Eliminating the Top Causes of Customer-Attributable Integrated Circuit Failures

Andrew H. Olney
Analog Devices, Inc., 804 Woburn St., Wilmington, Massachusetts 01887 USA
Phone: (781) 937-2362 Fax: (781) 937-1013 Email: andrew.olney@analog.com

***Abstract*- The failure rates of electronic systems can be minimized if Original Equipment Manufacturers (OEMs), Original Design Manufacturers (ODMs), and Contract Manufacturers (CMs) follow specific guidelines for eliminating the most common causes of customer-attributable integrated circuit (IC) failures. Most importantly, OEMs/ODMs/CMs should always buy ICs directly from Original Component Manufacturers (OCMs) or their Authorized Distributors to ensure that ICs are authentic and have full factory warranties. Appropriate electrical overstress/electrostatic discharge (EOS/ESD) protection techniques should be used at the board-level and/or system-level. For particularly high-reliability applications, IC operating voltages and currents should be maintained well below IC Absolute Maximum Ratings. Since the failure rate for many IC failure mechanisms increases exponentially with increasing temperature, electronic systems should be designed to provide adequate cooling. Finally, OCMs' instructions for proper storage, handling, and board mounting of ICs need to always be followed, with particular attention given to moisture-sensitive components.**

I. Introduction

Many semiconductor companies provide customers with the option to return ICs for failure analysis (FA) if the integrated circuits (ICs) do not function as expected. This post-sales support is generally only offered to customers that purchase ICs either directly from the semiconductor company that was responsible for manufacturing the ICs, also known as the Original Component Manufacturer (OCM), or directly from the OCM's Authorized Distributors. Customers may return ICs for FA due to purely mechanical issues (such as bent pins, illegible markings, and solderability problems) or due to electrical issues (such as parametric failures or complete loss of IC functionality). The scope of this paper is customer ICs that fail electrically, though it will be shown that some electrical failures are triggered by thermal-mechanical mechanisms. While some OCMs only offer FA as a service on ICs failing during the warranty period, other OCMs, including Analog Devices, Inc. (ADI), offer FA over the life of the product. OCMs generally do not know what percentage of failing ICs are returned for FA. However, customers with electronic systems that are expensive and/or require high reliability (such as safety-critical automotive applications) are much more likely to submit rejects for FA than customers that make audio greeting cards, electronic toys, or other low-end products. By conducting FA on ICs with time-to-failures ranging from zero (i.e., ICs failing the first time they are tested or used) to >100,000 hours (i.e., greater than 11 years of continuous operation), OCMs obtain valuable insight into the major causes of customer IC failures.

For most OCMs, the top bar on the Pareto chart of customer returns is ICs that pass electrical testing using Automatic Test Equipment (ATE) and/or bench testing. These returns, which are often referred to as "No Trouble Found" (NTF), "No Fault Indicated" (NFI), "No Evidence of Failure" (NEOF), or something similar, will not be covered in detail in this paper since they generally do not warrant corrective action by either the customer or the OCM. For example, some customers troubleshoot failing boards down to a handful of suspect components (rather than a single suspect component), so it is not surprising that many customer returns test good. In cases where the customer and the OCM do not agree that a returned IC is electrically good, the OCM's Field Application Engineers (FAEs) can usually work with the customer to resolve the situation, since often the reported failure is due to an applications issue.

Excluding FA results where the OCM found nothing wrong with the ICs, most OCMs that conduct FAs on customer returns categorize the top-level results as either customer-attributable or OCM-attributable. In cases where the FA results show the root causes of failures are "owned" by customers (such as subjecting ICs to voltages or operating temperatures beyond their data sheet limits), the failures are deemed customer-attributable. On the other hand, in cases where the FA results show the root causes of failures are "owned" by OCMs (such as IC design errors or defects introduced during IC manufacturing), the failures are deemed OCM-attributable. OCMs have highly advanced systems and processes for IC design, layout, characterization, wafer fabrication, wafer probe, package assembly, and package test. Thus, OCM-attributable IC failures are substantially lower than customer-attributable IC failures. Consequently, by addressing customer-attributable IC failures, the overall reliability of systems incorporating anywhere from one to tens of thousands of ICs can be substantially improved.

With this background, the focus of this paper is providing specific guidelines on how OEMs/ODMs/CMs can eliminate the most common causes of IC failures. While the Pareto chart of customer-attributable failures will vary based on the specific OCM, industry FA results typically show that the top causes of such failures, in descending order, are as follows:

1. Buying ICs from non-authorized sources;
2. Subjecting ICs to EOS/ESD damage;
3. Operating ICs at excessive temperatures;
4. Improperly mounting or using ICs.

2013 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)/©2013 IEEE
http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6599118&queryText%3DOlney

II. Buying ICs from Non-authorized Sources

OCMs sell their ICs either directly to customers or through authorized distributors and authorized resellers that are contractually obligated to exclusively procure ICs from OCMs. Semiconductor companies list their authorized distributors / resellers on their Internet sites. In addition, the Semiconductor Industry Association (SIA) [1] has partnered with SIA member company Rochester Electronics to create, develop and maintain the Electronics Authorized Directory website [2]. With this website, the user can readily search by OCM and by location to find authorized distributors worldwide.

Despite the ease of determining authorized distributors for a given OCM, IC purchasing agents routinely turn to the open market to buy ICs. The open market consists of every entity that sells ICs without authorization from the OCM, including brokers, independent distributors, web-based component exchanges, and other companies and individuals that obtain products from a wide range of suppliers. Purchasing agents buy ICs from the open market for a variety of reasons, including: low prices; immediate availability; supplier listings at or near the top of web searches; and lack of knowledge about the differences between the open market and authorized distributors / resellers. ICs available in the open market often pass through a series of different suppliers and may have been improperly tested, handled, or stored at some point. This significantly increases the risk for introducing quality and/or reliability issues. Unfortunately, some of the suppliers to the open market either purposely or unknowingly introduce counterfeit components into the non-authorized supply chain. As with other illegal activity, determining the magnitude of the counterfeit IC problem is not possible. However, in April 2012, market research firm iHS iSuppli reported that "The five most prevalent types of semiconductors reported as counterfeits represent $169 billion in potential risk per year for the global electronics supply chain" [3].

Consistent with this iHS iSuppli report, OCM data continues to show that the primary cause of integrated circuit failures is buying ICs from open market sources rather than from authorized sources. ICs purchased through the open market may fail the first time they are tested or used, or, they may fail after extended periods of end-customer use. The causes of these quality and reliability failures are numerous and include the following:

A. Package Cracking / Delamination and/or Die Cracking

Many open market ICs consist of used components removed from scrap Printed Circuit Boards (PCBs). Flexing of PCBs and removal of components can cause subtle package damage, including stress fracturing at the external pins or solder balls. ICs with stress fractures that are re-mounted on new PCBs may pass initial electrical testing but later fail, especially if the end-product is dropped or is subjected to vibration. Re-used ICs sometimes have no external package anomalies yet they are unreliable. For example, a subtle die crack initiated during PCB removal may propagate during field use, particularly if the end application includes significant thermal-mechanical stressing. If the crack severs a metal interconnect on the die, the IC can suddenly fail catastrophically. As a final example, counterfeiters that remove used ICs from PCBs often do so in an uncontrolled manner that results in delamination between the mold compound and the die. This delamination can result in multiple failure mechanisms, including lifted ball bonds and bond wires snapped at the neck above ball bonds.

B. ESD Damage Due to Improper Processing and/or Handling

OCMs and their authorized distributors and resellers consistently follow industry best practices for minimizing charge generation and ensuring discharge voltages are well below the failure thresholds for ICs. However, if even one person in the supply chain for open market ICs does not take proper ESD precautions, the quality and reliability of the ICs will be questionable. Processes used by counterfeiters, including grinding off original package markings and re-marking packages, often result in severe package charging. Counterfeiters rarely take any ESD precautions (such as using ground straps and ionizers). When charged ICs contact a metal surface, they will discharge via rapid, high-current transients that can slightly damage thin gate and dielectric layers. The resulting leakage currents may be too low to result in immediate electrical failures. However, during end-customer operation, the leakage currents can increase over time, resulting in permanent IC failure.

C. "Popcorning" of ICs During Board Assembly

While OCMs properly bake and dry-pack moisture-sensitive ICs, open market suppliers and particularly counterfeiters may skip one or both of these manufacturing operations or take shortcuts to save time and cost. Even if open market ICs are dry-packed in sealed moisture barrier bags, they may not have been adequately baked first. Consequently, during mounting on PCBs using high-temperature reflow ovens, the moisture in the ICs expands rapidly and can cause packages to "popcorn," resulting in package cracking or delamination. This mechanical damage can become worse during end-customer use, resulting in IC reliability failures.

D. Counterfeit Components Marked Deceptively

ICs "harvested" from old PCBs are often many years old, and consequently they typically contain lead (Pb) and/or other materials that are now banned by the Restriction of Hazardous Substances Directive (RoHS). Many IC packages historically used tin-lead (SnPb) solder which facilitated component mounting at relatively low peak solder reflow temperatures (typically 220 °C to 235 °C). However, with the industry transition to Pb-free packages over the past decade, IC packages are now usually mounted using significantly higher peak reflow temperatures (typically 240 °C to 260 °C). Therefore, OCMs re-engineered IC package materials (such as mold compound and die attach) to make them reliable at these higher temperatures. Since most of the electronics industry has transitioned to Pb-free packages to meet RoHS requirements,

the demand for Pb-bearing packages has decreased sharply. Thus, counterfeiters usually re-mark old ICs to indicate they are Pb-free (when they are not) to make them saleable. In addition to the use of these counterfeit ICs causing RoHS compliance issues, PCB manufacturers that mount what they believe are Pb-free ICs at temperatures above 240 °C can unknowingly induce major reliability hazards since the packages were not designed to handle these high temperatures. For example, counterfeit Pb-bearing packages that are mounted at Pb-free reflow temperatures may "popcorn," resulting in cracking or delamination of the package and the associated failure mechanisms that were previously detailed. While marking Pb-bearing packages as Pb-free is most common, counterfeiters will do the inverse and mark Pb-free packages as Pb-bearing to meet remaining demand for legacy Pb-bearing packages. Due to the lack of controls in "manufacturing" these counterfeits, this results in a risk for tin whisker formation that can cause shorting between adjacent pins and solder balls on ICs.

E. Counterfeit Components Improperly Laser Marked

In an attempt to mimic OCMs, counterfeiters have largely transitioned from ink-marking to laser-marking of IC packages. OCMs are experts at developing, characterizing, qualifying, and monitoring laser marking processes to ensure package integrity is not compromised by laser marking operations. However, counterfeiters usually do not know the depth of bond wires in plastic packages, especially in cases where they have thinned these packages by chemically or mechanically removing the original package markings. Consequently, counterfeiters sometimes partially melt bond wires while laser marking, thus jeopardizing the reliability of these bond wires. Hermetic packages can likewise have poor reliability due to laser marking by counterfeiters. In a recent counterfeiting incident, when counterfeiters laser marked iron-based lids plated with nickel and gold, the laser fully removed both layers of plating, thus exposing the underlying iron. Any prolonged exposure of these counterfeit ICs to moisture would cause the iron to corrode away, resulting in loss of package hermeticity and likely catastrophic IC failure due to moisture ingression.

F. Counterfeit Components Corroding Due to Acid Ingress

In their attempt to make old or used components look new, counterfeiters typically use acids to "recondition" package pins and solder balls. These acids are sometimes incompatible with the package materials, thus compromising package integrity. Even if the acids are compatible with the packages, they may not be fully rinsed off by the counterfeiters. Any acid residues left after counterfeiters clean oxides and other contaminants from package pins, pads, and solder balls will initially penetrate only the surfaces of packages. However, particularly if the counterfeiters induced package delamination during their "manufacturing" operations, acid residues can result in corrosion of active die circuitry after months or years of field use. For example, Fig. 1 shows a corroded die on a counterfeit IC that failed after months of use. In this case, acid residue left by the counterfeiters on the external pins combined with moisture from a humid operating environment, and the acid solution penetrated the package along areas of the leadframe that were delaminated from the mold compound. The acid solution subsequently migrated along the interface between a bond wire and the mold compound and reached the bond pad, corroding away both the bond pad and the adjacent metallization. Since this was a counterfeit IC, the Contract Manufacturer had no OCM factory warranty coverage. Therefore, the CM was responsible for substantial warranty costs associated with this and other end-customer field failures caused by these counterfeit ICs.

The preceding six major categories of quality and reliability issues with open market and counterfeit ICs underscore the critical importance of buying ICs from authorized sources. In fact, the single best way to maximize the quality and reliability of electronic systems is to always buy all components either directly from OCMs or directly from their authorized distributors. This will ensure that these components, unlike open market components, have both factory warranties and post-sales support. While IC purchasers may think they are getting a good deal in terms of pricing and/or availability by turning to the open market, there are no assurances that these ICs are consistently authentic and reliable. While open market suppliers may provide Certificates of Conformance and other documentation indicating components are traceable to the OCM, suppliers of counterfeit ICs are adept at generating shipping boxes, packing materials, shipping labels, and documentation that are essentially indistinguishable from those supplied by OCMs. As previously detailed, open market ICs that pass electrical testing after board mounting may pose significant field reliability risks. If even one counterfeit IC ends up in an electronic system with hundreds or thousands of components, the reliability of the entire system may be significantly compromised by this one fake IC. Classic system-level Mean Time Between Failure (MTBF) reliability calculations, such as those detailed in MIL-HDBK-217 [4], are useless if one or more components in the system are counterfeit.

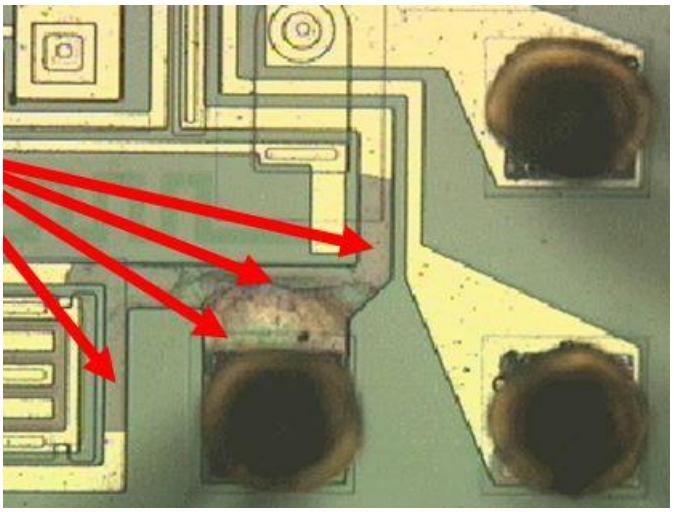

Fig. 1. Optical photograph of a field failure caused by acid used by counterfeiters subsequently corroding metallization on the die (see the arrows).

2013 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)/©2013 IEEE
http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6599118&queryText%3DOlney

III. Subjecting ICs to EOS/ESD Damage

The second most common cause of customer-attributable IC failures is electrical overstress / electrostatic discharge (EOS/ESD) damage. EOS damage can occur anytime an IC is subjected to voltage or current levels that exceed those specified in the Absolute Maximum Rating (AMR) section of a data sheet. EOS events can have any duration, but they typically are in the millisecond range. ESD events are a subset of EOS events, but ESD events are always very fast, ranging in duration from about one nanosecond for a Charged Device Model (CDM) or Charged Board Event (CBE) to several hundred nanoseconds for a Human Body Model (HBM) event [5]. As their names imply, CDM and CBE ESD occurs when components and circuit boards, respectively, become charged-up and then discharge due to contact with a metal object at or near ground potential. HBM ESD occurs when a charged person contacts an IC or a circuit board or an electronic system at or near ground potential. EOS failures almost always exhibit more severe damage than component-level ESD failures. However, when ESD damage occurs on an IC that is already mounted to a PCB, the ESD damage can be much more severe due to the discharging of the relatively large capacitance of the PCB, and thus board-level ESD damage can be difficult to differentiate from EOS damage [5].

OCMs include on-chip protection circuits on ICs to increase their robustness to EOS/ESD events. However, these protection circuits can degrade the overall electrical performance of ICs, particularly ICs with operating frequencies in the gigahertz range and/or with leakage currents in the picoampere range or below. Due to tradeoffs between on-chip EOS/ESD protection circuitry and overall IC electrical performance levels, it is not possible to make ICs immune to EOS/ESD damage. Therefore, both OCMs and their customers need to take precautions to ensure that ICs are not subjected to EOS/ESD damage.

While the HBM is better known than the CDM, almost all real-world component-level ESD failures are due to the CDM. Well-established HBM controls, including requiring personnel handling ICs to wear ESD ground straps to prevent any significant charging of body capacitance, are very effective at eliminating HBM failures on all but the most ESD-sensitive ICs. References [6] and [7] provide detailed information on preventing HBM failures. Automation in the semiconductor and circuit board assembly industries has caused component-level HBM failures to be largely a legacy issue [5]. Due to this automation, the CDM is now the dominant form of component-level ESD failures. CDM failures can be eliminated in one of two ways: either ensure ICs do not charge-up above the voltages at which they fail CDM classification testing, or, if ICs do charge above their CDM failure thresholds, ensure they are safely discharged before they contact a metal surface. Reducing charging is accomplished through various ESD control measures, including keeping non-essential insulators, such as plastic shields and bubble wrap, well away from ICs that are not enclosed in static-dissipative materials. Safely discharging any charged ICs is accomplished by additional measures, such as using static-dissipative materials (rather than metals) for any surfaces that charged ICs may contact, or by using ionizers to safely dissipate charges on insulating portions of IC packages. Use of ionizers during component pick-and-place operations onto PCBs is particularly important since these operations are a major source of CDM ESD failures. References [6] and [8] provide detailed information on preventing CDM failures.

Additional measures are required to minimize the possibility of EOS/ESD failures at the circuit board and the system levels. These measures should include the following as applicable:

1. Use extended ground pins (also known as first-mate-last break grounding pins) on all electrical connectors [9]. These extended ground pins prevent EOS/ESD damage that can otherwise occur during connecting and disconnecting of connectors.
2. Review application schematics and determine if any large external capacitors or large inductive loads are connected directly to IC pins. Rapid discharges of charged external capacitors or voltage transients due to rapid changes in the current in an inductor are major causes of EOS damage in ICs. If external capacitors or inductive loads may be causing voltage transients, consider adding an external series resistor to limit the current to a safe level. Alternatively, consider using a Transient Voltage Suppressor where the TVS is selected to prevent the voltage from exceeding the Absolute Maximum Ratings of the IC power supplies. A typical configuration for power supply TVS protection is shown in Fig. 2 [10, 11]. For maximum reliability, IC operating voltages and currents should be well below the AMRs whenever possible.
3. Ensure that discrete capacitors are not charged when placed on PCBs, since this can result in a high-current discharge that can damage ICs. One effective method of doing so is to use static-dissipative tips on pick-and-place equipment, with these tips bridging both terminals of the capacitor to safely discharge the capacitor before board placement.
4. Use a high-speed oscilloscope to check for voltage transients exceeding the Absolute Maximum Ratings of the IC during operation, particularly during power-up and power-down sequences. If such transients are identified and cannot be eliminated, consider adding an external series resistor or a TVS.

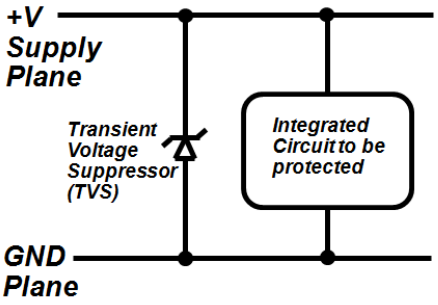

Fig. 2. Typical board-level TVS protection configuration.

2013 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)/©2013 IEEE
http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6599118&queryText%3DOlney

IV. Operating ICs at Excessive Temperatures

Most IC failure mechanisms are accelerated exponentially by temperature. For some of these mechanisms, such as electromigration and Time Dependent Dielectric Breakdown (TDDB), FA may not show any telltale signs that the failure was caused by excessive IC operating temperature in customer applications. However, one failure mechanism that is commonly seen on customer returns and is due to excessive operating temperature is Kirkendall voiding at the interface between gold (Au) ball bonds and aluminum-copper (AlCu) bond pads. Although use of Cu bond wires for plastic-encapsulated ICs is increasingly common, the majority of the hundreds of billions of ICs that are currently operating in customer applications use AlCu bond pads with Au bond wires. While these ICs will typically have no issues with Kirkendall voiding if operated for many years at or below the maximum operating temperature range on the IC data sheet (typically +85 °C to +125 °C), operation at well above this temperature for extended periods can result in Kirkendall voiding, which is also referred to as "ball bond wear-out."

A typical example of an IC field failure due to excessive operating temperature resulting in ball bond wear-out will be illustrated with a case study. An audio codec failed in a high-end audio amplifier due to excessive speaker noise after around one year of customer use. This IC was fabricated on a submicron CMOS process with AlCu metallization and assembled in an LQFP with industry-standard mold compound. FA showed multiple IC pins, including a supply pin, were electrically open. C-mode Scanning Acoustic Microscopy (C-SAM) revealed delamination between the mold compound and the die. Optical and scanning electron microscopy following package decapsulation showed the open pins were due to loss of continuity between Au ball bonds and AlCu bond pads caused by Kirkendall voiding as shown in Fig. 3a and 3b. Further investigation revealed that the cooling fan in the audio amplifier had failed, resulting in the junction temperature, T_J, for the IC significantly exceeding the +125 °C Absolute Maximum Rating for the case temperature per the IC data sheet. This excessive operating temperature resulted in Kirkendall voiding whereby Au from the ball bonds diffused into the AlCu bond pads, and Al from the bond pads diffused into the Au ball bonds. The resulting AuAl intermetallics included a brittle phase that initiated the physical separation between the intermetallics on the pad and the Au in the ball bond. This separation most likely occurred at the same time that significant mold compound to die delamination developed as a result of excessive IC heating.

Although the specific causes of excessive IC operating temperatures vary widely, this and other case studies underscore the critical importance of ensuring that IC T_J's do not exceed rated limits for extended periods of time. Ball bond wear-out is the fundamental life-limiting failure mechanism for many ICs operated at high temperatures. Exceptions include ICs assembled in hermetic packages and ICs that use Over-Pad Metallization (OPM) to eliminate AlCu-to-Au interfaces. However, unless all ICs in a system are rated for very high operating temperatures, Printed Circuit Boards (PCBs) and electronic systems should be designed to maintain IC T_J's at below +85 °C if at all possible. This will not only eliminate the risk of ball bond wear-out, but will also reduce the risk of failure due to IC fabrication and assembly defects with associated failure mechanisms that are accelerated by temperature. Providing detailed recommendations on how to minimize operating temperatures at the PCB-level and system-level is beyond the scope of this paper. However, the cooling methodologies employed need to be inherently reliable. For example, as illustrated by the preceding example, reliability should be one of the primary criteria for selecting cooling fans.

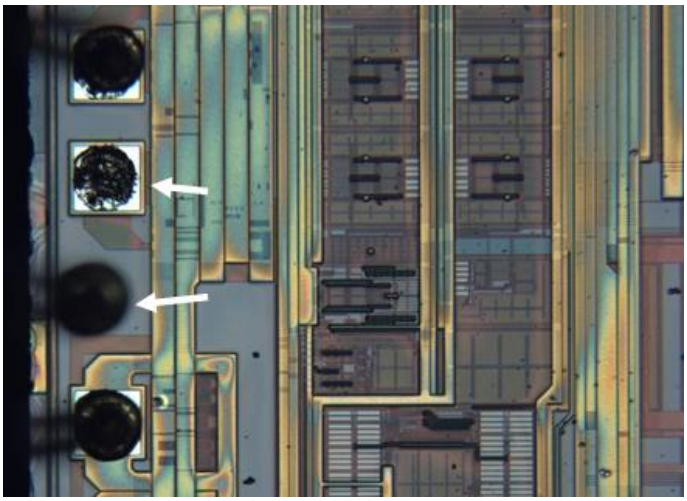

Fig. 3a. Optical photograph of a field failure due to Kirkendall voiding at the ball bonds. Note: One of the ball bonds completely separated from its corresponding bond pad during package decapsulation (see the arrows).

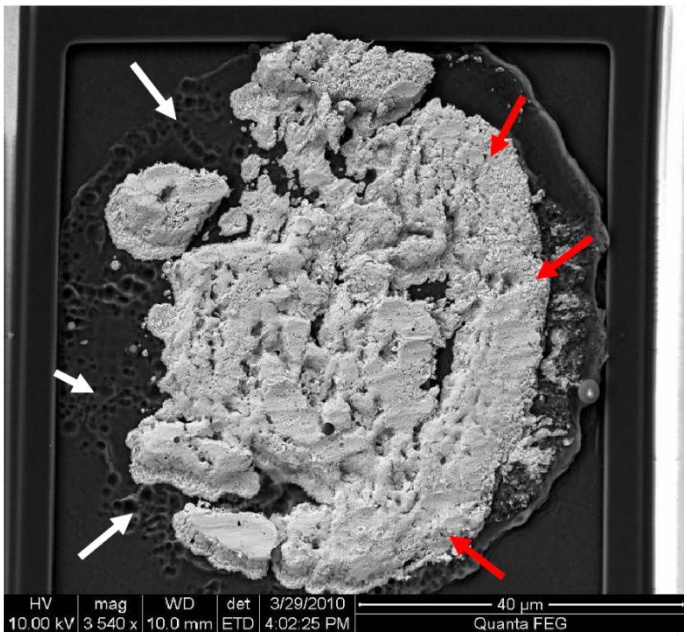

Fig. 3b. Scanning electron micrograph showing the Kirkendall voiding at one of the bond pads on the unit shown in Fig. 3a. The white arrows show where the Al from the bond pad diffused into the bottom of the Au ball bond, leaving voids. The red arrows show areas of excessive, porous Au-Al intermetallics.

2013 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)/©2013 IEEE
http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6599118&queryText%3DOlney

V. Improperly Mounting or Using ICs

IC data sheets and application notes include details on how to properly handle, store, mount, and use ICs to minimize any quality and reliability issues. The specific recommendations and requirements vary significantly based on the IC technologies of interest. For example, the Absolute Maximum Ratings (AMR) sections for most microelectromechanical systems (MEMS) products specify mechanical shock limits and/or drop height limits above which permanent damage to the MEMS structure may occur [12]. ICs with Moisture Sensitivity Level 1 do not require dry-pack but should nonetheless be stored at ≤ 30 °C and ≤ 60% RH to minimize oxidation of package pins and solder balls. (Brief exposure to higher temperatures and/or relative humidity should not be an issue.) Customers should always read and follow all recommendations and requirements in IC data sheets along with associated application notes.

Many customer-attributable failures can be readily prevented by following the instructions on moisture barrier bag (MBB) labels for dry-packed ICs. These labels specify critical information for correctly mounting ICs on PCBs, including the moisture sensitivity level (MSL) of the ICs; the peak package body temperature; and the maximum time ICs can be out of the MBB at ≤ 30 °C and ≤ 60% RH. The MBB labels also specify under what conditions baking of ICs is required prior to PCB mounting, and the labels include references to applicable industry specifications for proper baking procedures. Failure to follow the instructions on MBB labels can result in ICs failing due to various mechanisms. For example, Fig. 4 shows a case where a customer exposed an MSL 3 Lead Frame Chip-Scale Package (LFCSP) to excessive moisture prior to board mounting, and this resulted in significant delamination between the mold compound and the die paddle. This delamination caused the Au bond wires to snap at their necks. Fortunately, some of these wire breaks were severe enough to immediately result in open pins, and consequently the failures were detected by the customer in their manufacturing line.

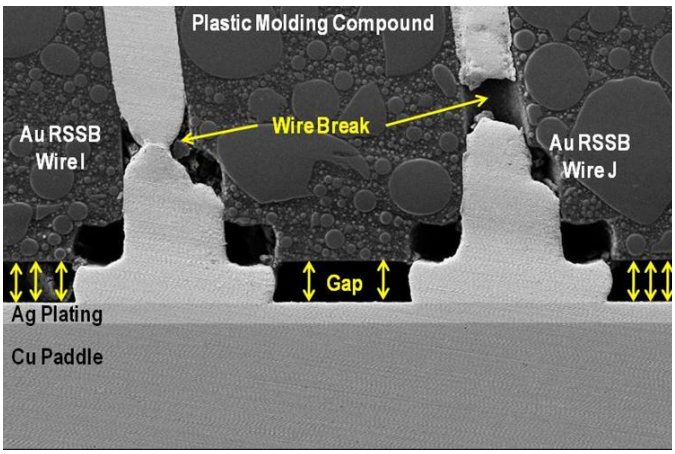

Fig. 4. Scanning electron micrograph showing how severe delamination between the package mold compound and the die paddle resulted in wire breaks above the gold Reverse Standoff Stitch Bond (RSSB) to the paddle.

VI. Conclusion

The failure analysis results obtained by semiconductor companies provide valuable data for identifying the most common causes of customer-attributable IC failures along with the associated actions to preclude these failures. By adhering to the following recommendations, OEMs/ODMs/CMs can greatly reduce customer-attributable IC failures:

1. Most importantly, all ICs must be purchased either directly from the Original Component Manufacturers or directly from their authorized distributors. This will ensure that ICs are authentic and have factory warranties. By always purchasing from authorized sources, customers will avoid the numerous quality and reliability risks with open market ICs, including counterfeit ICs.
2. Follow best practices for eliminating EOS/ESD damage, including using extended ground pins on connectors and Transient Voltage Suppressors on PCBs as appropriate.
3. Minimize the junction temperature for ICs during field operation through proper board-level and system-level design. This will preclude ball bond wear-out and will reduce the risk for other failure mechanisms where the failure rate increases exponentially with temperature.
4. Read and follow IC data sheets, application notes, and moisture barrier bag labels to avoid failures due to improper handling, storing, and mounting of ICs.

Acknowledgment

The author gratefully acknowledges support from the following colleagues at Analog Devices: Maurice Brodeur, Brad Gifford, Jean-Jacques Hajjar, James Molyneaux, Alan Righter, Tony Tollis, and Ed Wolfe. In addition, the author thanks the Semiconductor Industry Association Anti-Counterfeiting Task Force for their contributions to this paper.

References

[1] "Semiconductor Industry Association (SIA)." http://www.semiconductors.org/. Web. 08 June 2013.
[2] "Electronics Authorized Directory." http://www.authorizeddirectory.com/. Web. 08 June 2013.
[3] iHS Isuppli press release, "Top 5 Most Counterfeited Parts Represent a $169 Billion Potential Challenge for Global Semiconductor Market," April 4, 2012. http://www.isuppli.com/Semiconductor-Value-Chain/News/Pages/Top-5-Most-Counterfeited-Parts-Represent-a-$169-Billion-Potential-Challenge-for-Global-Semiconductor-Market.aspx . Web. 08 June 2013.
[4] "MIL-HDBK-217F: Military Handbook – Reliability Prediction of Electronic Equipment," December, 1991. http://www.sre.org/pubs/Mil-Hdbk-217F.pdf. Web. 08 June 2013.
[5] A. Olney, B. Gifford, J. Guravage, A. Righter, "Real-world Charged Board Model (CBM) failures," *EOS/ESD Symposium*, 2003.
[6] "ANSI/ESD S20.20-2007: Protection of electrical and electronic arts, assemblies and equipment (excluding electrically initiated and explosive devices)," *ESD Association*, Rome, New York, 2007.
[7] "White paper 1: A case for lowering component level HBM/MM ESD specifications and requirements," *Industry Council on ESD Target Levels*, September 2011.
[8] "White paper 2: A case for lowering component level CDM ESD specifications and requirements," *Industry Council on ESD Target Levels*,

April 2010.
[9] "White paper: First-mate-last-break grounding contacts in the automotive industry," *ZVEI*, Frankfurt am Main, Germany, 2011.
[10] M. Byrne, "Application note AN-311: How to reliably protect CMOS circuits against power supply overvoltaging," *Analog Devices, Inc.*, Norwood, Massachusetts.
[11] N. Lyne, "Application note 397: Electrically induced damage to standard linear integrated circuits: The most common causes and the associated fixes to prevent recurrence," *Analog Devices, Inc.*, Norwood, Massachusetts.
[12] A. Olney, "Evolving MEMS qualification requirements," *International Reliability Physics Symposium*, SAR/IRPS, Rome, New York, 2010.