Counterfeit or retrofit

M. Simard-Normandin
MuAnalysis.

The proliferation of counterfeit goods plagues our society. There are cheap imitations, which are sometimes clearly identifiable as such, and counterfeits that proclaim to be what they are not. When looking at a consumer product such as a watch, a hand bag, or a jacket, there may be tell-tale signs that the authenticity of the product is questionable, such as, not so subtle differences in color, weight, logos, as well as misspelled words. When it comes to electronic products the evidence is not always so obvious.

Most electronic products contain hundreds of electronic components: resistors, capacitors, integrated circuits, to name a few. One counterfeit electronic component in the build compromises the quality of the entire assembly. It is common practice in the electronic industry to use equivalent components and indeed many components of a given functionality can be purchased from different manufacturers. However some components are not what they claim to be. Some are clones, masquerading as originals, and some are re-branded components, components from various lots and origins remarked as one date code, thus implying a certain uniformity of manufacturing that is non-existent.

The implementation of the RoHS (Reduction of Hazardous Substances) directive in several countries has created demand for lead-free parts and generated a shortage of leaded parts as component manufacturers have migrated their process to meet the new regulations.

The need for obsolete components, the need for leaded components in a lead-free world, the need for lead-free older components for repairs or for special applications, have created an opportunity that has been met with “imagination” in some cases. An unsuspecting manufacturer may use such parts in its product completely unaware of their fraudulent nature and often with mitigated success. Indeed some of the examples presented here were detected in the analysis of failed products.

MuAnalysis offers a component authenticity verification service and below are some examples of parts that are not what they claim to be. The products shown in the images below have been tampered with by third parties with intention to deceive. They are no longer in the form in which they were manufactured and are no longer representative of the quality of the original product. The original manufacturer is also a victim of the deception as the poor quality of the tampered part may impact its reputation when the fraud is not detected.

Originally published at:
http://commsdesign.com/design_corner/showArticle.jhtml?articleID=216900022

Integrated circuits.

Integrated circuits (ICs) are expensive to manufacture and difficult to clone. However, cloning does happen as is shown in Figure 1. The suspicious part has a completely different die than the genuine part. A substitute part would have a different manufacturer's logo on the outside and would be sold such. Clones are cheap imitations that pretend to be originals.

More frequently seen are re-branded ICs. Generally the component's markings are abraded off and a new branding printed. Sometimes the counterfeiters are careful but more often than not they leave grinding marks or clipped or rounded-off corners as evidence that the part has been tampered with. Some examples are shown in Figure 2. The motivations to re-mark a part are varied. A bad batch, targeted for destruction, can be salvaged, given a new date code and sold as good. Slow devices can be re-marked and sold as fast ones. Older parts, with many different date codes, are grouped together and sold as a uniform batch with a recent date code. An example of this practice is illustrated in Figure 3, where X-Ray revealed that presumably identical parts had die of various revisions and sizes.

To meet the lead-free demand, older, not RoHS compliant, parts are cleaned of lead plating or, in the case of BGAs, have their leaded balls replaced by lead-free balls, and are then sold as RoHS compliant parts. Sometimes the counterfeiter will only re-brand the part and not bother replacing the balls. An example of this practice is shown in Figure 4. We call these parts retrofit, as they could possibly work, and the exercise could be valid, though in this particular case the intent is clearly fraudulent since the balls were not replaced. When lead plating has been removed in a deceitful attempt to pass a part as lead-free, our experience shows that the job is generally not perfect and that XRF testing close to the body of the device will likely find lead.

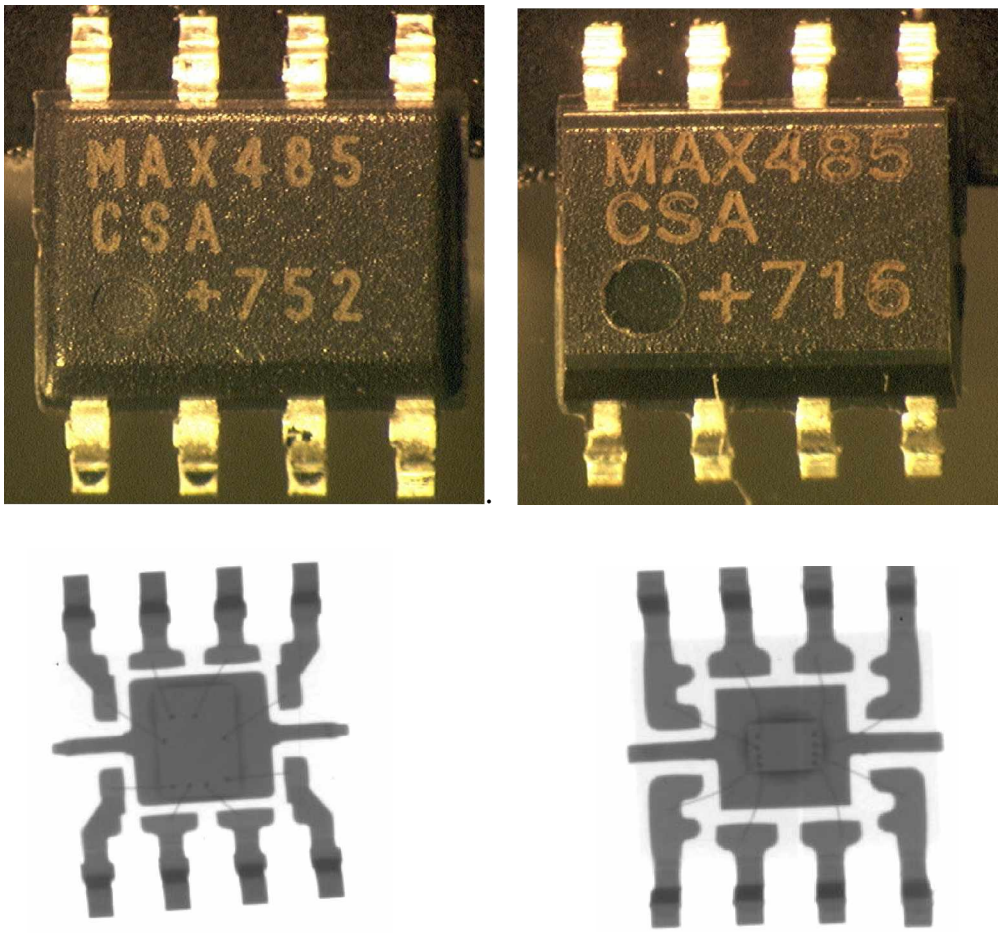

Figure 1. A genuine (left) and cloned (right) component. X-Ray shows the different die sizes. Inside, the counterfeit die does not have MAXIM markings.

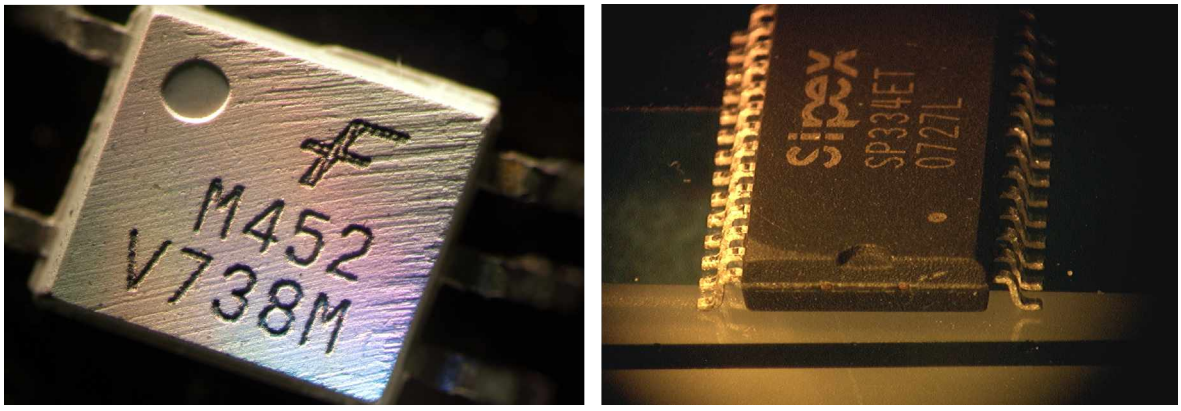

Figure 2. Grinding marks (left) and clipped corner (right) on re-branded components.

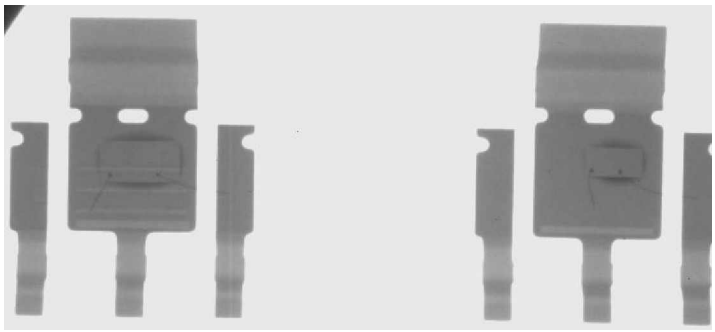

Figure 3. XRAY of 2 parts with the same date code. They have a different die inside.

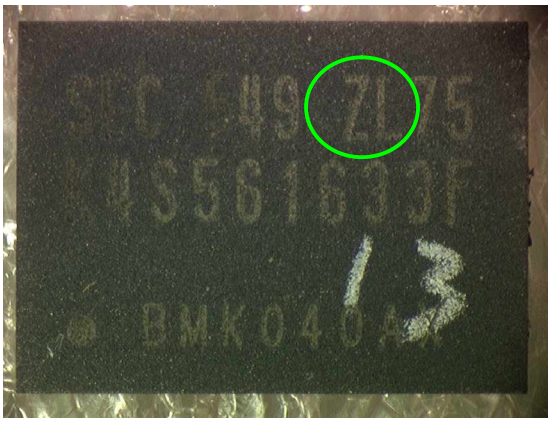

Figure 4. This chip is branded lead-free. A leaded component would have an X instead of a Z , yet its balls were leaded. Another evidence of re-marking is the poor quality of the branding. We have also seen this part obviously re-branded, but with its balls replaced by lead-free balls.

When markings look genuine and there is no evidence of tampering on the outside of the package, all is not necessarily well. Bad wafers can be recovered and packaged as good by counterfeiters. Sometimes there is no die inside the package, though this is not something that we have seen. In Figure 5, we compare two supposedly identical products, with different date codes. The product under scrutiny is missing a mask level compared to the known good part. Will this device have the same functionality? Will it work?

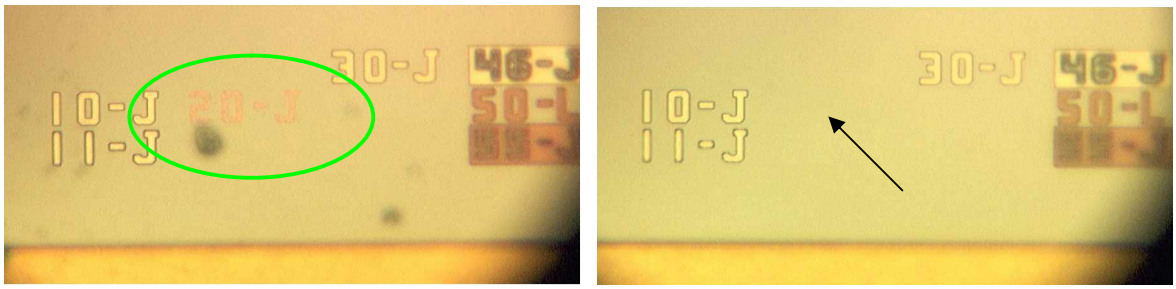

Figure 5. The die on the right is missing a mask level.

In Figure 6, two supposedly identical devices, based on exterior markings, do not have the same die revision. Since datasheets do not generally include die details, one is left to wonder whether these parts will have the same functionality.

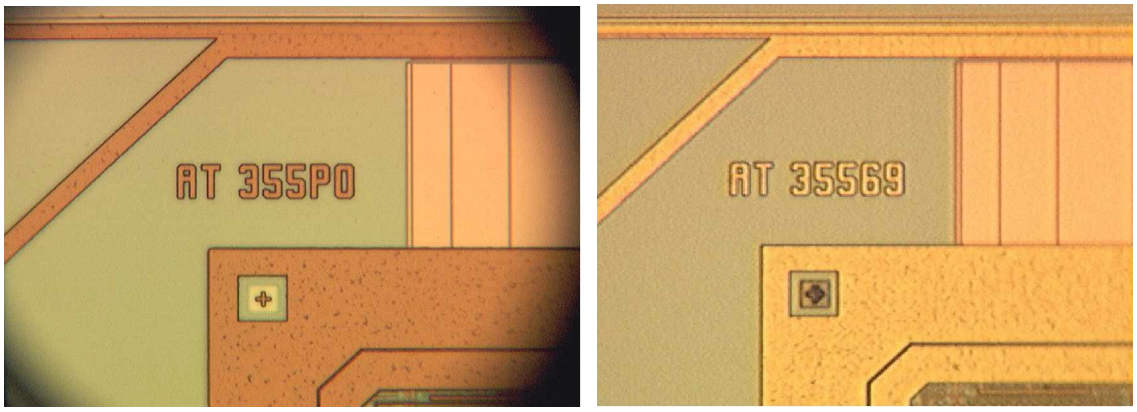

Figure 6. These two devices do not have the same mask revision, yet there are presumed identical.

Voiding in the die attach is easily picked up by X-Ray imaging. Generally it's not a good thing and one has to be suspicious of origin when a batch of hard to find parts shows serious voiding. Such components were possibly part of a rejected lot that found its way back into circulation.

Discrete components.

It is easier to clone diodes, capacitors and resistors than to clone ICs. The devices shown in Figure 7 appear to be an imitation of the genuine part, poorly put together. Such parts may test good, but will they have the same long term behavior and reliability as the original?

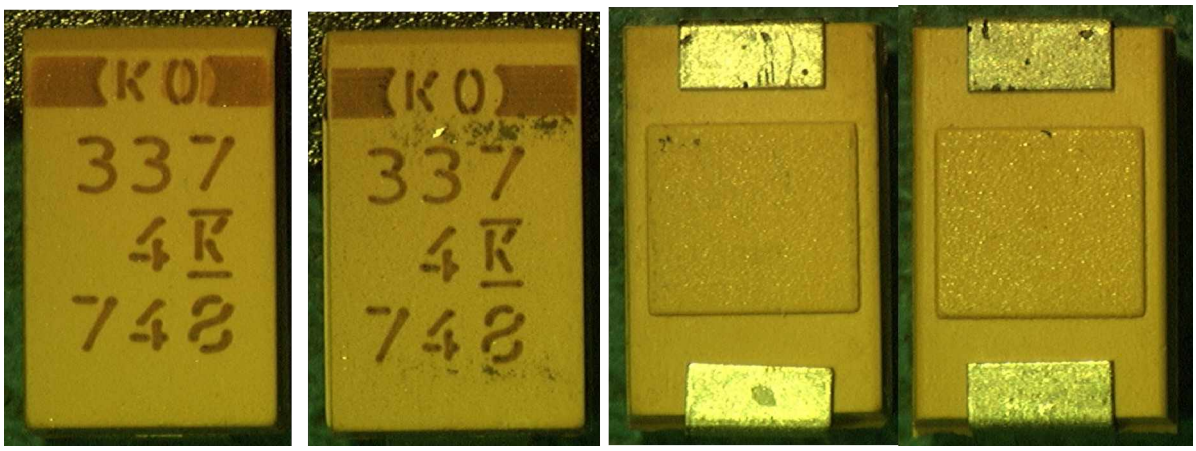

Figure 7. The three devices to the left show smeared markings and residue on the front, and crooked electrodes in the back. Are they genuine parts? The part on the right is of certifiable origin. The parts on the left are likely clones or counterfeits.

The parts shown in Figure 8 are two versions of the same diode with different internal constructions. The part on the right failed prematurely. The data sheet presented this part as a glass passivated diode, which accurately describes the part on the left but not the failed part.

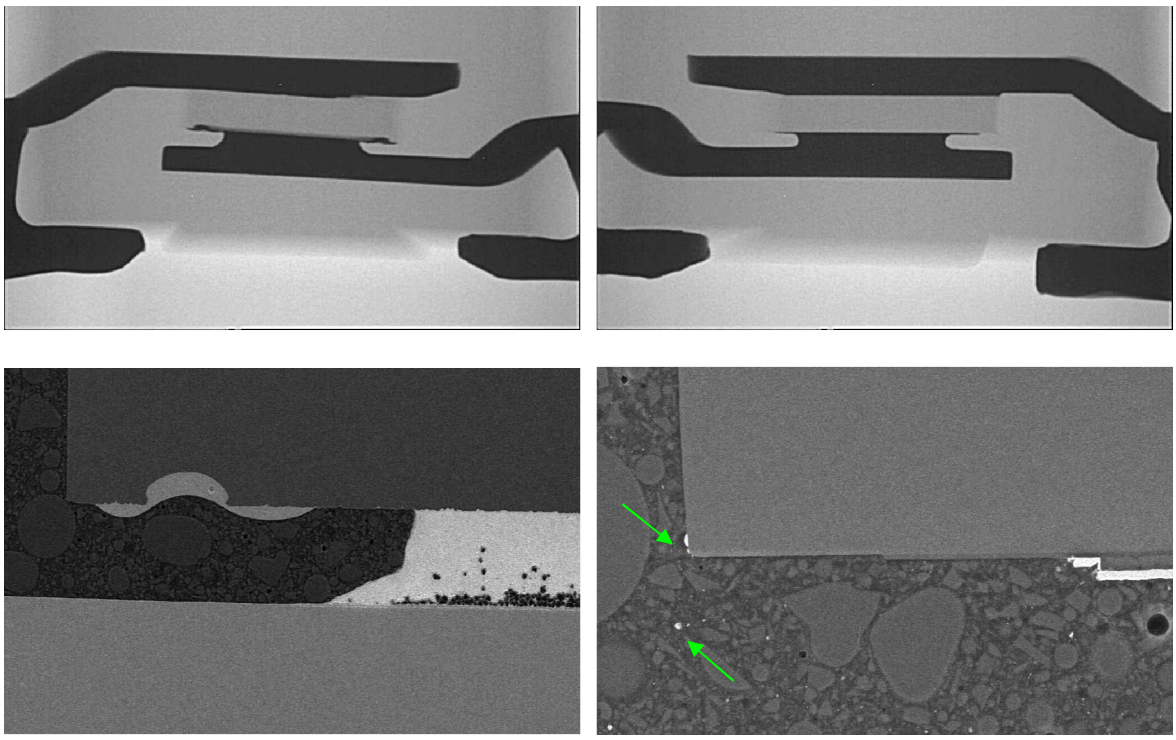

Figure 8. Two "identical" silicon diodes. Top row: X-Ray elevation images, bottom row: electron micrographs of the devices in cross-section, near the edge of each die. The parts have very different internal constructions. The part on the right failed prematurely.

In the left side part, the active region of the device is terminated before the edge of the die, and passivated with a bead of leaded glass. The part on the right has a different construction altogether and the active region extends all the way to the edge of the die. The failure mechanism was identified as small amounts of tin-lead solder embedded in the packaging material , indicated by the arrows in Figure 8 (you read correctly, these are not supposed to be there), that shorted the diode along the side of the die. Is the part on the right a genuine part or a clone? The presence of tin-lead solder within the encapsulation material is a strong indicator of poor manufacturing quality. This is not a failure mode that we had ever encountered before.

What does one look for to determine if a device's markings have been altered? Scratches, residue, non-uniformity from device to device, poor legibility, easily erased markings are all indicators of tampering. How about a hand written font? The device shown in Figure 9 was discovered during an authenticity test. Five devices were removed at random positions on a reel and two of them showed an unusual hand written font. There potentially are more of these on that reel, intermixed with good devices. In that exercise, 30% of the devices tested did not match their basic electrical specification.

Figure 9. This part is laser marked, but the font is hand-written.

Fortunately, the world of fraud is not laden with regulations, checks and balances. Quality and attention to detail are not requirements. If one is alert, fraud is often easily detected. In Figure 10, the fraudulent devices have been placed upside down on the reel. A closer look revealed that they have been re-branded as well.

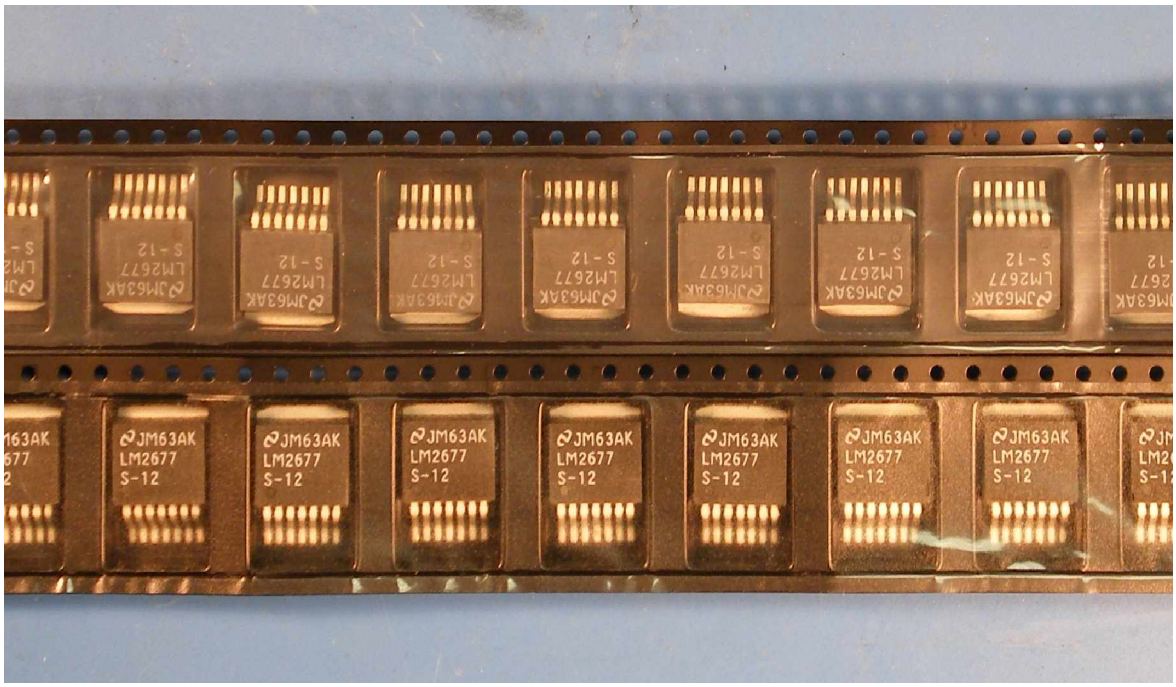

Figure 10. The devices in the top reel have been re-branded and placed upside down.

In Figure 11, the suspect part on the left is in a 35 mm package while the reference part on the right is in a 27mm package. They have different number of balls. The data sheet does not mention a 35 mm package or this pin-out. Inside we found a different die. This is a completely different product re-branded with a different logo and product name.

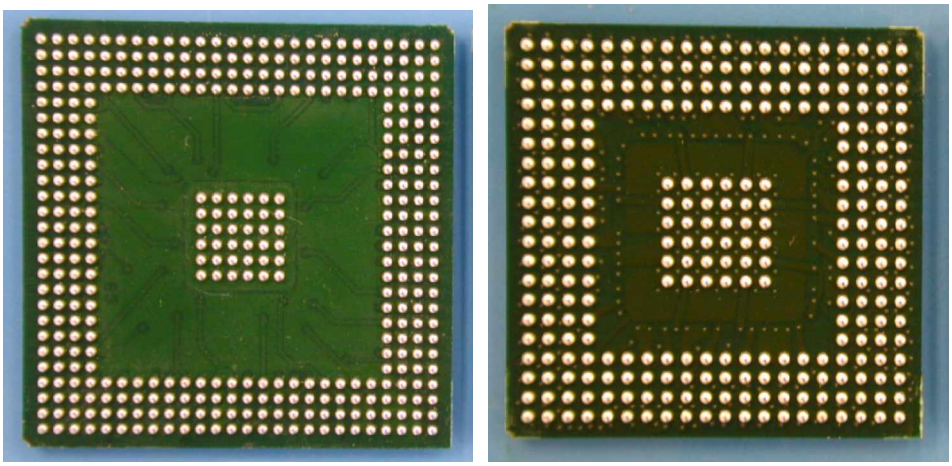

Figure 11. The suspect part on the left is in a 35 mm package while the reference part on the right is in a 27mm package. The counterfeit part does not even look like the genuine part.

Conclusion

Did you get what you think you purchased? The documentation accompanying the lot may not tell the whole story. It too can be a fake.

If a part looks suspicious, it probably is. Most parts are small but what is missed by the naked eye is obvious under a low power microscope. External dimensions are easily checked. Re-branded parts are invariably thinner than the datasheet specification.

X-Ray imaging can easily pick up differences in die size or configuration, indicators of a clone or an older version. A different die configuration is not necessarily a serious problem, but you may want to know about it and verify that the variation is valid and benign. X-Ray also detects die attach voiding, never a good thing, particularly if the part has high power consumption.

Mask revisions or missing mask levels can affect functionality. This is not an easy thing to spot, as it requires opening the part to see the die.

XRF testing can detect residual tin-lead plating quite easily. This should raise a flag if the part is sold as lead-free. Removing the lead from an older part may seem like a good idea but the part may not be designed for the higher reflow temperature and fail prematurely. RoHS compliance does not necessarily mean lead-free compatibility. RoHS enforcers may pick up the left-over lead too and you will have a lot of explaining to do.

Electronic components are easy targets for counterfeiters. They are small and usually sold in large volumes, neatly packaged on reels. The first few devices may be genuine, but what lurks further on?

Caveat emptor!
(Let the buyer beware)

Do look carefully before you solder parts similar to those shown in this article into your product.

Originally published at:
http://commsdesign.com/design_corner/showArticle.jhtml?articleID=216900022