bulgin

Understanding the Ingress of Dust and Particulates in your Electronic Designs

bulgin

Dust inside sensitive electronic equipment can lead to problems such as heat damage, resulting in system crashes, as well as data loss and service outages.

When it comes to protecting sensitive electronics from potential harsh-environment risks, many think that the issue is only important for systems deployed in the great outdoors or in industrial situations. However, even a shirt-sleeve environment can pose a significant environmental risk to exposed electronic products that aren't properly protected.

Indoor environmental risks can destroy or significantly reduce the operational lifetime of electronics, and the most hazardous risks deal with simple human error. A cup of coffee spilled in the wrong place can wreak havoc in any situation, and spilled coffee's effect on electronics is as bad as its effect on the papers on your desk. However, properly designed systems should be able to handle even accidental exposure of that nature.

The real indoor environmental risk to electronics is far more subtle and pernicious, as it cannot be avoided without monumental effort. That risk is dust ingress and accumulation, which is far more damaging to electronics than many recognize. Even the best systems can fail if dust exposure is not addressed and dealt with, as dust is an omnipresent agent in any unfiltered and unmanaged environment (Figure 1).

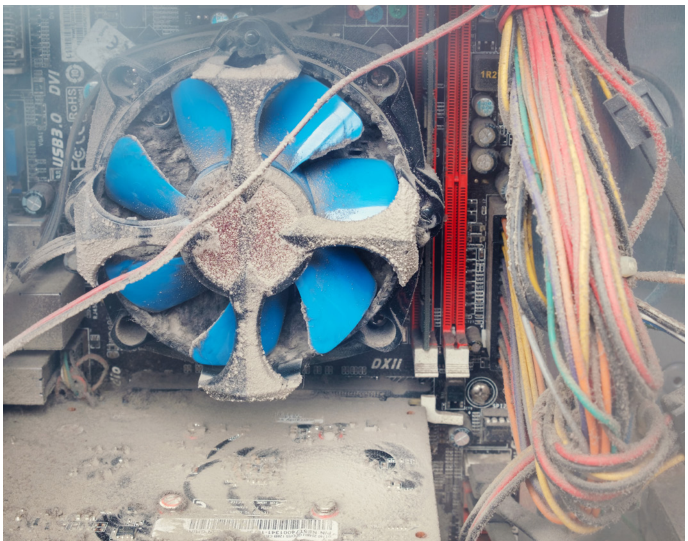


Figure 1: Dust is an omnipresent agent in any unfiltered and unmanaged environment.

What is Dust?

There is no exact scientific term for dust, but it is generally recognized as microscopic solid powders or fine particulates. The particles range in size, with the smallest dust particles being the most dangerous, as they are the most pervasive. If you can see larger dust particles, there are certainly smaller ones present as well. Not only are these particulates potential health hazards to humans inhaling them, they are serious hazards to the electronics that take them in as well.

Even if there are no sources of microparticles in a shirt-sleeve environment like a laser printer (toner grains) or electromechanical equipment, there is always a significant dust source in any room. Biological systems use ablative surfaces like skin, hair, and nails for protection, and these surfaces are constantly shedding dead skin, hair, and nail particles. Biological dust is highly underestimated, as people tend not to think about how dirty the human body actually is.

Toxic dusts are generally produced when working with substances which are themselves toxic, like lead, mercury, chromium, and others. If inhaled, this kind of dust can damage human lungs or get into the bloodstream, but aren't significantly different to electronic systems from simple human skin. However, some toxic materials are also highly flammable, conductive, or corrosive through galvanic mechanisms. More dangerous are products and processes that produce nuisance dusts like flour, sugar, paper, dried food, sawdust, and carbon black (toner). In a new legislative environment there could even be dust from plant materials like cannabis.

Dust is Damaging

One of the biggest dangers of dust beyond long-term damage to electronics themselves are secondary catastrophic events from flammable dust. A buildup of flammable dust on a circuit board could result in a fire that, depending on the ambient dust levels, could even result on a catastrophic thermal runaway that may spread to the entire facility. When flammable dusts settle on a hot surface in a product, they can potentially burst into flame or simply smoulder, even long after the source of ignition has been removed.

Figure 2: Dust can impact systems under different environmental conditions.

Beyond the risk of short circuits caused by conductive dust accumulation and the related fire risk, there is another significant source of damage to electronic systems caused by dust. Electronic hardware is meant to dissipate internal heat generated by the operation of the components within, and dust can prevent heat from dissipating. Accumulated dust inside electronic equipment will lead to a buildup of heat and its resulting damage, leading to system failure, as well as data loss and service outages.

Even poorly-conductive dust may cause electrical leakage, shorting vias on PCBs under different conditions, such as in times of high humidity that can cause mixed-media dust to change its conductive properties (Figure 2). Dust particles can also act as dielectric materials, inducing signal interference in contaminated signal connectors and lines. Moist (or wet) dust is a partial conductor, and is capable of initiating unwanted electrical shorts and high-voltage discharges that can cause catastrophic failure in electronics.

Addressing Dust in Systems

Indoors or outdoors, the impact of dust on the reliability of electronics is becoming more of an issue, as the trace-to-trace spacing on the printed circuit boards and lead-to-lead spacing on the components themselves have shrunk greatly. This makes them even more sensitive to dust particles dimension-wise. Traditional ways to address this in legacy systems include increasing the air flow and using filtration systems to trap airborne particles.

However, if you increase the airflow in an enclosure, it can accelerate dust accumulation inside the chassis and around the electronic components, and filtration increases airflow inefficiency, increasing operating temperatures as well as the system's energy budget. Dust accumulation around electronics components is bad news that will eventually lead to hardware failure. Dry dust is heavier than air, and will create insulating blankets on top of the PCB. With reduced cooling efficiency, dust-insulated components can easily overheat enough to reach the point of catastrophic thermal runaway.

There are well-established industry standards addressing the effectiveness of dust and moisture protection, such as EN 60529 (British BS EN 60529:1992, European IEC 60509:1989), which spells out the degrees of protection provided by enclosures, also known as the IP Code. IP, or "Ingress Protection" ratings, are used to define levels of sealing effectiveness of electrical enclosures against intrusion from little things like dirt and moisture as well as big things like parts and tools (Figure 3).

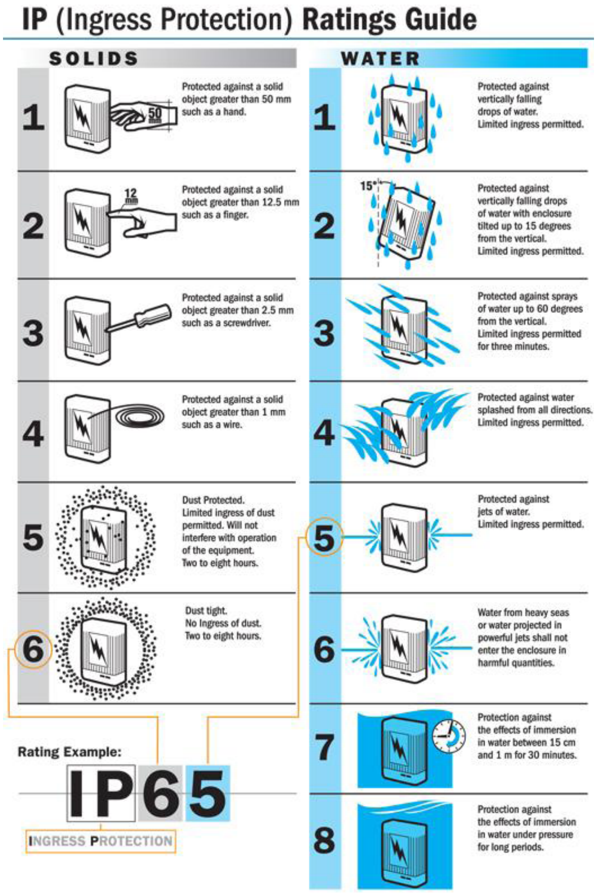


Figure 3: The IP Code is used to define levels of sealing effectiveness of electrical enclosures. IP Rating Chart courtesy of Blue Sea Systems

The first number in the rating indicates the degree of protection from moving parts, and the protection of enclosed equipment from foreign material. The second defines the protection level from various forms of liquid, such as drips, sprays, and submersion. Some enclosure manufacturers present their products as “IPxx” where the “x” simply shows that the value for that position is missing. This can be assumed to mean that the enclosure has not been made to or tested for that aspect.

The Connector As Last Bastion

One advantage in the latest generation of electronic devices is the reduction of enclosure ingress points due to advancing technology. For example, the ubiquitous use of touchscreens has eliminated the keyboard as a system ingress point for foreign materials. Other technologies that are reducing the potential for dust and moisture ingress include consolidation of power and signal into one connector.

In small portable and remote devices it may even be possible to eliminate all cable ingress points by using RF data connection and wireless power transfer, but that solution can only be applied to systems drawing low levels of power. In addition, data-infrastructure systems handle such a high level of traffic that an RF-only solution is not viable.

This means any solution that uses cabling for power and/or data connection must address dust and moisture ingress, regardless of the final environment the system is intended to operate in. Such solutions will have a certain baseline level of ruggedness, as the shells and gaskets involved must be able to handle multiple insertions and potential hard use (Figure 4).

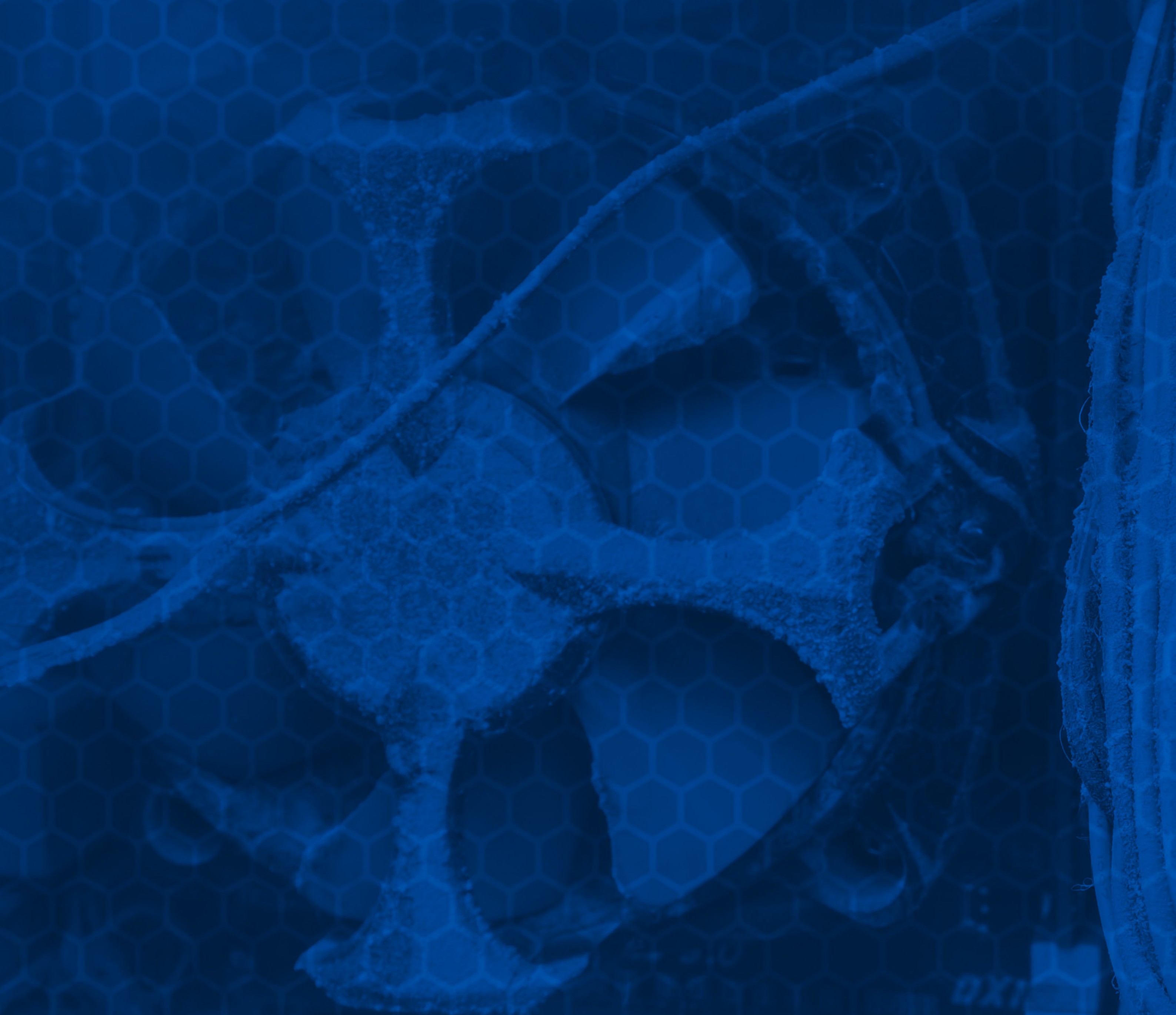
One of the most critical aspects to remember about the connection points in your system is that they are also the primary points of potential electrical failure from contaminants of any kind, as by definition the electrical contact points for both power and signal are exposed. Not only must a connector be dustproof when installed, it must be as easy and intuitive as possible to engage to reduce the change of fit error and forced connections.

The need for well-designed cables and connectors for even the most simple applications is significant for other reasons as well, as optimum form and function design reduces the chances foreign material will enter the connection as it is being created. Such ingress can come from particles stuck to gloves worn, for example, or material shed from the gloves themselves against the connector surfaces. The right design ensures the connector can be easily connected in the proper fashion to enable optimal performance as well as proper sealing against dust and moisture.

Looking Forward

Designing systems for use in the real world can present issues not easily foreseen in the development laboratory. Considering all potential threats and risks in the operational environment and implementing remedial solutions for them will ensure your design’s viability in the marketplace. Dust incursion management is a critical step to achieve that goal.

Figure 4: Dust-resistant cables also present a certain baseline level of ruggedness.



bulgin

www.bulgin.com

Europe

Bulgin
200 Cambridge Science Park
Milton Road
Cambridge, CB4 0GZ, UK
tel: +44 (0) 1803 407757
e: info@bulgin.com

Americas

Bulgin
10619 Painter Avenue Suite A
Santa Fe Springs
CA 90670, USA
tel: 760-343-3650
e: info@bulgin.com

Asia Pacific

Bulgin
10619 Painter Avenue Suite A
Santa Fe Springs
CA 90670, USA
tel: 760-343-3650
e: info@bulgin.com