Failure Through Electrical Stress

Failures in powered systems

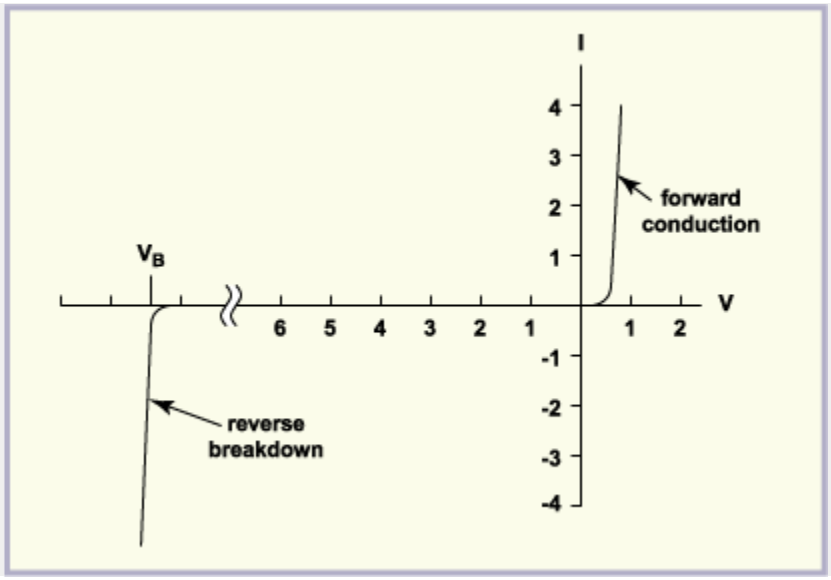
Electrical stresses can cause parts to fail whilst in circuit both during test and when the assembly is in the field. Some of these failures occur because of faults in manufacture, test or operation; others are the result of external events.

Typical of faults in the first category are those caused by the application of reverse voltage or by current overload; external events are primarily transient voltages, many of which are related to electrostatic discharges.

Reverse voltage

Figure 1 shows the transfer characteristic of a typical semiconductor junction: in the forward direction, substantial conduction takes place at low voltages, with a typical 'knee' occurring at 0.7 V for a conventional silicon device – Schottky diodes and diodes made of other materials, such as LEDs, have different forward voltages, but broadly similar characteristics. In the reverse direction, almost no current flows until the breakdown voltage (V_B) is exceeded, when the current growth is very fast indeed: if not limited in some way, total destruction will occur very quickly indeed.

Figure 1: Reverse breakdown of a typical semiconductor junction



For semiconductors, therefore, reverse voltages are more likely to result in device destruction than forward voltages. The most common exception to this is the zener diode, where the current is limited by the circuit, and the device is designed to be operated in that mode. Transistor junctions have also been noted to 'zener' quite happily, again provided that the current is limited and hot spots are not allowed to develop. Another device normally operated in reverse mode is the varactor diode, where use is made of the variation of junction capacitance with applied reverse voltage.

Passive components are usually not polarity sensitive, but one major exception is the electrolytic capacitor. Whether this is aluminium or tantalum, and whether the

construction is wound foil or ‘solid’, the thin oxide layer which is the dielectric of the capacitor is ‘formed’ by the application of forward voltage and destroyed by relatively small reverse voltages. In the case of large value, high voltage capacitors, failure may be accompanied by explosive rupture of the over-pressure vent (or even the entire component).

Typical reverse voltage limits for 25°C operation are a maximum of 3V, or 10% of forward rated voltage where this is less, reducing to 5% at 85°C and 1% at 125°C. Where ‘non-polar’ capacitors are supplied, these consist of two normal capacitors back to back, the series connection greatly reducing the available capacitance per unit volume.

Current overload

Ohm’s Law indicates that, in a linear device such as a *resistor*, power dissipation will increase as the square of the current. How the resulting temperature rise will vary with power will depend on which heat transfer mechanism predominates – for conduction, the temperature rise above ambient is a linear function of the power dissipated. The outcome is that overall device temperature increases very substantially for comparatively modest increases in current, with a consequence rapid increase in failure rate.

The situation is worst where the heat distribution within the device is not even, as this creates hotter areas which are the more likely to fail. Chip resistors, for example, dissipate power over only a relatively small active area, and there is usually a current ‘bottle-neck’ beside the laser adjustment cut. Pulse testing has confirmed that resistors become less tolerant of current overload once they have been adjusted.

The effect of such variations is even more significant in *silicon power devices*, where inconsistencies in the bond between die and package may result in different areas on the chip having different ‘thermal resistances’. Silicon has a negative temperature coefficient of resistance, and more current will tend to flow in these hotter areas, leading to the development of hot spots and, in severe cases, to thermal runaway and device destruction.

Similarly, when several devices are connected in parallel or bridge configurations, differences in heat sinking between components can lead to premature failure of the part which sees the highest junction temperature in operation.

With any *components containing contacts*, over-current can also cause failure, with overheating leading to the permanent welding of contacts. Typically switches and relays intended for high-current operation have heavy silver contacts, which are able to withstand the inevitable occasional overload. Whenever you see a pair of contact surfaces, bear in mind that they make contact only at the high points, and the area actually carrying current can be very much smaller than the apparent contact area.

Transient voltages

Electronic components are prone to damage by short duration, high voltage transients, caused by events such as the switching of loads, capacitative or inductive effects, or incorrect testing. The problem is particularly acute with products which provide a data interface between systems, of which a recent example is the Universal Serial Bus (USB), being introduced to interconnect computers with peripherals through a single high-speed serial link. Plug-in USB connections to peripherals both supply power and transfer data at up to 12Mb/s using a four-wire system which can be made and broken whilst live. In

this relatively uncontrolled environment, there are many opportunities for 'transient events' at the connections to the host computer!

Small semiconductor components such as ICs and low power transistors are particularly vulnerable, owing to their very low thermal inertia. The value of transient voltage which can cause failure (sometimes referred to as V_{ZAP}) depends on the duration of the transient. Maximum safe transient conditions are given in manufacturers' data books, and standard tests have been developed, for example:

- IEC 801.2, simulating an ESD event
- IEC 1000-4-5, simulating a unidirectional surge caused by over-voltages from switching and secondary lightning transients.

Passive components can also be damaged by transient voltages, but the energy levels required are much higher than for small semiconductor devices. For this reason, passive components do not normally need individual protection. However, MLC failures have been reported at voltages as low as 500V, and capacitor charge storage can make the situation worse when transient voltage 'events' are repeated without allowing time for discharge between pulses.

ESD failures to powered systems

An ESD event occurring near to, or directly to operating equipment can cause failures. This is because the ESD event has fast changing electric and magnetic fields, which can induce transient voltage and current impulses in nearby conductors. The impulses can have sufficient magnitude to change the state of a data line, cause unwanted reset or noise in a signal line.

The ESD induced failures can be 'soft' or 'hard' failures. Soft failures are temporary failures, due to corruption of data or some other recoverable mechanism. Hard failures are damage to the system that might require replacement of a part before the equipment operation can be restored.

ESD can affect the system through:

- Direct discharge of ESD into part of the system, e.g. the keyboard
- Voltage or current impulses induced in the system wiring or circuit board tracks by electromagnetic coupling
- Electrostatic fields directly affecting circuit operation.

The first two mechanisms are quite common, and direct effects due to electrostatic fields are relatively rare.

The possibility of direct discharge into the system, especially the user interface (keyboard, mouse, push buttons, and any other controls), and electromagnetic coupling into the system, must be taken into account in the design of a system. If these problems are detected late in the design phase it is often difficult and expensive to make necessary changes to achieve immunity required by EMC regulations.

Soft and hard system failures can be costly to the user, through

- Lost or worse, corrupted data
- Lost work and wasted user time, user irritation

- System down time
- Repair costs or data salvage time and cost.

Failures due to ESD during manufacture

Not all ESD events cause damage. The outcome of a discharge to a sensitive device or assembly will depend on many factors, including:

- device sensitivity
- severity of ESD stress
- actual strike site.

It is often difficult and expensive to quantify ESD damage with certainty, but it is relatively easy to prevent ESD damage by taking due prevention measures.

The cost of ESD failures

It has been estimated that customers may find 90% of ESD failures. The cost of such damage is high, including;

- Engineer time, including travel time and expenses
- Rework to assemblies
- Cost of replacement parts
- Customer service staff costs
- Additional facility costs
- Customer dissatisfaction, loss of reputation and possible lost future sales.

Some ESD failures are detected in-house. The cost of these may still be significant. A ‘rule of thumb’ often cited is that the cost of an assembly increases by about a factor of ten at each assembly stage.

If failure rates are known and cost of ESD failures are calculated, a strong case can often be made for investment in ESD measures. Monitoring failure rates can also give a good indicator of the effectiveness of ESD measures. If air humidity is also monitored, an increase in failures corresponding to dry conditions is a good indicator of an ESD problem.

ESD measures can be an extremely good investment – savings as high as 100 or even 1000 times the cost of the ESD measures have been reported!

Failure modes

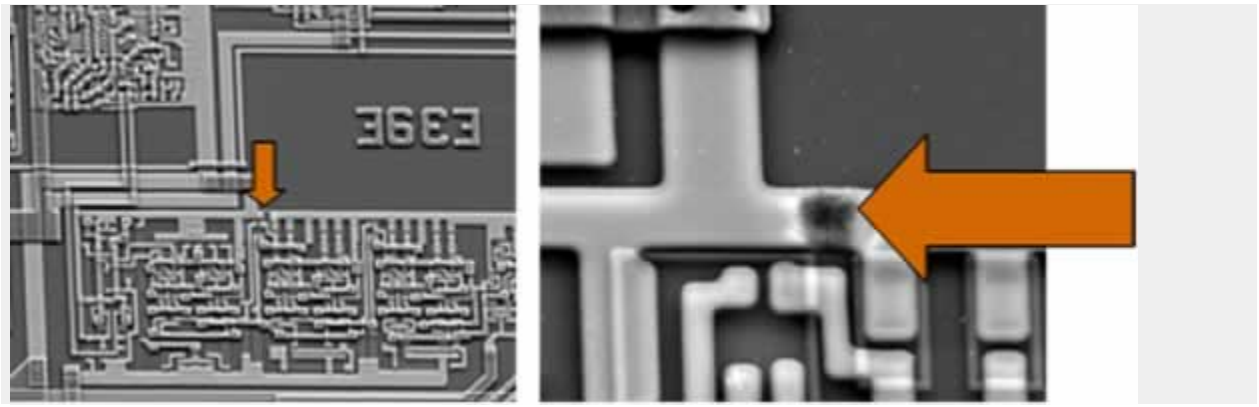
Direct ESD to devices may cause failures either through voltage breakdown damage to insulating oxide layers, or energy related damage to junction, metallisation and other features.

Oxide dielectric breakdown

Oxide layers are commonly used to insulate the gate in MOSFETs and metallisation in other devices. If the breakdown field strength of this oxide layer is exceeded, dielectric breakdown can occur. A subsequent current flow in a discharge through the gate rupture can melt silicon and form a conducting bridge.

Where subsequent current flow does not have sufficient energy to cause a short circuit, the device may continue to operate. It may have a detectable increased leakage current. The device may be weakened and prone to failure later. This is known as latent damage, and damaged devices are often referred to as the 'walking wounded'.

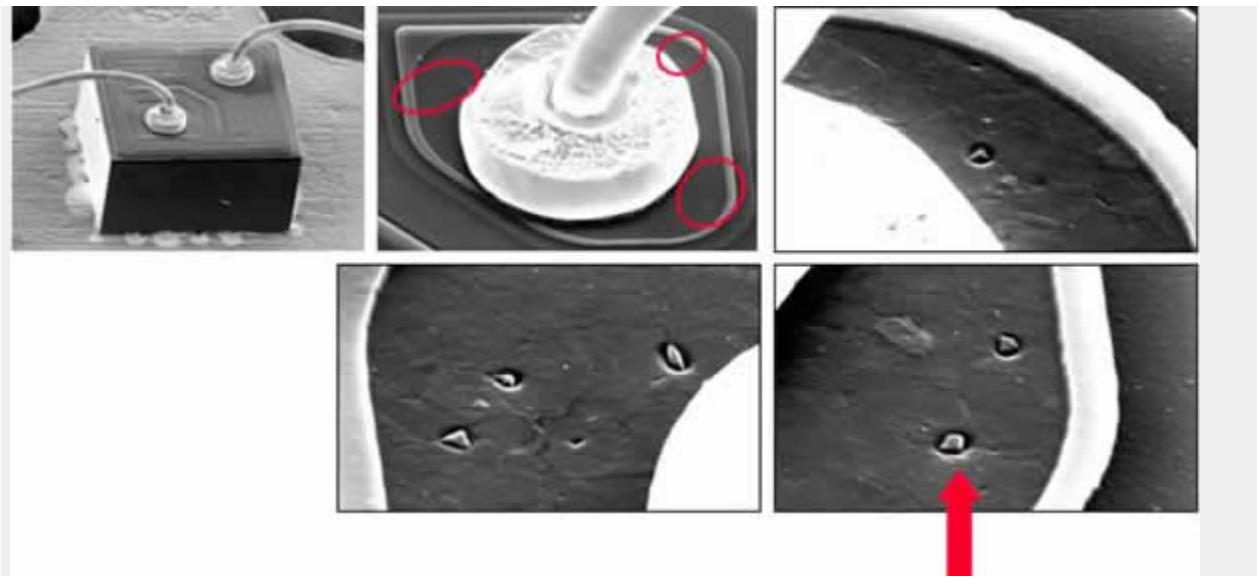
Figure 2: SEM images of ESD damage to an integrated circuit



Source: Rohm Electronics

Several samples of this IC were rejected as low input resistance (leaky) at a particular input pin. Sectioning the device revealed the partial short circuit through the silicon from the top. The top of the short circuit is shown by the small well on the track.

Figure 3. SEM images of ESD damage to a bipolar transistor



Source: Rohm Electronics

The transistor was also confirmed failed by ESD. The discharge found the weakest point(s) and punched through an oxide passivation layer to underlying silicon. Bipolar devices are becoming very small and susceptible

Junction burnout

An ESD event may pass through a transistor junction. The high current causes local heating, especially if the short timescale does not allow heat flow to the surrounding regions. Higher temperature material has a reduced resistance and attracts further current flow – a hot spot can form that may lead to melting and short-circuit of the junction.

Migration of a metal 'spike' across a diffusion layer can also occur as a result of thermal damage.

Metallisation melt

Metallisation melt or burnout happens when the current in an interconnection track is high enough to raise the temperature to melting point. The metallisation burns out like a fuse, and an open circuit track results.

Latch-up

Latch-up is a problem in powered CMOS devices caused by the inadvertent turn-on and latching of parasitic SCR structures in the device structure. Large currents can flow, leading to thermal damage. Latch-up can be a result of an ESD event or transient on power, input and output lines.

ESD sensitivity

What is an ESD sensitive device (ESDS)?

This may sound like an obvious question, but it often is not. An ESD Sensitive device (known as ESDS in the current EN61340-5-1 and ESD 20:20 standards) is a 'discrete device, integrated circuit or assembly that may be damaged by electrostatic fields or electrostatic discharge encountered in routine handling, testing or transit' (EN61340-5-1). It is often thought that a device becomes less sensitive to ESD when mounted on a PCB or assembly. This is not generally so – reflecting this, EN61340-5-1 states that the ESD sensitivity of an assembly is that of the most sensitive ESDS on an assembly. In practice the highest risk of ESD damage may occur when a board is held in the hand of a non-grounded person. The entire electrostatic charge on the person and board may pass through any victim component on the board when the board is touched to a conductive surface or object.

The ESD sensitivity of a device is measured by subjecting samples to HBM, MM or CDM type ESD. HBM is the usual form for specification of ESDS threshold voltage sensitivity – defined as 'the maximum voltage at which the device does not suffer any ESD damage.' In general the device withstand voltage will be different for each type of ESD, with MM withstand voltage typically a factor of ten less than HBM. There is no correlation between CDM withstand voltage and the other models.

IC manufacturers often include on-chip ESD protection networks to protect components against ESD damage. It has been found that in most cases manufacturing yields do not

improve significantly if ESD withstand voltage of a device is increased above 4 kV HBM, and so this is a target for many manufacturers. Some application areas, e.g. automotive, require much higher ESD withstand voltages. In practice 2 kV withstand is more often the achieved level, and many devices are a lot more sensitive than this. The component designer often must sacrifice ESD withstand in favour of maintaining high performance. Many devices, especially analog or RF components, have some pins which may be considerably more sensitive than the rest. Note that most people would not feel an ESD event that would damage many common devices!

Even a device that has a withstand voltage over 4 kV can be damaged in the unprotected environment, where electrostatic voltages over 20 kV are known to happen from time to time!

Often a part enters the facility as a sensitive device but leaves as part of a finished product that is not considered ESD sensitive, and may have been ESD tested for EMC immunity compliance. Somewhere in between it has made the transition from being a sensitive device – quite where is often unclear. The risk is that the assumption of ESD immunity may be made at too early a stage, and ESD damage during handling may result. In general, if the assembly has exposed ESD sensitive parts (e.g. a computer with the covers off), then it should be considered ESD sensitive.

Classification of ESD sensitivity of components

Devices may be classified for HBM, MM and CDM ESD withstand voltage according to MIL-STD 1686, ESD Association and the new IEC standards (Table 1) for testing and classification of the ESD damage sensitivity of components.

Trends in ESD sensitivity

As technologies develop there is a continuing trend to reduce device internal connection and junction sizes and oxide layer thickness, and lower operating voltages. This is because smaller devices give higher operating speeds, lower power consumption and a higher component density on a chip, all desirable goals for the designer. The effect of these developments is to increase the ESD sensitivity of the internal components.

Against this, many parts now have on-chip protection circuits that can raise the ESD withstand voltage considerably. Some technologies, e.g. RF parts, cannot be protected in this way without impairing their performance. For RF ICs, the added capacitance of a protection network can be too high and may be an intolerable load to a signal pin.

Exceptionally sensitive (sub–100 V) new technologies emerge from time to time, such as MagnetoResistive (MR) heads, which now have HBM withstand voltages in the volts range. Handling such sensitive components requires a challenging high level of ESD control for disk drive manufacturers.

Larger area devices have higher capacitance and become more susceptible to CDM ESD damage. On-chip protection networks may not always protect against this type of damage. Larger scale integration and higher pin counts give greater opportunity for ESD damage to an individual device, but when the system is considered the overall opportunity for ESD damage may be reduced.

Source : http://www.ami.ac.uk/courses/topics/0181_ftes/index.html