TECHNOLOGY NOTES

SecureAire and Data Center Corrosion Failures

According to most major IT equipment manufacturers, the number of Data Centers with contamination related corrosion failures are on the rise. Among the reasons being attributed to this increasing number of data center hardware failures is:

1. The change from lead-containing solder to lead-free solder (copper/tin/silver solder).
2. The continued miniaturizing of electronic components and increasing circuit package densities.
3. The proliferation of data centers into geographies with polluted environments.

Corrosion in the manufacturing and industrial sectors are known to cost billions of dollars every year in the US alone.

Contamination that Produces Corrosion

Corrosion is defined as “deterioration of a substance (usually a metal) because of a reaction with its environment”. Corrosion of metals is a chemical reaction caused primarily by the attack of gaseous contaminants that is accelerated by heat and moisture. Rapid shifts in either temperature or humidity cause small portions of circuits to fall below the dew point temperature, thereby facilitating condensation of contaminants. All metals eventually corrode. Some may take decades to corrode before it affects a product, and others can take only a few months.

It is important to note that even at low relative humidity (RH) levels corrosion may occur, depending on the temperature and contaminants present!

The most common metals used in the electronics industry are copper (Cu), silver (Ag), gold (Au), and nickel (Ni). Of these metals Cu is considered a base metal, which is most susceptible to corrosion and Au, which is considered a noble metal, is least susceptible to corrosion.

A printed circuit board (PCB) is used to mechanically support and electrically connect electronic components using conductive pathways laminated onto a non-conductive substrate. PCBs have conducting layers on their surface typically made of thin copper foil, which if left unprotected, will oxidize and deteriorate.

There are two types of gas contaminants that considered to be the prime candidates in the corrosion of data center electronics:

1. Acidic contaminants such as hydrogen sulfide, sulfur and nitrogen oxides, chlorine, and hydrogen fluoride.
2. Caustic contaminants, such as ammonia; and oxidizing gases, such as ozone.

The most critical of these is the acidic contaminants as it takes only 10 ppb (parts per billion) of chlorine to inflict the same amount of damage as 25,000 ppb of ammonia.

Active sulfur containing compounds when present at low ppb levels rapidly attack copper, as well as silver and aluminum. The presence of moisture and small amounts of inorganic chlorine compounds and/or nitrogen oxides greatly accelerate sulfide corrosion.

If a circuit board in a data center is exposed to small amounts of airborne sulfur, salt, chlorine, etc., they have the contaminants needed for corrosion. Accelerated corrosion has been observed on printed circuit boards in industrial environments that contain hydrogen sulfide and sulfur.

This problem is further compounded by the fact that sulfur is regulated by OSHA as a **nuisance dust**, and is allowed in the human working environment at the **parts per thousand** levels. Data shows that elemental sulfur present at the **parts per million** levels can cause computer systems to fail within 2 months of use.

When considering Data Center electronics equipment, the corrosion of copper and silver produces the same result: a disruption of electrical current flow. The severity of the environment (i.e. the types and levels of contaminants, humidity, and temperature) will determine the speed at which corrosion forms and how soon corrosion-related effects may appear. In addition, ozone plus certain chlorinated gas contaminants (chlorine, chlorine dioxide) are powerful oxidizing agents. Hydrogen sulfide, sulfates, and active chlorine compounds, have all been shown to cause significant corrosion in electrical and electronic equipment at concentrations of just a few parts per billion in air. Even at levels that are not noticed by or harmful to humans, these contaminants can cause serious damage to electronic equipment.

When corrosion occurs, the corrosion layer is not self-limiting. The base metal will continually corrode, and the corrosion product can even spread out from its point of origin. Any circuit can have bare edges. These edges are free to corrode, and the corrosion product can grow from the edges and slowly spread across the surface. This is known as creep corrosion as shown in Figure 1. Eventually, the corrosion product will interfere with the electrical connection and creates an open circuit. The sulfur-bearing gases and moisture can corrode any exposed copper metallization on the circuit board, producing copper sulfide, which can creep over the circuit board and short circuit closely spaced features.

Figure1: Copper corrosion created by copper creep.

The reduction of circuit board feature sizes and the miniaturization of components, necessary to improve hardware performance, have made the hardware more prone to attack by corrosive particles and gases in the data center (air) environment. The two common circuit board types suffering from creep corrosion are those with an immersion silver finish and, to a lesser extent, those with an organic soldered preservative coating.

Dust can degrade the reliability of printed circuit boards. The process involves the absorption of moisture from the environment by settled dust. The ionic contamination in the wet dust degrades the surface insulation resistance of the printed circuit board leading to an electrical short circuit of closely spaced features via ion migration. Figure 2 shows an example of copper corrosion caused by dust settling on a printed circuit board.

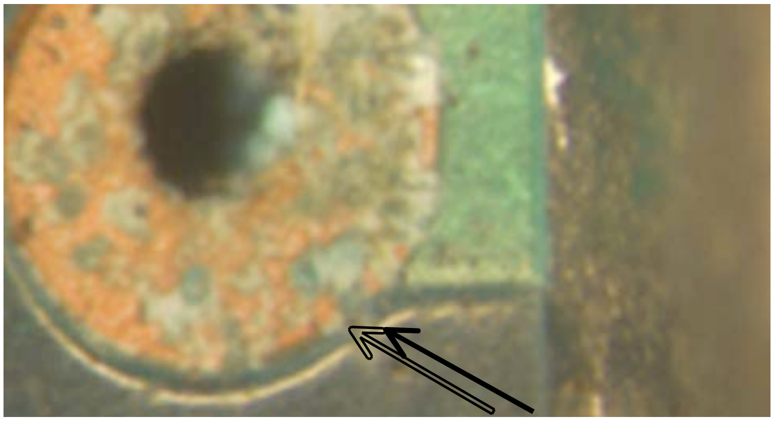

Figure 2: Copper corrosion causes a short circuit caused by ion migration.

Problems also occur when dust from paper, cardboard, and textiles get into heat sinks and disrupt equipment cooling. Whisker Growth is a type of corrosion that typically refers to electrically conductive, crystalline structures of tin, or zinc that sometimes grow from surfaces where they can be used as a final finish. Tin whiskers have been observed to grow to lengths of several millimeters (mm) and in rare instances to lengths up to 10 mm, which is long enough to connect portions on a board, chip, etc. and cause short-circuits. As an example, zinc whiskers threaten IT equipment when they become dislodged and airborne when tiles are removed or when pulling or removing underfloor cables. When zinc whiskers get pulled into IT equipment, short circuits are commonly the result.

RoHS Standards (Prevention or Cause)

The IT industry did not foresee the creation of creep corrosion caused by the transition to lead-free products mandated by RoHS (**R**estriction **o**f the use of certain **H**azardous **S**ubstances). Products with an immersion silver surface finish will creep corrode in environments that electronic equipment manufacturers consider to be high in sulfur, as in polluted regions across the globe. As a direct result, the number and types of corrosion failures have increased dramatically.

There will always be some imperfections in the plating of circuit boards. In many cases, platings will have pores, through which the base metal will be exposed. The degree of porosity depends on the plating thickness, application method, base metal roughness, and base metal cleanliness. Contamination or oxide on the surface of the base metal aggravates the situation. If the base metal is exposed to a contaminated air environment through these pores, pore corrosion occurs.

When a multi-layer circuit board is created, vertical interconnects must be added. These interconnects are called vias (*a*n electrical connection between layers in a physical electronic circuit that goes through the plane of one or more adjacent layers). In situations where a VIA hole is not completely coated, copper metal is vulnerable to atmospheric attack. When a more noble metal is coated on a

SecureAire

metal that is prone to oxidation in the presence of an electrolyte, atmospheric water, it is highly prone to galvanic corrosion.

The common thread connecting these corrosion failures begins with airborne contaminants that were allowed to enter the Data Center Environment from the outside environment.

“One of the primary sources of airborne contamination is the outdoor air used for ventilation, pressurization and or cooling of the Data Center!”

ASHRAE Guidelines

“In order to meet warranty requirements for new IT and data communication equipment, data center owners and operators must take action to eliminate airborne contaminants. It is imperative to maintain hardware reliability by “monitoring” and “controlling” particulate contamination.” ASHRAE

ASHRAE, in cooperation with many of the world’s leading manufacturers of computer systems, has developed guidelines that summarize the acceptable levels of contamination:

ASHRAE Guidelines for Data Centers

Data centers must be kept clean to ISO 14644-1 Class 8. This level of cleanliness can generally be achieved by an appropriate filtration scheme as outlined here: 1. The room air may be continuously filtered with MERV 8 filters (G4/F5, 2.5 - 3.0% dust spot.) 2. Air entering a data center may be filtered with MERV 11 (F6, 60-65% dust spot) or MERV13 (F7, 80-90% dust spot filters) Sources of dust inside data centers should be reduced. Every effort should be made to filter out dust that has deliquescent relative humidity greater than the maximum allowable relative humidity in the data center.
Gaseous contamination should be within the ISA-71.04.2013 severity level of G1-Mild that meets: 1. A copper reactivity rate of less than 300 Å per month **and** 2. A silver reactivity rate of less than 200 Å per month.
For data centers with higher gaseous contamination levels, gas-phase filtration of the inlet air and the air in the data center is highly recommended.

While these guidelines are a good start, the importance of “particle control technology” and its’ understanding within the context of critical data center contamination control continue to be overlooked.

As previously stated by ASHRAE, **“To meet warranty requirements for new IT and data communication equipment, data center owners and operators must take action to eliminate airborne contaminants. It is imperative to maintain hardware reliability by “monitoring” and “controlling” particulate contamination.”**

SecureAire and "Monitoring"

Particulate contamination is the major contributor to the corrosion previously described. Harmful dust in data centers is generally high in ionic content, such as sulfur and chlorine bearing salts. The source of this harmful dust is mostly contained in the outdoor air. Coarse dust particles (> 2.5u) have a mineral and biological origin, are formed mostly by wind-induced abrasion, and can remain airborne for a few days. However, fine dust particles (< 2.5u) are generally the result of fossil fuel burning and volcanic activity and can remain airborne for **years**!

A simple approach to monitoring the air quality in a data center is the use of SecureAire's AQM-100. The AQM-100 measures critical particle size ranges, namely **small** (>= 0.35u and larger) and **large** (2.5u and larger).

It has been confirmed that the most critical size particles are the **small** particles of which 98% of all particles are less than 2.5u in size.

SecureAire's AQM-100, provides you with the ability to monitor particle contamination levels!

SecureAire and Particle "Control"

The SecureAire Advanced Collector System (ACS) is a very efficient and effective air purification system that utilizes Particle Control Technology. It is composed of three parts, a Particle Conditioning System, a Collector System and an internal Collider System. These three parts together create todays single most efficient and effective particle control entity.

The ACS optimizes charge, ionization and polarization to collect small particles, TVOCs and gases very effectively. Unlike conventional filters the ACS, with its electronic characteristics, exhibits superior performance and is non selective in reducing and or removing all types of contaminants. The ACS conditions contaminants to adhere to the media material or other particles, which subsequently get captured. Utilizing and optimizing electric fields and charge to ionize/polarize contaminants as well as polarize the internal media material in the system, results in a significant reduction in airborne contamination. The ACS System also provides the critical aspect of pathogen inactivation thru the use of INACTIVATE™ Technology. INACTIVATE reduces viable organisms ability to grow and provides the necessary voltage strength to oxidize and kill viable airborne pathogens including mold.

The Data Center Corrosion Solution

Even though today's complex and sensitive Data Center equipment requires a higher level of environmental control for gaseous contamination this has been overlooked. Data Center equipment contamination if left unchecked can influence the reliability and the continuous operation of mission critical IT equipment within a facility. Contamination can result in intermittent equipment glitches, unplanned shutdowns, or failure of critical systems that often result in significant business and financial loss.

To maintain a high level of equipment dependability and availability, it should be understood that a data center is a dynamic environment where many maintenance operations, infrastructure upgrades, and equipment change activities occur on a regular basis. Airborne contaminants harmful to sensitive electronic devices can be introduced into the operating environment in many ways (e.g., chlorine can be emitted from PVC insulation, used on wires and cables, if temperatures get too high.) The outdoor ambient air that is often the primary source of corrosive contaminants and should be filtered before its introduction into the data center environment.

To significantly reduce or eliminate the problems of Copper creep corrosion on printed circuit boards and corrosion of silver termination in miniature surface-mounted components, ASHRAE, in cooperation with many of the world's leading manufacturers of computer systems, has developed guidelines that summarize the acceptable levels of contamination. It is further stated that, "**It is imperative to maintain hardware reliability by monitoring and controlling particulate contamination.**"

The optimum Particle Control and Monitoring Solution for Data Center Applications is SecureAire's combination of ACS and AQM-100 Product Platforms.

By properly employing these two platforms particles, small and large, as well as TVOCs and gases, can be brought under control resulting in better data center operations.

The simple principle of creating polar molecules and charged particles is the basis for SecureAire's Particle Control Technology Platforms. The ability of SecureAire's ACS System to treat Data Center contamination is no different than previously documented case studies where the monitoring, removal, reduction and inactivation of TVOC's, dissolved gases, smoke, odors and particles has been achieved. Furthermore, SecureAire's Particle Control Technology is "non selective", which means that the source of the airborne contaminant is simply treated as a contaminant and will be removed.

For further information, please contact SecureAire or your local SecureAire Representative.

References:

1. Reid et al. 2007; Cullen and O'Brien 2004; Veale 2005; Sahu 2007; Schueller 2007; Hillman et al. 2007; Xu et al. 2007; Mazurkiewicz 2006.
2. Comizzoli et al. 1993.
3. Particulate and Gaseous Contamination in Datacom Environments (ASHRAE 2009b).
4. What's Creeping Around in Your Data Center? Solving Air Contaminant Problems in Data Centers. (Muller, Singh, G. White, Finch)