Zinc Whiskers – What You Should Know Now!

Rich Hill, Data Clean Corporation

BACKGROUND

Metal whiskers have long been a known problem for electronics. For the last 10 years, the article *Are Zinc Whiskers Growing in Your Computer Room?* has been used as a guide to investigate and remediate Zinc Whiskers from data centers around the globe. Unfortunately, despite significant effort, Zinc Whiskers haven't gone away.

As an industry it was generally considered that the only serious source of Zinc Whiskers in computer facilities was certain types of access floor panels. Facilities without these specific panel types were assumed ineligible for whisker contamination.

How wrong was that assumption! Zinc Whiskers have been found on a variety of metal components within all types of facilities, including: steel building studs; electrical conduit; suspended ceiling T-bar grid and hanger wires; and of course access floor panels, pedestals, pedestal heads, and stringers. This may be surprising, but it's not really news.

PART I – Zinc Whisker Susceptibility

The real news is Zinc Whiskers are being discovered every day on cabinets, racks, and the servers and computers themselves. That's right! Zinc Whiskers may be growing on and in computer hardware.

How is this possible? It's simple really. Computer systems are a combination of electronic circuit cards mounted and contained within metal boxes and enclosures. The metal of choice is steel because it is conductive, strong, and reasonably inexpensive. The steel is often plated to prevent oxidation or rust. Zinc is still the plating material of choice because it's relatively inexpensive, is conductive, and yields a good finish appearance. Many computer enclosures are zinc plated; so are rack rails, cabinet shelf supports, and other structural elements.

If Zinc Whiskers are everywhere, aren't they noticeable? Remember that Zinc Whiskers are thinner than a human hair and roughly 0.5 – 5.0mm long. You have to be looking for them to find them. Look for them growing en masse. Seeing a single whisker is like looking for the proverbial needle in a haystack.

Zinc Whisker contamination should be considered whenever there are abnormally high failure rates – both catastrophic and less severe soft failures. The failure rate may peak within 72 hours of performing invasive maintenance work in or around the equipment.

Many factors determine the probability of Zinc Whisker failures. These include but are not limited to:

- Age of the source material and therefore the general length of the whiskers.
- Susceptibility to mechanical actions such as scraping, scuffing and vibration, that can cause whiskers to release from the host surface and migrate freely.
- Susceptibility of equipment to whisker failures.

Many users wrongly conclude only power supplies are susceptible to whisker related failures. This is likely because power supply failure tends to occur with a dramatically loud 'pop' and cause a system outage. Unfortunately, power supplies are not the only exposed electronics in a computer system. There are a myriad of integrated circuits (chips), leads, circuit traces, and other components. To be sure, parts of all the items on this list may be concealed by plastic or solder mask and generally unexposed.

But not everything is protected, and these uncovered leads are just as susceptible as the power supply. Zinc whisker bridges and shorts of exposed circuitry still have the potential to wreak havoc on a system. What happens if leads on the memory bus are intermittently shorted during the critical setup and latch portion of the clock cycle? Perhaps data will be corrupted. Perhaps the corruption will be detected and corrected by error correction algorithms. Perhaps the affected data is really an instruction for the processor. What if the processor tries to load and execute this corrupted instruction? Will the system failover or hang? Any engineer will agree that finding and fixing intermittent failures is one of the hardest things to do. "If you can't see it, you can't fix it." Whisker related failures fit into this category.

Many system anomalies are not logged or tracked. If a reset clears the situation, the problem is quickly dismissed as annoying but non-critical. Often, these on-the-floor fixes don't get the visibility of management. Ask an IT manager if equipment needs to be reset and they'll say, "…no, why do you ask?" Ask an operator if equipment needs to be reset and they'll answer, "…of course, all the time, why do you ask?"

So, if Zinc Whiskers are everywhere and affecting equipment, how come it is not common knowledge? Most users get their information from personal experience or from trusted sources. If personal experiences are not memorable, it's human nature to discount and discard them. If resetting a stuck machine is no more memorable than filling a coffee cup, it isn't remembered. A power supply popping is unusual and memorable. Clicking the <RESTART> button is not.

In the IT world, trusted resources are typically associates and vendors. Neither one is talking because neither one has an incentive to talk. Users don't admit they have Zinc Whisker problems because of fear of condemnation and repercussions from vendors. Users are supposed to honor their equipment contracts by maintaining suitable computing environments. Zinc Whisker contamination does not contribute to a suitable environment. Likewise, vendors aren't talking for fear of liability. Vendors are supposed to honor explicit and implied warranties that the equipment they produce and sell is free from defects. If the very equipment is vulnerable and or producing the whiskers, there is a legitimate fear of legal liability.

The result of all this silence is customer ignorance about a very serious topic.

PART II – The Reach of Zinc Whiskers and What to Do Next

How bad is it?

Evidence suggests that Zinc Whiskers may affect one or more components in 50% or more of the racks and cabinets in any given environment. Historically, manufacturers only tested equipment when problems were suspected. Users only tested when the manufacturers weren't providing answers. Recently, large users have been willing to sponsor broader, facility-wide testing. Unfortunately, for the reasons indicated above, the specific results of these tests remain confidential. Suffice it to say, Zinc Whiskers affect or have affected virtually all vendors.

If whiskers abound, why aren't there more problems?

The evidence suggests that Zinc Whiskers tend to remain reasonably well connected to the host surface. Until they reach a certain length, Zinc Whiskers will remain connected until they are liberated by mechanical means such as rubbing and scraping. After they reach a certain length, not only is liberation possible from direct mechanical means but also from more passive means such as vibration or airflow. Once dislodged, Zinc Whiskers are free to migrate within the environment.

Zinc Whisker failures need not be catastrophic. Bit errors, soft failures, and other anomalies may be attributed to Zinc Whiskers.

What is the cure for Zinc Whiskers?

Generally, the accepted cure for Zinc Whiskers is to remove and replace the root source material with an uncontaminated version. It is not reasonable to replace every contaminated piece of equipment, either from a logistics or financial perspective. That doesn't mean the problem should be ignored. . Zinc Whiskers will continue to grow. As they become longer, they become potentially more harmful.

Users can't stop using their equipment nor can they stop meeting the needs of the business through hardware migrations, moves and rearrangements. Users who want to proactively address the issue should develop a plan for managing the issue through staff training, vendor management, and equipment and facility handling procedures.

There are many suitable healthcare analogies that can realistically be applied: don't stop working with a sick patient; don't ignore the patient's condition. Rather, take proactive steps to help the patient while preventing the patient from infecting or sickening others.

Part III - Addressing Zinc Whisker Contamination

The following recommendations are based on a logical argument that to do nothing is neither proactive nor rational in the long term. Something must be done. Outlined below is one possible approach to dealing with broad Zinc Whisker contamination.

Users should require:

- All persons who enter the site will be informed of the presence of Zinc Whiskers and be required to sign a nondisclosure agreement. Violators of the NDA may jeopardize their employment or vendor status.

- All staff and visitors who have any business **touching** any equipment in the room must be trained and tested on **Zinc Whisker Awareness**.

- All staff and visitors who have any business **working on** any equipment in the room must be trained and tested on **Zinc Whisker Management**.

- Upon passing the Zinc Whisker management training, all staff and visitors will be required to sign the Zinc Whisker conduct pledge. This pledge will compel staff and visitors to treat Zinc Whiskers seriously and to take no action that would aggravate the problem. Their actions will reflect the best interests of the user and reliable computing.

- All cabinets will be examined for Zinc Whiskers. The results of the examination will be posted on the front and rear door of the cabinet.

- Identified Zinc Whiskers in or on cabinets will be so indicated with colored adhesive markers. The markers will serve to alert staff and visitors where the contamination is most significant.

- Staff and visitors will be expected, by virtue of their training and agreement with the pledge, to work around the contaminated areas to the best of their ability.

Users will:

- Require, by way of purchase agreement, all new equipment to be free of Zinc Whiskers for a period of 36 months.

- Work with all vendors to help understand the problem and develop solutions for future designs.

- Seek to replace (either by purchase or through vendor agreement) any equipment that is expected to be on site longer than 18 months.

- Seek to monitor and manage any equipment that is expected to be retired or replaced in less than 18 months.
- Establish a monitoring program for failures.
- Establish test sites with regular sampling to monitor conditions in the room(s).
- Establish a regular cleaning program for the facility.
- Establish a cleaning program for inside racks.
- Continue with the investigative process to locate and eliminate any additional root sources. All cabinets in the data center should be inspected and tested, as needed, to determine where additional sources exist.
- Planning should begin immediately to undertake a thorough investigation, tracking, and remediation program. The program should include:
    - Identification of sources.
    - Management of the sources.
    - Removal of the root sources, as possible.
    - Cleaning of the data center to remediate and mitigate the potential impact.

CONCLUSION

Zinc Whiskers are more prevalent than previously considered and acknowledged. At the same time, we can live with Zinc Whiskers and enjoy reasonably reliable operations. But it is important to acknowledge and manage the condition - not ignore it. Living with a chronic contagious disease provides a useful operational model. Once a surface becomes a Zinc Whisker source, it will always be a Zinc Whisker source. Left undisturbed, reliable operation may continue. Unless interaction with that surface is required, the Zinc Whisker status of that material need not be disclosed. However, if interaction with the Zinc Whisker source is required, then service staff should be informed and trained to take appropriate precautions to prevent an unnecessary release of Zinc Whiskers and possible equipment damage or broader facility contamination.

About the Author

Rich Hill is President of Data Clean Corporation, an international company specializing in cleaning controlled environments such as computer rooms, cleanrooms, and telecom facilities.

During his 25+ year career in the computer and telecommunications industries, Rich has toured hundreds of computer facilities. Early in his career, as a design engineer, he consulted with

clients on hardware and software issues. Today, with Data Clean, he applies that background when counseling facility administrators on contamination issues.

Rich holds a Bachelor of Science in Electrical Engineering from Worcester Polytechnic Institute and a Master of Management from the Kellogg School at Northwestern University.

For more information, visit www.dataclean.com.