ELECTRONICS COUNTERFEITING: RISKS AND REMEDIES

by **Alix Paultre,** Editor

When most people hear the word "counterfeiting" they think about money. That's because money is a great target for the activity, as it takes a relatively small effort (printing on paper) to get a significantly higher payout (the face value of the money). Counterfeiting in electronics is done for the same reasons, as a chip that you made/stole/obtained can sell for quite a price.

The nature of counterfeiting in electronics is multilayered, as what is considered counterfeit may not be a copy, it may be "gray" goods, or recycled parts presented as new. In the software space, this could extend to trojan programs intended to not only waste your money, but steal your data. Cybercriminal groups targeting semiconductor companies can use such counterfeit products to attack target organizations.

A good anti-counterfeiting process starts with microscopy and material analysis.

Hardware issues

To get an idea of the complexity of the issue and some ways the industry is addressing them, we reached out to Astute Electronics (https://www.astute.global/), a supply-chain infrastructure support company that has to address counterfeit products in its operations. We spoke to Geoff Hill, their Managing Director, about some of the issues involved and solutions available to the industry.

EE: Geoff, when we talk about counterfeiting, especially when it comes to hardware, there are levels, right? You can get a part that's quote-unquote 'counterfeit.' but it could be a real part, right?

Hill: Yes, absolutely. It comes in many different forms, like a device that's just been pulled off of a board, cleaned up, legs straightened, and then resold as original or new.

EE: That's the first thing that came to mind when the topic of counterfeit products came up. One can just picture somebody heating up a board over a hot fire somewhere, prying chips off with a screwdriver, and throwing it into a box that somebody later cleans up and sells as new.

Hill: A lot of that has come from the waste that was sent over to Asia to be disposed of, and basically that hardware waste or equipment then was harvested, originally in China, but then they became a little bit further down the food chain. Now it's harvested in Africa, around Nigeria. Then they send it off to China, who basically counterfeit it in one form or another.

Counterfeits in that form, which is your basic form, really, of getting a part that's used. So it could have been programmed, it could be used, and therefore its integrity has been compromised. You can also get parts that are just empty packages, so you've just got the packaging with no die inside, and they're sold as new.

But again, with the equipment that's available, nobody really should fall for that anymore. A lot of the other stuff is where you can get a bad product that has been intercepted from the factories, and for whatever reason, being destroyed, and they were intercepted and then sold back into the market as used, even though the product has obviously failed tests. So you get a whole range of different parts, and then also you get parts which are the same package, maybe the same family. This is where the real problem comes.

Good bad fakes

Hill: The counterfeiters now, in fact, have original manufacturers' equipment and they can silkscreen and really make the parts look to be very, very much the part that you require and in some respects, can actually go past first initial tests, electrical tests, or they could actually meet some of the characteristics that would indicate that it's the same family. So it's quite complex, and over the years, of course, the counterfeiters have become incredibly clever at what they do. They've invested fortunes because they're making so much, so it's not as basic as it used to be 10, 15 years ago. It's a really clever business.

Hill: If you're getting a part, and it should be $20 and you're only paying a dollar, the likelihood is there's something wrong with it.

EE: Which is always the case. Then there you go, because I would say at the microcontroller level, good fake parts are less of an issue. But I would imagine that when it comes to passives and magnetics, that's got to be rife.

Hill: It is rife. If you look in China, certainly outside in some of the country areas, a $600-a-year salary is a big salary and they can get that selling a real multilayer ceramic, especially when you've got tantalum that has historically been in short supply, and multilayers. So, yes, the attitude years ago was, "Oh, well, the counterfeits only want to sell your FPGA business because that's the high end, nice and expensive. No. No, no. They actually want to hit the low end because they don't think anyone's looking carefully in that direction.

EE: That's right. That's an excellent point, and who knows, maybe the capacitor will test out right.

Hill: The problem is that, depending on the printed circuit board, the capacitors of course are littered all over the board. It comes to two different events, really. One is an economic standpoint, where the recall of the boards for damage to reputation, your whole standing in the marketplace is compromised. That could have knock-on effects to your customers, to your product, to everything to do with the economy.

But when you really talk about safety-critical applications, some of these parts, they won't fail at the front end, but they'll fail at mission-critical status, especially if there's a temperature that's going to be affected, and things like that. Then you're talking about life and death. You're talking about a whole different topic of where it's not an economic thing, it could threaten thousands of lives.

So the whole thing has become, in some respects, the level of testing that you do on something that's nontraceable. Of course, nontraceability is driven by obsolescence. With mergers and acquisitions as strong as they are, that's very prevalent. So it becomes application-centric. If you're

making a coffee machine, you could argue, what's the damage that can be done? Not a lot. But if you're talking about some sort of decoy device for a fighter jet, it's fatal.

So it really becomes an education scenario, and we have to invest more and more in good behaviors, good tests. Where you can, you buy from authorized sources where you've got the provenance of the part, and that's the only way to beat it. When you've got behaviors that are driving costs down all the time, and there's no policing of your behaviors, the reality is, then you're going to drive people to make very bad choices.

Obtaining secured product from authorized sources ensures full traceability

EE: Geoff, you were saying coffee machines, but there is a lot of growth in smart and advanced devices. My coffee machine, if it broke on me, I'd be quite upset, because it cost me a healthy penny. It grinds the beans, it checks the temperature. You're talking about three to five hundred bucks worth of coffee machine, depending on whose brands you buy, for a modern top end. But then you could apply that to anything. A new web-enabled refrigerator, or a toaster that now gives me internet updates, and could print pictures on the toast or something. All of these devices are now smart, and there's more opportunities for bad chips.

Hill: There is. It comes down to, again, how you treat your washing machine or your toaster. If it goes wrong, generally people throw them away and they buy a new one. If you're selling something that is airborne and it's safety-critical, then you need to... basically the cost to investigate, to put corrective actions, look up the origin of the problem, could cost hundreds of thousands, if not millions.

We don't have to go very far. Looking at the 737 Max scenario, I know that was a software issue with Boeing, but it only takes one issue to ruin years and years of a reputation. That's where it comes down to, really, it's how people are going to react to an issue. Then, of course, it comes down to negligence. If there's culpable negligence, then of course, then you're talking to legalities and lawsuits. It can be quite a big issue, if it's not managed with a certain amount of responsibility.

EE: Excellent point. Now, having laid out all of the dangers, let's talk a little bit about mitigation. What can you do to address this issue?

Hill: Obviously, you need to review your buying techniques, your behaviors, you've got to buy from authorized sources, so you get full traceability, full manufacturer's warranty. That's your first point of call. Now, as I mentioned before, with mergers and acquisitions, there are so many companies now that are on this aggressive acquisition trail, especially in the semiconductor business. Because even if you look at what's happening, Intel with Arrow, Xilinx now with AMD, Nvidia on Arm, it's huge, Maxim and Analog Devices. What happens is, obviously, they make a lot of parts end-of-life straight away, and just because the investment in getting ahead of the curve on new technologies is such a great return for them.

Then they go into last-time-buy scenarios, and we offer that, nitrogen cabinets and that sort of thing. You store the die, you can make them forever more, but that is really reliant upon you having good forecasting. My experience with my customers is they really haven't got a clue. So, often they get it wrong. The numbers are always going to be wrong. It's going to be too high, too low, whatever else. Actually, a lot of the manufacturers or the OEM equipment, there's always requirements and demand for many, many years, following their expectation of when they could say goodbye to it.

So what happens is they have to go to the gray market, and the gray market is not always a bad market because a lot of that product could be excess. It's where the manufacturer, they've got too much product because they overbought on a last-time buy and they want some dollars back for their investment. So it goes back into the market, but this is where the issue comes. When you're buying products without any warranty or traceability, you have to test. There's an AS6081 spec that we use mainly for semiconductors and for components generally. It ranges a whole range of equipment that we've been doing for many, many years.

Our process starts off with visual microscopy, at 20x magnification. Then it goes into spectrometry and material analysis for material elements that might be different. So the amount of gold in there, amount of silver, that sort of thing, which could throw up an anomaly. You've also got marks and permanency. So, obviously, if the marking of the device suddenly comes off, even with basic things like your-

EE: Soap and water.

Hill: Yeah, yeah, pretty much. Then you've got a problem, but actually they're very, very complicated now. Then we also do heated solvent testing using Dynasolve, and the disruptive test on that marking, that highlights any ghost markings. So you can see what originally was marked underneath. We also do scrape tests for blacktopping, which was one of the initial things they did. Obviously blacktopping is a giveaway, although some manufacturers do blacktop, if they do a special run.

So it's not always 100% assured, and we've had many manufacturers that have done blacktopping. Then you've got real-time X-ray. Obviously, you're

looking for the consistency of bond wire that surrounds the die, and making sure that's 100% consistent within the batch. Then you do a decapsulation, and then topography. You're looking really at the recognition of the actual die. Then going back to verify that that die or whatever, its second source is absolutely as per the manufacturer. You do that with high-powered microscopy.

Scanning electron microscopy and energy disbursement goes back and uncovers the original coatings, coating upon coating upon coating. That really gives it away, that that top surface has, in some respects, been changed or altered, and there's some stuff on there that shouldn't be there. That's really good because it draws you a very good diagram of what it should look like, with the carbon and everything else that should be there, and that's not there.

Then after that, you do the solderability, you might have an issue with water ingress. It might affect the solderability. You check whether the parts are programmed. Then we also do electrical tests using diagnosis. So we're actually putting some parametric and functionality tests through electrical capability. All of that, these are fairly advanced, and expensive, and long-winded ways of basically reverifying your device.

What happens nowadays, you can buy products off the gray market and use things like escrow, so it gives you time to test the product without any money being transferred. But in the early days, they used to say, "Oh, well, we'll do 50/50, give us 50% upfront and 50% when you've tested them," knowing full well they're going to fail, but they've already got your 50% money and done a runner. It took a long, long while for people to get familiar with behaviors, and understanding the con that was in place.

So what happens now is, you tell people you're going to test, and that you do it yourself. That often is a barrier, because all of a sudden they'll turn around and say, "Oh no, we've sold them. No, we haven't got them any more," just so that it puts you off the scent, really, because they know that they're trying to have you over, so to speak. So it's a fairly dynamic business, because their abilities to counterfeit are improving all the time.

The money they're making seems to be increasing as well. That's a cultural thing, as well as anything else. You would have actually thought, if they actually put that amount of money and effort into something legit, that they would make as much if not more money, but I think it's a cultural thing. They get a kick out of it.

EE: Some people look short-term.

Hill: People always look short-term, that's the problem. The only way to overcome it is to have robust testing and good education, and the communications of what the market is and how we overcome it, and to look for those signs. That's the only way you can stop it.

EE: Agreed. Are there any other things that Astute provides to help address the issue?

Hill: We're probably looking at some other forms of equipment to invest in, and probably enhance a bit more of the electrical testing capability. We have 17 nitrogen cabinets, so we stock a lot of die for customers, just to help them. Because if they stock die, then they're not basically taking on the whole cost of that last-time buy. They've got that security to turn, to package it, as and when the need is there.

So we support them in that, and in any sort of long-term and end-of-life buy that goes over several years, but generally what it comes down to is the experience and your data library. Because there are more and more parts... you'll find you're doing the same parts time and time again, so you've got to create a history, a lot of knowledge, and that communication is very valuable because you're really going from a position of strength, saying, "Well, I've seen this before. I know about this device. I know about that."

Also, enhancing your relationship with the component manufacturers is crucial, because they need to understand that you're not there to take food off their table, you're there to protect their reputation. Because a lot of times, they would say, "it's not my problem, it is your problem", because if you haven't helped to identify a potential problem before it gets into a safety-critical application, then hang on to your hat. It is literally life and death. I think the main thing that we're doing more and more is education. If you don't need to take a risk, don't take a risk. That's the message.

Software issues

The role of software in the electronics industry continues to grow, and that sector also has its issues with counterfeiting. We talked to one of our industry experts in the space, Alan Grau, VP of IoT and Embedded Solutions at Sectigo (https://sectigo.com), to talk about the state of that part of the industry.

EE: Now, with hardware counterfeiting, it's easy to sit at face value and just say, "Yeah, well, it's a fake product," but with software it goes deeper than that. Doesn't it?

Alan Grau: Well, there's lots of different levels in hardware. It can be everything from a knockoff product, a fake product, companies that are using a manufacturing facility that's like a contract manufacturer that's not trusted where they'll do overruns. Or components that are fake or from an untrusted manufacturer, whether it's chips or boards or other elements of the solution, or the software piece. So there's multiple different ways to look at it.

EE: The overrun aspect is a very threatening aspect on the counterfeit side for the manufacturer. At least it's less of a problem for the end user because they're still getting a good product. It's not kosher as it were, but at least they're not getting something that was pried off of a board over a fire and dusted off, wiped up and repackaged and sold to you.

Grau: Yeah. They may not get the same support, but at least the product is real. That's true. I actually was talking to a major manufacturer who everybody would recognize, this had been several years ago, and they were talking about a support issue where a customer that kept complaining about the device that they bought not working right.

They couldn't figure out what was wrong with it until they finally sent somebody out there and opened it up, and realized that it looked really good on the outside, but when they got inside, it was not their product. It was packaged well,

it looked great, but yeah, exactly. It didn't work properly.

EE: You could say mislabeled consumer product is also counterfeit, because I've seen people buy, say, for example, it says a 1-terabyte drive for 5 cents, and of course they don't think about the fact that how can you have a 1-terabyte drive for 5 cents? They order it, they plug it in, it runs. And then they realize that it's a 256K USB drive hot glued into an empty box.

Grau: That's pretty bad. But yeah, there are all sorts of scams out there. As you said, some more obvious and blatant and some more problematic than others, but in all cases it's costing people revenue, it's causing frustration for the end-user.

EE: It's all flavors of the same bad recipe, multiple issues and multiple facets to the problem. Are there multiple solutions? Or are there solutions to protect against multiple counterfeiting vectors?

Grau: There's definitely not one silver bullet that's going to solve this problem. On the software side, which is where I live, there are certainly well-known techniques to help mitigate against this risk. The main one of course is code-signing techniques so that you can validate the code being installed on the device, or the code being downloaded, and depending upon the system, is the code that was produced by the OEM, the manufacturer, or the software vendor.

This is really, with the recent SolarWinds hack, which was a multiple-level attack, right? There were some very patient attackers who were able to get into SolarWinds' system, and I heard different theories on how they got in. And I haven't actually read up on that lately to see if anyone's confirmed where that originated, how they initially breached SolarWinds. But once they got in, they were able to insert malicious firmware into the build system of the SolarWinds, one of their products.

This became a cybersecurity issue. So then people were updating this trusted cybersecurity product on their network, with code from SolarWinds, and even though it was code signed, it still had malicious content in the update package. And the reason for that is hackers were able to insert their malicious code into the build process.

The way code signing works, once you trust what the manufacturer built, SolarWinds could sign it and say, "Okay, this is our trusted, good software," it would be downloaded to thousands of organizations. Those organizations would check and say, "Oh yeah." Or, well, the update process would validate that it had been signed by SolarWinds and it hadn't been changed. It was bit-for-bit the same software produced by SolarWinds.

So everybody installed it and ran it, and there was this malicious code in there, and that was because that malicious code had been inserted upstream of the signing process. So you're trusting the signature, which is the right thing to do, but what was signed was bad. So that really shows there's a step missing in that process, and once somebody had breached their build process, they really were able to do tremendous damage and a very, very broad attack. I mean, it has affected thousands of organizations.

But code signing fundamentally is still a great technology. So things like secure boot and secure code updates that use code signing and are still critical technologies. You can verify that what you are installing was in fact from a trusted party, and it's just that you're trusting they weren't breached. In SolarWinds' case, they were. But on the software and firmware side, code signing is a critical technology and helps ensure what you're receiving ... Again, they actually were installing what was the authentic code from SolarWinds, it's just that it had been tampered with prior to that signature process.

EE: Got it. Now, as far as protections, there are obviously things you can do before the product leaves the building, and then there are things you can do once the product leaves the building. But again, are we concerned about counterfeit parts within the product? Are we concerned about counterfeit software being downloaded to those products? Or are we worried more about counterfeit software being sold to the users of those products once they've left your control?

Grau: Yeah. So we can talk about each of those individually because they are all different. If it's an IoT or an embedded product, typically the update process is an integral part of the device, right? So if I'm updating my software on my home router, typically the home router will go retrieve the software. It knows where to retrieve it from. Ideally that's an authenticated process where each end is using a certificate to verify that it's connecting to the OEM to get new software, so that it can validate, "Yes, I'm going to the OEM."

Then it uses another signed code package, certificate-based signing to say, yes, the software is actually valid as well. But, another case where I've seen an attack is someone hacked into the update server for an OEM and put malicious firmware on the download site. And this was before code signing was widely used. So if you validate, again, using a validation of the server you're connecting to, and then validating the software that's being downloaded, it's a pretty robust mechanism.

The human factor

Grau: The next one though, that you're talking about is a human's involved. So for users going to update the firmware, how do you or how does the user know he's pointing to the right site or getting software from the right place? Again, you can use the same techniques, right? If you're using signed code and doing all that, again, you've got a strong level of protection.

So if we shift out of the embedded world into, say, the Windows or Mac world, where you're downloading software, we're seeing much more software that's code signed, and then the installation process when you go to update it, on a Windows PC, for example, it will pop up a window and you can verify who had signed the code. The system will look at the signature, will look at the certificate used to sign the code and say, "Oh, you're installing code from Alan Grau software, do you trust this supplier?"

Again, that's a pretty robust mechanism, right? Because the user should be able to know who they're getting the software from. But humans are more prone to error, so there's always a risk there that someone will click, "Yes, I trust this source," when they shouldn't. But one of the defenses against that with code signing is

the certificate used to sign the code, if it's discovered that that person or that entity shouldn't be trusted, they're doing malicious things, the certificate can be revoked.

So security companies come to us and say, "Hey, we see that the code signing cert that was issued to Alan Grau Software is doing malicious things. It should be revoked." The CA will revoke that certificate, and then the next time somebody tries to install software that was signed by that certificate, the operating system will check and say, "Hey, this is not trusted software, the certificate's been revoked." So it will then either not allow the software to be installed, or display a much stronger warning message. In general, if the certificates revoked it probably shouldn't install it at all. But again, that's handled specifically by the OS.

EE: In the context of the aspect of counterfeiting, are IP blocks considered hardware or software? For example in certain microcontrollers, they'll purchase an IP block from a vendor for X, Y, Z functionality on their device. And now, obviously they're going to usually just buy direct from the vendor there. You don't really walk up and pull that kind of stuff off a shelf. But is there a danger that you could wind up getting bad intellectual property products from someone?

Grau: That's a great question. I'm sure that there is. So I guess it depends a little bit whether or not those IP blocks are capabilities that are baked into the hardware, that can be simply enabled through purchase. In which case, if it's already in the hardware, it's unlikely that it would be tampered with, unless it was tampered with earlier in the cycle.

If something's built into the hardware where when you buy the hardware, it's got additional capabilities in the hardware that you just enable and disable, and there's lower risk there. It would have to have done an attack earlier in the supply chain to tamper with that. If it's essentially firmware, microcode, or software that's running from when it's downloaded over the air, then there's the same risks as there would be otherwise. But, again, if it's something baked in, then you're pretty safe unless it was tampered with prior to manufacturing.

But if we switch over and start talking about hardware attacks, again, there's several flavors there. The first one, or one of them, is how you handle overruns, and how you ensure that if your manufacturer isn't fully under your control, how do you guarantee that there are no overruns? And there's multiple ways that you can address that. Some of them are as simple as physical security where you've got cameras and things like that.

But what we're starting to see are people that are actually building product-based solutions to have better control over the manufacturing. So there's actually a company that is out of the UK, called Secure Thingz, actually owned by a company called IAR, that has developed a solution that they can deploy into manufacturing facilities, where basically they're encrypting the firmware in the device provisioning solution.

Each time they program that solution or the package, the firmware package is programmed into a device. It gets decrypted for that individual device in a manner that has traceability. So you have to have something on the device that can be encrypted, and you can track then, "Okay. We've just hit 10,000 units, turn it off now." Or if it keeps going, at least you've got an auditable report that says, "Hey, the manufacturer produced 11,000 units." And so you've got accountability.

EE: "We've got 15,000 clients in the field."

Grau: Yeah, exactly. Well, you can go back to the manufacturer and say, "Hey, you were authorized to produce 10,000 units. The report says you produced 11,000 or 15,000. Where are my other units?" And if they shipped those out the back door to somebody else, then you can deal with the problem right away. So, there are companies that are developing solutions very specifically targeted for exactly that problem. Some of the other things that can be done that don't require quite that... That's a fairly comprehensive solution that has to control the whole and be involved in the whole manufacturing process.

A lighter-weight solution that's still pretty effective is just a matter of issuing device identity search to the devices as they roll off of the manufacturing line. It depends a little bit on the functionality of the device. So if you're producing a device that's going to connect back to a cloud service and it's only useful if it connects to that cloud service, say you've got a monitoring system that collects some data and sends it back to a cloud service where you can analyze it and use that information, you can require that the device have a certificate issue to connect back to the cloud service.

That way you can monitor how many certificates are issued, if you've got the right system to control how certificates are issued. And then you've got an audit on that. So if somebody produces additional devices, either you would know that they had issued additional certificates, or if they create them without certificates or with certificates from a different source, and they try to connect back to the cloud service it would fail. That doesn't work if it's a completely standalone device that doesn't require that outside connectivity. So it depends a little bit upon the type of device you're building.

Then the other place where it can become problematic is people producing counterfeit components. And there, again, it can come back to the same capability, if you can issue a certificate onto the components. So if you've got a processor chip or an SoC and you're using the products, if the manufacturer of the SOC can insert a certificate into the SoC, then when you're doing manufacturing, or when you're first doing your system test on the device, you can retrieve the validation of the certificate to make sure that the SoC is authentic. So you can do things like that to protect the supply chain.

EE: Can the same secure block used for crypto be used for verification?

Grau: Yeah. You just need the data, a certificate in there that was issued by a known, trusted CA that you've got control over, so that you can control it against that. So you can somehow know that, oh, this wasn't produced by a TI, or Microchip. It's a knockoff version. So you need that other piece in there so that you've got something to inspect, to validate the components. EE