Assessing the Reliability Risk of a Maverick Manufacturing Anomaly

William J. Roesch and Dave Littleton

TriQuint Semiconductor, Inc., 2300 N.E. Brookwood Parkway, Hillsboro, Oregon 97124-5300
Phone: (503) 615-9292 FAX: (503) 615-8903 EMAIL: broesch@tqs.com

KEYWORDS: outlier, excursion, escape, defects, metallization, screen, detection, prediction.

ABSTRACT

Compound semiconductor manufacturing processes occasionally experience an unusual event during wafer fabrication. Depending on the severity of the event and the coverage of the detection methods and control systems, the event could produce a wafer that has reliability outside of the normal population of wafers. If the anomaly exists in products which elude the normal supplier detection methods, there might be a possibility that some samples would reach a customer before the event was discovered. In the unhappy situation of recalling this type of anomalous material, the customer will invariably ask "***What is the reliability risk*** of choosing to deploy the anomalous devices?" This work is intended to describe a methodology to answer that question, and demonstrate data obtained from an actual maverick event.

CURING THE COMMON CAUSE

One of the first considerations of investigating an anomaly is to determine the cause of un-reliability (or un-quality). One categorization of causes is to consider common-cause versus special-cause.

Common-causes are all of the natural variation that exists in device fabrication, assembly, and testing. Special-causes are unique events, incidents, or accidents which produce some result which is neither predictable nor assignable to the general population of devices. Some comparisons of common-causes and special-causes are shown in Table 1.

TABLE 1
COMMON- AND SPECIAL-CAUSES OF VARIATION.

Common-Causes	Special-Causes
normal Fab tool degradation between maintenance events	skipped maintenance
normal tool variation	machine malfunction
raw material variation	unapproved source of raw material
variability in settings	operator error
machine-to-machine variation	skipped step or doubled step
normal process vacuum variation	leak to atmosphere
poor design	power surge (ESD or EOS)
within-family	out-of-family
present in all batches	rare occurrence
population straddles spec limit	Non-standard rework to center population

The reason for determining the type of cause is that the cure, (or the mitigation) is quite different for each type. Reducing common causes is accomplished by reducing variation. Improvements in one area may affect other areas and there is an overall synergy. Semiconductor processing will naturally mature by repetition. Process improvement experiments can pinpoint sources of variation and provide methods for reducing variation. Statistical process control provides ongoing measurement of process capability and measurement of inherent variability.

On the other hand, special causes may not have synergy with anything, either with common causes or with other special causes. Special causes can occur on mature processes which already exhibit very low common cause variation. While many special causes can be prevented by rigorous methods and a disciplined processes, the best mitigation is to permanently eliminate the root cause and verify the elimination by improving the detection methods and by preventing recurrence. One of the obvious and largest groupings of special causes is defects.

Another correlation that is important in reducing customer reliability failures is the relationship between outliers and mavericks. In many cases, outliers and mavericks are considered as the same thing, and the terms are used interchangeably. However, a maverick population is one that causes fallout in the final application and otherwise goes undetected during fabrication, assembly, and manufacturing.[1] On the other hand, outliers are a population that can be within specification but are unusual compared to the prevailing population. The definitions of outliers and mavericks depend critically on what is being measured and where it is measured. The correlation is important since most of the process control monitoring and component measurements are considerably different than the system measurements in the final application.

METHODS OF DETECTION: ESCAPE POINTS

For modern semiconductor processes, detection is achieved by the use of escape points. Escape points are defined as steps in a manufacturing/fabrication process where fallout can be caught. Escape points are often measurements of physical attributes or electrical properties. The idea here is to consider not only the root cause of a problem, but equally as important, what went wrong with the control system in allowing this problem to escape downstream. Reliability engineers must work with their

process engineering teammates to identify and verify all of the applicable escape points. In semiconductor processing the escape point is more precisely defined as the earliest control point in the Fab Process following the appearance of the root cause that should have detected the problem but failed to do so. The potential value in considering escape points is the redundancy of not only solving the root cause of problems, but also in improving the detection of future problems. A robust problem solving process would include selection of corrective action, verification, implementation, and validation of both the method to eliminate the root cause, and also the method to improve the effectiveness of the escape points.

PROBLEM DESCRIPTION & DATA

The following case study will provide a template showing the timeline of an actual maverick event. Several key variables are identified which lead up to the determination of reliability risk of anomalous products. Following is a timeline of major events in this example:

TABLE 2.
TIMELINE OF MAJOR EVENTS:

9/27/10 – 1st Escape Point triggered: parametric signal at wafer test.
9/28/10 – Tool commonality analysis result: Tool A down + quarantine
9/30/10 – 2nd Escape Point triggered: physical signal at shear test
10/1/10 – Identify root cause: fault reproduced in Tool A.
10/3/10 – Process experiment confirms/verifies root cause correction
10/9/10 – 2nd Escape Point re-triggered: physical signal at shear test
10/9/10 – Increased sampling of 2nd Escape Point
10/22/10 – 3rd Escape Point triggered: physical signal at wire bond.
Disposition: Scrapped all wafers through Tool A for 15 days prior to anomaly
12/08/10 – First customer return. Confirmed as anomaly from Tool A
Very few customers experienced fallout.
4/1/2011 - Completed recall of suspect parts.
All fallout confirmed from Sept. 2 to Sept.13

During the course of this case study, the anomaly was detected in several lots by the existing escape points that were part of the prevention system. As a result, the original classification was as an outlier event. However, additional outliers were detected at subsequent escape points. Eventually, some anomalous samples did reach a customer, and so this event was reclassified as a Maverick event.

The chronological boundries of the anomaly grew at every step of the timeline shown in Table 2. In terms of the original escape point, three particularly affected wafer lots signaled the problem. (see Figure 2) This amounted to less than 25 wafers which gave the initial signal. However, by the time the tool commonality investigation had indicated a single tool (named "Tool A") was responsible, twelve more lots had been processed and 19 more wafers were caught at the initial escape point.

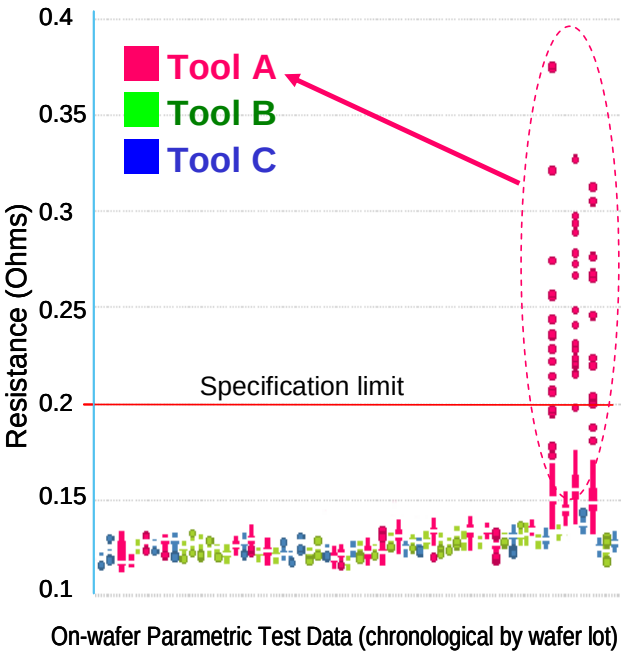

FIGURE 1. DETECTION OF ANOMALY BY 1ST ESCAPE POINT. PARAMETRIC WAFER MEASUREMENT.

The Tool A identification triggered the immediate containment action of shutting down the tool and initiation of a search for the root cause. All lots and wafers through Tool A during the initial detection period were quarantined, regardless of any indicator by the initial escape point. This was expected to be containment. As the root cause analysis was underway, the second escape point was triggered. This additional test was able to detect the anomaly and the offending lot was also quarantined. Containment now included the new lot which triggered the 2nd Escape point.

Eventually, the root cause of the anomaly was determined, duplicated, corrected, and verified on Tool A. However, another lot was detected by the second escape point, and a third escape point detected yet another affected lot – all of these were produced by the anomalous Tool A prior to the detections caught at the initial escape point. Eventually, all wafers were scrapped that had been processed through Tool A in the anomalous time period. Because the detection proved to be only partially successful by any of the 3 escape points mentioned, and as a precaution against a maverick event; wafers processed through the anomalous tool for 15 days prior to the escape point detection were also quarantined and scrapped – even if the escape points detected no outliers for that extended time period prior to the detection.

In order to improve the detection of the anomaly, a special "protect" characterization vehicle was selected. The characterization structures were developed for reliability aging and they include layout features which were designed

to be sensitive to the processing anomaly. Figure 2 shows the results of measuring the special structures and the Process Control Monitor structures that were tested as part of the first Escape Point. In this particular trial, the 1st Escape Point (upper part of Figure 2) would NOT have detected the outlier samples produced prior to the corrective action (left side of Figure 2 compared to right side). So the 1st Escape Point test would not have been able to confirm the corrective action.

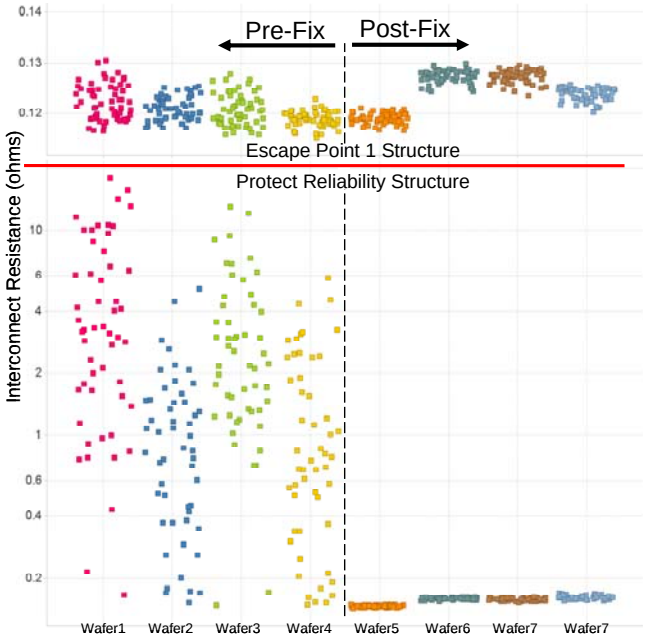

FIGURE 2. DIFFERENCE IN DETECTION BETWEEN FIRST ESCAPE POINT (UPPER DATA) AND SPECIAL PROTECT CHARACTERIZATION STRUCTURE (LOWER DATA).

On the other hand, the special characterization structures (at the bottom of Figure 2) exhibited up to 100X more resistance increase prior to the corrective action (left side) versus after the corrective action (right side). Both structure types were side-by-side on the same wafer. No other escape points, protect methods, or customers have detected the recurrence of the anomaly since the corrective action.

The physical shapes and sizes of features were varied in order to exacerbate the anomalous nature of manufacturing lots and how the delectability of defects can be enhanced using various structures. In fact, the effect of "amplifying" defects was utilized, and has been previously reported.[2] The physical layout of the protect structures included various sizes of interconnect features, an array of interconnect densities, and varying number of connections. For the anomaly, the density and number of connections proved to be important variables. For example, the first Escape Point structure included 300 connections and the Protect structure contained 6,400 connections. The data shown in Figure 2 is normalized by number of connections. Both structures had the same density, same feature sizes, and the same number of samples per wafer for the protect vehicle. However, product wafers can support less than one fifth the number of samples compared to the specially designed protect wafers.

Eventually, all samples in the verification study shown in Figure 2 were also subjected to the aging stresses of autoclave, temperature cycle, and high temperature lifetest. These environmental stresses were selected to emulate and accelerate similar degradation expected during a lifetime of normal use. The autoclave was found to cause the most aging degradation during wafer scale testing.

ANSWERING THE QUESTION OF RISK

Once a maverick event occurs, there are usually questions about risk. Customers want to know what risks are involved with maverick lots that have been deployed, what risks are possible with maverick lots that have been assembled, and what risks are likely with maverick lots that are in inventory.

The question of determining risks of a maverick population is a difficult dichotomy. In order to meet the definition of a true maverick, the material must have been undetectable (using normal escape points and protect mechanisms) by the supplier. An additional complicating factor could be unique aspects of the customer application. So the challenges for the supplier include: obtaining maverick samples, inventing a detection methodology, and duplicating customer use and stress conditions.

Finding Samples. The most obvious source of maverick devices is to ask for return of a lot caught by the customer. However, the customer's detection method is likely to include the use of the samples by assembling them into the end application. In mass production applications, it is very likely that all samples are consumed prior to detection. Even though each wafer in a lot can be diluted with other samples in a production environment, finding any virgin material from the same wafer, or wafer lot is problematic. In this particular example, happenstance had separated a sub lot from one wafer during packaging, so >30,000 untested samples were available.

Detection. We were lucky again. For the particular device in question, the failure mechanism occurred on only one location on the design, and that mechanism was detectable from external pins on the device. Other designs were different. In order to match the customer's detection capability, six 5,000 piece samples were utilized.

Picking a Stress. Several environmental stress methods were selected to emulate the physical stress of the customer's application: solder reflow simulations, liquid-to-liquid thermal shock, and unbiased humidity methods were found to have particularly interesting results. By

applying a spectrum of three stresses to actual devices multiple successful detections were obtained.

DATA AND RESULTS

Figure 3 shows the stress matrix utilized to measure the reliability risk in this study. Each experimental leg was completed on two samples of 5,000 parts each. Stresses were interchanged and applied following the matrix shown.

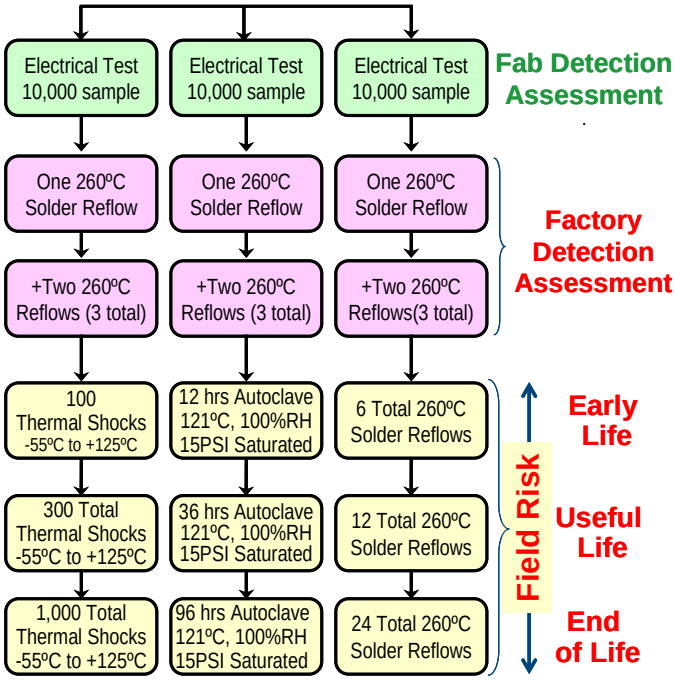

FIGURE 3. INITIAL RISK ASSESSMENT TEST PLAN.

All of the tests (except 1000 thermal shocks) shown in Figure 3 were completed over a single weekend of marathon stressing and highly automated electrical measurement. Eventually, additional stresses, representing multiple lifetimes of actual use were applied to the six legs – until the fallout rate dropped below 33 parts per million.

As a result of the methodology applied in this example, the question of reliability risk can be answered as shown in Figure 4. Although this data is for a particular mechanism, on a specific lot, with a population of affected devices, the relative risk for this mechanism is now known for any lot, regardless of the population affected. Because of the intermittent nature of the anomaly discussed in this example, there was considerable variation in the defective population from wafer-to-wafer and from lot-to-lot. However, once the relative ratio of fallout was determined, the ratio of risks at each point in the lifetime of an affected population is likely to apply universally in terms of the delectability and the percentage of affected material within each lot. In fact, fallout from all legs were combined at each interval to calculate the rate for the total population.

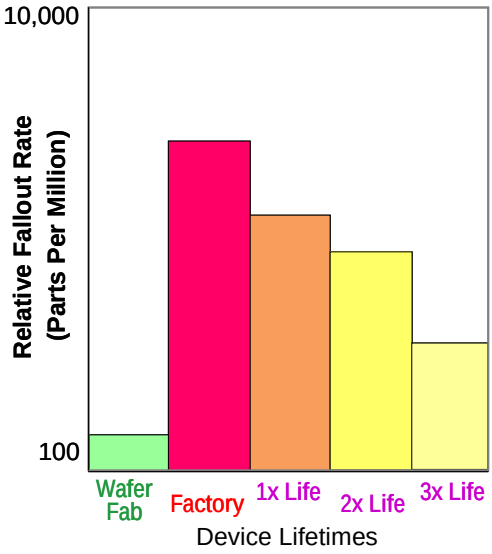

Figure 4. Customer fallout risk assessment based upon multiple accelerated stress tests of 30,000 sample devices from a known maverick lot.

In particular, the results in Figure 3 confirm that the highest reliability risk exists as line fallout at the Customer's factory. Figure 3 also shows the defect was detectable at the supplier's Fab, albeit at a very low level. Because we were able to perform a targeted measurement on virgin samples, the yield loss for the failure mechanism of interest was 0.0133%. After three reflows, the customer's factory should have detected fallout approximately 20 times higher – representing the peak of risk. For the remainder of use in a typical lifetime, just about 50% of the peak fallout would have occurred. In order to determine the entire maverick population, stresses were swapped and the "field risk" portion of Figure 3 was repeated, and swapped once again and repeated, for an equivalent of 3 full lifetimes. The total maverick population was forced to degrade by tripling the normal lifetime aging stresses. For the sample in the study, less than 0.5% of the parts (148 samples) were detected.

CONCLUSION

Reliability risk was determined for a particular mechanism by subjecting 30,000 samples to 4 types of accelerated stresses in amounts expected to represent several lifetimes of nominal use. By the luck of catching a maverick lot and knowing the most applicable detection method, the relative fallout in the Fab, the factory, and the field was measured and can now be predicted.

REFERENCES

1. JEDEC Specification JESD50 – Maverick Product Elimination and Outlier Management.
2. Roesch & Hamada, "Measuring Liftoff Quality and Reliability with Special Test Structures," CS MANTECH Conference, pp.191-194, April 14-17, 2008, Chicago, Illinois, USA.