

This is the energy available to be delivered from the IEC 61000-4-5 generator into a matched resistive load, which is not the same as would be delivered into a non-linear clamping device

Figure 10   Surge energy versus applied voltage

In some applications it is feasible to include some extra series impedance at the interface, which allows the energy rating of the surge protector to be reduced, although this is not usually possible for power supplies. But such a series impedance will be exposed to the lion's share of the surge voltage, assuming the clamp works correctly, and this often means that providing the impedance is not trivial; for instance, a 1kV peak surge applied through a few hundred ohms to that 39V surge protector will drop around 950V across

the resistor, which has to withstand this voltage without arcing over or breaking down. Your standard quarter-watt 0805 part can't do this, and a (larger) surge rated resistor is needed.

The clamping device(s) have to be located directly across the appropriate interface terminals to which the surge will be applied, bearing in mind that the whole purpose of such a device is to conduct a current when the surge occurs. Therefore any stray inductance in the path will drop a voltage given by $-L \cdot di/dt$, which will unavoidably be added to the clamp voltage.

Power supply variations

AC mains supplies

Finally, but by no means trivially, we have to consider low frequency supply variations. For AC supplies this means dips and interrupts, and inrush current control. Apart from defining a hold-up time for allowing the product's power supply to ride through short supply droops (which is usually determined by the power supply's DC link reservoir capacitor), the main design challenge posed by dips and interrupts is ensuring that the equipment re-starts correctly after a brown-out or black-out. For any processor-based product, this means a power management sub-system, which monitors the incoming supply, saves the state of the processor when the voltage drops below a critical value, and initiates a controlled power-up sequence when it rises above another critical value. Of course, many ICs are available which deal with these functions in a single package. The designer still has to check that the sub-system can deal with all variations that the power input can throw at it, and these are legion. Not only straight power-up and power-down, but also voltages which may hover around the brown-out thresholds for milliseconds or even seconds, should be anticipated. Selecting the correct hysteresis between the power-down and power-up thresholds, and matching this to the worst case ramp-up, hold, and ramp-down time constants of the PSU and the start up and shut down response times of the processor, are critical to this design process, as is rigorous testing of the result.

Control of inrush current is not strictly an immunity issue, but it is included here because its design aspects are integrated with the rest of the power supply input. For low power products it is hardly relevant. However, the flicker standard IEC 61000-3-3, which applies to everything mains-supplied below an input current of 16A, does place an effective limit on inrush. It limits d_{max}, the maximum step voltage change introduced by the product on the mains, to 4% of the supply voltage (if no additional conditions are invoked). The voltage change is measured through a "reference impedance" of 0.4 + j0.25 ohms. For a 230V supply, and neglecting the reactive part of the impedance for simplicity, this corresponds to a maximum allowable inrush current of 23A.

The standard is of course more complicated than this and requires detailed study if your design is likely to approach this level. And more specific inrush current requirements may apply due to customer specifications, or your own policies. There are two typical design approaches which can be used to control inrush:

- The simple one, using an NTC thermistor in series with the supply. When it is cold, its resistance limits the current that can be drawn, but the operating current heats it up, causing the resistance to fall, and a stable operating point is reached where the part dissipates enough power to keep it hot and low-resistance. It's cheap, and has no unpleasant interactions with other EMC-related issues such as RF or transient interference. But it is intentionally a hot, dissipative component, and although

effective from a cold start it doesn't work if the power goes away momentarily, so won't control inrush resulting from a short interruption.

- More complex circuits using triac or MOSFET devices to ramp up the input current under control of a specific time constant. Although offering a much better controlled and less dissipative characteristic, and perhaps being integrated with a power factor correction circuit where this is necessary, such circuits use many components and are hence expensive, and may be affected by incoming supply interference if they are not carefully designed. They should always be located downstream from the RF and transient protection filter, which must be the first thing the incoming supply sees.

DC supplies

DC inputs have similar requirements to those above, plus may need reverse polarity protection and have a more extreme overvoltage specification. Reverse polarity protection can be implemented with a single series diode, but if this takes too much voltage drop it may instead be done using a series MOSFET and control circuit, which can be integrated with inrush current control.

Some DC inputs have a much wider supply voltage range than the public AC mains supply; ±25% or 30% might be expected from an automotive or marine battery; a one second overvoltage withstand of 1.4 times nominal voltage is mandated by railway procurement standards. These aspects must be anticipated at the start of the power supply design, since they can be dealt with by suitable component rating if understood early enough.

Conclusion

Immunity requirements come in many shapes and sizes, but have a common basis, which is the need for a product to be fit for purpose in its intended electromagnetic environment. All such requirements have implications for product design over and above its straightforward functionality, but provided they are expected and anticipated in the design process, they can be successfully addressed.

References

[1] *Pitfalls & Practice of IEC 61000-4-6 conducted immunity testing*, Tim Williams and Richard Marshall, EMC Journal 58, May 05

[2] *The Ground Plane: Lord of the Board*, Tim Williams, EMC Journal 72, September 07

[3] *EMC for Printed Circuit Boards: Basic and advanced design and layout techniques*, Keith Armstrong, Nutwood UK January 2007

[4] *Uncertainties of immunity measurements, Annex F: circuit susceptibility investigation*, DTI project R2.2b1, Schaffner/Elmac 2002, available from www.elmac.co.uk/r22b1_dl.htm

*Tim Williams is a consultant with Elmac Services and is the author of **EMC for Product Designers** (4th Edition, Elsevier 2006)*

This paper forms the basis for the author's presentation on the second day of the EMCUK training sessions at Newbury, 14th October 2009.

Elmac Services, Wareham, Dorset: phone 01929 558279 www.elmac.co.uk