Session No. 635

Emerging Issues; Navigating "UFOs" Unidentified Foreign Objects

David Dogan, CSP
Chubb and Son, Inc
Pleasanton, California

Michael Ruddy, CSP
Chubb and Son, Inc
Indianapolis, Indiana

Jay Taylor, ARM, CSP, CPCU
Chubb and Son, Inc
Whitehouse Station, New Jersey

Louise Vallee, CSP, CIH, CPE
Chubb and Son, Inc.
Whitehouse Station, New Jersey

Nanotechnology; No Small Matter

The Next Industrial Revolution

Research and commercial applications of nanotechnology are rapidly advancing. Thousands of companies all over the world are employing this new technology in research and development and production. Current applications cross a variety of industries, including electronics, cosmetics, pharmaceuticals and biomedical, photography, metals/minerals and energy.

Nanotechnology is the generic term for applications and products that contain extremely small particles, tinier than 100 nanometers. A nanometer is one-billionth of a meter. Matter this small has unique properties which are being harnessed for technological innovation.

While research and development efforts still dominate this developing field, an estimated 700 nanotechnology-based consumer products are now on the market, according to a recent survey by the Project on Emerging Nanotechnologies at Woodrow Wilson International Center for

Scholars.[1] Nanoparticles can be found in the composite materials in golf clubs, tennis racquets and bicycle frames to make them stronger and more wear-resistant. These particles also are ingredients in paints and coatings, tools, air sanitizers, self-cleaning glass, long-lasting tennis balls, stain-free coatings for clothing and mattresses, dental material, burn and wound dressings, cultured diamonds, inks, appliances and flat screen televisions. So far, the greatest use of nanotechnology mineral and metal particles is found in cosmetics, sunscreens, fabric coatings, electronics and composite materials.

Nanotechnology offers significant opportunities for nearly every industry, but it also comes bearing a host of questions. Advances in nanotechnology products and applications are outpacing research into possible adverse effects, as well as regulations that might govern the use of these products and applications. This is why it is critical that safety managers understand and keep pace with the implications of this the exponentially growth of this field.

The very small size of nanoparticles makes them highly reactive with properties that differ from larger particles of the same substance. Their small size potentially increases health effects, risk of fire or explosion and/or environmental persistence.

Unknown Risks

Exposure to nanoparticles potentially poses a greater threat to the body than larger particles of the same substance. Experimental rat studies, for instance, have shown that nanoparticles, such as carbon nanotubes, can affect lung tissue by causing inflammation and initial lung fibrosis[2]. Other pharmaceutical studies have found that nanoparticles are able to cross the blood-brain barrier, which safeguards the brain from chemical contamination.[3] While there is concern for workers exposed to nanoparticles, the research on potential health effects is just beginning. Initial results indicate that the use of the "precautionary principle" for worker protection would be prudent at this time. Nanotechnology substance Material Safety Data Sheets often do not contain nano-specific information, reporting hazard information for larger sized particle substances. This situation may under-represent user exposure hazards as well have failure to warn implications for manufacturers.

The U.S. Bureau of Labor Statistics has no current, comprehensive data on the number of workers in businesses using nanotechnology. *Small Times*, a bimonthly publication that focuses on micro and nanotechnology, reported that in 2004 an estimated 24,388 people worked in companies engaged only in nanotechnology.[4] Many more workers may be exposed in firms where nanotechnology is a portion of the production process. An estimated two million workers will be employed in the nanotechnology sector over the next ten years.

---

[1] Woodrow Wilson Institute for Scholars Project on Emerging Nanotechnologies, *Nanotechnology Consumer Products Inventor*,

[2] Muller, J et al, *Respiratory Toxicity of Multi-Wall Carbon Nanotubes,* Toxicology and Applied Pharmacology, September 15, 2005, 207(3) 221-31.

[3] Koziara, J. et al, *In Situ Blood–Brain Barrier Transport of Nanoparticles,* Pharmaceutical Research, November, 2003, Volume 20, 1772-78

[4] http://www.cdc.gov/niosh/topics/nanotech/faq.html#howmany

All the unanswered questions in this fast-evolving world of nanotechnology make it imperative that businesses adhere to conservative risk management practices. Companies need to develop their own nanotechnology risk management plan to consider raw materials in terms of toxicity, expected applications, potential exposures and appropriate control measures. Safety managers must identify points of possible employee exposures in the production process and mitigate those exposures. Those control measures will be costly, so limiting exposed employees will assist on both exposure and expense sides.

Quantity vs. Size

From a health and safety standpoint, the past focus for worker chemical exposure in the workplace was the quantity of chemical contamination. An employee's chemical exposure was monitored and compared to air contaminant exposure standards and guidelines. Elevated levels pose potential injury or illness hazards.

But regarding nanotechnology material exposure, the highly reactive nature of nanoparticles makes particle size and counts potentially better exposure indicators. With this shift, companies are facing a very different way of evaluating workplace contaminants.

This means that traditional, industrial hygiene air sampling methods may not completely measure up when it comes to gauging employee exposure to nanoparticles. Instead, companies may have to use several methods to judge not just quantity, which reflects the total amount of materials, but to evaluate the size and actual number of particles. It follows, then, that monitoring methodology will have to become more complex to handle this task. Small process leaks or short term maintenance tasks, which may not have been a concern with larger particle materials, may pose greater risks with nanoparticles.

Standard industrial exposure control practices apply, including enclosure, isolation and ventilation of the process with now an emphasis on HEPA filtration. Also essential are protective clothing and respirators, as well as good hygiene practices, such as clothing change areas and facilities for showering and washing hands. Employees should, as usual, be prohibited from consuming food and drink in the workplace to avoid accidental ingestion of nanoparticles. Clean-up procedure must include vacuuming with a High Efficiency Particulate Air (HEPA) filter to trap the nanoparticles instead of dispersing them via dry sweeping.

Additionally, companies need to follow special procedures for cleaning up spills. With potential fire risk magnified due to small size, containment of materials and segregated storage are also important. Fire suppression and extinguishing systems must be in place, as well as explosion venting, where necessary due to combustibility.

Safety Guidelines

Based on the limited research on nanoparticles that does exist, nanotech applications must undergo rigorous scrutiny to incorporate the safest use of them at the present time. To aid in this effort, companies can look to the advice and leadership of NIOSH, which established a Nanotechnology Research Center in 2004. The agency has developed a nanotechnology research

strategic plan. Much of what we rely on so far for nanotech workplace safety comes from NIOSH in the form of best practices guidelines. [5]

NIOSH has sponsored a series of international symposiums that promoted the sharing of nanotechnology research results and discussions on safety and health. Reports on the NIOSH Web site summarize the results of these forums.

In 2003, President Bush signed the 21st Century Nanotechnology Research and Development Act, which authorized funding for nanotechnology research and development for four years, beginning in 2005. The legislation put into law programs and activities supported by the National Nanotechnology Initiative (NNI), a multi-agency research and development priority of the Bush administration. The NNI aims to aid scientific breakthroughs and maintain U.S. competitiveness in nanoscience. Its stated goal is to ensure that nanotechnology research leads to "the responsible development of beneficial applications by giving high priority to research on societal implications, human health, and environmental issues related to nanotechnology."[6]

Nano Is Poised to Grow

There's no doubt that nanotechnology is not only here to stay but flourishing. The U.S. National Science Foundation predicts that by 2015, the global market for nanotechnology-related products will reach $1 trillion and employ one million workers in the United States alone.[7] The prospect of burgeoning nanotechnology applications affecting nearly every industry makes it all the more important for every safety manager to assess the need for state-of-the-art controls, because these involve advance planning and budgeting. Concerns exists that adequate safety expertise may not exist at the R & D and pilot plant phases of these emerging companies, resulting in increased employee exposures and costs to retrofit control systems.

Nanotechnology is here to stay. Rapid growth and changes coupled with the knowledge gaps that confront us on the possible human and world impact of nanoparticles, make it imperative for safety managers to get up to speed now on the potential risks, as well as exposure assessment and best practice control technology for nanotechnology.

Supply Chain Management

Moving Beyond "Four Walls"

These are exciting times with the opening of new markets due to the expansion of globalization. Comprehensive management of the domestic supply chain is already a "work in progress" for many U.S. companies. Globalization stretches the supply chain beyond the traditional "four walls", adding new challenges and complexity.

---

[5] NIOSH, *Publication No. 2007-123 Progress Toward Safe Nanotechnology in the Workplace*

[6] National Nanotechnology Initiative Strategic Plan, December 2004

[7] Roco, M. C., National Science Foundation, *Government Nanotechnology Funding: An International Outlook,* June 30, 2003

A 2008 newly released IBM CFO study found that over the previous three years, 62% of companies with sales exceeding five billion dollars experienced a supply chain disrupting event. Further that 42% of those affected were unprepared.8 This aligns with observations from a 2004 Purchasing Magazine survey which found that half of respondents had partial or no supply chain management programs.[9] Supply chain disruption can impact stock value and bottom line for up to two years, as well as a company's reputation, a critical asset.

Globalization Challenges

The challenges of globalization present multiple opportunities for safety and risk managers to mitigate risks through careful assessment and "best practices" implementation. Business disruption can arise from issues related to the following;

- Business continuity
  - Natural disasters; earthquakes and epidemics
  - Geopolitical; terrorism, market and supply shortages
  - Fires, floods, storms
- Supply chain management
  - Production and sales problems
  - Injury, delays, and loss of reputation
  - Regulatory compliance
- Green initiatives
  - Global warming
  - Toxic materials restrictions
- Energy shortages and pricing

Imported product liability issues have figured prominently in the news media over the past couple of years. These headlines have focused world attention on the lack of supply chain management on the part of U.S. companies, as well as problems arising from lack of regulatory infrastructure in developing countries. A visit to the Food and Drug Administration web site clearly indicates that problem products come from all over the world, including the U.S. U.S. regulatory agencies do not have the resources to examine and test all imported products, nor inspect all overseas facilities. Companies must take responsibility for the development and implementation of comprehensive supply chain management programs.

Demand for the cheapest price may not be the best course in the long run, potentially resulting in inferior substitution or "shortcuts". Visibility along the supply chain decreases with each sub-tier and in combination with language and time zone differences makes supply chain management a challenge, but one which must be addressed. Integration and enhanced communication between the tiers of the supply chain is a goal which will result in quicker response to specifications and changes. These practices increase costs and reduce risk while the "four walls" position greatly

---

[8] *Balancing Risk and Performance with an Integrated Finance Organization , The Global CFO Study,* IBM, 2008

[9] Atkinson, William, *Supply Chain Management: New Opportunities for Risk Managers*, Purchasing Magazine, June, 2006

increases risks. Integration has worked well for inventory issues, but now the focus is being expanded to encompass the critical area of quality control.

Each year goods, from 825,000 importers, valued at two trillion dollars pass into U.S. ports. [10] The largest exporters to the U.S. include China, India, Mexico, Canada, Germany, and the UK. Los Angeles/Long Beach port is busiest, receiving 43% of all imported containerized cargo. [11] Half of the containers arrive from China and particularly Shanghai which is the world's busiest port. Other top U.S. ports include Southern Louisiana, Houston, and New York. The largest U.S. importers include retail chains, produce companies, electronics and consumer products distributors, and tire vendors. There is a current trend towards "high technology" growth overseas including computers and telecommunications, as well as pharmaceuticals and machinery.

Imported Goods Regulatory Oversight and Inspection Less Than Public Realizes

Importers must provide advance documentation to U.S. Customs and Border Patrol who conduct the duty collection process and may inspect depending upon commodity. Customs notifies other agencies, such as the Food and Drug Administration, Department of Agriculture, and Consumer Product Safety Commission which may do additional inspections. The FDA is only able to inspect about 1% of imported goods falling into its jurisdiction due to limited resources.[12] Few U.S. regulations apply to cosmetics and pet foods, produced domestically or overseas. Dietary supplements regulations are in the process of being upgraded to include proof of good manufacturing processes, but this will not include overseas inspection. While the National Highway Traffic Safety Administration sets tire safety standards, no inspections are completed. The FDA does not inspect foreign food producers, but does inspect exporting manufacturers of pharmaceuticals and active pharmaceutical ingredients. Due to lack of resources, these inspections lag behind at every eight to twelve years, instead of every two years as in the U.S. The USDA certifies 37 countries for meat exports and conducts annual facility and port arrival inspections. The Consumer Product Safety Commission has over 300 voluntary and mandatory standards for high risk products, including toys, electrical and consumer products, and fireworks. Customs conducts many CPSC inspections and the U.S. Congress is moving towards increased funding for CPSC inspections and tightening of toy and consumer product lead regulations.

Under Health and Human Services Secretary Leavitt, U.S. goals are evolving from stopping products at entry into working with developing countries to build safety and quality control infrastructure. Two Memos of Understanding have been agreed upon between the U.S. and China to address quality control and certification of high risk foods and pharmaceuticals.[13] There are early talks underway proposing an FDA office in India. These efforts indicate initial positive momentum, but do not supplant current need for vigilance and best practice controls.

Best Practices

Companies importing products into the U.S. can mitigate product liability risks by developing comprehensive supply chain management best practices. The hallmarks of these practices include supplier pre-qualification and audit, integrated communication along the chain, validated quality

---

[10] Overview of the Import Program, Food and Drug Administration

[11] "Losev, Stepehen, "*Technology Helps Keep Border Traffic Flowing Safely*", Federal Times, July, 2005

[12] Schmit, Julie, "U.S. Food Imports Outrun FDA Resources", USA Today, 3/18, 2007

[13] Interagency Working Group on Import Safety, "*Action Plan For Import Safety*"

control programs, and recall programs. Returned product should be evaluated for defects requiring production or supplier change or counterfeit possibility. Paper documentation of testing results or insurance coverage should be validated. Fraudulent Certificates of Acceptance test documents can result in misplaced confidence in quality.

U.S. recycled electronic waste may be shipped overseas, where in some cases it is reconfigured into "new" products that may contain some original or counterfeit labeling. Tracking of waste stream and safeguarding against unauthorized reuse is another best practice.

A Call to Action

U.S. entities need to realize that until major changes take place in international regulatory practices, that they will be considered, in the eyes of the US legal system, as the manufacturers of all the products they distribute. They will not be able to hide behind the mantra of "I'm only the distributor", even if that is exactly what they are. When dealing with international suppliers, there are really two broad categories:

- "Known" entities – These manufacturers are from countries having established product controls, safety standards, and adhere to international treaties. For the most part, a U.S. importer can deal with these entities with confidence.
- "Unknown" entities – These manufacturers are located in countries with partial or no controls. All QC is the responsibility of the purchaser, and at their own risk.

However, there is always the wild card of "Active Fraud", which can come from either of the two entities, but involves a supplier actively attempting to deceive in order to gain a competitive/financial advantage. This is more likely from an "unknown" entity, but not unheard of from a know entity as well. It is this issue that will be the most difficult and critical to manage on a continuous basis.

The next step in this saga will involve political solutions, in the form of treaties between countries that go beyond the "Memorandum of Understanding" that have currently been produced. In addition to international solutions, there will no doubt be internal legislative solutions. Most recently, H.R. 5069, the Food Safety and Product Responsibility Act of 2008 has been introduced, with similar legislation being taken up in the Senate. The bill would require manufacturers to demonstrate sufficient means to cover, for certain products distributed in commerce, costs of potential recalls. [14] The most likely demonstrable method would be insurance. While product recall insurance, and product liability insurance in general are common products and concepts in the US, they are only beginning to obtain acceptance in other parts of the world, particularly Asia.

In the meantime, and for the foreseeable future, US importers need to remember these basic points:

---

[14] Dowding, Tony, "*Consumer Attitude and Legislation Make Their Mark on Food Recall Risk*", Business Insurance, December 17, 2007

- Know your supplier – Conduct a credit and/or background check. Always work directly with the owner, not just a broker.
- Quality Control – Accept responsibility for this. Don't trust in a government system or a certificate. Do your own testing. If you start finding quality problems, address them immediately.
- Contract – This should spell out responsibilities and liabilities. Countries that might not enforce a legal judgment might have arbitration agreements. Obtain legal assistance to determine if this might be the case in your situation, and make sure it is represented in the contract.
- Know the history of your supplier, and replace problem suppliers quickly.
- Marketing – Do not state that your product meets a standard (ANSI, UL), unless you have verified via product testing. Do not accept on face value a certificate from your supplier.

Tin Whiskers

Tin whiskers are electrically conductive metal crystals that grow spontaneously outward on surfaces with tin containing finishes as a result of post electroplating compressive stresses on the tin film layer. Within an electronic device, tin whiskers can grow between adjacent electrical conductors of differing electric potential, causing transient or permanent electrical shorts resulting in component or system failure. They are typically only a few microns (.001 millimeters) in diameter but can grow to lengths of more than 10 mm (0.4 inches). Whisker annual growth rates have been measured at 0.03 to 9 mm.[15] Once whiskers are long enough to bridge electrical leads, component electrical short can result. Historically, this has been a concern for safety-critical electronics with an anticipated long product life. However, with recent trends toward smaller devices and more components on the printed circuit board real estate, smaller length whiskers are now presenting similar problems.

In most cases formation occurs over > 1000 hours and whisker formation is not caught during product "burn in". Six month post-production predictability tests can be run, but whisker formation, in some cases, can take years to develop. High reliability applications, such as medical, aerospace and utilities, have been targeted as the focus of tin whisker concern as failure may result in catastrophic or very expensive equipment failure and recall. Tin whisker failures have been recorded in pacemakers, satellites, radar equipment, missiles, rocket motors and nuclear power utilities.

Tin whiskers' known risks have fallen into four categories [16];

1. Stable short circuit in low voltage, high impedance circuits
2. Transient short circuits.
3. Metal vapor arc; should a short occur under conditions of high current and voltage, the whisker vaporizes into highly conductive plasma sustaining an arc. This catastrophic phenomenon has led to the total failure of three orbiting satellites.
4. Debris/contamination; whiskers or portions that break free and bridge isolated conductors

---

[15] NASA, "*Basic Information Regarding Tin Whiskers*"
16 " " " "

History

The tin whisker phenomenon was first recognized in the 1940s. However in the 1950s companies began adding small amounts of lead (Pb) to the tin (Sn) to make solder. Solder had many advantages over pure tin; one of which was that the small amount of lead inhibited tin whiskers development. However, because of the "green initiatives" that have been implemented in Europe, China, South Korea, and California, in particular the European Union's Reduction of Hazardous Substances (RoHS) Directive, lead is for the most part being banned from electronic and electrical equipment. The most common and least costly approach among electronic component suppliers to meet the green initiatives was to eliminate lead from the solder, thus reintroducing the whisker problems of the past. Many companies are unfamiliar with the tin whiskers phenomenon and have not considered that exposure in alternate process specifications. The electronics industry has had to rapidly find potential solutions for a problem that is not completely understood

Specific Types of Vulnerable Products/Processes

Semiconductor Devices – Lead (Pb) has been used in a process known as lead finish ('lead' here refers to the external pins of the package that are used as connectors). Lead finish is the application of a layer of metal over the leads of the device to improve its solderability, protect it from corrosion and mechanical damage, and improve its appearance. Tin-lead solder has been commonly used as lead finish material, which is deposited either by solder plating or solder coating. Semiconductor companies have now switched to using tin-zinc, tin-copper, tin-bismuth, tin-silver, tin-indium, tin-silver-copper or nickel-palladium coatings for the finish material on the external pins. Many of these may be more expensive or have higher melting points or other processing issues.

Printed Circuit Board (PCB) Assembly Processes – The semiconductor devices and other components need to be attached to the circuit board, which has had thin narrow electrical circuits printed on to its surface. The devices/components historically were attached to the PCB with tin-lead solder. When pure tin is used, whiskers can grow between the external pins or leads of semiconductor devices and form an electrical short. This especially is a concern when the pins are very close together, known as fine-pitch. The short will be transient if the resulting current flow is enough to 'fuse' open the whisker. Otherwise, the short will be stable and can result in device failures. Metal vapor arcing may last for a few seconds or become self sustaining.

Reliability and Compliance Concerns

Whiskers should be considered as a potential cause of loss when evaluating electronics products liability. While "high reliability" components and products may be submitted for RoHS exemption, concerns exist about the availability and validation of specified materials. Lead free soldered components may inadvertently find their way into safety-critical assemblies.

Because of the RoHS lead restrictions; the industry has had to suddenly make changes in their production processes. For some high-volume low-cost products, reliability may not be a major issue, especially for products with short product life cycles. At the other end of the spectrum are the high reliability devices going into products used for safety critical applications. There is currently no complete understanding of whisker formation and growth and many different tin whisker mitigation strategies are being utilized. Although companies' products may now be compliant with industry standards, only over time will reliability be determined. While companies

may claim their lead free plating technology prevents whisker formation, but there is no long term proof.

A tin/lead plated component availability concern is shared among manufacturers that are exempt from the RoHS lead restriction requirements. These include companies with server, storage and telecommunication infrastructure applications and high-reliability equipment producers that support the aerospace, military, medical, and monitoring and control equipment industries. Although they are allowed to continue to use parts that contain (whisker-free, traditional/proven) tin-lead solder, they must rely on COTS (commercial off the shelf) components and parts. They are concerned that since they represent such a small market that soon many of these devices with tin-lead solder will not be available. Since these are often long service-life products, as noted above they are concerned about long term reliability if they use new lead-free components. So they are investigating how to modify lead-free parts to meet their requirements, which sometimes means giving them a subsequent tin-lead coating but quality/reliability concerns persist.

Companies now more than ever rely on others for sub-assembly/final-assembly work as well as components and parts. Often those sub-contractors will source the components and parts for the company based on generic performance specifications. There have been reported instances of companies who specify tin/lead components identifying post-production lead free components with the associated reliability problems identified above. The U.S. Food and Drug Administration recommends third party validation of soldered high reliability medical component materials content.

Loss Experience Attributed to Tin Whiskers

There is quite a bit of published information about incidents caused by tin whiskers which is available by electronic link in the reference section below. Failures include loss of operations involving satellites in space (1998 – 2000), heart pacemaker failure resulting in a recall (1985), problems at large power plants (2005), concerns at computer data centers, and other events. The NASA Goddard Space Flight Center's Tin Whisker web site has extensive information concerning tin (and other metal) whisker induced failures.

Tin Whisker Industry Standards and Best Practices

The International Electronics Manufacturing Initiative (iNEMI) along with the Joint Electron Device Engineering Council (JEDEC), Center for Advanced Life Cycle Engineering (CALCE), and the IPC (Institute for Printed Circuits) Association have been very active, publishing key industry standards and research papers. Much of this research has been driven by the iNEMI Tin Whisker User Group that consists of eleven large manufacturers of high-reliability electronic assemblies and is focused on tin whisker mitigation techniques and associated testing to provide objective evidence of mitigation efficacy.

The iNEMI Tin Whisker User Group in December 2006 published "Recommendations on Lead-Free Finishes for Components used in High-Reliability Products, Version 4".[17] They based these recommendations on 20 whisker mitigation guidelines. The paper lists commonly available mitigation practices, less common viable mitigation practices, finishes to avoid and mitigation

---

[17] iNEMI Tin Whiskers User Group, "*Recommendations on Lead-Free Finishes for Components used in High-Reliability Products, Version 4*", December, 2006

practices needing further study. iNEMI also lists base materials and finishes which are acceptable and unacceptable and level of whisker testing required.

In 2006, JP002, "Current Tin Whiskers Theory and Mitigation Practices Guideline" and JESD201, "Environmental Acceptance Requirements for Tin Whisker Susceptibility of Tin and Tin Alloy Surface Finishes" were published.[18] JP002 provides guidance in understanding the prevalent theories at this time regarding tin whisker formation, the driving force behind tin whisker growth, and mitigation practices used to minimize whiskers. JESD201 provides a uniform environmental acceptance testing and reporting methodology for tin whisker susceptibility of tin and tin alloy surface finishes used in the electronics industry. It is intended to be used with JESD22-A121, "Test Method for Measuring Whisker Growth on Tin and Tin Alloy Surface Finishes". The mitigation practices detailed in JP002, combined with the test and acceptance criteria outlined in JESD201, form the cornerstone of a three-fold strategy of mitigation practices, plating process controls and tin whisker testing that helps to reduce the risks of failures due to tin whiskers. At this time there is no "whisker free" tin plating process.

Electrical products companies should be adhering to "best practice" soldering guidelines from iNEMI or JEDEC guidelines. Solder selection and thorough extent of follow up testing should be documented. History of whisker problem development and resolution steps should be assessed. Purchaser third party qualified component analysis of solder content will substantiate compliance with specifications.

Zinc Whiskers

Zinc whiskers are tiny metal threads that develop over time in computer rooms with older style zinc plated flooring and structural hardware. Companies with computer rooms should have an awareness of zinc whisker implications and inspection methods, particularly for aging installations.

The risk posed by zinc whiskers has grown because of;

- Electronic circuitry advances and miniaturization
- Reduction of circuit voltages and currents which keeps whiskers from melting
- Aging computer room floors and equipment racks
- Upgrade activities debris generation

Zinc whisker problems may be suspected when;

- Unexplainable system failures occur at the same time as maintenance activities requiring floor tile handling or within weeks afterwards
- Newer equipment experiences more failures than older equipment
- Equipment closest to floor vents experience a greater failure rate

---

[18] JEDEC, "*Current Tin Whiskers Theory and Mitigation Practices Guideline*" and JESD201, "*Environmental Acceptance Requirements for Tin Whisker Susceptibility of Tin and Tin Alloy Surface Finishes*", 2006

Formation

Zinc electroplating places stress on plated materials which results in the production of zinc crystals and whiskers. The most frequent source of computer room zinc whiskers is the zinc plated flat steel sheet underside of the raised wood or concrete core floor tiles.[19] This problem is, however, a multi vendor/manufacturer issue including manufacturers of computers, device cases, cabinetry and support structures, mechanical hardware, and flooring, as well as OEM suppliers. Equipment typically does not present the same degree of whisker growth density as the floor tiles. The whiskers grow on computer room floor tiles, pedestals and stringers, equipment racks and rails and card cages, as well as mechanical hardware like nuts and screws because they have a zinc electroplated anti-corrosion coating. These whiskers develop over many years and range from 2 microns to several millimeters in length. The whiskers may break free from the surfaces becoming airborne. The underside of a computer room floor is an air plenum which can readily circulate zinc fibers throughout the room. Normal computer room air filters do not catch these minute particles. Numerous hardware manufacturers have warned about the potential impact of zinc whiskers on electronics.

Risks

Zinc whisker release is a problem in older computer room installations, particularly post construction or maintenance work which disrupts and releases fibers. [20]Walking on the tiles or moving them for electrical inspection or repair can dislodge these fibers.

Zinc plated tile bottoms have a flat, dull to somewhat shiny, unpainted appearance. Other computer room hardware may still contain zinc plated components and should be part of an exposure evaluation.

Should the zinc fibers be drawn into electronic equipment and/or land on electronic equipment circuitry, an intermittent or complete short may result. An intermittent short causes fault conditions and periodic drive problems and it is often difficult to pinpoint the cause. Problems observed range from nuisance issues, like data corruption, voltage variances which interrupt electrical service and system resets, or serious concerns such as power supply failures, which can lead to catastrophic hardware breakdowns. The short circuit condition often dislodges or vaporizes the causative whisker leaving a "no trouble found (NTF)" result. Low voltage applications are less likely to vaporize the whisker. Sometimes the whisker is dislodged during shipping when suspect equipment is returned to the vendor. Zinc whiskers from floor tile plating are not expected to cause fires.

Best Practices

Recognition of the potential zinc whiskers problem, particularly for aging computer centers may prevent continuing problems from intermittent, continuous or catastrophic shorts. This can be accomplished by the client or qualified contractor performing the following steps:

1. Visual inspection to determine whether or not floor tiles have zinc plated undersides.
2. Periodic inspection of computer room floors and racks for zinc whiskers to identify potentially impending problems.

---

[19] Brusse, Jay, NASA, "*Could Zinc Whiskers Be Impacting Your Electronics*?", 2003

[20] Brusse, Jay and Michael Sampson, "*Zinc Whiskers: Hidden Cause of Equipment Failure*", IT Pro, December, 2004

3. Zinc whisker containing tile handling should be minimized.
4. Maintenance and construction in computer rooms should be evaluated for the potential to disturb zinc fiber debris.

If zinc whiskers are discovered on raised floor tiles in a computer or telecommunications room a recommendation should be submitted to have them professionally replaced. Special attention should be directed at whisker containment and clean up to mitigate fiber release during this process. [21]

Bibliography

Atkinson, William, "*Supply Chain Management: New Opportunities for Risk Managers"*, Purchasing Magazine, June, 2006

Brusse, Jay, *"Could Zinc Whiskers Be Impacting Your Electronics?",* NASA, 2003

Brusse, Jay and Michael Sampson, "*Zinc Whiskers: Hidden Cause of Equipment Failure",* IT Pro, 12/2004

CALCE, *"Position Paper on Risks to High-Reliability Electronics and Associated Hardware from Pure Tin Coatings", July 25, 2002*

Dowding, Tony, "*Consumer Attitude and Legislation Make Their Mark on Food Recall Risk*", Business Insurance, December 17, 2007

FDA, *Import Program Systems Information*

IBM, "*Balancing Risk and Performance with an Integrated Finance Organization, The Global CFO Study"*, 2008

iNEMI, "*Recommendations on Lead-Free Finishes for Components Used in High-Reliability Products*", December, 2006

iNEMI, "Recommendations *to Electronics Industry Component Supply Base*", August 19, 2005

iNEMI, "*Pb-Free Manufacturing Requirements for High-Complexity, Thermally Challenging Electronic Assemblies*", February 16, 2006

Interagency Working Group on Import Safety, "*Action Plan For Import Safety*", 2007

JEDEC, JP002, "*Current Tin Whiskers Theory & Mitigation Practices Guideline*", JEDEC/IPC, March, 2006

JEDEC, JESD201, "*Environmental Acceptance Requirements for Tin Whisker Susceptibility of Tin and Tin Alloy Surface Finishes*", JEDEC/iNEMI, March, 2006

[21] Miller, Sandra Kay, "Whiskers in the Data Center", Processor, Volume 29, Issue 30, 7/27/2007

JEDEC, JESD22A121.1, "*Test Method for Measuring Whisker Growth in Tin and Tin Alloy Surface Finishes*", JEDEC/iNEMI,, May, 2005

Koziara, J. et al, *In Situ Blood–Brain Barrier Transport of Nanoparticles,* Pharmaceutical Research, November, 2003, Volume 20, 1772-78

Losev, Stepehen, "*Technology Helps Keep Border Traffic Flowing Safely*", Federal Times, July, 2005

Miller, Sandra Kay, "*Whiskers in the Data Center*", Processor, Volume 29, Issue 30, July 27, 2007

Muller, J et al, Respiratory Toxicity of Multi-Wall Carbon Nanotubes, *Toxicology and Applied Pharmacology, September 15, 2005, 207(3) 221-31*

NASA, *Tin Whiskers and Zinc Whiskers*

National Nanotechnology Initiative, *NNI Strategic Plan,* December 2004

NIOSH, *Nanotechnology, and Occupational Safety and Health Research - Frequently Asked Questions*

NIOSH, Publication No. 2007-123 Progress Toward Safe Nanotechnology in the Workplace

Roco, M. C., National Science Foundation, "*Government Nanotechnology Funding: An International Outlook"*, June 30, 2003

Schmit, Julie, "*U.S. Food Imports Outrun FDA Resources*", USA Today, March 18, 2007

Woodrow Wilson Institute for Scholars Project on Emerging Nanotechnologies, *Nanotechnology Consumer Products Inventor*y