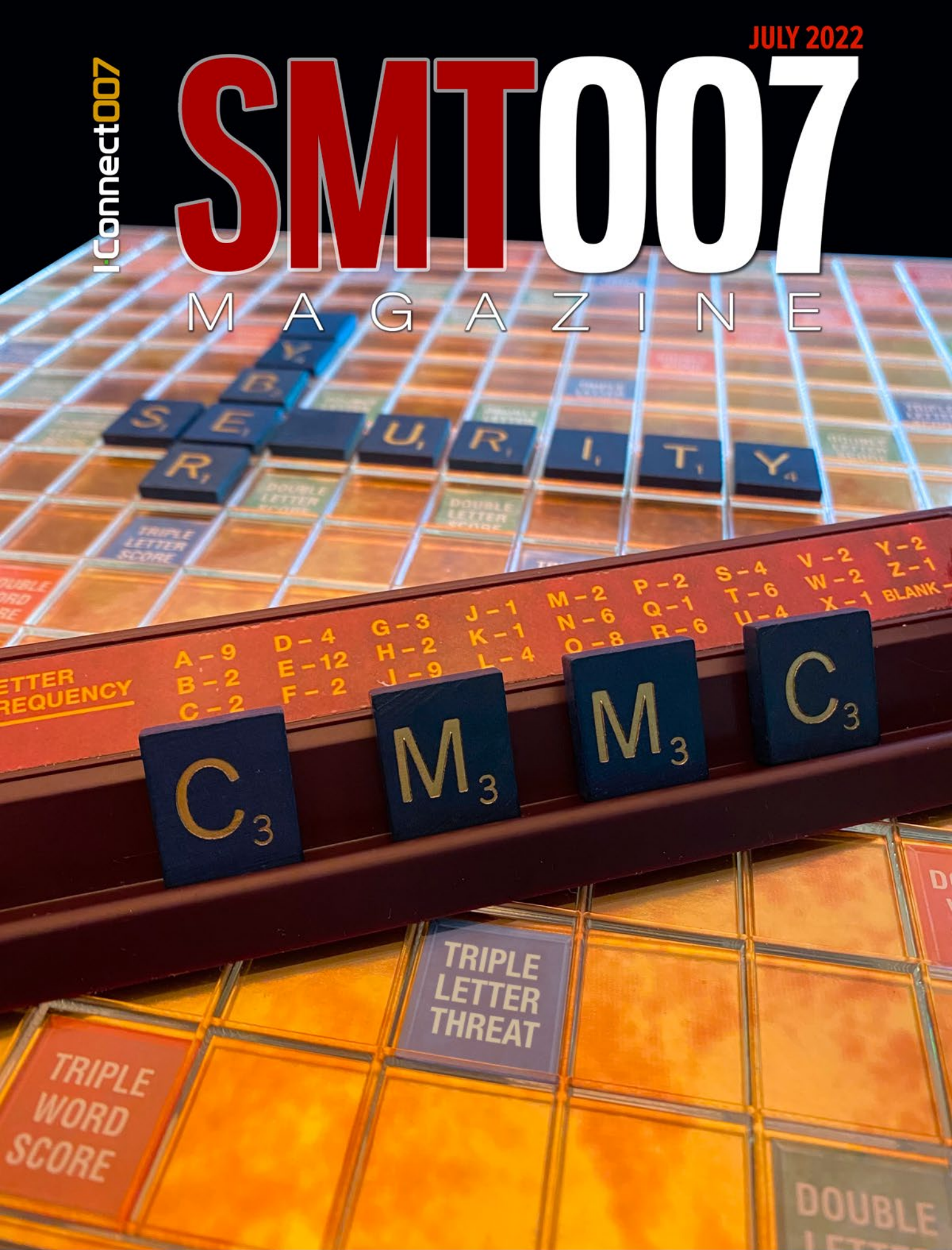
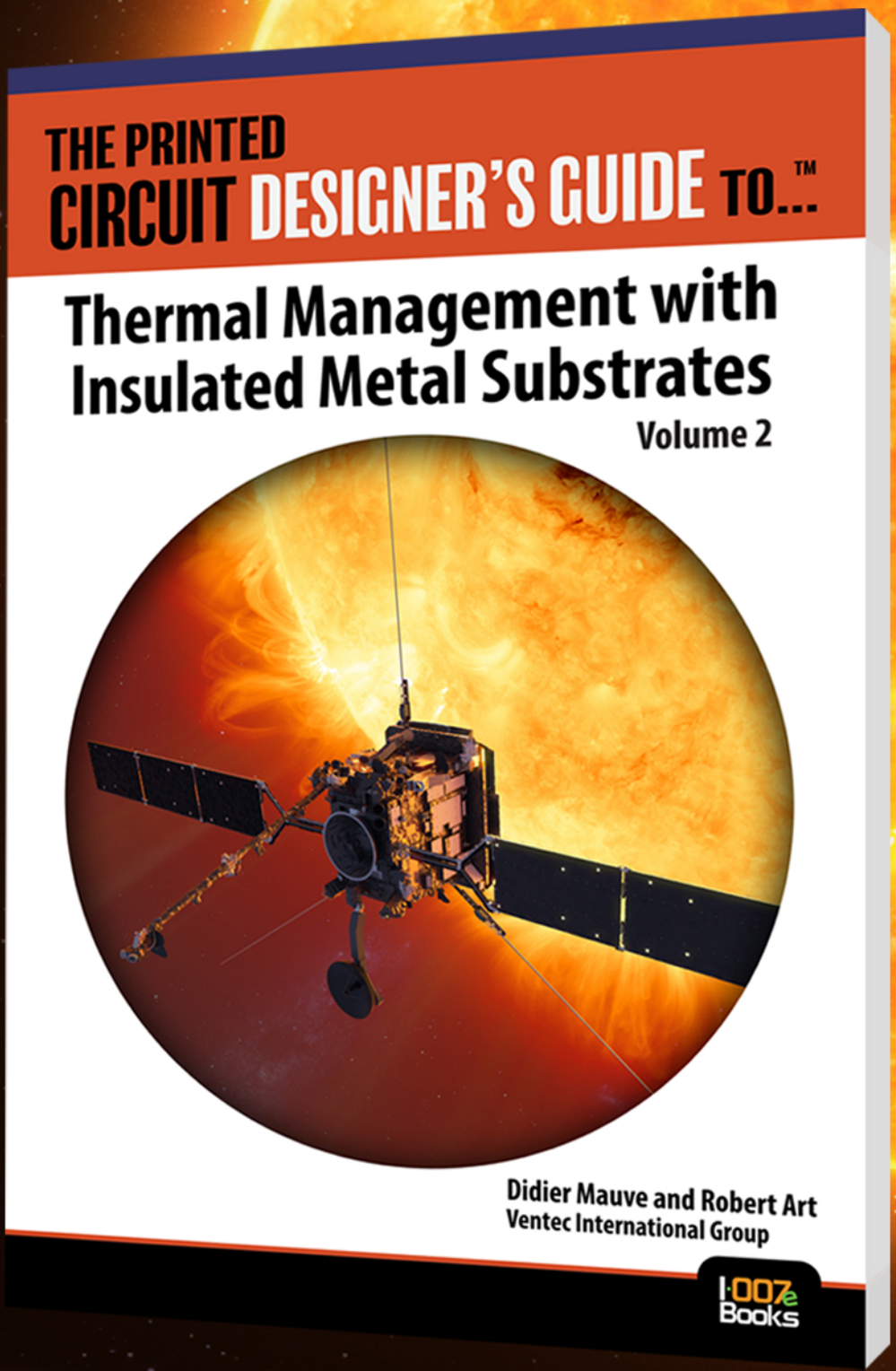
JULY 2022

I-Connect007

SMT007 MAGAZINE



The heat is on!



I-007e Books

Download Now

SMT007 MAGAZINE

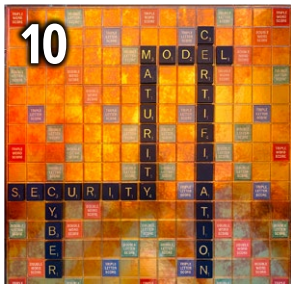
Solving Data Security

Data security is now a business imperative. You've likely heard already of the Cybersecurity Maturity Model Certification (CMMC), for instance. But what does that mean to us in the industry? Whether your approach to data security is defensive, evolutionary, or competitive, your timing can either be reactive or proactive. Either way, you will be responding to data security whether you like it or not. In this issue, we look at data security initiatives and ask, "Can this be accomplished affordably?"

FEATURE INTERVIEWS & ARTICLES

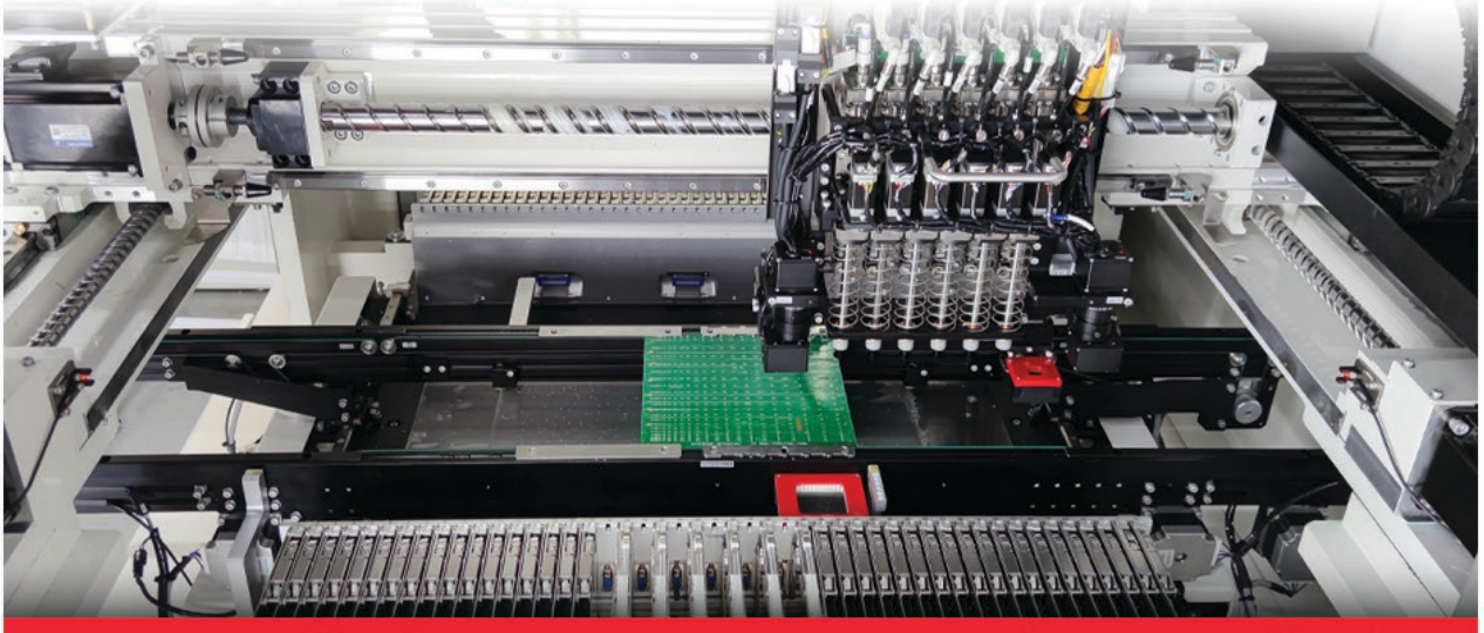
FEATURE ARTICLE

FEATURE COLUMNS



Reduce Your Cost Per Placement

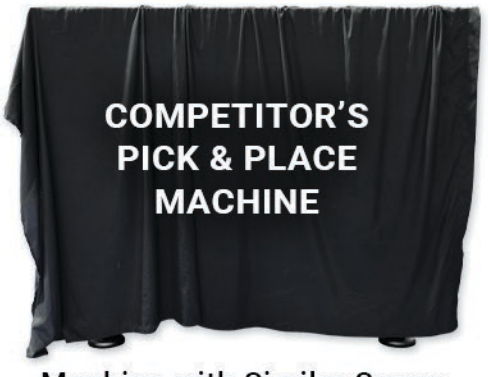
6-Heads. 20,000 CPH. *Under $150,000!*



The MC889 Pick & Place machine sets new standards for precision, flexibility, and affordability. Places components from 01005 to 100 x 150 mm.

Manncorp MC889 Pick & Place vs. Competitor's

Manncorp MC889
6-Head, 20,000 CPH
List Price: $145,995



Machine with Similar Specs
6-Head, 17,100 CPH
List Price: $259,900

Save more than $100,000 *when you purchase the MC889 from Manncorp!*

Read Our Blog

CONTACT US!
Chris (East) 215.869.8374
Ed (West) 215.808.6266
sales@manncorp.com

Manncorp™
www.manncorp.com
Hatboro, PA | San Diego, CA

55 YEARS

SMT007 MAGAZINE


We are dedicated
to excellence through
innovation,
technology
and most importantly,
service.
COMMERCIAL • MILITARY • MEDICAL • BAREBOARD
U.S.C.
U.S. CIRCUIT
www.uscircuit.com
ISO
9001 CERTIFIED
ITAR

Data Security: It's Incumbent Upon You

Nolan's Notes

by Nolan Johnson, I-CONNECT007

The news broke in Portland, Oregon, in May that the city government had suffered a "cybersecurity breach" and lost $1.4 million in city funds. The city's official statement announced, "Preliminary evidence indicates that an unauthorized, outside entity gained access to a City of Portland email account to conduct illegal activity."

KATU-TV reported that the city's Office of Finance confirmed the breach occurred in late April with a fraudulent money transfer. The first transaction did not trigger a warning flag, and the breach was not detected until that email account attempted a second transaction.

Multnomah County's spokesperson Dennis Tomlin told KATU, "It's not a matter of if you're going to get hit but a matter of when you're going to get hit. So, what's incumbent upon the county is to do as much as we possibly can to reduce the risk of a serious event from occurring." We should note that the City of Portland encompasses most of Multnomah County, making Tomlin's comments even more meaningful.

Andrea Peterson, reporting on the incident for *The Record*, referred to a similar attack on Erie, Colorado, in 2019, where it was believed that $1 million intended for a bridge project was stolen.

These are incidents from just two U.S. city governments, however, we know such attempts are widespread. As we spoke with cybersecurity experts for this issue, the "human factor" was a constant concern. Fraudulent email remains the number one method for hackers to gain access to a company's internal systems. In fact, the FBI has issued two dire warnings, with the most recent detailing Business Email Compromise/Email Account Compro-

mise (BEC/EAC) scams account for $43 billion in fraudulent take. We found the FBI announcement to be so on point with the topic that we decided to reprint it in its entirety in this issue.

With all that we know about the risks of being involved in a cyber world, we must be getting a handle on it, right? Unfortunately, no. In a recent *Washington Post* article[1], the author cites two industry experts on the state of cybersecurity in the U.S. in general.

"[We're] less vulnerable against the threats of five years ago. But I see no evidence that the threat has stood still, and in fact, it is likely that it has grown at a faster rate than our defenses," said Herb Lin, senior research scholar for cyber policy and security at Stanford University.

"We've become ever more vulnerable with each passing day," warned Lauren Zabierek, executive director of the Cyber Project at the Harvard Kennedy School's Belfer Center. "I don't know where the bottom is."

It may feel like it's all doom and gloom, but my point is that cybersecurity is our collective responsibility. As an industry, if we want to grow, thrive, and endure, we need to ensure any private and protected information passing through our hands stays private and protected. The key here is "passing through." The data moves along with the physical assemblies. We must ensure secure entry, processing, and exit for that data set. This is the core intent of the Cybersecurity Maturity Model Certification (CMMC).

Data security is now a business imperative. Whether it's defensive (to repel hackers and data leaks), evolutionary (to support digital twins and industrial automation), or competitive (certifications and new capabilities), you can be *reactive* or you can be *proactive.* Either way, you will be responding to data security in some form. In this issue, we look at three main security initiatives underway, and ask, "Can this be accomplished affordably?"

That last question is the one that's the hardest to nail down, of course. In our interview with Divyash Patel of MX2 Technology, he says that basic cybersecurity "hygiene" (as he calls it) is lacking in a significant percentage of our facilities. We must start there before we can build a solid cybersecurity system. If your organization has already secured your basic email hygiene, you are well ahead of many others. You won't need to fund that part of the project.

What we didn't find—and not that we realistically expected that we would—was a formulaic approach to cybersecurity budgeting estimation. It's not like one can estimate dollars-per-line, Euros-per-facility, or pounds-per-employee. But as Ryan Bonner of DEFCERT explains in his interview, the CMMC assessment preparation documents make for a valuable self-assessment. IPC's Validation Services programs are equally valuable not only in providing a certification recognized by government purchasing agents, but also as a process and security verification step. Look for Randy Cherry's IPC 1791 discussion in this issue as well. In short, with a well-trained IT department, much of the work can be done in-house.

Here at I-Connect0007, we trust that digital security is high on your to-do list (if it isn't, hopefully this issue will change your priorities). While digital security is not an insignificant project, achieving certification continues to become more clear and more focused. Now is a good time to move security to the top of your priority list. **SMT007**

Reference

1. "The U.S. Isn't Getting Ahead of the Cyber Threat, Experts Say," by Joseph Marks, *Washington Post*, June 6, 2022.

Nolan Johnson is managing editor of *SMT007 Magazine*. Nolan brings 30 years of career experience focused almost entirely on electronics design and manufacturing. To contact Johnson, click here.

Time to Get Serious About CMMC Readiness

Feature Interview by Nolan Johnson and Barry Matties
I-CONNECT007

Divyash Patel of MX2 Technology is a leading cybersecurity expert who's sounding the alarm about getting your company into a state of readiness. But he's not yelling fire in a theater. Whether it's aligning with DoD's CMMC, or just ensuring your company's data and processes are protected, Divyash can see what's coming. "This is a must-have compliance program," he says. "It needs to be taken seriously and maintained."

Nolan Johnson: Divyash, we are here to learn more about CMMC, and how it fits into today's current cybersecurity concerns.

Divyash Patel: From a manufacturing standpoint, I've seen a lot of inconsistencies on how companies treat government data—general government, not even DoD. Many manufacturing companies don't have any processes or formal cybersecurity awareness training in place regarding such information, especially when it's confidential, especially involving the DoD. There are many businesses where this information was just flowing through as if it were written on a napkin somewhere.

That shows me there is a big gap. These companies are nowhere near meeting the most basic standards, not even CMMC level one. That's a problem, especially if the DoD is requiring compliance to be pushed up and down the supply chain. Executives don't seem to be taking this as seriously as they should, but it could become a deal-breaker for continuing

vayo
intelligent software, pleasant work

www.vayoinfo.com

Ever experienced 3D DFM/DFA/DFX solution for PCB/PCBA?

Time to transform and upgrade Now!

VayoPro-DFM Expert

- ☑ 3D DFM/DFA solution to facilitate review of PCB details
- ☑ 1,500+ checking rules to automate PCB design & assembly analysis
- ☑ Innovative 3D report to improve communicating efficiency

【Vision Awards&Innovation Award】

- Locate design omissions
- Predict assembly difficulties
- Reduce prototyping times
- Improve product reliability

Apply for free trial now! Click Here

www.vayoinfo.com business@vayoinfo.com Linkedin Youtube

Vayo (Shanghai) Technology Co., Ltd.

Divyash Patel

to do business at any level within the DoD supply chain. Other government agencies will follow suit; it's not just DoD.

Johnson: Hypothetically, I'm a circuit board assembler and one of my customers sends a board for me to build. That board happens to get used in a vision system in the general marketplace, but then I find out that vision system has been specified into a surveillance drone being sold to the U.S. military. As the assembler, I have no idea; I'm just working with my customer. I don't have visibility to where that board might ultimately end up. Now it's in a military application. That pushes the CMMC requirement all the way up the supply chain, not just to me but beyond to my suppliers. Is that correct?

Patel: If you're part of that supply chain, and you handle controlled unclassified information (CUI), absolutely. If you're a printed circuit board manufacturer, for example, that board may be part of a bigger assembly, and you'll be accountable for meeting CMMC requirements. The bigger problem is that there's no cybersecurity hygiene anywhere in the supply chain. And beyond the DoD, companies that don't have compliance requirements like CMMC are failing to take security as seriously as they should. Yes, it is going to be up and down the supply chain, at least for those building these printed circuit boards.

Lack of Information Is the Weakest Link

Johnson: Tell me more about cybersecurity hygiene.

Patel: I'll give you an example. Cybersecurity hygiene is having security awareness training across the organization, having access control, and adhering to best practices of cybersecurity for office productivity tools like email (no clicking links from unknown sources, no sharing sensitive files with vendors, etc.).

Cybersecurity hygiene is not willfully doing something "the way we've always done it." For example, those who share confidential documents via email were never following the ITAR or cybersecurity hygiene processes. ITAR states that users cannot forward CUI documents via email to a vendor—but many simply aren't aware.

This highlights the need for cybersecurity hygiene training.

Those who have taken CMMC more seriously are asking their vendors to fill out something as simple as a cybersecurity questionnaire. Questions include:

- What would you do with this type of information if we were to send it to you?
- What type of information are you sending?
- Do you use email as your main form of delivering?
- Do you also have a secure method of delivering documents?
- How are you controlling these?

The company says, "We've got this nice customer agreement that came in and we have to

follow the requirements stated." The ISO has certain mandates the company adheres to. But at some point, someone is not managing it like it should be and now can receive confidential unclassified information (CUI) through email.

What happens to that email? Does your staff understand what they just received?

The problem in the industry is that nobody's maintaining the security posture. I've seen this happen several times where companies start off with clean protocols, but the breakdowns can be as simple as endpoints not being patched and kept up to date. That's simple cybersecurity hygiene. People like to take showers regularly and feel clean. Cybersecurity hygiene is the same.

Barry Matties: What's the risk, though? What are they jeopardizing by neglecting this area?

Patel: Specific to electronic manufacturing services (EMS), you find many types of devices, such as reflow ovens, AOI/SPI machines, screen printers, solder, and other equipment. If you don't update the firmware, the security, or operating patches, they're vulnerable to attacks. We've seen this repeatedly in EMS companies, where ransomware comes in, or they exploited the vulnerability, and then it wreaks havoc on the entire company.

Here's another example. A customer is running older-line assembly equipment with Windows NT from the 1990s. It's working and producing, and it's expensive to replace; it's doing the things it needs to do. From a security perspective, however, we have not isolated that older-line assembly equipment or the end-of-life systems that are critical to its operation.

It's a different game today, and attackers go after this kind of stuff. Manufacturing is a very old industry, but still evolving and developing. It hasn't been able to keep up with attacks. Once you set up a manufacturing company, you're just thinking about producing and getting product out the door. Your focus is bottom line revenue and you're not thinking about your vulnerabilities. Attackers are not people who want to randomly have fun on a network. They have a mission. They find vulnerabilities, exploit them, and make financial demands. That's a big problem in our industry.

Matties: You mentioned an older piece of equipment as an entry point for a hacker. Is that the most common entry point? And how common is email compared to the equipment?

Patel: The entry point is usually going to be through email or a phishing scam. That's the low-hanging fruit.

Matties: What is the red flag when it comes to emails? How do you safeguard a company against such emails?

Patel: It usually involves end-user, security awareness training. The biggest challenge for companies that want to safeguard their email is to know what to look for. It's as simple as, "Do you even recognize who's sending you the email?" A lot of people click on links, because it says, "click here" and "do this." End users are not fully trained on what to look for. If you know you're expecting an email, do you know the person who's sending it? Even if you did "know" them, what are they asking you to do? Does it sound like them? You must be more conscious and aware of what is being asked.

In one instance, accounts payable was asked to send $110,000 to their vendor. The accounting person noted the email was coming from the CEO, which suggested the email was legitimate. However, the email sender asked that the vendor change the banking details. Why? This request was made in the final hour of the transaction. Something triggered in the accounting person's mind to ask the CEO if they'd sent this email; the answer was "no." It happens just like that. You click on the email and suddenly something is running in the background, like a keystroke logging system, that sort of thing.

The chain starts from a simple email. That's often the entry point.

Matties: That's an extremely vulnerable point to protect because you're relying on user judgment.

Patel: But if you have users trained and aware, you're less vulnerable. The next question to ask in reducing vulnerabilities is whether the IT folks know what to do with the technology on the production floor. In a contract manufacturing organization or a cable assembly house, you might have things like cable stripping machines and that sort of thing. Are those vulnerable? How much do you know about the vulnerability of the systems running in your company? That will tell you how vulnerable your entire business is.

> If you have users trained and aware, you're less vulnerable.

Johnson: That's a situation where a prime contractor for a system to the government, say, might find themselves liable, and sanctioned or penalized in some way for a component of their product from multiple steps up the supply chain. Of course, that prime contractor is going to start taking ownership of everything, all the CMMC certifications in the supply chain upstream from them. They must.

Patel: That's correct.

Matties: The people upstream are at risk as well, aren't they?

Patel: Everybody in the supply chain gets affected one way or another. Upstream vendors will be affected the most. If the incident is a downstream vendor, you have proper controls in place, and if there is a breach, what happens? It affects everybody upstream from that point on and possibly downstream as well. It affects everybody in the supply chain.

That's why vendor risk assessments are so important. ISO primarily requires this, but there are other compliances, and DoD is based on NIST 800-171, but very heavily modified. Level one of CMMC is the easiest level, but there are many companies that couldn't self-attest to compliance today. Other companies may need to be compliant with level two, which has more controls in place. It depends on the nature of your business with the DoD.

This is about risk mitigation. If there is a breach or an incident, what sort of incident response plans do you have in place? For example, do you notify your upstream vendors of what happened? Do you even have the capability to determine what was breached, what was taken, and what the ramifications may have been to the business and your business partners? Those things are nowhere near being in place at many EMS companies I have come across.

Taking it Seriously

Matties: If these houses aren't taking this seriously, why is that? If the penalty is severe enough, obviously they would. Or are they just willing to gamble?

Patel: They just don't understand why it's important. I'll give you an example. At IPC APEX EXPO in San Diego this year, a CEO and I discussed the CMMC. He said, "I don't care because I don't do any business with the DoD." Well, maybe you don't have a direct DoD customer, but does your business do business with other vendors who are part of the supply chain?

When HIPAA first came out, healthcare providers refused to take it seriously. They were just saying, "We'll deal with it when—and if—we have to." Twenty-five years later, there's a

similar mindset in our industry with security issues. An executive is saying one of two things. Those who are taking the more proactive approach ask, "What do we do? Where does our business stand today?" The other response is, "I don't understand it and my business doesn't work with the DoD." Those who are being proactive know that there's a bigger problem coming, and we need to take it seriously now. Those not taking CMMC seriously will be too relaxed about security in general; they frankly don't care and that's scary.

Matties: Most of these pieces of equipment now are online in some fashion, connected in some way, right?

Patel: Oh yes. Everything is connected to the network, which could be connected to the internet someway or somehow.

Matties: The OEMs or the equipment manufacturers, in many cases, will have remote access points back into this equipment for updates. These are vulnerable openings as well.

Patel: Yes. Let's say an EMS company has an air compressor for their production lines. To report errors on those production lines, that compressor could be sending event or maintenance notifications. Those are connected to the network and they're communicating with other systems. People don't think about this. Air compressors can get on the network using WiFi. There are IOT devices inside these devices and a lot of sensors that report information. We can get output on all sorts of things. Those devices are on a network.

Companies can get an inventory of what's running inside their network, not just computers, but devices such as IOT sensors. Are your AOI machines on the network? What are they doing? Do they have to be connected because they're communicating with other devices? Can they be isolated? My recommendation would be to get an inventory, then understand what the vulnerabilities are. Go back to the firmware or the manufacturers and check for updates to the firmware; take a proactive and measured approach.

Matties: We're seeing a flood of IOT sensors, as you know, coming into the marketplace, both in personal life, but also in Industry 4.0 specifically. Every sensor is going to be connected so every sensor is also an entry point. How does an EMS company bring in sensors and know that they're safe? How deep should that concern go?

Patel: You can do vulnerability scans—a database that contains all the vulnerabilities that have been discovered. Say a company runs one every quarter, and they find new devices being introduced; they can look to see if there are any vulnerabilities found on these devices. If you don't want to do that, the simplest thing you can do is run a vulnerability scan. It will come back with a report that could be less than 50 pages or up to a few thousand. We ran a vulnerability scan for a 15-person company, for example, and came back with 1,000 vulnerabilities.

It's amazing what you'll find with something that simple, "Here's my network. Go find what you can," and it will scan the entire network and look for vulnerabilities.

Remote Networks

Matties: We've been talking about facilities, but in this remote work environment, we have to rethink cybersecurity. Now you have all these home networks connected to your network as well. What advice are you giving companies regarding that?

Patel: For customers who are running remotely, we've set up virtual desktops that give them connectivity to their workplace. When the pandemic first hit, those who were thinking ahead had virtual environments set up so that even if an employee works from their home-based computer—not a company-issued computer—it's still safe. To log into their system and do their work, they must log into a virtual desktop.

A virtual desktop is controlled; it has the security controls in place by the company, even if they're using their Microsoft home computer without any security in place. For those who are really working from home, look into a virtualized desktop, and leverage network security that you can control vs. relying on the home user's PC to keep the company data secure.

The CMMC Planning Strategy

Johnson: Manufacturers are facing staffing shortages. It's becoming a good argument to automate, add the sensors, and make factories more digital because they may not be able to hire all the staff that they want. At the same time, they need to be adding additional security and working on their certifications so they can continue to keep their customers and their top line revenue. Those two requirements really are at odds, but it makes a very strong case that you need to have a very consistent, measurable, documented cybersecurity process, especially for CMMC.

Patel: Yes, I think it can be simple. It doesn't have to be this 100-page cybersecurity document. Level 1 has 17 requirements which are the basis of cybersecurity hygiene. It's not as onerous as people think.

Now with the Level 1 certification, the basic questions are:

- Who has access to what?
- Do you have an inventory of the systems running in your environment?

Basic hygiene doesn't have to be an extravagant cybersecurity document.

Now, when you get to Level 2, there are more requirements; absolutely you should have a cybersecurity program, or work with a company which can monitor these things for you.

At Level 1, you need to have only the basics in place. Understand what policies and procedures must be there. When deploying a new user PC or equipment, for example, you must consider:

- Do you have a checklist?
- Have you verified the firmware on the equipment or whether security software patches are installed?
- Is a computer being deployed?
- Does it have the basics in place like malware protection?
- Has the user been trained for security awareness?

Depending upon your specific situation, it could be as simple as that. It doesn't have to be something only a cybersecurity professional knows how to interpret. Keep it simple; take an inventory of all the devices running on your network and ensure the users have been trained.

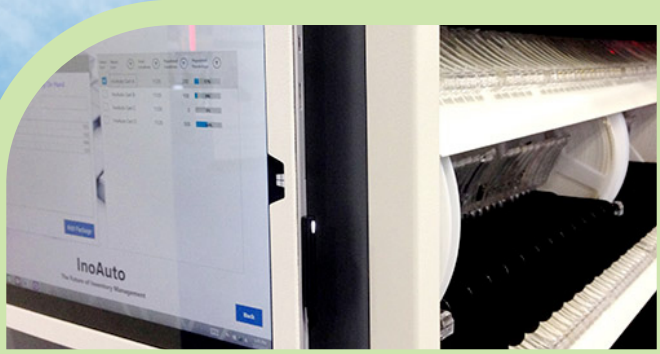
Next, are your systems physically secured? If you have servers onsite, do you have a lock and key to the server room? Who has access to your ERP and what roles do they have? Does

Smart Material Management for Smart Factory 4.0

Incoming Goods

- Intelligent automated label reading
- The ideal relabeling station for incoming goods

MODI
Vision for Identification



Innovative Material Handling Solutions

Smart Storage: Material is located and processed in seconds with InoAuto

INOVAXE
Innovative Material Handling Solutions

XRH Count
Automatic SMD-Counting

VisiConsult
X-ray Systems & Solutions

- 95% reduced counting overhead
- Global component database
- Warehouse system integration

Cogiscan
★ Track Trace Control

Middle Ware Software

Trace, Track and Control (TTC)

Real-time visibility of materials on the shop floor, improved quality and elimination of human errors

TECHNICA, U.S.A.

Fulfilling Manufacturing Needs Throughout the Electronics Industry

1-800-909-8697 • www.technica.com

CELEBRATING 35 YEARS

the sales group have access and permissions to do what the stockroom group does? Technically they shouldn't. If it's simple and documented, you can meet a lot of the CMMC Level 1 requirements. Right now, in a typical company, everybody has access to the entire file server. Your quality department documents are accessible by your sales folks. There's no control. It's a free-for-all. I've seen this too many times.

Johnson: What are the implications of being at a particular CMMC level? If I'm Level 1, does that make me fully qualified to do DoD or government work? If so, why the other levels?

Patel: Level 1 should be the place to start and help you evaluate whether you need level two. Level 2 is when you get into controlled unclassified information. Many of the manufacturing companies should look at Level 1 to begin. Now, as you move up the supply chain and the vendors start into a DoD project, they'll be required to certify at Level 2.

Johnson: Can you quantify this for me? What's involved regarding effort, resources, and expense to get a Level 1 certification?

Patel: If you don't have any documents or inventory of your systems in place, it will take time and effort to gather, document, and organize this information. Let's say you're 50% there; look at the requirements, check them off, and address whatever gaps you find.

For example, EMS company A has nothing in place; it's configured with one big, open network, with no cybersecurity processes or procedures. Starting there takes a good amount of effort. Depending on the size of the organization and the number of devices, it could take six months to a year to document the systems and processes.

If you've got some things in place, it could take three to six months. It really depends on where the company is and how much information has been documented, how proactive they've been.

But if you don't have anything in place, it's time to be thinking about it. Just recently,

there was an announcement that by this time next year, you must comply with CMMC level one self-attestation. A lot of companies are falling way behind already.

Johnson: Is this a process that is best suited with a consultant or a contractor?

Patel: Yes, because even with CMMC Level 1, there could be a lot of ambiguity translating what the DoD is really looking for. IT has one set of understanding, but you need to organize it in such a way that you can self-attest compliance. You need methods in place to maintain and control it. You must make sure that the people are following the process and not just doing it to comply with the self-attestation requirement. This must be taken very seriously and maintained properly.

Leaders of an organization must take a better approach to security overall. This is a big deal. It could result in business interruption, loss of revenue, and worst case, shut down their company. It could affect their reputation. A consultant can help you protect yourself.

Matties: Would you recommend using Level 1 CMMC as an audit?

Patel: Yes, or more accurately, as a self-attestation exercise. Level 1 has the foundational pieces in place, whether it's CMMC or another standard that comes out two years from now. I caution, though, not to do it for the acronym. As I have said many times, manufacturing businesses must take these things seriously. The manufacturing sector is an older industry, and they typically have systems in place that, once they start producing, get left alone. Companies don't go back later and check that they're still secure.

Matties: I think you're bringing up a good point. Your IT department is going to help set up the capture points, the sensors, and all the servers, but it must be an ongoing process. It's going to take a business intelligence or a cybersecurity intelligence person or consultant.

Patel: Yes, exactly; maintaining and monitoring is key. For example, in ISO 9001 a document control department helps maintain quality management systems related to its processes and procedures. It's a similar thought, similar concept; it's an ongoing process.

The Cybersecurity ROI: Implementing on a Budget

Matties: Aside from the business shutdown of a ransomware attack, how does someone justify the ROI? Are there silver linings where they may find some new capacity opportunity? For example, as an assembly house, I'm spending a lot of money on this because I have to. It's like buying insurance; protecting yourself against a catastrophic event. If we put that protection aspect aside, are there any operational ROIs that they may benefit from? Maybe because you're now following some cybersecurity protocol, your equipment is being updated and maintained in a more efficient and optimal way, which is giving added capacity?

Patel: Yes, that's true, but it's not exactly like buying insurance, because insurance won't help protect you from ransomware or help you win more business. While security is an added expense to any manufacturing company, if you have these security protocols and documents in place, you will have credibility in the eyes of the market. You'll gain the confidence of your customers. Furthermore, having compliance certifications in general can attract more business for an organization.

If other companies are not doing this or not taking these things seriously, those vendors will lose potential business opportunities.

As far as the investment, let's say you budget $1,000 every month. This will allow you to put the right security protocols and com-

pliance requirements in place, which perhaps your competitors are not doing. You can then show prospective customers the cybersecurity program you have in place. They will be more likely to want to do business with you. At the same time, you're protecting your company. Companies who spend the money are going to gain that much more revenue share.

Companies who spend the money are going to gain that much more revenue share.

Matties: Acknowledging your $1,000 example: Isn't it an expensive proposition for people to put money into this?

Patel: It is an expensive proposition, but it's much less than the risk of not doing it.

Matties: I get it. Still, some people are going to roll the dice. They don't have the resources. What if you don't have the resources? As you're pointing out, margins are tightening up.

Patel: Your January issue of *SMT007 Magazine* had an article on a breach in a company with two locations. What was the revenue loss on that over the course of two years?

Matties: We did an update with them, and it was really interesting. They were sitting there with the FBI in their conference room, getting advice on whether to pay the ransom. That becomes a question whether you can keep the business open. It was a horrible position to be in.

Patel: It's a mess. It's a crime scene. I think cybersecurity hygiene is part of the business plan now and must be properly budgeted and funded.

Matties: I like what you said, the other ROI is the added marketability of your company, because you have elevated your cybersecurity. You can demonstrate it.

Patel: This is a must-have compliance program, like ISO, that shows your security posture. Level 1 doesn't have to be expensive. It just needs to be taken seriously and maintained, so it doesn't become expensive later.

Matties: Right. That's great advice.

Johnson: ISO is generally a "nice to have." Lots of people ask for it. There certainly is customer pressure to make sure that you're ISO certified. But CMMC, especially if you want to be in the DoD supply chain, is going to be more than just a "nice to have." You either have it, or you don't. If you don't have it, you don't get to do the work.

Patel: My opinion on CMMC and companies in general: Go through it no matter what. It is the foundation. CMMC is built off NIST 800-171, which is a standard. Just to have CMMC Level 1, you are that much better positioned than you were yesterday. Having that posture in place is critical to any business. It doesn't matter if you do business with DoD or not; you're a small operation, control the environment. Even if you're a small 10-person company, control the environment.

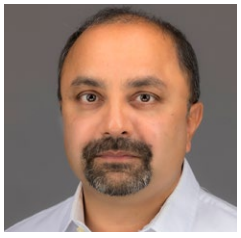
Matties: Good advice. Thanks, Divyash.

Patel: Thank you for allowing me to do this, gentlemen. SMT007

If you have questions for Divyash or want to learn more, click here.

ARTICLE EXCERPT:

Don't Hit the Snooze on Cybersecurity



By Divyash Patel
MX2 TECHNOLOGY

Editor's note: We reached out to Divyash Patel earlier this year to continue the pressing conversations about the need to stay vigilant in keeping your data secure. Divyash pulls no punches; if you're not protecting your data, your risks can be catastrophic. Here is an excerpt from that article. Follow the link at the end to read the entire piece.

Instead of looking at CMMC as yet another set of regulations, we encourage our clients to see it as a description of baseline security—similar to the way ISO sets out basic quality standards. You might be ISO certified already, without regulations telling you to be. You do it because it's a good practice, and your customers expect you to have it.

CMMC is not much different. Certification will show your customer base that you have taken the steps necessary to protect their data and your own operations. The protections necessary for Level 1 certification will be all that most of you will truly need. They amount to basic risk avoidance, not that different from requiring hearing protection, safety glasses, or safe processes in your production environment. We can take potential customers on tours of the shop floor, but not the digital sub-floor, so to speak, on which operations rest.

Because we can't visualize our networks, it's hard to see risks in them—until something happens. But what if we could see? Imagine your budget spreadsheets, payroll information, confidential client files, or other mission critical documents were only available in hard copy. Would you keep them piled in front of an open window, stack them next to a fireplace, leave them in the hands of a disgruntled employee, or give them to someone you bumped into on the street to deliver to your customer or accountant? If you saw any of these things, you'd stop everything and make sure these key items were locked in a fireproof, water-tight safe to which only you and a few trusted staff had the combination.

What I'm describing might sound ridiculous, but I assure you it is not. We see these issues regularly on networks of companies large and small, but that is because we can see in the digital environment in a way most manufacturers simply cannot.

The hard truth for the leaders of manufacturing organizations—especially those that serve the DoD—is this: You might already be safe, and you might not.

Take Strategy-Level Action

The risk is in not knowing what you don't know. I'm not suggesting you should become a technology expert on top of what you already do—not at all. I am suggesting that your digital operations should get strategy-level attention, as in a well-thought-out business continuity or disaster recovery plan that includes protecting your data.

If you and I were meeting in your office right now, I'd be asking you three key questions:

1. Where and how often is your company data backed up?
2. How would the company access and deploy the backed-up data if you needed it right now?
3. Who in your organization has access to what?

How would you answer them?

Not long ago, I asked these questions to a new client—a good-sized manufacturer. The leaders in the room weren't sure, so I excused myself from the meeting, called my office and had one of our tech team meet me with an external hard drive. We made immediate back-ups (snapshots) of the critical systems. Now at least we could all be certain that the client had a moment-in-time back-up.

Pausing the meeting sounds like theatrics, but it was not. In fact, if you answered "no" or "I don't know" to any or all of them, I suggest you stop reading this right now and find out. It's that important. Why? Because the future is uncertain, and accidents happen.

To read the entire article, which appeared in the January 2022 issue of *SMT007 Magazine*, click here.

Zombie Cars: The Next Pandemic Is Digital

Smart Factory Insights

Feature Column by Michael Ford, AEGIS SOFTWARE

In the manufacturing world, we increasingly rely on internal and outsourced security partners to keep our IT networks safe. One report stated that as many as 50% of manufacturing companies have already been the target of ransomware attempts. Therefore, there is more work to do, especially on the neglected IT network. Industry requirements, such as CMMC, invoke costs and difficulties. But like traceability in the past, with the right preparation, this "burden" can be turned around to become a near zero cost, or even a benefit.

You vs. the Hackers

As operational security in the market evolves, hackers are increasingly "left-shifting" their operations toward the source of targeted products: manufacturing. Unlike biological viruses, hackers often share their intrusion tools freely to disguise their origin, resulting in a whole stream of concurrent attacks, each with different motivations and intents. Risk increases so that our seemingly genuine Smart personal, household, automotive, medical, and defense products could suddenly turn against us.

It's no joke that there may be hackers who would like to create a game of "Zombie Cars," taking remote control of vehicles. They would suddenly take over as you drive along the freeway and use it as a tool to extort money from you; this is technically possible. (Examples of such remote control can easily be seen on You-

$10 MILLION IN RECENT TECHNOLOGY CAPEX INVESTMENTS

NIST 800-171 COMPLIANT CYBERSECURITY PROCESSES

250,000 SQUARE FEET SUPPORTING ALL TECHNOLOGIES

4 STATE-OF-THE-ART NORTH AMERICAN FACILITIES

VIEW OUR QUICK TURN VIDEO NOW

U.S. Partnership USPAE for Assured Electronics

SUMMIT INTERCONNECT

www.summit-pcb.com

Tube.) Imagine a group of vehicles taken over and used for coordinated disruption. As vehicle control security is ever heightened, the hackers simply get more resourceful; they are focusing on manufacturing, with even the simplest and seemingly innocuous Smart/connected devices as targets. Cars have hundreds of interconnected controllers, where a simple media player or window winder module could become the cyberattack entry point. In the same way, a compromised USB stick on the manufacturing shopfloor could easily be the attack mechanism.

Once they succeed into a manufacturing network, it is open season on:

- **Competitive information:** Customer and supplier names, capacities, capabilities, schedules, and shipping information that anyone from counterfeiters to dishonest competitors can use against you
- **Private information:** Organizational and structural details, investors, employee details, payroll records, travel, and expense information
- **Intellectual property:** Product design and technologies, bill of materials, which together enable the creation of clones and counterfeits in the market
- **Product alteration:** The changing of data related to product documentation, bill of materials, and embedded software to establish quality or security vulnerabilities
- **Hijacking:** Implementation of ransomware or parasite programs mining for bitcoin using computers built into automation
- **Sabotage:** Machine instructions can be altered, either to damage processes and cause downtime, or to make subtle changes leading to quality issues, new product launch delays, or product-related issues in the market

Though these may sound a little ambitious, consider that there have been complex attacks in which design information, for example, was intercepted between design and manufacturing such that cloned products could be manufactured but with alterations that allowed embedded spyware to be active. Shipping information was also hacked so that substitutions of real products with the cloned products could be made. Traceability data was hacked so that legitimate serial numbers would be matched. Noticing a single cybersecurity incident within an organization often represents just the tip of the iceberg of what has been unknowingly happening, which, in at least one documented case, went on for over a decade.

Further Complicating the Problem

Industry regulators are responding to the threat, but with requirements that significantly impact the profitability of most manufacturers and increase the burden on executive accountability but do little to reduce risks. The idea that a firewall and virus checkers keep things relatively safe in IT networks may be true in the office, but this is not true when it comes to manufacturing floors. Most production automation has internal computers, which have been designed for the single purpose of operating the machine and use the same common operating systems, such as Windows. These machines are often now connected for the purposes of MES, machine learning, closed loops, dashboards, program management etc., so in most manufacturing facilities, there is a manufacturing network (OT) in place. These machines, however, typically cannot run antivirus software, as that may affect the precise timings of the machines, and very often operating systems cannot be upgraded due to the fixed hardware and software limitations. They continue to contain known security vulnerabilities with no checks in place for the latest known vulnerabilities. Any cybersecurity intrusion can spread almost instantly from a single point of entry to every machine on the network.

The reality is that in almost all factories there are many types of automation, from many vendors, with many versions of unprotected software. This is further complicated by numerous instances of middleware; the OT network connection to the IT network has therefore become a critical security concern. In some cases, connection is not allowed at all, as firewalls allow legitimate traffic to flow, which are emulated by viruses that may already be present in the OT network. Data breaches are a major concern as product data, traceability data, and electronic visibility and control are all somehow inevitably transferred to and from the OT network, often using uncontrolled USB drives, middleware, or in-house developed software. It is an absolute nightmare for IT teams, which cannot practicably be expected to be in control all the time.

Become Solution-Oriented

I wish I could describe a perfect and simple solution, such that manufacturing can avoid the cost, compromise, and burden of security measures that will imminently be required in manufacturing, but I cannot. The reality is that there is no easy answer. There are some principles that can and should be established as soon as possible to reduce the cost, risk, and impact from security breaches, or requirements for protection, which enable easier compliance and benefit the factory. Think back to the early days of traceability, where data collection and collation quickly became a major burden for the industry, with accuracy and usefulness of reporting, as well as long-term storage of data being quite a challenge. As technologies developed, native traceability data extraction mechanisms became normal with the IPC-1782 traceability standard defining exactly what is needed and how to communicate requirements. The IPC-CFX standard securely extracts traceability data in a single standard language. This enables the use of traceability data for machine learning and active quality management, thus building value from contextualization of events in many ways, turning an everyday burden into an everyday benefit. Preparedness and utilization of the right technologies and solutions turns situations around.

Preparedness and utilization of the right technologies and solutions turns situations around.

Trying to bolt on a high-security regime on top of an existing shop-floor network, more reminiscent of the "wild west," is likely to invoke a life-changing experience. Instead, there are several things that can be considered and prepared that will secure production, while at the same time modernizing and streamlining the operation for improved performance and quality, thus reducing costs and risks. Some things for immediate consideration are:

Is the current exchange of data on the shop floor secure?

- Is any of the data open and not encrypted end to end?
- Is there any third-party middleware involved?
- Are there one or more "translations" of machine data?

If the answer to any of these questions is "yes," then consider the use of IPC-CFX (Connected Factory Exchange) which is already supported by an increasing list of machine vendors.

Are the shop-floor solutions secure?

- Are there home-grown solutions that cannot be modified or maintained?
- Are there multiple solutions that share data through an automated or manual translation process between solutions?

- Are USB devices to transfer data ever needed?
- Is sensitive data ever sent by email?
- Is my IT network connected somehow with my OT network?

If the answer to any of these questions is "yes," then the infrastructure and interoperability of solutions should be reviewed with the ideal being a single, secure IIoT-based MES platform that provides secure interoperability with other solutions, such as ERP, PLM, etc.

Are my people secure?

- Does anyone have access to data that is not of immediate relevance for their tasks?
- Does anyone have contact with key intellectual property relating to the product, such as when preparing automation programs or work instructions?
- Are there people operating computers or automation that have not been appropriately trained in cybersecurity?
- Are there areas in which enforced and monitored best practices for security are not established?
- Does my OT network have a flat structure, not segmented according to customer/product/environment?
- Do the IT team refuse or are unable to take full 24/7 responsibility for OT network security?

If the answer to any of these questions is "yes," then it is important to now start identifying vulnerabilities and to establish best practices, such as the replacement of procedures. For example, this might involve emailing multiple documents relating to the design of a product between engineering groups with applications that utilize PCB layout and 3D CAD design data through secure digital manufacturing engineering tools that don't require users to manually access the raw design data. It is also advised to implement an OT-specific cybersecurity package that detects abnormalities on an OT network, including the operation of machines and other automation.

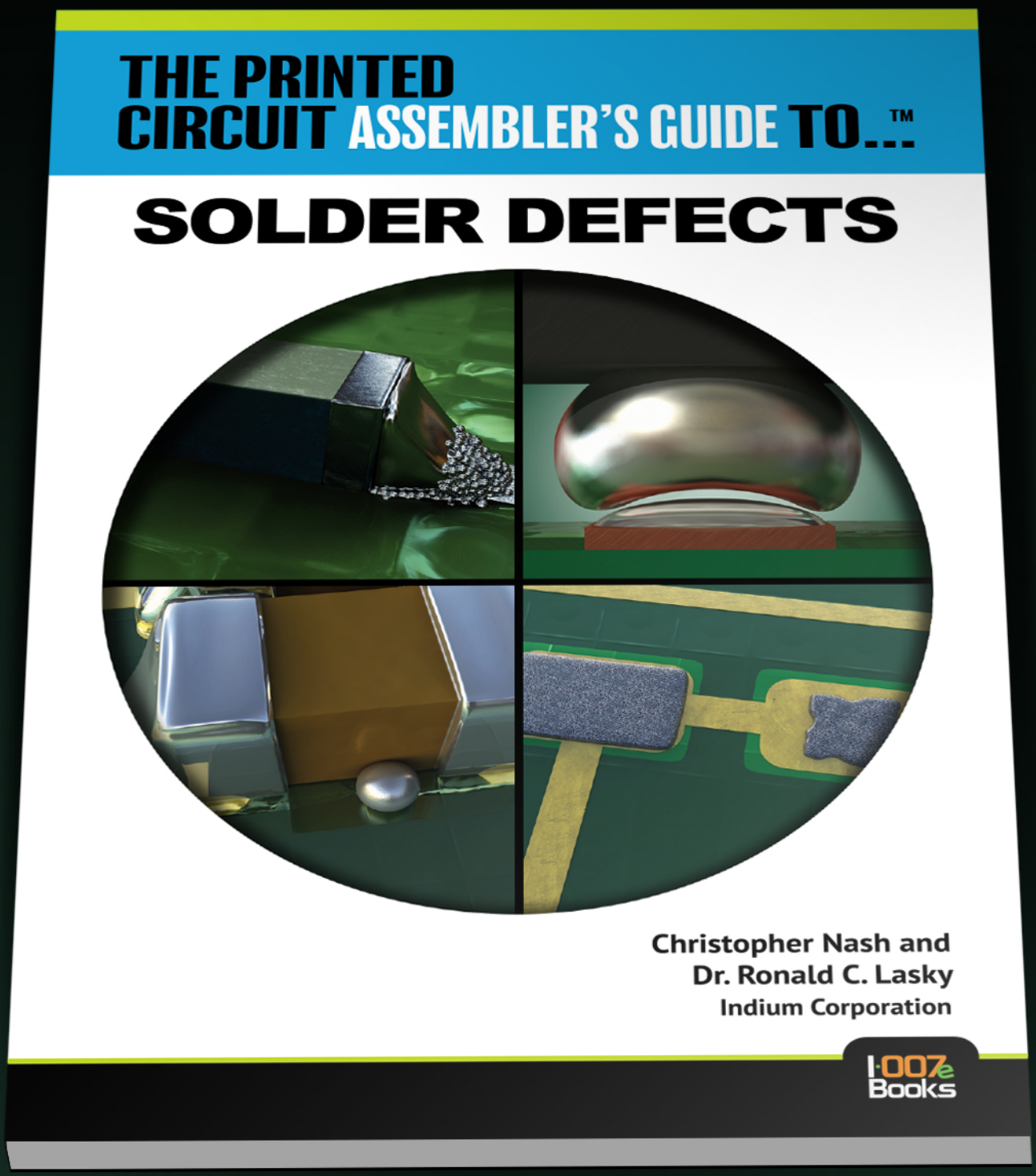
Are my products secure?

- Am I sure that there has been no manipulation of product or manufacturing data due to any cyberattack?
- Where a cyber-intrusion has been detected, can I identify and quarantine those materials and products that may have been affected and inform the supply-chain appropriately to prevent issues from further escalating in the market?

If the answer to either of these questions is "no," then implementation of the new IPC-1793 Cybersecurity standard is advised, which includes exact traceability in manufacturing of the association of material to products, such that potentially affected specific products can be identified and quarantined.

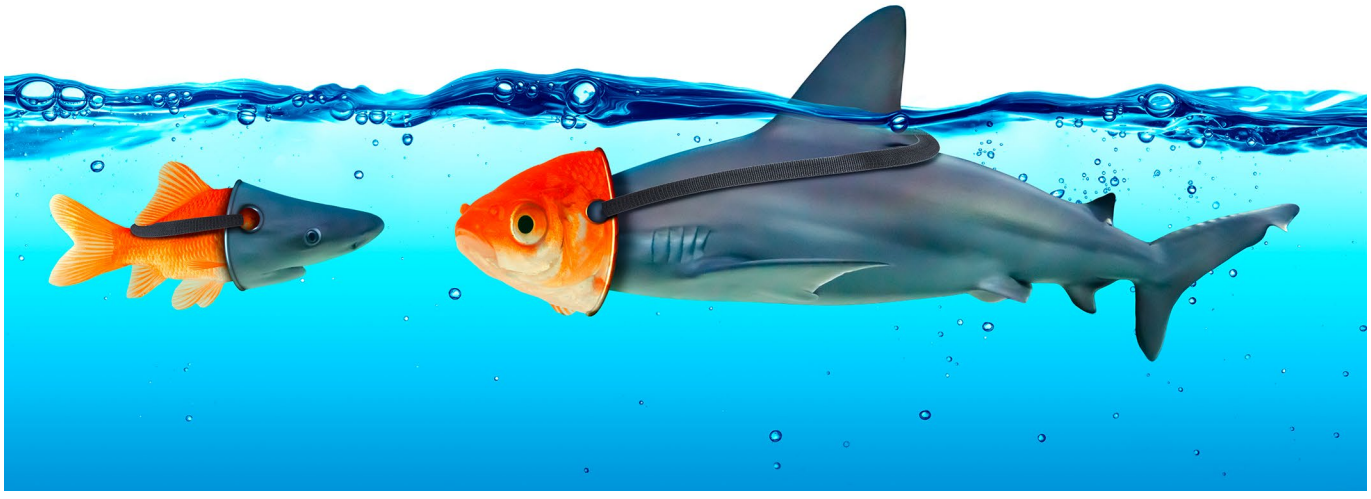
For sure, almost no facility should feel as though it is well prepared for coming security requirements; there is no magic pill. But by implementing some intelligent practices as part of digital transformation projects, most requirements can be addressed without excessive cost or burden to the operation, and just like modern traceability, can bring with it best practices that directly and positively impact profitability. SMT007

Michael Ford is the senior director of emerging industry strategy for Aegis Software. To read past columns or contact Ford, click here.



Available Now Download Here

How Important Is Trust?



Feature Article by Randy Cherry
IPC VALIDATION SERVICES

If you work for a U.S. defense prime contractor, do you have concerns about the safety of the controlled unclassified information (CUI) for your printed circuit boards, printed circuit board assemblies, and cable and wire harnesses? What about the design and the development process for your products? Is the controlled technical information (CTI) safe and protected? Are the suppliers that your company selected maintaining a quality system, a supply chain risk management process, a security system to protect products and services from unauthorized access, and a Chain of Custody policy for electronic and physical materials?

Once again, if you work for a U.S. defense prime contractor, how do you know that your suppliers are following the ITAR and EAR regulations?

CUI and CTI

Your company needs trusted suppliers that can demonstrate the ability to meet or exceed industry standards to ensure that your CUI and CTI is protected. You deserve to have those questions answered.

Let us define some terms. Controlled unclassified information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies, but is not classified. Controlled technical information (CTI) is a subset of CUI and is technical information with military or space applications that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. In other words, CUI and CTI are especially important to protect and, at all

Free Checklist: Vulnerability Assessment

MX2 TECHNOLOGY
Executive IT Leadership

The Checklist helps CEOs understand what to expect from their Vulnerability Scan, so they can be prepared to better understand risk and make necessary changes. Topics include:

- The CEO's role before, during and after a Vulnerability Scan.
- Baseline cybersecurity tenents that CEOs need to be confident in.
- Questions CEOs should be asking to understand and justify the risk associated with each of the findings.
- How CEOs can communicate the results of a Vulnerability Scan.

Download at: **mx2technology.com**

costs, prevent the theft of this confidential information.

Why do CUI and CTI need protection? The answer is simple. Defense companies spend substantial amounts of money and countless hours developing the next generation of technology and equipment to protect our country. U.S. citizens/persons take comfort knowing that their way of life is protected by our military and government institutions. If critical information (CUI or CTI) is stolen and sold to another organization or country, our security comes into question. The ability of the U.S. military and our government to protect us becomes a concern. That is why protecting CUI and CTI becomes so important.

The ability of the U.S. military and our government to protect us becomes a concern.

The Birth of IPC-1791 and QML

There is concern within the Department of Defense (DoD) that the trustworthiness of printed board and assembly designers and manufacturers for national defense systems is not consistently sufficient. As a result, requirements for defense systems, including all products on the U.S. Munitions List (USML) using electronics are vulnerable to tampering with malicious intent, supply chain disruptions, counterfeit parts and materials, physical security, cybersecurity, and substandard quality and product assurance. Although requirements are available to protect defense electronics, they are not consistently applied by the program managers and DoD contractors.

About six years ago, IPC and the Executive Agent for Printed Circuit Boards and Interconnect Technology worked together to form an IPC Committee (2-19b Trusted Supplier Task Group) that was tasked with developing a trusted supplier standard. The team, comprised of industry and government representation, defined the four pillars of trust as: quality, supply chain risk management, security, and chain of custody. The standard was developed to assure that the requirements were practical, clear, and measurable. In August 2018, the IPC-1791 Trusted Electronic Designer, Manufacturer and Assembler Requirements standard was released. Today the standard is at revision B with the committee actively working on revision C. In fall 2019, the Executive Agent and IPC Validation Services developed the IPC-1791 QML (Qualified Manufacturers List) program. IPC Validation Services continues to qualify company locations and displays the trusted suppliers on the QML[1].

What is the IPC-1791 standard and why is it so important? The scope of the standard focuses on providing the minimum requirements of policies and procedures for printed board design, fabrication, assembly, and cable and wire harness assembly organizations and/or companies, to become trusted sources for markets requiring high levels of confidence in the integrity of delivered products and services. Today the standard targets the military, defense, and aerospace sectors. Future IPC committees plan to target the commercial industries (examples: automotive, medical, telecommunications, industrial, etc.).

The benefit of using this standard assures customers that their suppliers:

- Maintain a quality system (AS9100)
- Maintain a supply chain risk management (SCRM) system addressing threats, counterfeit disruption, obsolescence of material, and vetting suppliers on their approved vendor list
- Provide security requirements (including protecting your CUI/CTI from unauthorized access, demonstrating compliance to NIST SP 800-171, ITAR and EAR regulations)

In times of challenging allocations, you need a supplier that will LEAD you through thick and thin
We accept the challenge! Utilizing our global supply network, we DELIVER an All-in-One solution!

WE DO IT ALL ...

We offer an All-in-One solution through our experience, integrity, and clear communication. Get on board for our joint journey into the future.

www.PCB-technologies.com

ALL IN ONE

PCB TECHNOLOGIES™
leading the way

- Having a chain of custody policy controlling electronic and physical materials, providing traceability, handling scrap materials, and tracking finished goods that are shipped

The standard also covers non-U.S. electronic design, fabrication, and assembly organizations. The U.S. defense prime contractor must approve and sponsor these non-U.S. organizations before any attempt to qualify this company location can occur.

IPC-1791 vs. CMMC 2.0

How does the IPC-1791 standard/QML program compare with the Cybersecurity Maturity Model Certification (CMMC) 2.0 program? Both the IPC-1791 standard/QML program and CMMC 2.0 Level 2 program require compliance to the 110 practices of the NIST SP 800-171. CMMC 2.0 is being driven by the DFARS 252.204-7012 and requires formal certification by the CMMC Accreditation Body. DFARS 252.204-7012 covers cybersecurity incident reporting. The IPC-1791 standard/QML program is being driven by a few U.S. defense prime contractors that want to make sure their supply base is vetted, and their suppliers are viewed as a trusted source. The IPC-1791 standard/QML program goes into a much deeper dive with quality, SCRM, security (including compliance to NIST-SP-800-171), and chain of custody. CMMC 2.0 today focuses only on the NIST SP 800-171 for level two certification. The major difference is the IPC-1791 standard/QML program is ready today for any company that supplies products and services to the DoD. It is unclear exactly when CMMC 2.0 becomes a requirement. CMMC 2.0 may happen in Q2 2023 or later. Companies can visit the CMMC website (cmmcab.org) for the most current information and developments.

If you are a U.S. defense prime contractor, trust is important, as is protecting your CUI and CTI. The IPC-1791 standard, along with the 1791 QML qualification program, provides the only means today to validate that your suppliers are protecting your confidential information.

A special thank you to Richard Snogren, IPC 2-19b committee chair, for his guidance and input. **SMT007**

References

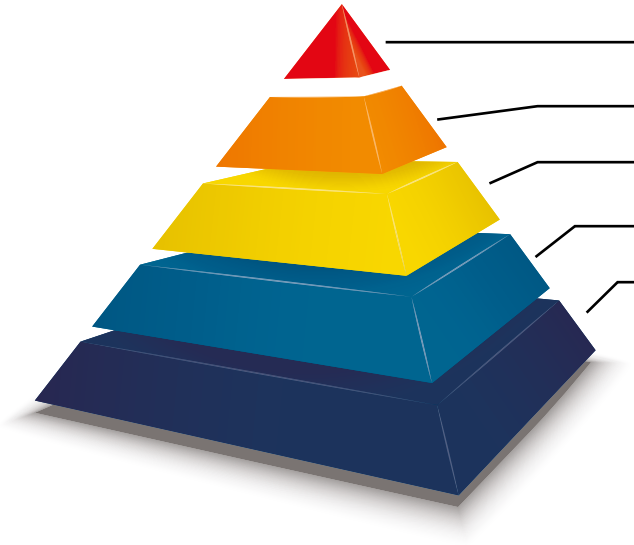
1. IPC Validation Services, IPC-1791.

Randy Cherry is director of IPC Validation Services. He can be reached at randycherry@ipc.org.

CMMC 1.0 vs CMMC 2.0

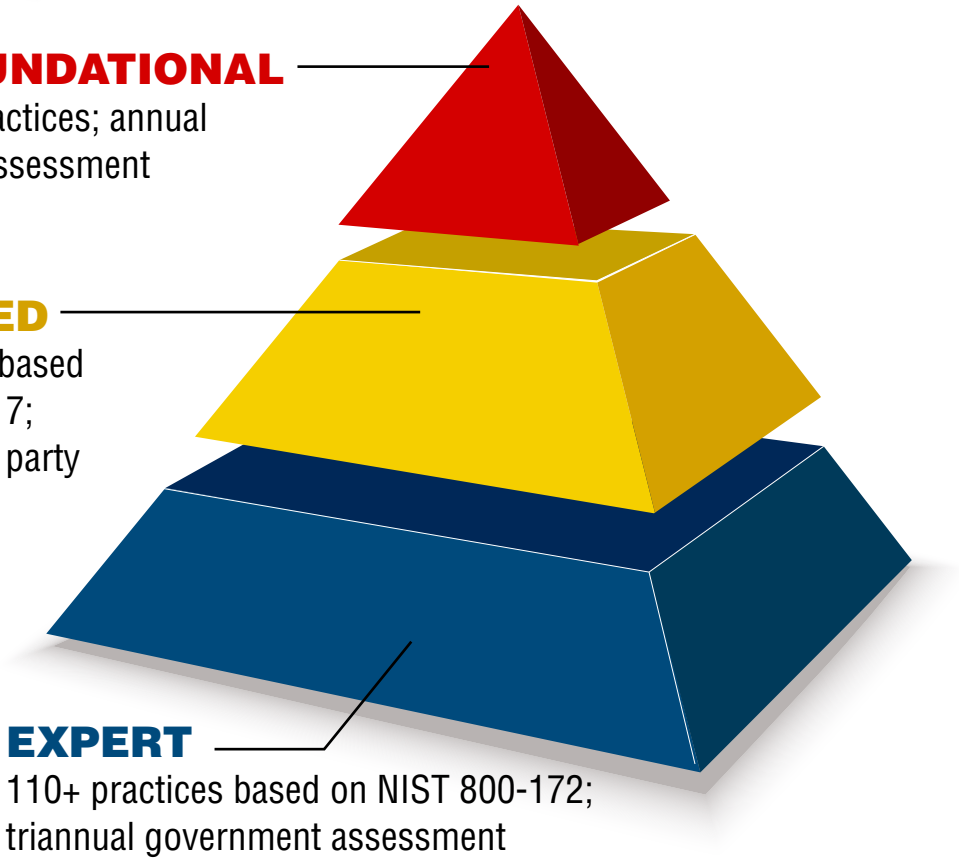
CMMC 2.0 has been restructured from five maturity levels to three levels of security. Levels 2 and 4 have been removed entirely to streamline the process.

1.0



- **BASIC**
- **INTERMEDIATE**
- **GOOD**
- **PROACTIVE**
- **ADVANCED**

2.0



FOUNDATIONAL
17 practices; annual self-assessment

ADVANCED
110 practices based on NIST 800-17; triannual third party assessments

EXPERT
110+ practices based on NIST 800-172; triannual government assessment

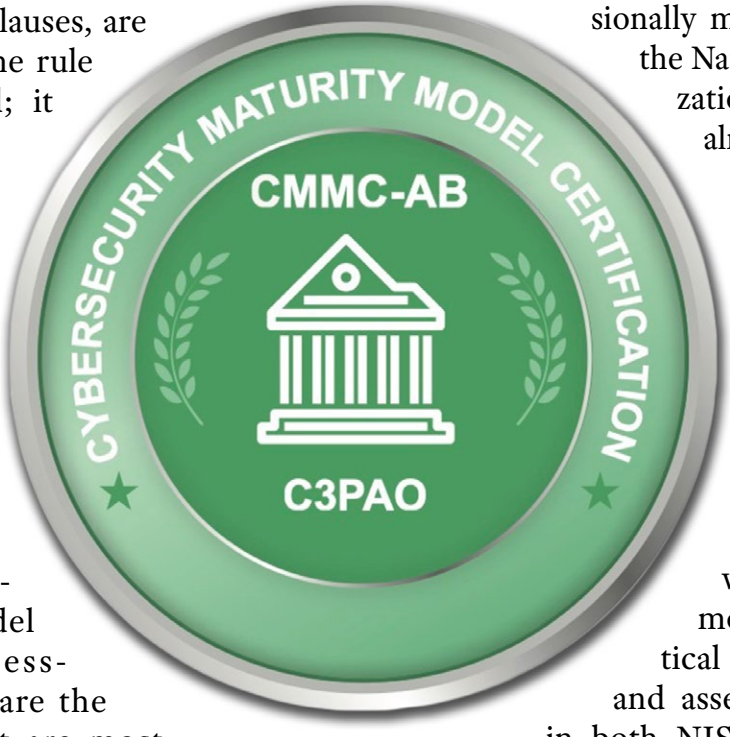
007e FAST FACTS

Source: National Institute of Standards and Technology

CMMC 2.0: Are You Ready?

Feature Interview by Nolan Johnson
I-CONNECT007

Nolan Johnson discusses with Ryan Bonner of DEFCERT exactly where and how EMS companies should aim for CMMC certification. Organizations, he says, "need to avoid false dichotomies where they assume that either CMMC is a go or it's not happening at all. All the government mandated reviews to keep CMMC moving forward, resulting in new contract clauses, are already underway. The rule making is scheduled; it will happen."



Nolan Johnson: Ryan, what's the status of CMMC 2.0?

Ryan Bonner: The aspects of CMMC 2.0 that those contractors can act on now, even while we wait on other components, are the model itself and the assessment guide. Those are the two documents that are most appropriate for contractors. Because those two items are in place, there is a path forward for CMMC, even while secondary aspects of CMMC, like the C3PAOs assessment process or the eventual contract clauses that will drive adoption, are under the surface, if you will, and are going through rule making.

Johnson: There is something tangible that we can proceed with in anticipation of everything else coming into place.

Bonner: Absolutely. Many organizations don't realize that the shift to CMMC 2.0 was the outcome of a review by the Government Accountability Office. I believe it was congressionally mandated as well under the National Defense Authorization Act. That process has already been completed.

The big change coming out of that review process was to shrink the model back to only the requirements described in the original parent document, NIST 800-171. That creates a situation where now the CMMC model under 2.0 is identical to the requirements and assessment content that's in both NIST 800-171 and NIST 800-171A (the document used to assess 800-171). Those are identical. They're in lockstep. There's no appreciable difference between the two.

Johnson: If my company has already completed NIST 800-171, what does this mean regarding CMMC?

KOH YOUNG TECHNOLOGY

Those who demand more, demand Koh Young.

KY-P3 SERIES

COMBINATION PIN, TERMINAL AND SMD INSPECTION

Founded on world-class 3D AOI technology, Koh Young designed the KY-P3 to overcome long-standing industry challenges like escapes and false calls. The KY-P3 combines advanced high-resolution optics with innovative 3D vision algorithms for precise pin measurement. The M3 model incorporates dual reciprocating shuttles to eliminate transfer time and maximize efficiency. The KY-P3 measures height, absense, offset, coplanarity and more on myriad pin and terminal configurations. Using quantitative 3D measurements, the KY-P3 delivers unmatched accuracy and repeatability. The recognized leader in electronics inspection, Koh Young continues to deliver award-winning solutions for the industry.

20 2002 - 2022 YEARS OF INNOVATION

Koh Young America, Inc.
1950 Evergreen Blvd., Ste 200
Duluth, GA 30096 USA
+1-470-374-9254
america@kohyoung.com

kohyoungamerica.com

Bonner: You should be aware of two ways you might be assessed or graded against what you've already done. If you have already worked on 800-171, or even completed your implementation, you have two pathways. The first is being assessed by the government or the defense contract management agency that's done through their DIBCAC (Defense Industrial Base Cybersecurity Assessment Center) teams. But the DIBCAC teams, at no cost to you, schedule either a moderate confidence or high confidence assessment and, because of that, assign you a completion score using their assessment methodology. That's one way to be assessed against NIST 800-171.

> Organizations should be aware of how compressed a 180-day window is for completing your implementations.

The other pathway is a proactive approach where you seek CMMC certification. This involves the accreditation body and their authorized assessing organizations, which are the C3PAOs coming in and, at your cost, you are assessed and then certified. That certification is expected to be good for three years. The difference there is that contracting officers are allowed to request your CMMC certification as a source selection criterion for awards. That's the big shift. Organizations that want to skip many of the government audited steps can go straight to private sector certification, and then have that on file to show you've completed everything in NIST 800-171.

They're not mutually exclusive, so if organizations haven't completed NIST 800-171 implementations, there is an additional change to rulemaking that we expect next March. It will involve setting either certain minimum threshold scores or specifying which of the 800-171 requirements must be done as a prerequisite for contract awards while other, perhaps less vital implementations, can be saved until a 180-day window after-contract award.

Johnson: Sounds like there's room there to transition without being completely locked out.

Bonner: Correct. Organizations should be aware of how compressed a 180-day window is for completing your implementations. It's not a lot of time based on how long it seems to take most contractors to implement.

Johnson: Let me ask the question in a different direction. If a company achieves CMMC 2.0 certification, does that automatically get them NIST 800-171?

Bonner: CMMC is the third-party verification method for NIST 800-171; all 110 of the requirements are validated. In that way, it does act as a hand-in-glove verification for 800-171.

Johnson: There are some components needed, including a checklist?

Bonner: Yes. There's an entire document called NIST 800-171A. Its contents are also repeated verbatim in the CMMC assessment guide. That's why we can make the claim of identical models. The contents of the assessment guide are really the measure of success for a contractor's implementation of 800-171. Organizations need to know that in any assessment, whether it's run by the government or by a C3PAO.

Those assessments all follow the same 320 assessment objectives. If you want to get a passing outcome or a full points value for your implementation, then you can't just meet the requirement. You must satisfy all the objectives for that requirement. Organizations that might have done just a basic implementation against the list of 110 requirements (back when

those were released) and perhaps overlooked the later publication of the assessment guide could be in for a rude awakening when they open that document for the first time and realize there are additional details in those objectives and in the lists of objects that will be used in an assessment.

Those lists of assessment objects are the best way for contractors to understand where they stand now, even without engaging the services of a third party to validate their implementation. This is because each of those lists for each requirement has unique characteristics that organizations can seek out in their implementation to see if they are matching what's described there. I'll give you the examples here.

For each of those lists of objects, we have examinable documents, responsibilities assigned to personnel, and some sort of testable process or mechanism, something that can be observed or viewed in system configurations. If I'm not finding any described objects in those lists that sound or feel like something I have, whether it's an assigned responsibility or a specific document on a certain topic, or perhaps the ability to show someone in a system that something is configured, that should be a yellow flag to me; I'm not finding any home on these lists for the work that I've done. You don't need an exact match for what's described in the list, but you should have something that serves the same function or purpose as what's described in those lists.

Johnson: Makes sense. The process right now is to find your gaps.

Bonner: Absolutely. If I don't have any policy statements as described in the assessment guide for a requirement or any of the documented procedures, if I have no one in my organization who's been assigned responsibilities that are germane to that set of objectives, if I can't show any physical or systems proof that something has been done—either through a shoulder surf or in documents—that should tell me that assessors will struggle to validate the work that I've done.

Ryan Bonner

Johnson: Which of course all leads back to the fact that we can expect that everybody is going to need CMMC certification because undoubtedly somewhere along the whole supply chain they're involved in something that will be CMMC required.

Bonner: Yes. The key thing to remember with the shift to CMMC 2.0 is that level one has fallen back into a self-attestation model for meeting those minimum requirements. That shifts the focus significantly to CMMC level two and deciding early as to whether that is required for your organization based on your contracts profile and the kind of information that you handle.

Earlier this year, I asked Stacy Bostjanick, who leads the CMMC PMOs office, whether she believed ITAR, which is export-controlled information or controlled technical information (CTI), would ever be allowed to be self-attested for its safeguarding or protection under the bifurcated model that's being dis-

cussed. Her direct response was, "Not likely; it would be very difficult to do that."

That's because of the sensitivity of the data. When we look at that and at the industries we're most often interacting with—manufacturing, electronics, microelectronics, semiconductor industry, you name it—they thrive on complex technical information, so they're more likely to have the kinds of information that qualifies for CMMC level two and are likely to consider or to require third party validation or certification.

Johnson: It sounds like companies should be aiming for CMMC level two.

Bonner: I would say that in most cases, that's true. We see organizations dropping down to CMMC level one when they almost exclusively sell commercial off-the-shelf goods to their customers. The only information that they exchange is related to the procurement or purchasing of those COTS products. Conversely, the only time we see organizations pursuing a higher level, such as CMMC level three, is very clearly communicated up front by the program managers or contracts officers for that program, because they understand that it is a critical weapons system or DoD platform, and is more often targeted by advanced persistent threats, which is the entire purpose of CMMC level three. For most organizations we interact with, especially in electronics or precision manufacturing, CMMC level two is where they land.

Johnson: Does level three certification go all the way through the supply chain, even to the board fabricator for that particular component? In other words, must everyone in the supply chain be CMMC level three?

Bonner: When we think about the way requirements can flow down from a higher CMMC level into the supply chain where subcontractors may be producing less detailed or less significant parts of an overall component or an overall assembly, there's a huge opportunity and a need for contractors to control their own destiny through better data management.

By default, a higher level, and more robust requirements like CMMC or even CMMC level two, will continue to flow down, adding additional burden and cost to the supply chain unless subcontractors and suppliers work together to reverse the flow of that trend. That only happens when organizations have complete control and discretion over how much information from customer designs and requirements is brought into their internal designs.

It requires a distinct understanding of which data sets are proprietary to the contractor and which data sets belong to the government under full or shared use rights. That is the dividing line between proprietary information and controlled unclassified information, which activates CMMC levels two and three. Classified information is above and beyond the CUI side of the house. This is a match pair to classified information: it's controlled unclassified information.

Johnson: That makes sense. If the component that I'm providing ends up in a system intended for government or milaero-type use, and that system is subject to CMMC, then the subsystem I'm supplying is not required to be CMMC level three. Am I oversimplifying?

Bonner: Information that you create internally and fully own outright, meaning that it is proprietary according to the National Archives and Records Administration (NARA) which runs the CUI program— that information is not CUI, even though it may be marked as CUI upon receipt, just to make sure it's protected at the same level. But for the organization that owns it, it's not CUI.

That's rather confusing because you could very well be handling information that belongs to you marked CUI and it would not be con-

Printed Circuit Boards
LOOK NO FURTHER

SUNSTONE®
CIRCUITS

sidered CUI for you. The more likely situation when you're producing parts that are proprietary is that other laws or regulations will still apply. For example, I might create product designs that are completely proprietary, but they may still be export controlled under the International Traffic and Arms Regulation (ITAR) or the Export Administration Regulation (EAR). Those are based on the nature of what you make, not who owns the data.

Johnson: There are different scopes of interest here.

Bonner: There really are. And that's why data management becomes so important in these discussions. It's a skill set that is not often developed inside manufacturing organizations, especially when they mostly execute on someone else's designs. There needs to be a patron, if you will, somewhere up the supply chain who is the design authority on finished goods and is able to better slice and dice or disseminate the data they own in ways that stay inside all the legal bounds and don't over prescribe CUI protections.

Johnson: But that's the conundrum, isn't it? For an EMS company, their role is to be a service provider; they take the pieces and solder them together. For the board fabricator, they're creating a circuit board with no real knowledge of its purpose or function.

Bonner: Absolutely. The real question becomes how customer data is leveraged in the performance of that work. Someone we call a process provider, who solders and assembles individual components into an overall assembly, in many cases, they don't generate many internal data sets. They're leveraging what is sent to them with the task order or the technical order.

In those cases, they have very little control over the type of data they're receiving and whether it is export controlled or CUI. In those cases, these organizations must be prepared to match or meet the safeguarding requirements of the data set without prior knowledge of what it is before they receive it.

Johnson: It gets tricky. You were just implying that somebody must own this. In the overall process, who owns it?

Bonner: I think there's a misplaced sense of trust that DoD program managers own this, in the sense that they will create a pristine data protection plan for their program that com-

pletely delineates classified and unclassified information in all its forms, document names, and so forth. That's simply not true.

Program managers are saddled with many tasks and responsibilities, and it's unlikely that subcontractors will ever have access to even the original security classification guide used on these contracts. With that in mind, the reality of who needs to own this should be the first organization in the supply chain, the one that acts as its own design authority. Those organizations are best positioned to preserve their own supply chain and to more effectively separate proprietary information from CUI early in the process.

Johnson: Ultimately, it's the designers, the specifiers of the bill of materials for the components and the board, who are the ones on the hook.

Bonner: Absolutely. This becomes a discussion of not just designing the part, but designing the data set, meaning it's determined early on which documents are expected to flow to third parties and which documents are expected to adapt the requiring activity or agencies needs into technical designs and match those with contract clauses, determining the technical rights for those data.

There is a strategic process these OEMs need to follow by which they understand which data sets will be owed to the government as a deliverable, and which ones will not—to create that clear divide between CUI and proprietary information early on, and not allow cross-contamination between those data sets. That's how you preserve your supply chain and avoid situations where you are flowing CUI to suppliers when you don't need to.

Johnson: This conversation is opening my eyes to some of the implications here. Suddenly this becomes a very important step for a design bureau. They will be on the hook. The design bureaus will need to be CMMC certified, won't they?

Bonner: This idea of an independent design function is increasingly common in many industries, whether you're working in the construction trades with architectural and engineering firms or in product design with rapid prototyping; you name it, this is a commonly outsourced function. It is absolutely a leverage point in the entire equation for data rights, data sensitivity, and data management.

Johnson: It most certainly is. What's your recommendation to the electronics manufacturing supply chain, Ryan? How would you recommend they respond right now?

Bonner: Organizations need to avoid false dichotomies where they assume that either CMMC is a go or it's not happening at all. All the government mandated reviews to keep CMMC moving forward, resulting in new contract clauses, are already underway. The rule making is scheduled; it will happen. Rather than waiting for it to surprise you, organizations can begin work now to prepare themselves for that eventuality, regardless of when it fully crystallizes.

All the government mandated reviews to keep CMMC moving forward, resulting in new contract clauses, are already underway.

When we look at how long it takes organizations to implement their safeguarding obligations, I believe that there are some defensive positions, if you will, these organizations can adopt that will make them successful regardless of timelines and outcomes. The first step is to truly know your data ownership posture for

both customer data, whether it's CUI, export controlled, or regulated by other means, and have the same set of knowledge and understanding for your own data as well. That will serve the business regardless of what happens with CMMC or other regulations.

The next posture an organization can adopt is to pursue as many of the NIST 800-171 requirements that are assigned a five-point value in the DoD assessment methodology. Those are the best chances you have of increasing your overall score in case new contract clauses introduce minimum scoring thresholds for a requirement to have all five-point requirements completed to be eligible for award.

From there, organizations should use what they now know about their data and the difficulties of individual controls implementations and execute scope control. Do not apply CUI safeguarding requirements to systems that don't absolutely require it unless there is a clearly identified business benefit. Organizations need to get across their minimum CUI safeguarding finish lines before they can then think about things like optimization and continuous improvement. There's a series of milestones along the way that I would pursue.

Organizations that want to attempt this DIY approach should really use NIST 800-171A as their primary reference document. The assessment objectives for a requirement tell you something about the process to follow and what goals you should be achieving along the way. The assessment objects, those documents or responsibilities or organizational processes described in those lists, should give you a breadcrumb trail as you go where you can confirm that you are indeed generating those proofs in the process. This is where I would recommend almost every organization begin.

Johnson: From your perspective, where do IPC Validation Services fit? Does that process complement CMMC?

Bonner: The IPC-1791 process can serve value in two ways that are evident to me. One, it accustoms the organization to outside validation and makes the assessment and validation of information security measures an integrated part of their overall certification process. Creating that comfort level with being validated by a third party is useful information on security topics.

The other area where it provides value is the IPC-1791 process is integrated with an organization's quality management. Information security programs need to function like quality management programs. Wherever there are parallels being drawn between those two functional areas, that's important and useful.

When I look at the experience IPC has working with these types of industries, the real value that will emerge over time for the 1791 program is taking the generic requirements that are in 800-171 and CMMC and adapting them into something that's well-suited for a more specialized industry. The 1791 process has the potential to provide value by contextualizing what's in CMMC and maybe even assessing and validating against that unique context.

Johnson: Ryan, thank you for the insight.

Bonner: You're very welcome. SMT007

APEX EXPO IPC 2023

MEETINGS & COURSES Jan. 21-26

CONFERENCE & EXHIBITION Jan. 24-26

SAN DIEGO CONVENTION CENTER | CA

ADVANCE IN A NEW ERA

technology

packaging

data analytics

cyber security

automation

networking

Factory of the Future

substrates

innovation

transformation

CALL FOR PARTICIPATION

You asked. We listened. Abstract submission deadline for IPC APEX EXPO 2023 has been extended to Monday, August 8.

IPC is accepting abstracts for technical paper presentations, posters, and professional development courses at IPC APEX EXPO 2023 in San Diego, the premier event for the electronics manufacturing industry!

TECHNICAL TRACKS

- Factory of the Future Implementation
- Enabling Future Technologies
- Meeting Extreme Requirements
- PCB Fabrication and Materials
- Design and Component Technologies
- Quality, Reliability, Test and Inspection
- Assembly Processes
- Electronics Materials
- Conscientious Engineering

ABSTRACTS DUE

MONDAY, **AUGUST 8, 2022**

View more details

Business Email Compromise: The $43 Billion Scam

Editor's note: The FBI released this public service announcement, which was an update and companion piece to Business Email Compromise (PSA I-091019-PSA) posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to December 2021.

Business email compromise/email account compromise (BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

The scam is frequently carried out when an individual compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds.

The scam is not always associated with a transfer-of-funds request. One variation involves compromising legitimate business email accounts and requesting employees' Personally Identifiable Information, Wage and Tax Statement (W-2) forms, or even crypto currency wallets.

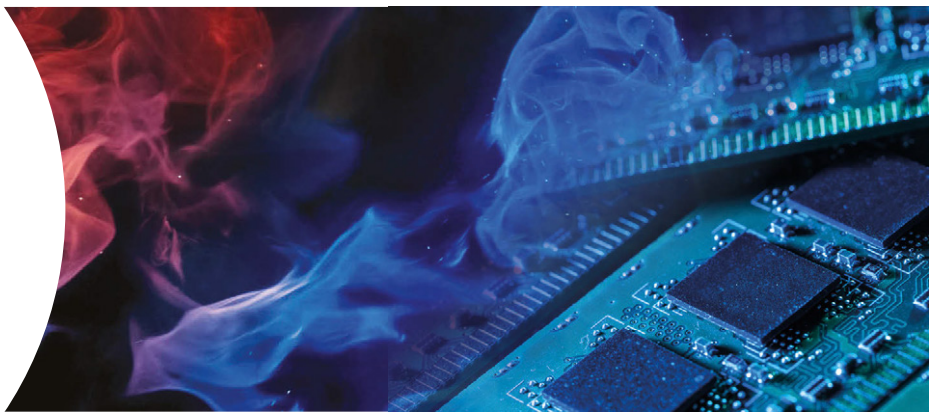
Statistical Data

The BEC/EAC scam continues to grow and evolve, targeting small local businesses to larger corporations, and personal transactions. Between July 2019 and December 2021, there was a 65% increase in identified global exposed losses, meaning the dollar loss that includes both actual and attempted loss in United States dollars. This increase can be partly attributed to the restrictions placed on normal business practices during the COVID-19 pandemic, which caused more workplaces and individuals to conduct routine business virtually.

The BEC scam has been reported in all 50 states and 177 countries, with over 140 coun-

alpha

f(x)



Low Temperature Soldering is a function of design.

It starts with designing an alloy to meet reliability requirements. Next, a chemistry that optimizes how the alloy reflows and solders. And finally, working with the customer to see how PCB design and assembly can optimize performance and reduce costs and defects.

Process Expertise

Mechanical reliability
Reflow optimization
Reduced material cost
Lower energy consumption

Innovative Products

High Reliability Alloys
Solder Paste
Solder Preforms
Cored Wire

Let's get started.

Alpha's low-temperature soldering (LTS) solutions have revolutionized high volume applications, including conversion from Wave to SMT and from SAC alloys to Low Temperature SMT. Let's work together to find the optimal LTS solution for your process.

alphaassembly.com

MacDermid Alpha
ELECTRONICS SOLUTIONS

tries receiving fraudulent transfers. Based on the financial data reported to the IC3 for 2021, banks located in Thailand and Hong Kong were the primary international destinations of fraudulent funds. China, which ranked in the top two destinations in previous years, ranked third in 2021, followed by Mexico and Singapore.

The following BEC/EAC statistics were reported to the FBI IC3 law enforcement and derived from filings with financial institutions between June 2016 and December 2021 (see sidebar).

BEC and Cryptocurrency

The IC3 has received an increased number of BEC complaints involving the use of cryptocurrency. Cryptocurrency is a form of virtual asset that uses cryptography (the use of coded messages to secure communications) to secure financial transactions and is popular among illicit actors due to the high degree of anonymity associated with it and the speed at which transactions occur.

The IC3 tracked two iterations of the BEC scam where cryptocurrency was utilized by criminals. A direct transfer to a cryptocurrency exchange (CE) or a "second hop" transfer to a CE. In both situations, the victim is unaware that the funds are being sent to be converted to cryptocurrency.

Domestic and international incidents: **241,206**
Domestic and international exposed dollar loss: **$43,312,749,946**

The following BEC/EAC statistics were reported in victim complaints to the IC3 between October 2013 and December 2021:

Total U.S. victims: **116,401**
Total U.S. exposed dollar loss: **$14,762,978,290**

Total non-U.S. victims: **5,260**
Total non-U.S. exposed dollar loss: **$1,277,131,099**

The following statistics were reported in victim complaints to the IC3 between June 2016 and December 2021:

Total U.S. financial recipients: **59,324**
Total U.S. financial recipient exposed dollar loss: **$9,153,274,323**

Total non-U.S. financial recipients: **19,731**
Total non-U.S. financial recipient exposed dollar loss: **$7,859,268,158**

Direct transfer: Mirrors the traditional pattern of BEC incidents in the past (Figure 1).

Second hop transfer: Uses victims of other cyber-enabled scams such as extortion, tech

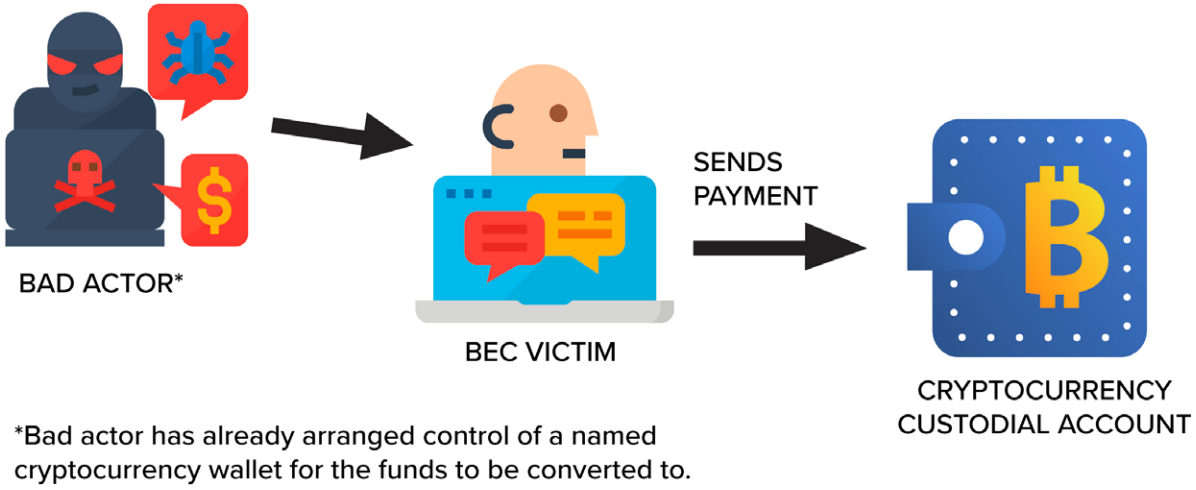


Figure 1: Example of a direct transfer method.

support, and romance scams. Often, these individuals provided copies of identifying documents such as driver's licenses, passports, etc., that are used to open cryptocurrency wallets in their names (Figure 2).

In the past, the use of cryptocurrency was regularly reported in other crime types seen at the IC3 (e.g., tech support, ransomware, employment), however, it was not identified in BEC-specific crimes until 2018. By 2019, reports had increased, culminating in the highest numbers to-date in 2021 with just over $40M in exposed losses. Based on the increasing data received, the IC3 expects this trend to continue growing in the coming years (Figure 3).

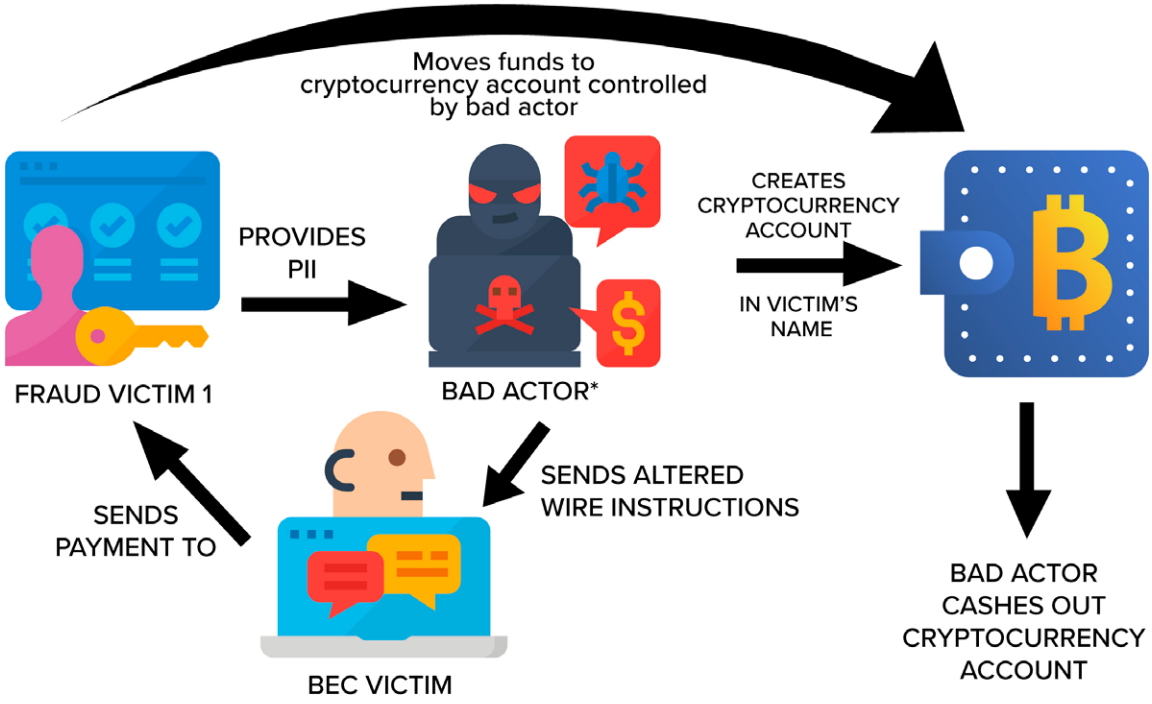


Figure 2: Second hop transfer method.

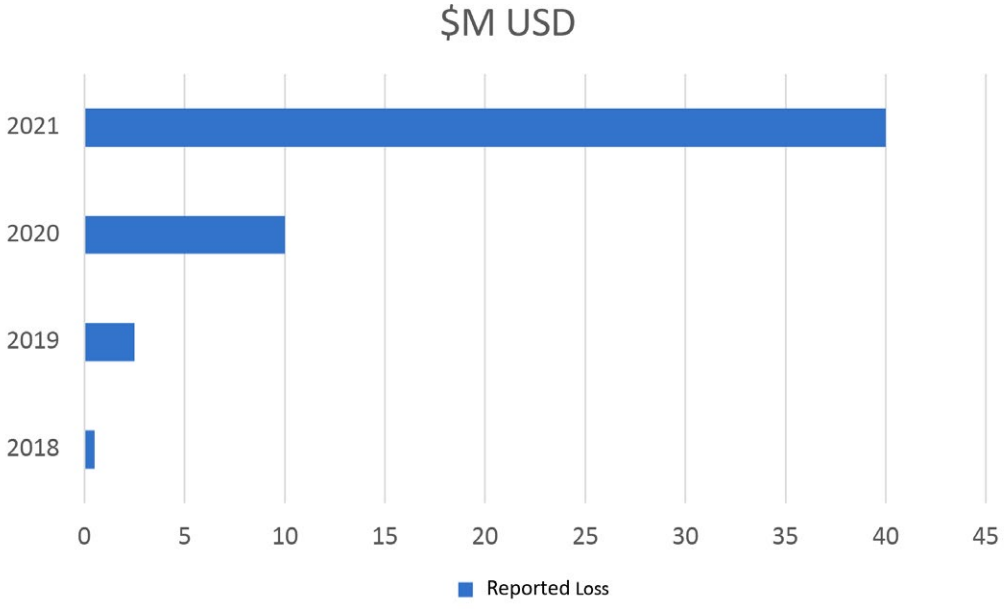


Figure 3: Reported loss associated with BEC/cryptocurrency complaints.

Suggestions for Protection

- Use secondary channels or two-factor authentication to verify requests for changes in account information.
- Ensure the URL in emails is associated with the business/individual it claims to be from.
- Be alert to hyperlinks that may contain misspellings of the actual domain name.
- Refrain from supplying login credentials or PII of any sort via email. Be aware that many emails requesting your personal information may appear to be legitimate.
- Verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring the sender's address appears to match who it is coming from.
- Ensure the settings in employees' computers are enabled to allow full email extensions to be viewed.
- Monitor your personal financial accounts on a regular basis for irregularities, such as missing deposits.

If you discover you are the victim of a fraud incident, immediately contact your financial institution to request a recall of funds. Regardless of the amount lost, file a complaint with www.ic3.gov or, for BEC/EAC victims, BEC.ic3.gov, as soon as possible. **SMT007**

Scientists Create New Method to Kill Cyberattacks in Less Than a Second

A new method that could automatically detect and kill cyberattacks on our laptops, computers, and smart devices in under a second has been created by researchers at Cardiff University.

Using artificial intelligence in a completely novel way, the method has been shown to successfully prevent up to 92% of files on a computer from being corrupted, with it taking just 0.3 seconds on average for a piece of malware to be wiped out.

Using advances in artificial intelligence and machine learning, the new approach, developed in collaboration with Airbus, is based on monitoring and predicting the behaviour of malware as opposed to more traditional antivirus approaches that analyse what a piece of malware looks like.

"Traditional antivirus software will look at the code structure of a piece of malware and say, Yeah, that looks familiar,'" co-author of the study Professor Pete Burnap explains. "But the problem is malware authors will just chop and change the code, so the next day the code looks different and is not detected by the antivirus software. We want to know how a piece of malware behaves so once it starts attacking a system, like opening a port, creating a process, or downloading some data in a particular order, it will leave a fingerprint behind which we can then use to build up a behavioural profile."

By training computers to run simulations on specific pieces of malware, it is possible to make a very quick prediction in less than a second of how the malware will behave further down the line. Once a piece of software is flagged as malicious the next stage is to wipe it out, which is where the new research comes into play.

(Source: Cardiff University)

The Test Connection, Inc.

Leading in Quality Test Engineering Since 1980

Test Solutions & Services for Test Programming, Board Test, Testability In-Circuit, Flying Probe, Functional and Boundary Scan

Fast Turnaround for Board Tests!

ASTER Technologies

TestWay

ITAR Registered and NIST 800-171 Compliant

112 Lakefront Drive, Hunt Valley, MD 21030, USA
Phone: (410) 205-7300 • E-mail: info@ttci.com

www.ttci.com

We have the latest equipment -- What sets us apart is our team!

The Virtual Via Drum

The Big Picture

Feature Column by Mehul Davé, ENTELECHY GLOBAL INC.

"And finally, in the years to come, most human exchange will be virtual rather than physical, consisting not of stuff but the stuff of which dreams are made. Our future business will be conducted in a world made more of verbs than nouns." —John Perry Barlow, 1994

A key to the success of the Roman empire was its extended roadway system. Designed by planners called mensors, and executed by Roman legions, they were transnational, connecting the then-known world across culture and region. They are seen as an infrastructure of empire, expanding economy by trade, knowledge, and security, bringing prolific wealth and new ideas to every corner of Rome's vast territory, and creating a superhighway for defense and conquest. As wonderful as they sound and as much good as they did for antiquity, they were not always safe. Knowing the amount of wealth they carried, the roads were frequented by bandits and criminals[1]. Jesus Christ of Nazareth expanded upon this in the Good Samaritan parable in the gospel of Luke. While a factitious story, the parable is based on a real fear faced by denizens of the ancient world.

Today's internet is the modern version of the *Via Publicae*[2]. It's an apt metaphor. The internet has changed the world for good in many ways, bringing a wealth of knowledge, opportunity, and equality to nearly every corner of the globe. Its value to the global economy, and in effect the end consumer, is priceless. If the internet were to crash, our way of life would be severely affected. However, where we tend to stop short in this metaphor is how our virtual

When you need to know what's hidden in your boards...

...Gen3 gives you the Process Control Tools you need to establish Objective Evidence.

Qualify your material set using SIR and your process control using PICT*

Gen3's AutoSIR2+ and CM Ionic Contamination equipment conforms to all international standards and are the primary tools for this requirement. They are the principle instrument of choice by test laboratories including, NTS, SGS, UL, NPL and others with over 500 users globally.

Do your testing the right way.

Speak to Gen3.

*Process Ionic Contamination Testing

#THEPEOPLEWHOPROTECT

GEN3
PRECISION AS STANDARD

sales@gen3systems.com
+44 (0)12 5252 1500
www.gen3systems.com

assets are just as exposed and available for the taking as the physical assets were on the roads of the ancient world.

In the early 2000s, a gang of criminals unsuccessfully broke into the Millennium Dome in London's South end. A division of Scotland Yard foiled their plans, preventing an estimated $700 million (in today's currency) from being stolen[3]. Eighteen years later, halfway around the world, another heist took place. This time there were no car chases, men in hoods, or canvassing of the "target." The thieves, instead, used a keyboard and mouse to walk away quite literally with over $530 million[4]. No authorities were aware of the impending attack.

The internet has changed the world for good in many ways, bringing a wealth of knowledge, opportunity, and equality to nearly every corner of the globe.

As we reflect on the quasi-prophetic postulate by John Perry, a gut check comes to fruition. We realize that, while our natural understanding of the world is being shaped and reshaped by an intangible digital reality, the lens which colors our perspective still holds fast to safe-deposit boxes, dead bolts, and security cameras.

The world is slowly waking up to and realizing that the greatest store of value in the history of mankind is sitting in the open, as if on the road to Rome, with threat actors drooling at the prospect, and no sign of a Roman legion anywhere near to protect it. Every company, organization, and more than half the global population has their virtual worth caravanning across the digital highway, many of whom are oblivious to the criminals who await just around the bend.

As Roderick Jones[5], a leading security expert and former detective with the Scotland Yard explains, there is no legal offensive capability for today's virtual merchants. You can't hack back, or rather, you shouldn't. It's illegal, and most definitely reckless. Practically speaking, the internet is still in the early days of conceptualization. We are in the Wild West, exploring a new frontier, the law and government catching up to innovation. We must rely entirely on our defensive posture, giving criminals second thought before attempting to raid our businesses, and battling off any attacker that comes after us. Just as important as physical security has been, so goes cyber security.

Take a moment to reflect on your digital caravan and who or what someone could do to take that. Would prospective thieves be staring at a helpless, defenseless walking dollar sign, or a robust, armored wagon with defensive weaponry? Have you put as much thought and resources into your cybersecurity as your physical security? If not, reach out to a cybersecurity professional and get some advice in setting up your digital defenses. **SMT007**

References

1. *Fayûm Towns and Their Papyri*, B.P. Grenfell, A.S. Hunt and D.G. Hogarth, London, 1900 (Egypt Exploration Society, Graeco-Roman Memoirs 3), pp. 259-60.
2. "Internet: A Modern Roman Road System?" The Motley Fool, Dec. 21, 2016.
3. "The Millienium Dome Diamond Heist," The True Crime Edition, July 9, 2021.
4. "$530 million cryptocurrency heist may be biggest ever," CNN Business, Jan. 29, 2018.
5. Rodrerick Jones, CNAS.org.

Mehul J. Davé is CEO and chairman of Entelechy Global Inc. and chairman of Linkage Technologies Inc. To contact Davé or read past columns, click here.

SMTA International

Connect. Learn. Advance.

The Midwest's Largest

ELECTRONICS MANUFACTURING EVENT

Save the Date

Conference:
October 31 - November 3, 2022

Exposition:
November 2 - 3, 2022

Minneapolis, MN, USA

**Co-located with* MD&M MINNEAPOLIS

www.smta.org/smtai

Electronics Industry News and Market Highlights

Strengthening Domestic Chip Research, Design, Manufacturing ▸

The Semiconductor Industry Association convened a productive roundtable discussion between Sen. Mark Warner (D-Va.)—one of the senators tasked with negotiating the U.S. jobs and competitiveness package—and more than a dozen senior executives from SIA member companies.

Worldwide Semiconductor Market Expected to Increase 16.3% in 2022 ▸

The European Semiconductor Industry Association reports on the release of the new semiconductor market forecast generated in May 2022 by the World Semiconductor Trade Statistics.

New IPC Initiative Focuses on E-mobility Quality & Reliability ▸

From battery fires to non-functional charging stations, from dendrites to poor cable connections, electronic system failures have caused massive recalls.

Hitachi High-Tech Launches Dark Field Wafer Defect Inspection System DI2800 ▸

Hitachi High-Tech Corporation announced the launch of the Hitachi Dark Field Wafer Defect Inspection System DI2800, a critical component in any semiconductor manufacturer's metrology capabilities.

Flexible Patch Detects Real-time Changes in Water Temperature ▸

Researchers at Tokyo Tech invented a flexible patch containing carbon nanotubes and stretchable conductors that can fit inside a pipe to detect real-time changes in water temperature or the presence of contaminants.

SEMICON West 2022 Hybrid to Spotlight Sustainability, Smart Technologies, Talent ▸

Sustainability, smart technologies, and workforce development will take center stage at SEMICON West 2022 Hybrid, July 12-14 at the Moscone Center in San Francisco.

SEMI Foundation Awarded $1.5M Grant to Bolster Michigan's Semiconductor Industry Talent Pipeline ▸

SEMI and Michigan Governor Gretchen Whitmer announced with the Michigan Economic Development Corporation that the SEMI Foundation has been awarded $1.5 million in funding to design and develop the SEMI Career and Apprenticeship Network in Michigan.

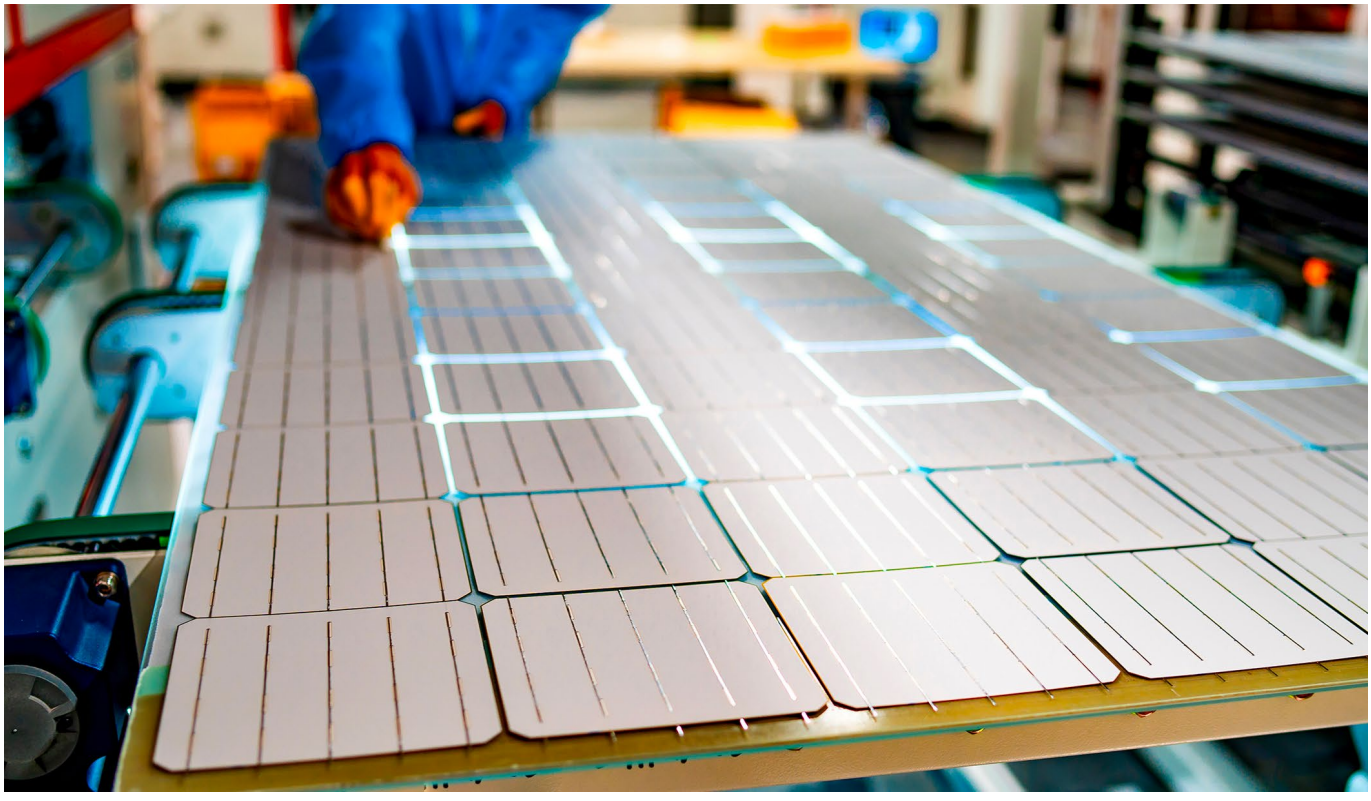
Qualcomm Unveils Next Generation Powerline Communication Device ▸

Qualcomm Technologies is working with virtually all global, leading automakers and their supply base in support of the Combined Charging Systems international standard for charging electric vehicles.

Cadence Design IP Portfolio in TSMC's N5 Process Gains Broad Adoption Among Leading Semiconductor, System Companies ▸

Cadence Design Systems, Inc. announced a wide range of leading semiconductor and system customers have successfully adopted the comprehensive line-up of Cadence® Design IP in TSMC's 5nm process technology.


When your name
means continuous improvement
YOU ARE NEVER SATISFIED
WITH GOOD ENOUGH
KEVIN
KYZEN
Where Science and Care Converge.
LEARN ABOUT OUR NEWEST AQUEOUS CLEANING SOLUTION,
AQUANOX® A4626, TODAY! | KYZENPREMIER.COM
Because KYZEN means innovation and continual improvement, we work 24/7 to research, create and improve the industry's most advanced electronics assembly cleaning solutions and processes. KYZEN.COM
WORLDWIDE ENVIRONMENTALLY RESPONSIBLE CLEANING TECHNOLOGIES



Solder Paste Printing and Optimizations for Interconnecting Back Contact Cells

Article by Narahari Pujari and Krithika PM
MACDERMID ALPHA ELECTRONICS SOLUTIONS

Introduction

The interdigitated back contact (IBC) is one of the methods to achieve rear contact solar cell interconnection. The contact and interconnection via rear side theoretically achieve higher efficiency by moving all the front contact grids to the rear side of the device. This results in all interconnection structures being located behind the cells, which brings two main advantages. First, there is no frontside shading of the cell by the interconnection ribbons, thus eliminating the need for trading off series resistance, losses for shading losses when using larger interconnection ribbons. Second, a more homogeneous looking frontside of the solar module enhances the aesthetics[1]. This combined increased power yield and improved aesthetics make back-contact modules particularly suited for special applications such as vehicle and building integration.

Out of many ways of interconnecting the IBC cells, busbar stringing, which is similar to conventional tabbing and stringing of two-side contacted cells, is the most common method[2]. In this technique, the metallization design of the cell contains multiple parallel-printed busbars distributed over the cell, allowing shorter finger length, and ribbon on busbar soldering. This reduces the resistance losses in the metallization compared to the edge stringing[2]. With the advent in multibar bar (MBB) technology, the width of these busbars is also reduc-

Is Your Current PCB Supplier Pushing Out Lead Times That Are Unthinkable?

APCT Values Being A Partner, Not Just A Supplier

- **Operational Support** to Assure Availability & Required QTA Lead Times
- **Engineering Expertise** to Advise on New & Emerging Technologies
- **Customer Service** "That Is Best In Class"

The Solution Is APCT

APCT
Passion I Commitment I Trust

Work With A Partner, Work With APCT

APCT.com

APCT Santa Clara HQ	APCT Anaheim	APCT Orange County	APCT Wallingford	APCT Global
408.727.6442	714.921.0860	714.993.0270	203.269.3311	203.284.1215

ing and is down to around 300 to 500 microns. The interconnection can be carried out by either ECA (electrically conductive adhesives) or by using direct ribbon/wire. Both materials have created some challenges. The poor peel strength is often the major issue. The uniform IMC (intermetallic layer), which is characteristic of reliable bond strength, is absent with ECA. The metallization paste used in IBC is low-temperature-curing silver paste. The paste is fired at lower temperature around 500°C or less and deposited on silicon cell. In addition to that, the height of the paste is only about 8-12 micron. Because of this, silver leaching during interconnection is commonly observed (Figure 1). The metallization just comes off during interconnection at high temperature. If used, solder wire, cold solder joints, and solder diffusion through the cell are the major issues. Poor adhesion between cell and ECA, and interconnecting wire, high contact resistance are other common problems. Accordingly, when a circuit or conductive layer or interconnection is formed on a substrate using such conventional pastes, damage to the substrate or failure in reliability of the device may occur. Further, when ECA is used, silver in the ECA is expensive and appears on various restricted chemicals lists due its short supply.

We present solder paste as an alternative material for interconnecting back contact cells. Solder paste offers many advantages over ECA and traditional tabbing methods, such as[3]:

- Formation of reliable joints
- Can be dispensed or printed
- Stable viscosity and higher shelf life compared to ECA
- Low voiding
- Better thermal and electrical conductivity compared to ECA
- Resistant to moisture
- Lower cost than ECA

In this work, we investigated application of low temperature lead-free solder paste in printing and optimizing interconnection joints in IBC cells. A design of experiment (DOE) was performed to evaluate effect of reflow conditions in attaining complete wetting and reliable bond strength on metallization paste and ribbon or wire. We also studied the role of the solder paste on the electrical and mechanical properties of soldered cells. Study included evaluation of printing, voiding, microstructure, reflowing properties of solder paste for making it suitable for interconnecting IBC cells in existing automated machines or modified tabbing machines.

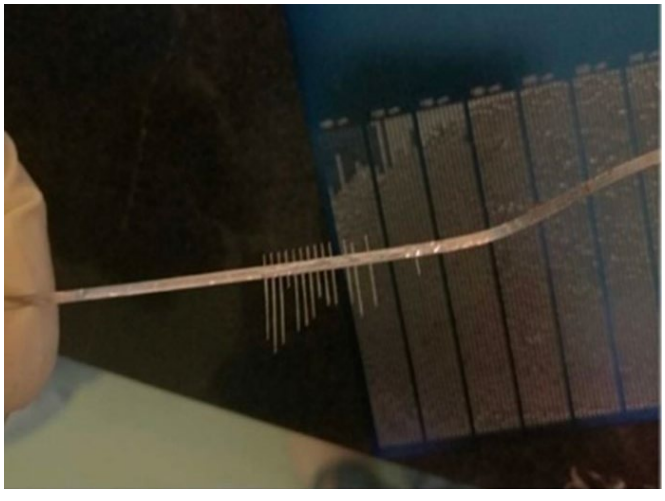


Figure 1: Silver busbar leaching from the cell.

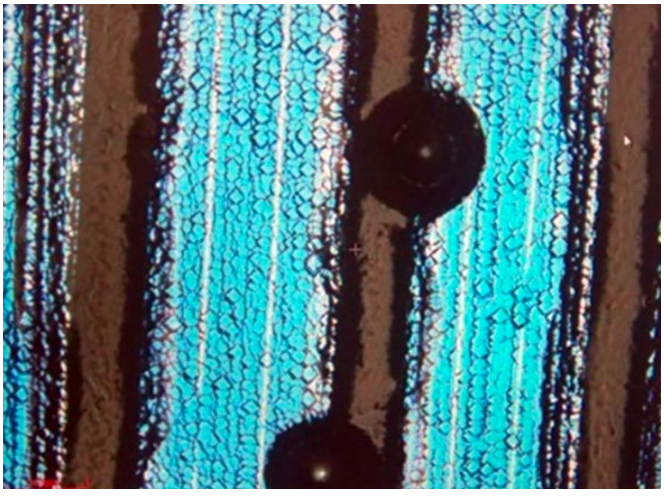


Figure 2: Solder ball formation in IBC interconnection when processing parameters are not optimized.

Table 1: Solder paste properties

Solder Paste	Alloy	Powder type	Liquidus °C	Yield Strength MPa	Reflow Temp °C
OM550	HRL1 (non eutectic)	T4	152	37.5	175

Experimental

Low temperature lead-free solder paste was used in this study. This is non-eutectic tin-bismuth paste, namely, OM550® HRL1 from Macdermid Alpha (Table 1).

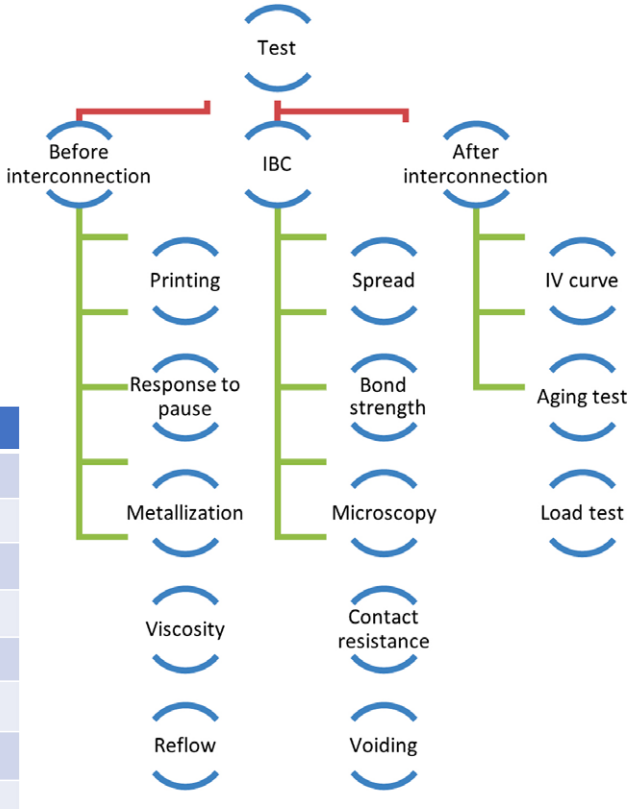
N-type monocrystalline M6-IBC cells were used. Efficiency was 23% with thickness 170±20 micron. Scheme 1 shows the complete test matrix. Typically, print optimization and reflow optimization were carried out to evaluate a paste's wetting characteristics on the metallization pad. During interconnection, reflow optimization work was thoroughly conducted, and bond strength and other reliability aspects were investigated. In the last set, once the minipanels were prepared, they were analyzed for IV-curve values, EL (electroluminescence) and accelerated aging tests. Test conditions are given in Table 1 and Scheme 1. The idea of doing the DOE was to optimize printing as well as reflow optimization for solder paste to achieve good wetting on the metallization pad and form reliable bond with the silver paste as well as ribbon or wire.

Table 2: Solder paste IBC assemblies: Process parameters

Attributes	Value
Paste	OM-550 HRL1 (lead-free)
Stencil	3 mil through cut
Soak	100–130°C
Conveyor belt speed	22–35 inch/min
Peak temperature	160–240°C
Heat	Conduction, 7 zone Electrovert Omniflo oven
Cell	IBC cell (M6, 23% efficiency from DS new energy)
Soldering Side	Back
Ribbon	Sn-Pb ribbon, 1 x 0.2 mm/0.4 x 0.2 mm wire

Results and Discussion

ALPHA® OM550 HRL1 has a melting point significantly lower than standard SAC305 (tin-silver-copper) alloy. A peak temperature of only 165°C is also equivalent to most ECA curing temperature. This reduces energy consumption in the PV application process and stress build-up on the cells. The solder paste is lead-free which means there is no environmental hazard and it can be snap reflowed like ECAs. The alloy is specifically designed to improve reliability of the solder joint. In a back contact cell, due to moderate adhesion between silicon and silver paste, soldering is difficult and standard soldering fluxes may not



Scheme 1: Schematic of back-side soldering of structured ribbon using solder paste.

work. To strengthen and maintain the electrical and mechanical properties of the interconnections, including the bulk of the material and the solder-pad interfaces, solder paste is best suited. Low temperature solder joints, especially with this alloy, can withstand cyclic contractions and expansions that can deteriorate and weaken the solder joints.

As a first part, 3- and 6-mil stencils were fabricated for the experiments. These are through-cut stencils made with stainless steel. A DEK03Xi printing machine was used to do automated printing. Similarly, paste could also be dispensed on the cell just before the assembly. The paste volume was optimized by printing/dispensing paste pads from 300 to 900 microns on the 1-mm and 300-micron wide busbar (Figure 3a). Solder paste, if not processed properly, can give several problems[4]:

- Solder ball formation
- Silver metallization leaching
- Solder diffusion through the metallization paste
- Non-wetting on the pads

Figure 2 shows typical solder ball formation after reflowing. This is a common problem in the semiconductor industry. At reflow, different sizes of spherical solder particles are formed. These solder balls lead to short circuits and leakage current in circuitry[4]. Although there are many potential causes for this defect, stencil aperture, metallization quality, fast ramp rate, wetting of a paste, and reflow profile characteristic are the dominant ones. The silver leaching and solder ball formation defects were minimized in our study by doing the printing and reflowing optimization.

From 300–900-micron range tested, 600 micron or 1:0.6 aperture yielded sufficient solder volume and spread (Figure 4a). Solder paste spread well across the busbar and there was no slump formation. Wetting was also acceptable under optimized conditions. We observed that 3 mil of roughly dispensed solder paste at a height of ~65 micron reduces to around 55 microns after the reflow (Figure 4a) at 600-micron aperture. This is just enough paste on the busbar to avoid any stress or cracking during IBC assembly. Unlike ECA, solder paste has better wetting and spread. Paste coalesces after reflowing and yields volume transfer efficiency of over 80% (not shown) at varying printing speed. This proves that print-

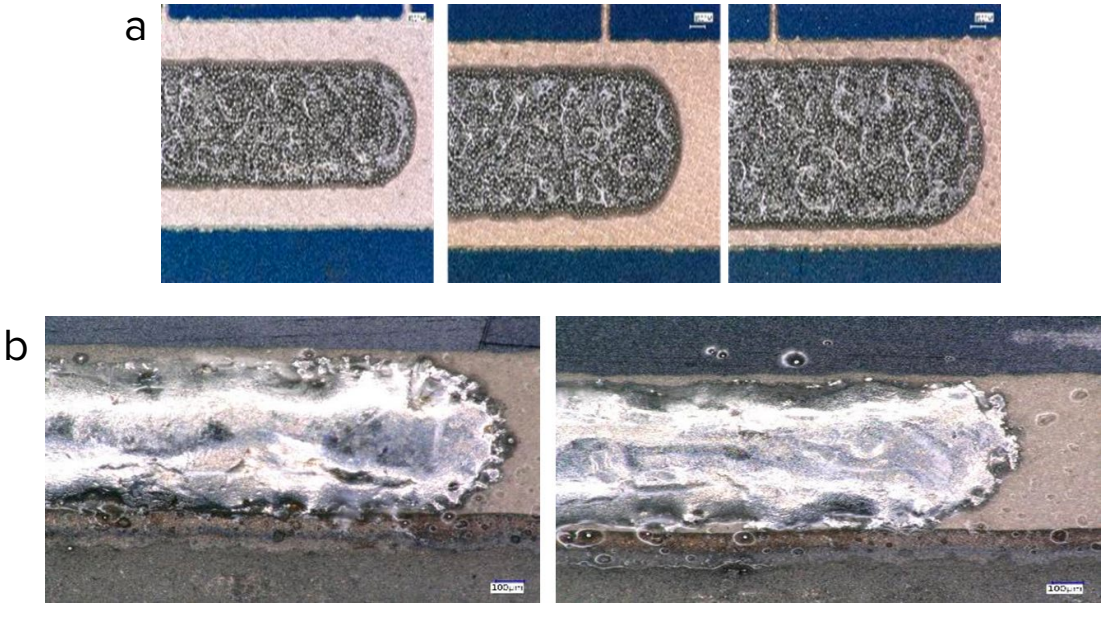
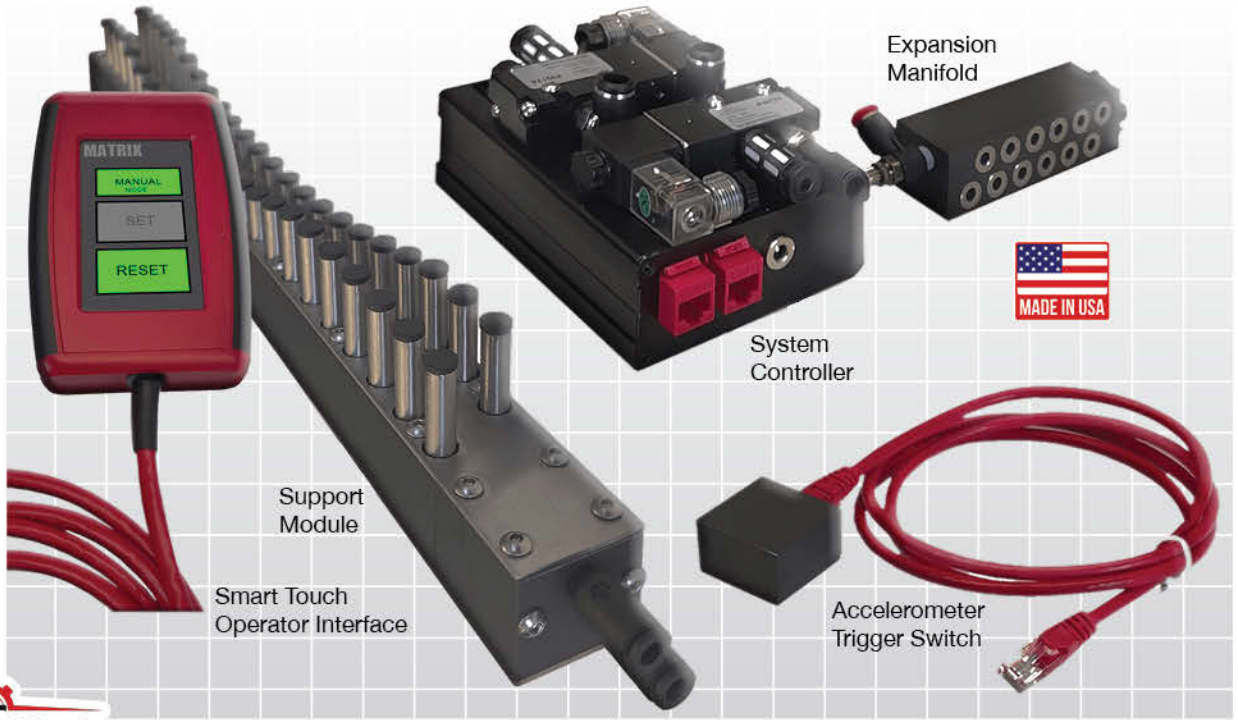


Figure 3: a) Paste printed through 300–900 micron pads on the busbar; b) Solder paste spread well across the busbar and there was no slump formation.

SMT Tooling

Scan Area



AR Experience

Scan Area

Faster. Easier. Better.

From the inventor & designer of **Grid-lok** and **Quik-Tool** comes **Matrix** SMT Tooling solution

Why Matrix™?

- Installs on the Screenprinter and Chip Shooters in minutes
- Sets up any PCB automatically
- Provides more PCB support than any other method available
- Lowest cost in the industry

Scan QR code below to download the PSA app. Use that to scan AR Areas (Scan Areas indicated with AR Experience)

GET IT ON Google Play

Download on the App Store

PSA PRODUCTION SYSTEMS AUTOMATION

ing characteristics of the pastes is consistent and in high throughput manufacturing, paste is likely to produce defect-free printing.

The solder paste has excellent stability and metal content remains almost unchanged even after 12 hours of continuous printing[3]. The binder and solvent system are formulated in such a way that viscosity buildup is restricted, and paste can be printed for hours without cleaning the stencil[3]. In addition, the high print definition and speed works in favor of paste. Even at higher printing speed, the observed transfer efficiency with solder paste was over 90%. Generally, ECAs do not have stencil/screen life of more than four hours. After that, the viscosity of ECA increases rapidly and often insufficient transfer and screen pore clogging is observed. Material waste is also a big problem with ECA. ECA additionally needs higher pressure to print and through-cut stencils do not work with ECA.

A response to pause (RTP) study was conducted which is measured by the difference in volume of solder paste deposition as a function of number of prints and pause time. This is to mimic a typical production scenario. A large variation in the print volume after the pause is not acceptable as this causes end-of-line defects such as shorts and opens. A good solder paste shows less variation in the volume of the prints after pause. However, another may show large variation and an overall decreasing trend in volume. Figure 4b shows the comparison between ECA and OM550 HRL1 paste. As can be seen, the solder paste volume is constant and its transfer efficiency is around 80% over a period of test. ECA, on the other hand, does not pass RTP test due to viscosity build-up.

Once the printing parameters are optimized, it is the reflow profile that plays a crucial role in making the interconnection. Low soak and ramp profile were evaluated (Figure 5). In addition, conveyor speed and its effect on solder ball formation were also evaluated.

This solder paste could be reflowed at low temperature. The conveyor speed of 28 inch/min gave acceptable wetting on the metallization pad (not shown). With too slow or too fast conveyor speed, solder ball formation was observed. A slow steady ramp (1°C/sec) permits moisture and solvents to evaporate gradually prior to rosin/resin softening. Hot slump is minimized. Pastes with long stencil life and tack time generally require a slow ramp so environmentally stable solvents can evaporate it and allows the solvent to gradually evaporate. Study of different peak temperatures gave a good understanding of the paste's performance in wetting metallization pads. As can be seen in Figure 6, a 190°C peak reflow tem-

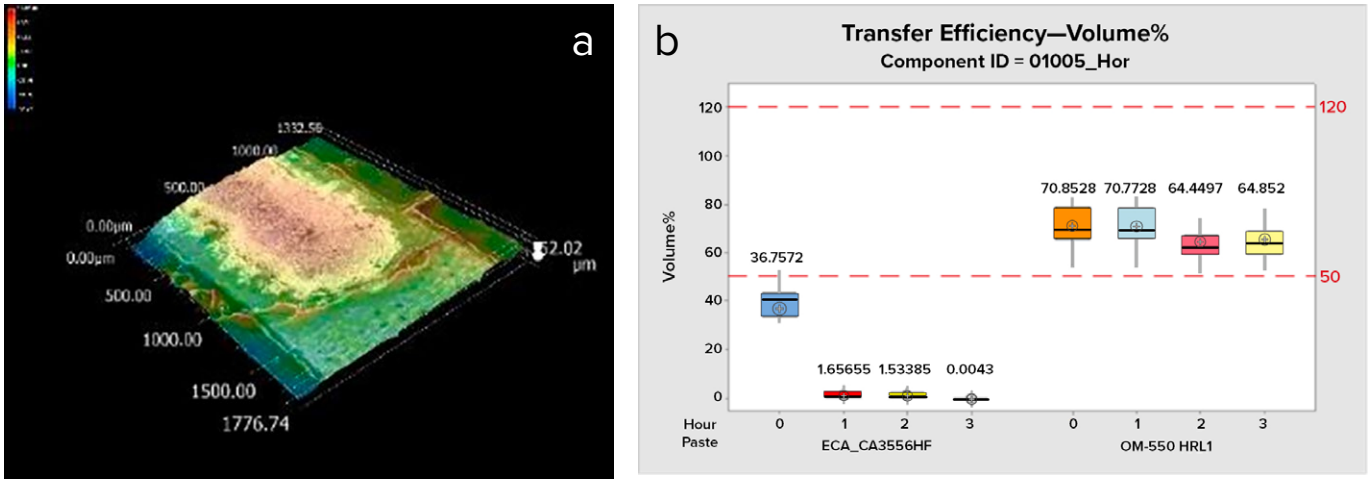


Figure 4: a) Solder spread across the busbar with 600-micron aperture; b) Response to pause capabilities of ECA and solder paste.

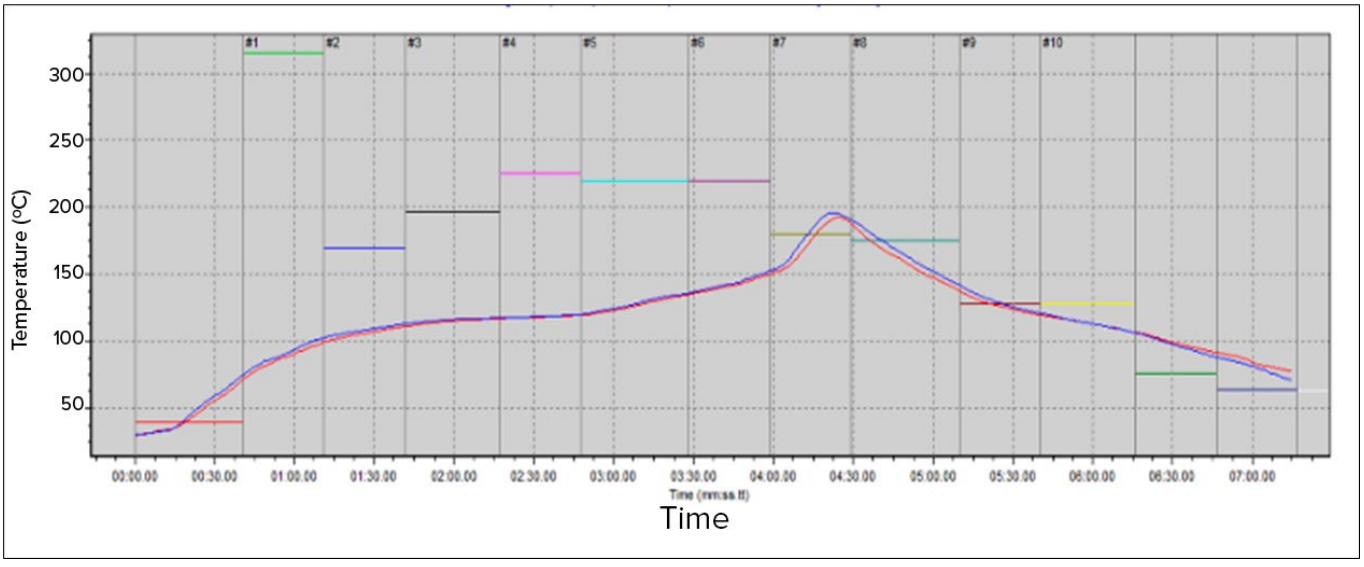


Figure 5: Typical low soak profile for OM-550 HRL1 paste.

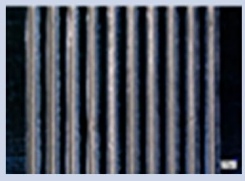
Paste	160°C Peak	190°C Peak	210°C Peak	240°C Peak
OM-550 HRL1 Paste				
Results	Moderate spread	Good spread	Good spread	Overheat

Figure 6: Effect of peak reflow temperature on solder paste wetting on metallization pad.

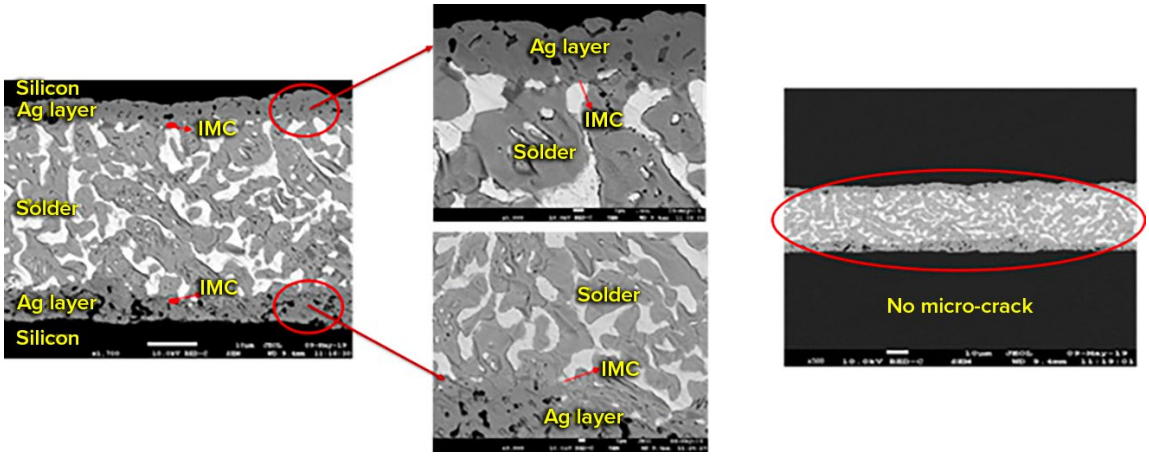


Figure 7: SEM cross-sectional analysis of solder joints formed, OM-550.

perature gives complete wetting and no silver leaching. Too low or too high a temperature usually results in forming solder balls or silver leaching.

Microscopic analysis revealed complete wetting, continuous IMC (intermetallic compounds) formation and no micro-cracking with solder paste (Figure 7). The wetting

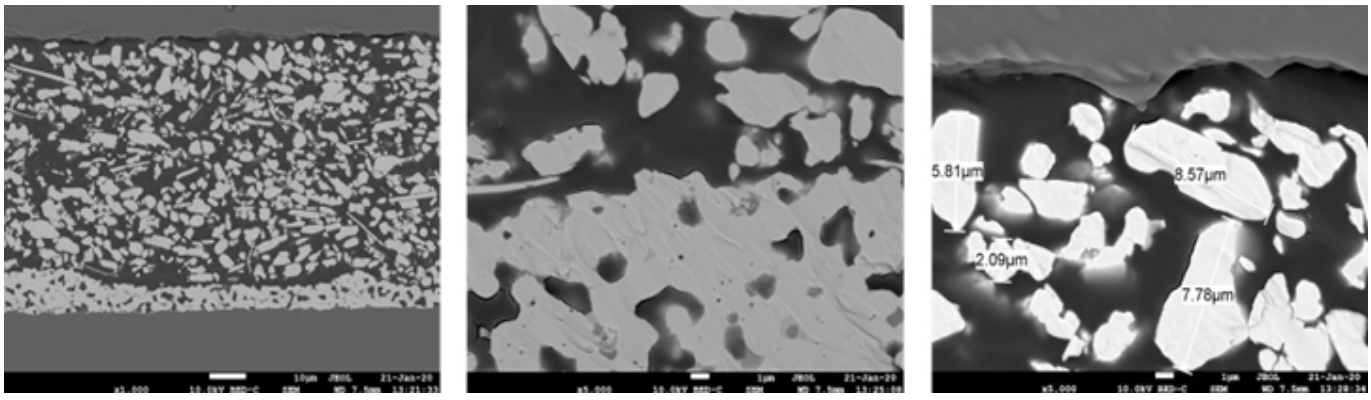


Figure 8: Silver flaking observed with joints formed with ECA.

angle was found to be 13°C. No silver leaching observed. ECA, on the other hand, does not form any IMC and there is pseudo-bonding between silver pad and silver flakes in the ECA[3] (Figure 8). The quality of the joints was also analyzed by X-ray. This determines voiding in the joints. The solder paste spread well over the busbar and no solder balls were observed. The voiding was less than 10% (Figure 9) in each assembly which means there is good thermal contact between the joining surfaces. Many voids reduce the solder joint reliability. Voids also reduce the thermal conductivity of the solder joints, and can cause solder bridges and solder transfer between neighboring solder joints during the reflow soldering process. In small solder joints, voids can significantly reduce their current carrying capacity.

Soldered cells were analyzed for peel strength at 180°C using an Imada peel tester. The results are presented in Figure 10. Paste gives acceptable peel strength, much above the required 1 N/mm as per DIN EN 50461. The bond strength between paste and silver metallization pad was assessed by die shear strength. The average gram force was about 294 gF. This is excellent bonding without any kind silver leaching. Fracture surface analysis (Figure 10) done at different peak reflow conditions showed that, at 190°C and 210°C peak, the maximum peel strength and nice cohesive bond failure can be achieved.

Laminated minipanels were exposed to climatic testing, conforming to IEC 61215, at 1000 h of damp heat (DH) and 200 temperature cycles (200 TC). Power measurements

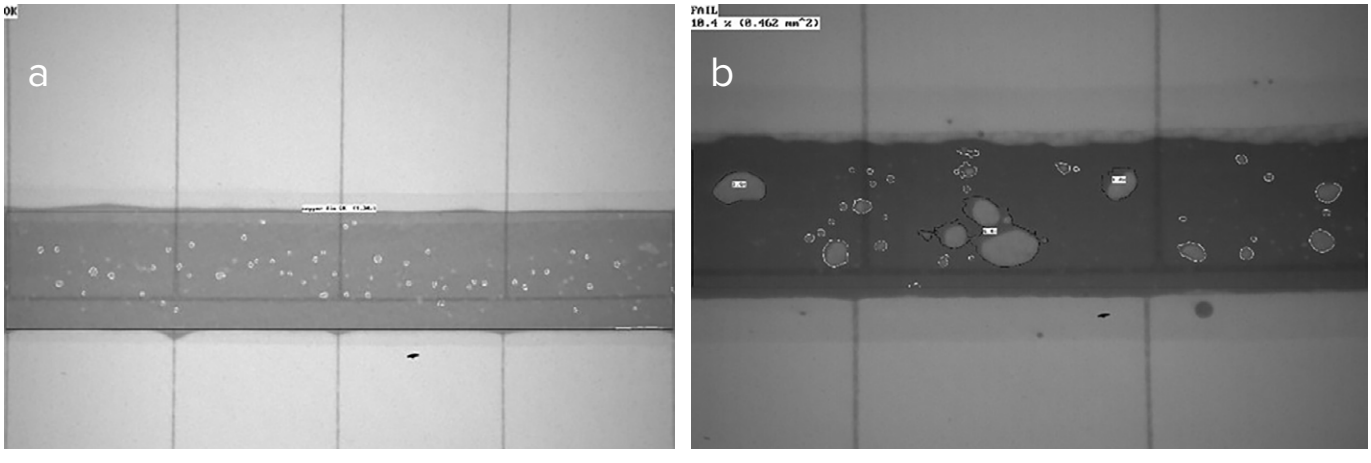


Figure 9: X-ray analysis evaluating voiding in joints of ECA and OM-550; <10% voids observed for both the pastes.

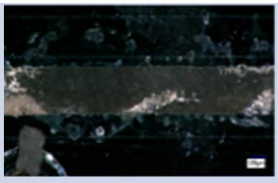
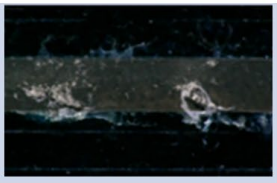
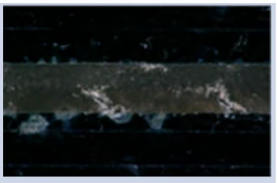
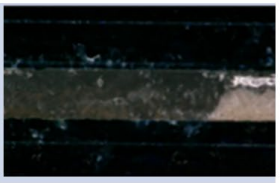
Paste	160°C Peak	190°C Peak	210°C Peak	240°C Peak
Fractured surface				
Fractured ribbon				
Peel strength	3.07 N/mm	4.1 N/mm	4.2 N/mm	1.2 N/mm

Figure 10: Peel test result of R276 and OM-550 HRL1 assembled soldered cells.

and electroluminescence imaging (EL) were performed before and after the tests. No degradation in module performance or other functional properties was noted (Figure 11). EL analysis also shows no evidence of cracking or other defects for both the pastes (Figure 12)—the maximum power (P_{max}) loss permissible according to IEC 61215 is ±5% after the test. None of the samples reached this value. The maximum change in P_{max} was less than 1%

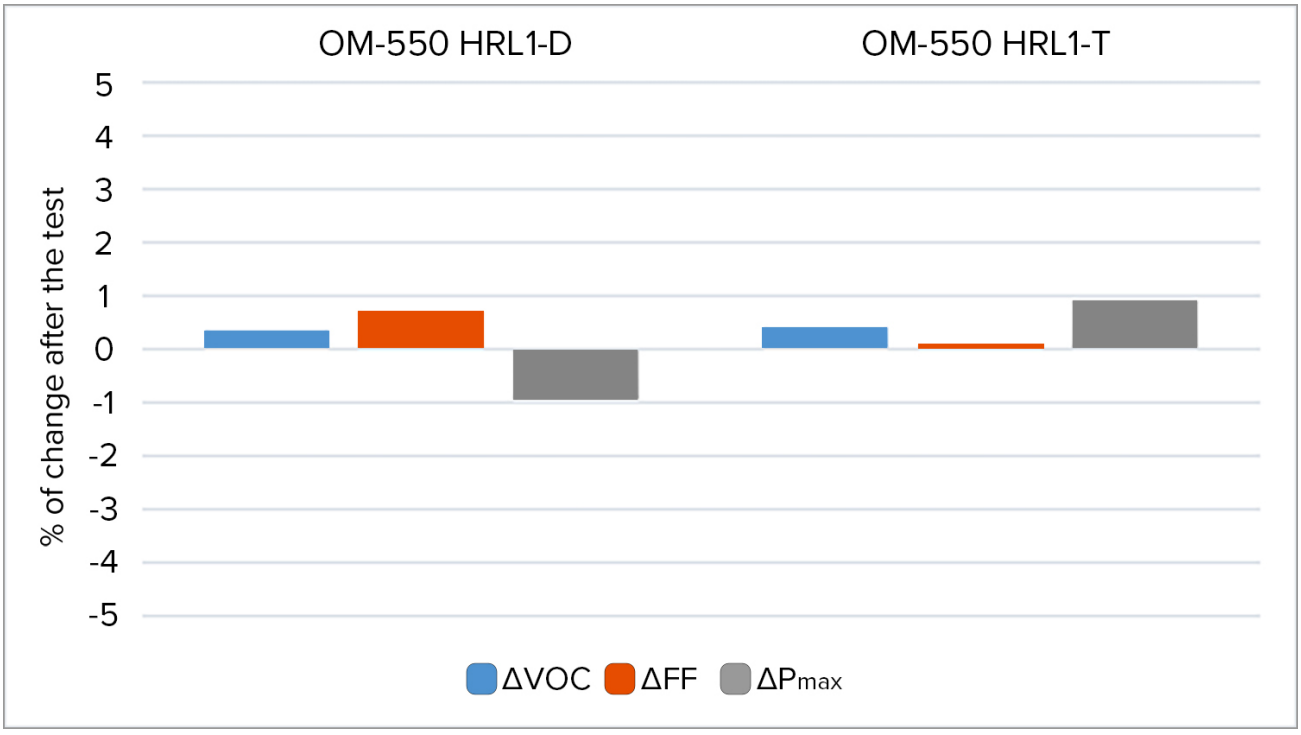


Figure 11: Damp heat and thermal cycling results of OM550 HRL1 assembled minipanels. D: 1000 h damp heat test. T: 200 cycles thermal cycling test.

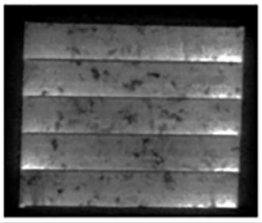
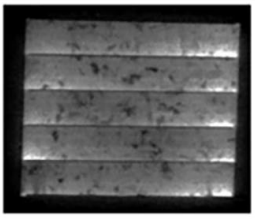
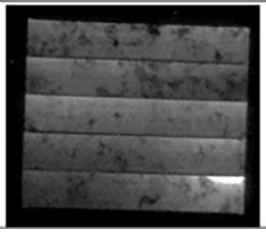
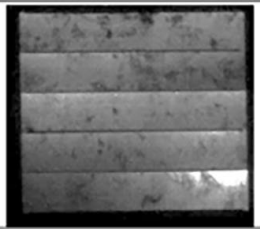
Solder paste	1000 hours	2000 Hours
ECA		
OM-550 HRL1		

Figure 12: Electroluminescence analysis for ECA and OM-550, up to 2,000 hours of damp heat studies.

in both damp heat and thermal cycling tests. These results demonstrate that OM550 HRL1 paste is resistant to oxidation and is resistant to changing weathering conditions. These results further confirm that the standard tin-lead and lead-free low-temperature-alloy paste can be used for interconnecting IBC cells. The paste can withstand the expansion and compression forces produced during thermal cycling.

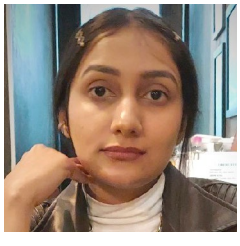
Conclusion

We report low temperature lead-free solder paste for interconnecting IBC cells. We found an acceptable wettability and printability of this paste. The paste shows excellent stability, longer stencil life, and consistent transfer efficiency. A seven-zone reflow oven was used for the study to analyze and evaluate solder paste performance. OM-550 paste with 190°C to 210°C peak temperature slow ramp profile and conveyor speed (28 inches/minute) yields reliable bond strength. Solder joints were strong with peel strength more than 2 N/mm and voiding less than 10%, indicating bonds have better contacts and complete wetting has happened. Paste could be fast reflowed and laminated with EVA. The modules assembled using this paste pass thermal cycling and damp heat reliability testing according to IEC 61215. Based on these results we conclude that the solder paste can be used to make IBC cell interconnection and other advanced interconnection assemblies. **SMT007**

References

1. "Back-contact solar cells: a review," by E. Van Kerschaver, G. Beaucarne, Prog Photovolt Res Appl. 2006; 14(2):107-123.
2. "Three-dimensional multi-ribbon interconnection for back-contact solar cells," by R. Van Dyck, T. Borgers, J. Govaerts, J. Poortmans, and A.W. Van Vuure, Prog Photovolt Res Appl, 29(5), pp.507-515.
3. "Lead-free low temperature solder pastes for shingling interconnection," by N.S. Pujari, Krithika PM, P. Vishwanath, S. Sarkar, and C. Bilgrien, 37th European Photovoltaic Solar Energy Conference and Exhibition, Lisbon, Portugal, 2020, pp. 29-32.
4. "Stencil printing of solder paste for fine-pitch surface mount assembly," by J.R. Morris, and T. Wojcik, IEEE Transactions on components, hybrids, and manufacturing technology, 1991, 14(3), pp.560-566.

Narahari Pujari is senior global technology manager, PV and applied materials, at MacDermid Alpha Electronics Solutions.



Krithika PM is a research scientist at MacDermid Alpha Electronics Solutions.

IPC BUILD ELECTRONICS BETTER

IPC — PROVIDING THE STANDARDS YOU **NEED FOR OPERATIONAL EXCELLENCE**

Stay ahead of the curve with resources to enhance your work, help train your staff and support your company's strategic planning efforts.

- Industry standards on design, board fabrication, and assembly
- IPC certification programs
- Information on Solutions
  - IPC-CFX
  - Factory of the Future

Learn more: Meet Your Standards | IPC International, Inc.

MilAero007 Highlights

NASA Supports Small Business Research to Power Future Exploration ▸

NASA has selected hundreds of small businesses and dozens of research institutions to develop technology to help drive the future of space exploration, ranging from novel sensors and electronics to new types of software and cutting-edge materials.

Industry Groups Urge U.S. Congress to Fix Weaknesses in Electronics Supply Chain ▸

Three top industry organizations this week urged U.S. Congress to support legislation that would address challenges confronting the U.S. electronics supply chain.

IPC Training Course: PCB Design for Military, Aerospace Applications ▸

This course addresses specific challenges encountered in military and aerospace applications, including the effects of vibration, shock, radiation, and altitude, extended operating temperature range, and other design considerations for high reliability applications.

Calumet Students Take First Place in 'Michigan Girls Future Flight Challenge' ▸

Two Upper Peninsula girls recently took the Michigan aerospace industry by storm. CLK Washington Middle School students Jordan Hicks and Kristen Ylitalo outperformed more than 20 teams throughout the state in the "Michigan Girls Future Flight Challenge," hosted by the Women of Aerospace Industry Association of Michigan.

Sypris Wins Electronic Warfare and Communications Program ▸

Sypris Electronics, LLC, a subsidiary of Sypris Solutions, Inc., announced that it has recently received a follow-on multimillion-dollar contract award from a U.S. global defense contractor to manufacture advanced integrated electronic warfare and communications avionics system modules.

Prototron Circuits Upgrades Capabilities with Two PHI Lamination Presses ▸

Dave Ryder, president of Prototron Circuits, announced that his company has increased their lamination capabilities by adding two PHI 4 Opening Lamination Presses, one of which is a vacuum press with cool-down capability.

Deutsche Telekom, Inmarsat Collaborate with Tampnet to Strengthen European Aviation Network Connectivity ▸

Deutsche Telekom and Inmarsat have boosted the capacity of their award-winning European Aviation Network inflight broadband solution by collaborating with Tampnet, a global provider of high capacity, low latency and reliable connectivity to offshore installations, mobile rigs, and vessels.

FTG Circuits Fredericksburg Requalifies for IPC-1791 QML ▸

Firan Technology Group Corporation announced that IPC's Validation Services Program has awarded requalification for IPC-1791, Trusted Electronics Fabricator Requirements Qualified Manufacturers Listing (QML) to FTG Circuits Fredericksburg, Virginia.

www.prototron.com

Serious About Speed

For over 30 years Prototron Circuits has led the pack when it comes to providing quality circuit boards FAST.

Be it Class 3, AS9100, ITAR or MIL-PRF-31032, Prototron has the speed you need.

Prototron Circuits

America's **Board Source**

Balancing Talent and Procurement Challenges

Interview by Nolan Johnson
I-CONNECT007

Ron Preston, vice president of supply chain at Green Circuits, outlines the company's specific challenges with high-mix work. While the company excels at turning around boards in just a few days, difficulties in supply chain, materials, and staffing remain ever-present. What is to be done and how is Green Circuits working its way through these issues? The answers might surprise you.

Nolan Johnson: Ron, we're investigating the challenges of high density, and while we expected pick-and-place to be one of the challenges, we've heard a lot about unreliable consistency for component packaging and feeder technology, especially for the smaller components in combination with high-density boards. Do those two challenges line up with what you see?

Ron Preston: We're dealing with a lot of quick turns and small, short runs. One of our problems is obviously with the supply being a challenge. We're getting broker buys and going wherever we can to find parts. We don't have the normal source of supply that you would expect. A year or two ago we would place orders with franchise distributors, and packaging would be very consistent. That's not so much the case now.

Johnson: When it gets down to the manufacturing floor, you still have to get the boards put together and the components placed in the proper orientation regardless of what they were packaged in or how they're oriented. In a short run environment, that adds to the challenge because there's proportionally more setup that goes on. How do you respond to those challenges?

Free Trial

INTELLIGENT, DYNAMIC SCHEDULING FOR PCB ASSEMBLY

Utilize existing production resources and improve yield

Before investing in costly new equipment, manufacturers need to evaluate whether they can better utilize their existing production infrastructure to improve yield. Dynamic, real-time scheduling solutions can optimize line planning and capacity, helping meet deadlines and increase production without major investments in new infrastructure.

www.siemens.com/OpcenterSchedulingSMT

SIEMENS

Preston: It's very reactionary for us. We average about 150 customers a quarter. Now, multiply that times the number of SKUs or assemblies. Furthermore, those same 150 are not quarter over quarter. We have maybe close to 750 customers in our backlog right now. So, when you talk about the complexity and the variability, it changes quite a bit month over month, build over build, day over day. When we're changing over lines, we must be nimble.

Johnson: As this work ebbs and flows, how do you respond? Is there potential in the current situation to start looking at the processes differently to be nimbler without a spike in labor hours?

Preston: That's a good question. It does vary. It can be very labor-intensive depending on the type of packaging that we're getting. One particular customer will literally bring us a bag full of parts, which requires a new level of work.

Johnson: You sort them out piece by piece, don't you?

Preston: Yes, and you must figure out the polarity. Speaking of that, we recently had a case with a franchise part from a broker. The part was good, but it was marked wrong from the manufacturer. You don't see that every day. We must pay closer attention and be more cognizant of what we get in and what goes on the green board.

Johnson: Have you found that you need additional checkpoints to catch these sorts of things?

Preston: Yes, for a couple of the really critical applications. We have a couple of customers with extremely expensive boards where we can't afford to find issues at a later stage. The challenge is that we just don't have the resources. Talent is the other shortage. We may want to add another incoming inspection

Ron Preston

or in-line checkpoint but getting the talent to fill those roles is not easy.

Johnson: Does that shine more light on mechanization, automation, or additional sensors on the line?

Preston: Yes, but consider that 70% of what we do is quick turn. Once all the parts are here, customers want their boards in five days, and they may have given me an additional five days to get the parts here. Those 10 days really don't allow me a lot of the programming time, or the dock control checks available to conventional processes. Our quick-turn side of the business runs with nimble production.

Johnson: Does the challenge of finding qualified talent to be on the shop floor, while also needing to do more inspection right now, thanks to the less predictable supply chain, start to tip the scale toward investing in automation? Sounds to me like you're not quite there yet.

Preston: My COO is doing the ROI on that to see if we are really that deficient on labor vs. the payback of automation.

MS2 can reduce your lead-free and leaded bar solder purchases by up to 80%

How much can you save?

Calculate your savings with just 3 easy inputs:

Choose your alloy

Production hours/day

Wave machines

Calculate your savings

PK METAL

+1 (323) 585-5058 www.pkaymetal.com

Johnson: When it comes to doing high-density board placement and that sort of work, what are your greatest challenges?

Preston: To be honest with you, the factory itself runs extremely smoothly. We have the gear set up identically line by line so we could put jobs on any line. The real challenge is getting all the material onsite, auditing it, and then issuing to the floor. Once it's issued, everything usually runs very smoothly.

We do a pretty good job on the programming. We're able to do some of that setup magic before the parts are issued. Stencils are ready, along with everything else, even though I have only five days. We check and recheck, do the first article setup; everything is done and ready to roll. But materials are still a challenge.

The real challenge is getting all the material onsite, auditing it, and then issuing to the floor. Once it's issued, everything usually runs very smoothly.

Johnson: What about feeder technology? We're hearing this area could certainly use some improvement, especially when you start talking about the very small components. What's your take on that?

Preston: It is somewhat dated technology. We could use an upgrade as a potential benefit long term; that will help us in the long run, changing out that technology and the feeders, the barcoding and scanning placements, for the manual parts of the setup.

Johnson: Speaking of the long run, let's look ahead two years with Green Circuits doing high density work. What are the one or two key things that you would like to see change to make the job easier for that?

Preston: For the company or for my role?

Johnson: For the company, for doing that kind of work.

Preston: I've worked at Tier 1 for six years, and then at a midsize EMS player for nine, and now, at Green Circuits. I've seen the range of expertise and I can say that, at the end of the day, the large production houses crank out the widgets all day long. They have the big hammer to beat up the suppliers, and they have all the machines. But when you say, "Hey, make this board for me and do it in five days," everything just shuts down. They don't know what to do. It clogs up their system.

At Green Circuits, we're the opposite. We're extremely nimble; we're doing that all day long. But you tell us to build something six months from now and we're not sure how to do that. So, we're the opposite here.

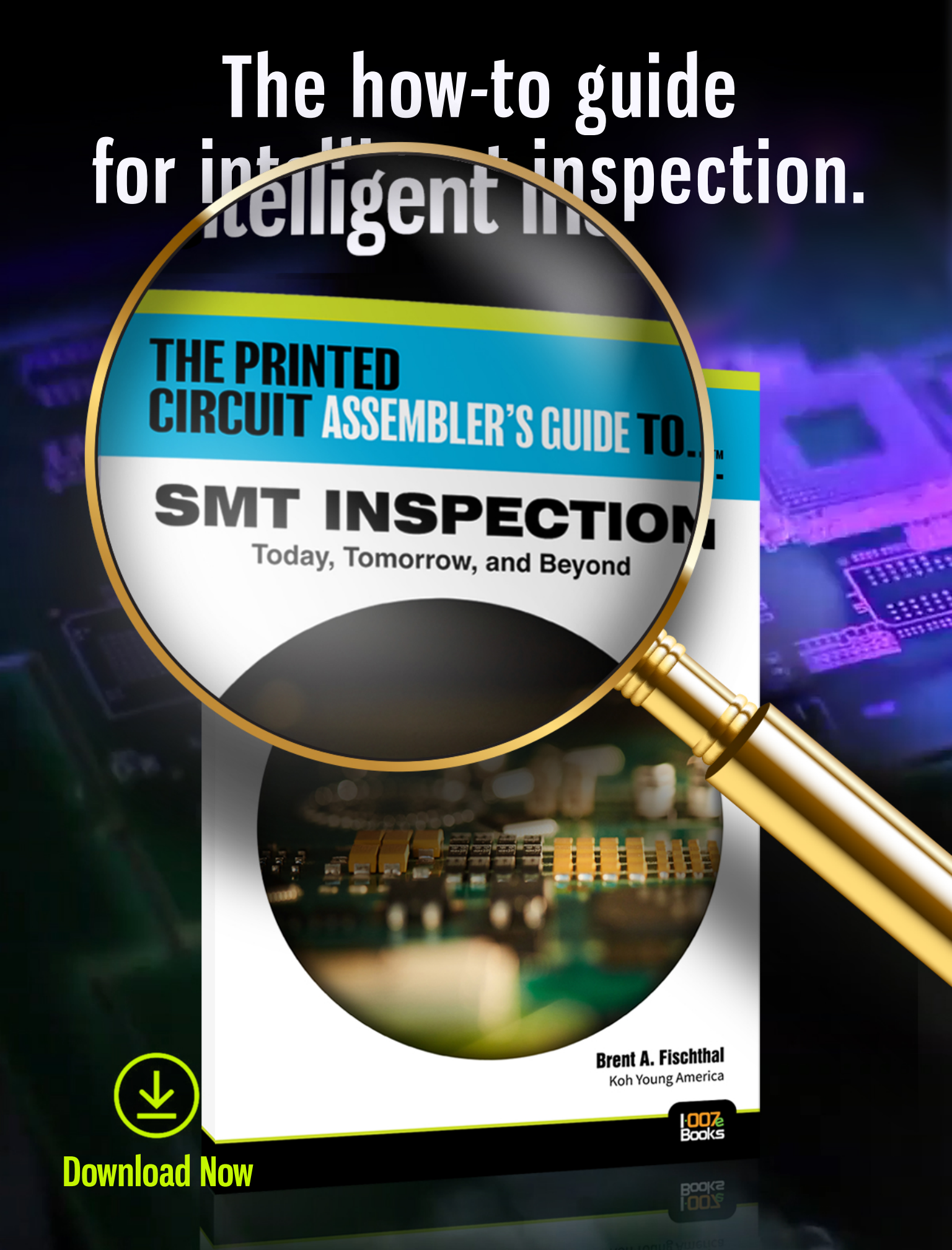
Our ability is in maintaining our secret recipe for doing things quickly, efficiently, and with high quality standards at a reasonable cost, while also expanding our production and box build business.

For us the goal is to have the systems and tools; that's what we're looking at now. We just started the due diligence phase for what we need to do. What are those tools and systems that will allow me to be more efficient and predictable for both quick turn and production?

Johnson: That's a great answer. Thanks for that, Ron.

Preston: All right. Great talking with you. SMT007

The how-to guide for int[illegible]elligent ins[illegible]pection.



Download Now

Supplier Highlights

Maggie Benson's Journey: Take Your Assembly Skills to the Next Level ▸

In this month's column, two of Ivy Benson's young employees respond to Maggie's challenge to improve their assembly knowledge and skills. Does it have the desired effect?

GEN3 Provides the Solution for PCB Assembly for Stewart Technology ▸

Gen3 supplies two Nordson Cerno 300.1S Selective Soldering Systems at Stewart Technology's production facility in Tweedbank, Galashiels, Scotland.

Yamaha Names Kamil Stasiak Product Marketing Manager for SMT Section ▸

Yamaha Motor Europe SMT Section has appointed Kamil Stasiak as product marketing manager to promote the complete portfolio of inline surface-mount assembly equipment and solutions including software applications to enhance productivity.

The Mannifest: Resourceful Solutions During Nationwide Shortages ▸

As supply chain issues and chip shortages continue plaguing the world, companies are still struggling to get SMT components. A variety of solutions have risen to combat these struggles.

PVA Receives Patent for New Optical Bonding Method ▸

PVA, a global supplier of automated dispensing and coating equipment, is pleased to announce that it received a new patent in Japan for "optical bonding machine having cure in place and visual feedback."

Saki Corporation Launches Next-generation 3D AOI System ▸

Saki Corporation has developed the new 3Di series of high-speed, high-precision, next-generation in-line 3D AOI systems for complex inspection of high-density PCBs and boards with a combination of very small and tall components.

SMarTsol Technologies Opens Nordson TEST & INSPECTION Lab in Mexico ▸

SMarTsol Technologies, a technical services and equipment provider for Mexico and the US, announced that it has opened its new Nordson TEST & INSPECTION Lab at its demo center in Guadalajara, Jalisco, México.

Pro-Active Engineering Accelerates Growth with SIPLACE TX Line from ASM ▸

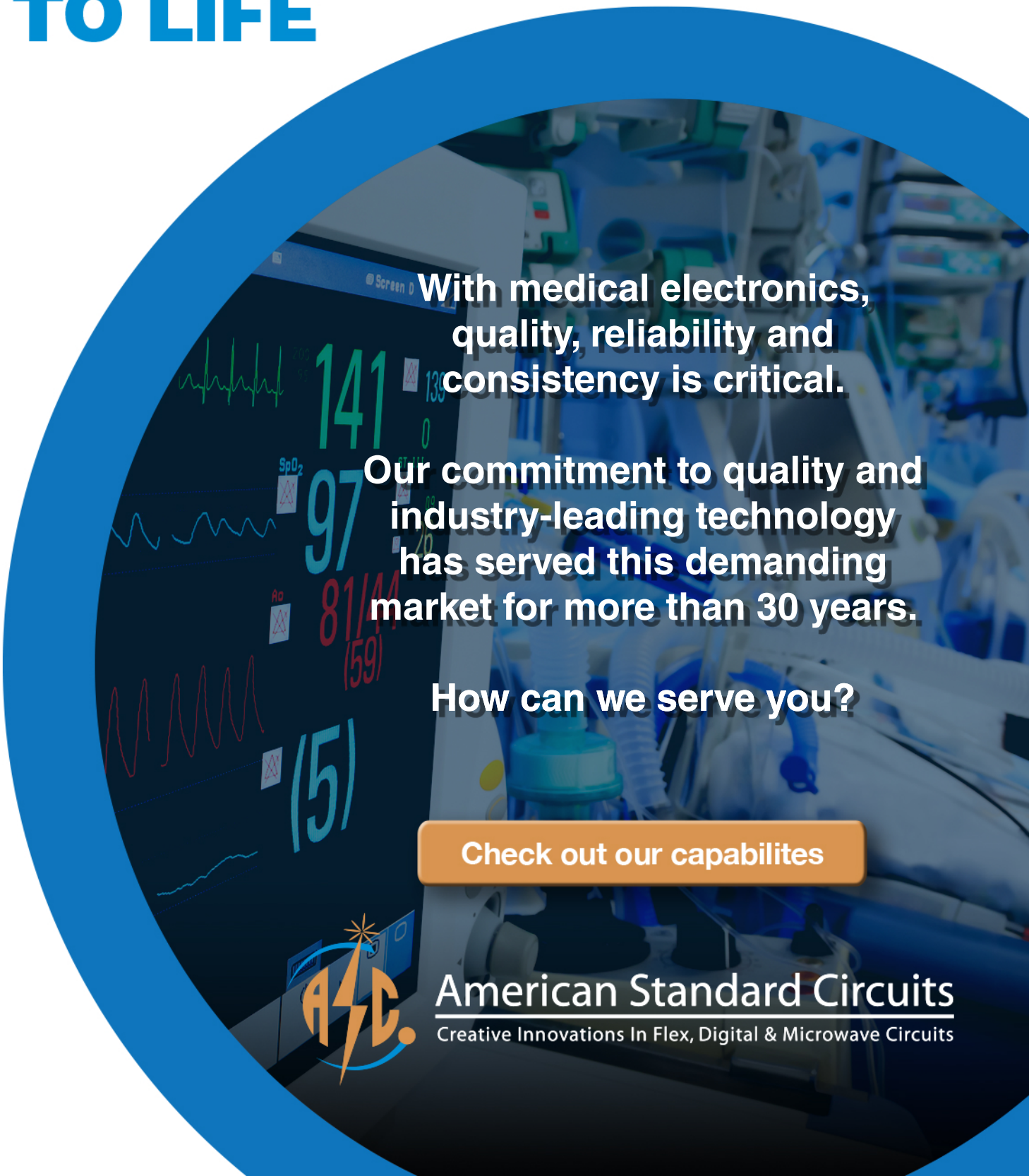
ASM Assembly Systems (ASM) announced that Pro-Active Engineering, Inc. has integrated an ASM high-speed line, which includes a DEK NeoHorizon screen printer and three SIPLACE TX placement platforms.

Electrolube's UL94V-0 Approved Alternative to 3M Novec 2702 Electronic Grade Coating ▸

Electrolube has formulated a conformal coating specifically to resolve a number of issues experienced by a specific user of surface modifier materials. The product now just been awarded UL94V-0 approval, further advancing the proposition.

asc-i.com

WE BRING MEDICAL ELECTRONICS TO LIFE



Opening New Opportunities in Mexico

One World, One Industry

by Guest Columnist David Hernandez, IPC

IPC and WHMA have long supported the electronics assembly and wire harness manufacturing industries in Mexico, but recent regional growth coupled with supply chain disruptions necessitated a closer relationship. Lorena Villanueva, the new director of IPC Mexico, will be based in Mexico City and her presence will help IPC provide better support, training, and engagement with Mexico-based companies and personnel.

Lorena has more than 15 years of experience in client relationship management, strategic planning, and project management for companies such as Genpact, GMAC, American Express, GE, and Lucent Technologies. She is a certified Six Sigma Black Belt and holds a master's degree in economics.

Lorena Villanueva

Lorena and I have reviewed each of the 130+ IPC and WHMA members operating 315 manufacturing facilities in Mexico. More than 4,000 IPC certifications have been earned by workers in Mexico, facilitated through our partner certification centers in 12 locations throughout Mexico. The National Statistical Directory of Economic Units (DENUE) in Mexico estimates there are 481 electronics manufacturing sites in Mexico and IPC strives to play a role in each one, including the facilities not yet built.

BLACKFOX
Premier Training & Certification

Experience the Blackfox Difference!

Premier IPC Training & Certification

- High quality training and customer service
- Offering 6 certification programs at 6 locations and online
  - *Colorado, Arizona, Guadalajara & Queretaro, Mexico, Malaysia and Singapore*
- Military Veterans Advanced Manufacturing Program
- IPC/WHMA-A-620 Space Addendum for trainers and specialists
- Online store supporting the training industry

CLICK FOR COURSE SCHEDULE

For more information contact us at
888.837.9959 or sharonm@blackfox.com

www.blackfox.com

The impact of global events on supply chains has opened more opportunities in Mexico. OEMs are expanding the number of suppliers they use, and Mexico has proven it can produce assemblies for verticals like automotive, medical devices, aerospace, and communication equipment.

As shifting supply chains move to Mexico, the industry needs more trained workers. IPC has always offered IPC standards and certification exams in Spanish, but in 2021 we launched two operator training courses in Spanish to help meet this need. Lorena and I discussed IPC's commitment to supporting and growing our Spanish-speaking membership. When she accepted the position, she told me that IPC creating education courses in Spanish was a deciding factor.

Another exciting event is scheduled for September 27–29. IPC and WHMA are producing the M-EXPO Wire Processing Technology show in Ciudad Juarez just across the border from El Paso, Texas. Leading companies in the wire and cable harness assembly industry are exhibiting and we are working to build a series of educational workshops like those at our upcoming Electrical Wire Processing Technology Expo (EWPTE) show in Milwaukee, Wisconsin. IPC/WHMA is also providing an instructor-led training session for wire harness operators to help local facilities train effectively. IPC and WHMA are proud to produce M-EXPO and believe it is important for the industry to hold these shows in the regions where the work takes place.

The executive teams at IPC and WHMA are thrilled to have Lorena join our team. Her commitment to excellence has been illustrated throughout her career and we cannot wait to see her success with IPC/WHMA. If you have operations in Mexico or anywhere in Latin America, feel free to reach out directly to LorenaVillanueva@ipc.org and start the conversation in English or Spanish. **SMT007**

For additional information, visit https://mexico.ipc.org/, or email us at mexico@ipc.org.

Guest columnist **Dave Hernandez** is vice president of IPC Education. To read past One World, One Industry columns by John Mitchell, click here.This column originally appeared in the June 2022 issue of *PCB007 Magazine*.

Lean Digital Thread:

The Secure Digital Thread

By Zac Elliott

Securing intellectual property has become a priority for manufacturers, and recent reports from the U.S. and EU governments highlight the risks and direction for securing the supply chain. In February, the U.S. Department of Homeland Security published an assessment of supply chains supporting electronics manufacturing[1]. Following closely in March, Europol released the 2022 Intellectual Property Crime Threat Assessment report[2], bringing attention to the risks counterfeit electronic components pose to supply chains. Then in April, the direction for the U.S. Department of Defense Cybersecurity Maturity Model (CMMC) program became clearer as NIST released a draft of Special Publication 800-82[3], which serves as the framework for securing operational technology within the defense contractor network. Let's look at some of these recent publications and how they affect manufacturers.

Intellectual Property Security

The CMMC program is an initiative to improve information security within the U.S. defense contractor network. The program has been ongoing for a few years, but last November, the Department of Defense announced plans to clarify and enhance the program in an update dubbed CMMC 2.0. The goal of the update is to make CMMC a program that can be implemented by the entire defense industrial base, including smaller subcontractors that may not have expertise in cybersecurity.

Three key components of the CMMC program are:

- Contracts with the U.S. Department of Defense that include clauses requiring security for controlled unclassified information (CUI)
- Security frameworks and guidelines built on NIST standards and publications
- Third-party auditing of the CMMC controls implemented at manufacturers

Securing information is not necessarily a new topic for most manufacturers. Security controls around information technology (IT) processes are generally in place for most publicly traded companies to adhere to financial regulations, and ongoing concerns about malware and hacks lead most organizations to keep their network secure from external threats. Even smaller companies can leverage outsourced IT contractors and cloud-based systems to have a well-managed, secure infrastructure. Of course, exploits occur, companies get hacked, and intellectual property is stolen, but not because we do not know how to secure IT systems. It is usually the case that some generally accepted control was not implemented, or social engineering was used to exploit the organization.

What may be a new challenge for manufacturers is the requirement in CMMC 2.0 to secure the operational technology (OT)—the machines and processes building the products. Typically, these machines are on segregated "unmanaged" networks that fly under the radar of traditional IT security. But with CMMC 2.0, manufacturers will need to implement similar security controls in this relatively uncontrolled environment.

To read this entire column, click here.

Breaking Down the Math

Maggie Benson's Journey

by Dr. Ronald C. Lasky, INDIUM CORPORATION

Editor's note: Indium Corporation's Ron Lasky continues this series of columns about Maggie Benson, a fictional character, to demonstrate continuous improvement and education in SMT assembly. Andy and Sue work at Maggie's company, Ivy Benson Electronics.

Andy Connors and Sue March were heading to their favorite pizza parlor before pre-calculus, their first class at Valley Tech.

"I really enjoyed dinner at your house on Sunday," Andy said. "Your parents were so welcoming to me. I'm touched."

"Well, I've never had a boyfriend until now and they're happy for me," Sue replied.

"I, I, I'm your boyfriend?" Andy stuttered.

"Unless, you don't want to be," Sue responded.

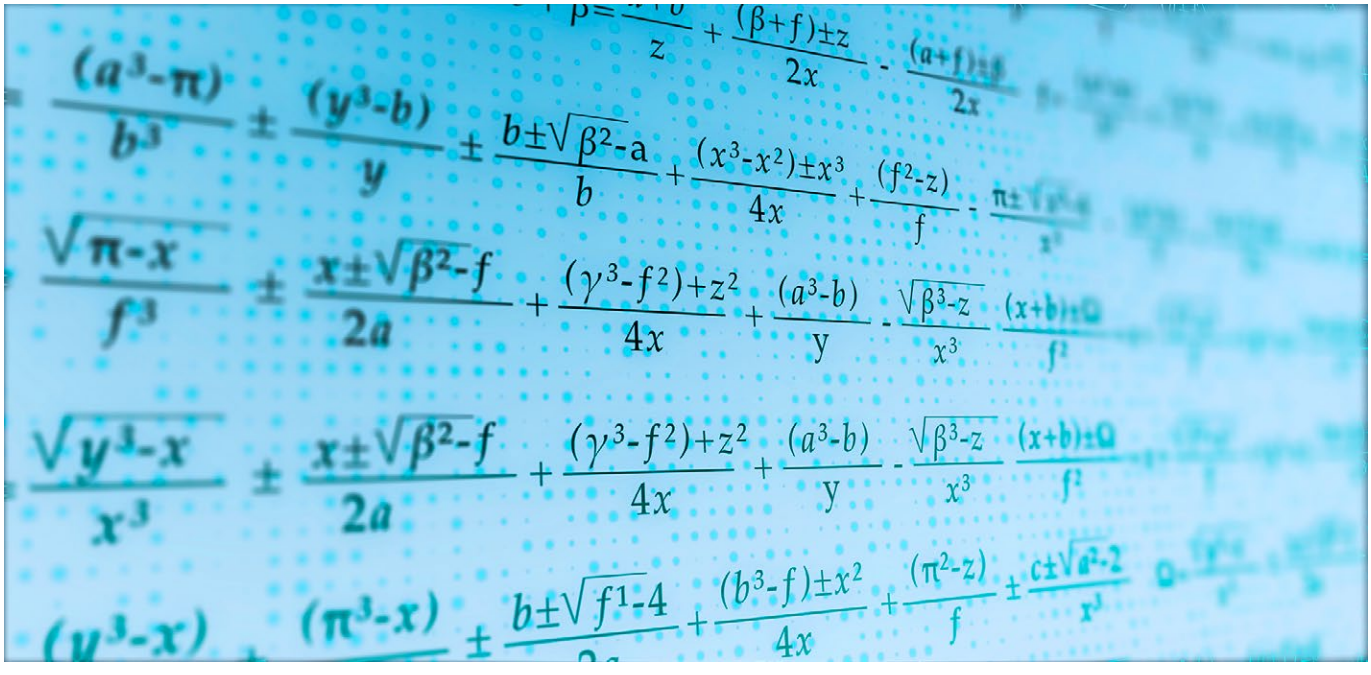
Andy knew instinctively that maybe words were not needed. He stood up, went to Sue, pulled her up, and gave her a long hug. An observant customer might have noticed a tear forming in his eye.

"Okay, Romeo, let's discuss what we expect in tonight's class," Sue teased.

"Well, the syllabus says we will review algebra and exponents. I'm comfortable with algebra, but not so much with exponents," Andy said with a sigh.

"Let's try one," Sue suggested. "If $X^3 + X^5 = 64$, what is X?"

"Well," Andy said, "as you taught me a few days ago, the exponents are added, so it is $X^8 = 64$. So, what times itself 8 times equals 64? Is it 2?" He knew he was right. After a few more examples, which Andy got right, they left for class.



PREMIER GLOBAL SUPPLIER to the **MEDICAL DEVICE INDUSTRY**

FLEXIBLE CIRCUITS | EMS/ASSEMBLY | CONTRACT MANUFACTURING

Industry leading Flex Design Support

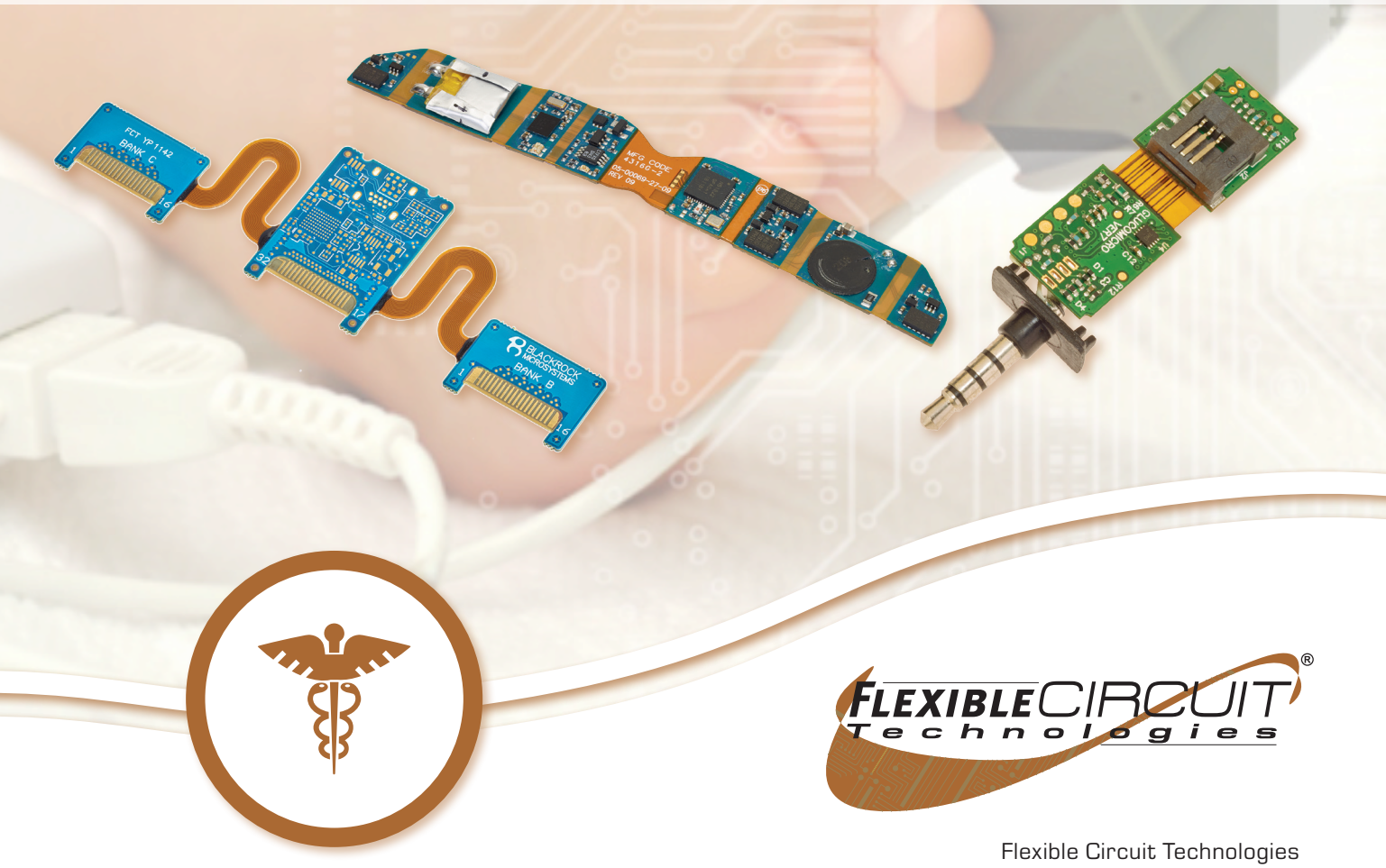
Flexible Circuits, Rigid Flex, Flexible Heaters Membrane Switches, Plastic Moldings

Specialized EMS/Assembly Services

Product Module to Complete Product Box Builds

ISO 13485 – FDA registered Box Builds

EXPLORE the POSSIBILITIES!



FLEXIBLE CIRCUIT Technologies®

Flexible Circuit Technologies
9850 51st Ave. N. | Plymouth, MN 55442
www.flexiblecircuit.com | +1-763-545-3333

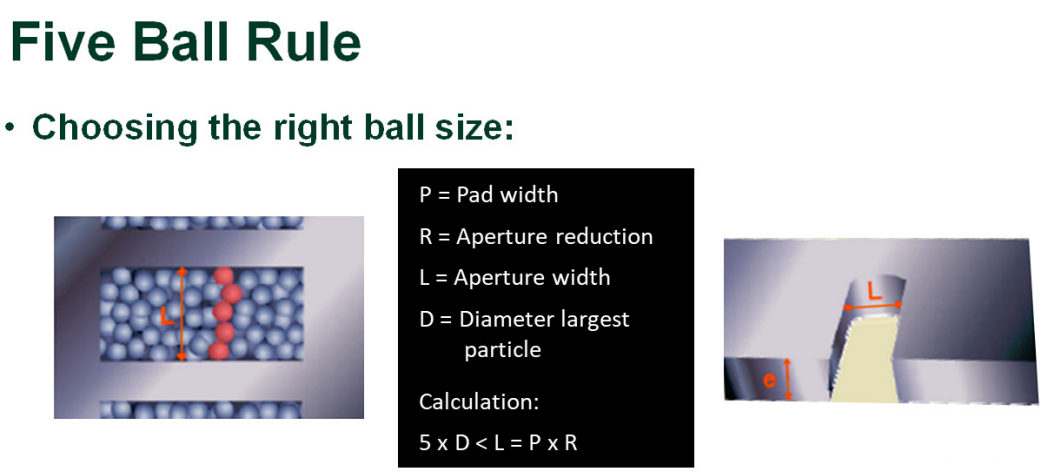


Figure 1: The Five Ball Rule is important in stencil design.

Later, both Sue and Andy felt the first class was easy and Sue suggested they get some ice cream then discuss what they learned in Chuck Tower's stencil printing class.

"I thought the stencil design discussion was quite straightforward," Sue began.

Andy's heart sunk a bit. Everything was straightforward to Sue. But this was one of his strengths.

"Well, for one thing, the 'Five Ball Rule' was clear," Andy began. "At least five 'balls' of the solder paste to fit within the width of the stencil aperture is easy to understand."

"I found out we typically use solder pastes with Type 3 or Type 4 solder powder[1] so we can determine the range of solder ball sizes and the largest solder ball from the Solder Powder Type Chart," Sue commented.

"And the aspect ratio, the width of the aperture divided by the height, being greater than 1.5, is now clear to me, but the area ratio..." Andy said.

"I agree, it's a little more complex. It is the area of the aperture opening divided by the area of the sidewalls. To make the solder paste stick to the printed wiring board pads more than the side walls of the aperture, the ratio must be greater than 0.66," Sue explained.

Powder Size

TYPE	MESH	LARGEST PARTICLE (mils)
1	-100/+200	5.90
2	-200/+325	2.96
3	-325/+500	1.77
3	-325/+500	1.77
4	-400/+500	1.50
5	-500/+635	0.99
6	-635	0.79

Figure 2: The Solder Powder Size Chart is helpful to determine if a stencil aperture obeys the Five Ball Rule.

"You know, I think I finally get it," Andy said.

"But can we derive what the area ratio is?" challenged Sue.

Andy proceeded to draw a circular aperture. "Well, we know the area of the opening is pi times the radius squared," he said.

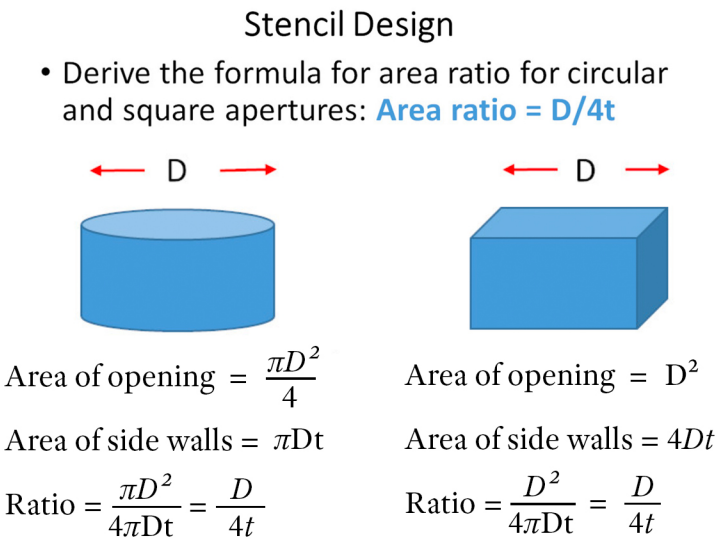


Figure 3: The area ratio is important in round or square stencil apertures. Note that the formulas are the same for both.

"What about the area of the side walls?" Sue teased. Andy paused and seemed stumped.

"Well, what is the perimeter of the circle?" Sue teased.

"Two pi times the radius?" Andy said with uncertainty.

"Yes, so then the area of the side walls would be?" Sue questioned.

"Wait, now I see it—two pi times the radius times the stencil thickness!" Andy said triumphantly.

"Isn't it interesting that the area ratio is the same for square apertures?" Sue commented.

"And I actually understand how it is derived," Andy said, beaming.

As they were chatting, Chuck and Tanya Brooks came to their table. "Andy, Sue, it's great to see you here," Chuck said. Andy, Sue, Chuck, and Tanya shook hands, and Sue and Tanya hugged each other.

"This place has the best ice cream around," Chuck opined.

All agreed and small talk ensued for a few moments. Finally, all sensed Chuck wanted to say something.

"Sue and Andy, you two are the superstars in our SMTA certification prep class. We need some more instructors. How about you two joining our instructor team?" he asked.

"Sure," Andy said, "we would love to!"

Some more small talk ensued, and eventually the group broke up and headed to the doors of the shop. As Sue and Andy walked to Andy's car, Sue looked extremely upset. "What's the matter?" Andy asked.

"I'm afraid to speak to a group; I don't think I can be an instructor," Sue replied.

Andy thought for a while and then gave her a hug. "How about this? I will speak and conduct the class and you will answer questions that you are comfortable answering," Andy suggested.

The relief on Sue's face was palpable. "Thanks, Andy, maybe approaching it this way will make me feel more confident speaking in front of a group," she said with an obvious sigh of relief.

Will Andy ever catch up to Sue intellectually? How will Sue handle helping teach the class? Stay tuned to find out. **SMT007**

All figures are used with permission of the copyright owners, Jim Hall, Phil Zarrow, and Ron Lasky.

Reference

1. "Does Solder Paste's 'Five Ball Rule' Remain Valid in SMT Today? by Ron Lasky, Indium Corporation.

Ronald C. Lasky is an instructional professor of engineering for the Thayer School of Engineering at Dartmouth College, and senior technolo-gist at Indium Corporation. To read past columns, or contact Lasky, click here.

TOP TEN

EDITOR'S PICKS

The Government Circuit: U.S. Congress Gets Serious About Boosting U.S. PCB Sector

A great deal of work must be done continuously to reinvent and rebuild our industry for the future. Here in Washington, we are encouraged by new legislation indicating a bipartisan commitment to U.S. manufacturing that is long overdue.

SMS Electronics in Collaboration with UK Design-House SmartSentry

Smart Made Simple (SMS) has joined forces with SmartSentry, a design-house who specialises in turning ideas into reality using modular technologies. They offer an innovation acceleration service, to help customers to bring their products to market faster with economies of scale.

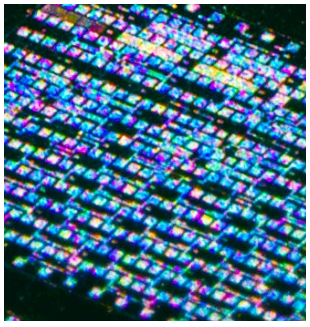
Social Responsibility and Ethics in Manufacturing

Customers, partners, and employees are increasingly moving toward companies that care about people and the environment, not just about their economic profitability. Corporate social responsibility has thus become essential, even in the manufacturing sector.

Nolan's Notes: What's the Point of Collaborating?

Creating close working relationships with manufacturing specialists who can extend your capabilities for your customers is one obvious way to collaborate. But there are others. For example, collaboration can also look like proactive communication with customers as well as vendors.

How Will Emerging Chiplet Technology Affect PCBs?



In a recent conversation with Ventec's Alun Morgan, the I-Connect007 Editorial Team discussed semiconductor packaging developments and emerging technology trends.

The Double-edged Sword of CMMC 2.0

For the past few years, those whose SMT provider organizations supply or contract with the U.S. Department of Defense have been hearing about the implementation of the Cybersecurity Maturity Model Certification program, better known as CMMC. By this, I mean that you were gearing up for CMMC 1.0. Today, we have CMMC 2.0, and there are a number of changes in the new version that impact both the standards for compliance and how you certify that compliance—especially if you run a small business.

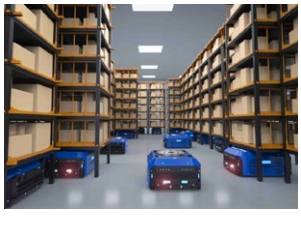
Rocket EMS Improves Inspection Capabilities with Scienscope's X-Scope 1800

Scienscope International, a leading American supplier of cabinet-style micro-focus X-ray systems, announces the purchase of an X-Scope 1800 X-ray inspection system by Rocket EMS, a Silicon Valley-based full-service EMS supplier, for its new Carson City, Nevada facility.

Smart Factory Insights: Fractional Materials and High-Mix Manufacturing

We used to discuss manufacturing paradigms in terms of high- or low-mix, coupled with high- or low-volume, with many shades of grey in between. Now, we have a new dimension, that of high-volatility, as key dependencies on labor, materials and logistics contribute challenges to production, which in turn, is subject to the volatility of customer demand.

X-Rayted Files: Smart vs. Intelligent SMT Factory



Amazon currently employs over 200,000 robots across 175 fulfillment centers around the world. The robot ranks at Amazon grow every year and, in some facilities, outnumber humans. I don't know what the future holds for surface mount technology manufacturing, but I'm certain it depends on our intelligence. We spend a lot of time discussing the Smart factory. Instead, we should aim for the "Intelligent" factory.

Flex Expands Automotive Manufacturing Hub in Jalisco, Mexico

A new, 145,000 square-foot state-of-the-art facility will serve as the strategic in-region automotive manufacturing hub dedicated to producing advanced electronic components that will accelerate the era of electric and autonomous vehicles.

Career Opportunities

Is your team growing?

Find industry-experienced candidates at I-Connect007.

For just $750, your 200-word, full-column ad will appear in the Career Opportunities section of all three of our monthly magazines, reaching circuit board designers, fabricators, assemblers, OEMs, suppliers and the academic community.

In addition, your ad will:

- be featured in at least one of our newsletters
- appear on our jobConnect007.com board, which is promoted in every newsletter
- appear in our monthly Careers Guide, emailed to 26,000 potential candidates

Potential candidates can click on your ad and submit a resume directly to the email address you provide, or be directed to the URL of your choice.

No contract required. Just send over your copy and company logo and we'll do the rest!

Contact barb@iconnect007.com to get your ad posted today!

+1 916.365.1727

I-Connect007
GOOD FOR THE INDUSTRY

smt007 pcb007 pcb design007

Career Opportunities

Field Sales Engineer, North America

Location: New Hartford, NY

JOB SUMMARY:

The Field Sales Engineer, North America, is responsible for serving as Indium Corporation's lead sales contact and customer advocate to maintain existing sales and to drive new qualifications and sales of Indium Corporation products and services through effective account management and coordination of efforts throughout Indium Corporation's Metals, Compounds, Solar and Reclaim (MCSR) organization.

REQUIREMENTS:

- Associate's degree in a business or technical discipline
- Minimum 2 years related sales or technical field experience
- Technical aptitude
- Personable individual, with excellent oral and written communication skills
- Strong organizational skills
- Able to travel upon short notice
- Proficient in Word, Excel, PowerPoint

apply now

Electrical Engineer/PCB/CAD Design, BOM/Component & Quality Support

Flexible Circuit Technologies (FCT) is a premier global provider of flex, rigid flex, flex heaters, EMS assembly and product box builds.

Responsibilities:

- Learn the properties, applications, advantages/disadvantages of flex circuits
- Learn the intricacies of flex circuit layout best practices
- Learn IPC guidelines: flex circuits/assemblies
- Create flexible printed circuit board designs/files to meet customer requirements
- Review customer prints and Gerber files to ensure they meet manufacturing and IPC requirements
- Review mechanical designs, circuit requirements, assembly requirements, BOM/component needs/and help to identify alternates, if needed
- Prepare and document changes to customer prints/files. Work with application engineers, customers, and manufacturing engineers to finalize and optimize designs for manufacturing
- Work with quality manager to learn quality systems, requirements, and support manager with assistance

Qualifications:

- Electrical Engineering Degree with 2+ years of CAD/PCB design experience
- IPC CID or CID+ certification or desire to obtain
- Knowledge of flexible PCB materials, properties, or willingness to learn
- Experience with CAD software: Altium, or other
- Knowledge of IPC standards for PCB industry, or willingness to learn
- Microsoft Office products

FCT offers competitive salary, bonus program, benefits package, and an outstanding long-term opportunity. Location: Minneapolis, Minn., area.

apply now

Career Opportunities

Prototron Circuits

Sales Representatives

Prototron Circuits, a market-leading, quick-turn PCB manufacturer located in Tucson, AZ, is looking for sales representatives for the New England and Northern California territories. With 35+ years of experience, our PCB manufacturing capabilities reach far beyond that of your typical fabricator.

Reasons you should work with Prototron:

- Solid reputation for on-time delivery (98+% on-time)
- Capacity for growth
- Excellent quality
- Production quality quick-turn services in as little as 24 hours
- 5-day standard lead time
- RF/microwave and special materials
- AS9100D
- MIL-PRF- 31032
- ITAR
- Global sourcing option (Taiwan)
- Engineering consultation, impedance modeling
- Completely customer focused team

Interested? Please contact Russ Adams at (206) 351-0281 or russa@prototron.com.

apply now

Koh Young America

Technical Support Applications Engineer

Full-Time — Duluth, GA

Koh Young Technology, founded in 2002 in Seoul, South Korea, is the world leader in 3D measurement-based inspection technology for electronics manufacturing. Located in Duluth, GA, Koh Young America has been serving its partners since 2010 and expanding team with an Applications Engineer to provide helpdesk support by delivering guidance on operation, maintenance, and programming remotely or on-site.

Responsibilities

- Provide timely, complete helpdesk support for Koh Young users
- Train users on proper operation, maintenance, programming, and best practices
- Recommend and oversee operational, process, or other performance improvements
- Effectively troubleshoot and resolve machine, system, and process issues

Skills and Qualifications

- Bachelor's in a technical discipline, relevant Associate's, or equivalent vocational or military training
- Knowledge of electronics manufacturing, robotics, PCB assembly, and/or AI; 2-4 years of experience
- SPI/AOI programming, operation, and maintenance experience, preferred
- Domestic and international travel (valid U.S. or Canadian Passport, required)
- Able to work effectively and independently with minimal supervision
- Ability to readily understand and interpret detailed documents, drawing, and specifications

Benefits

- Health/Dental/Vision/Life Insurance with no employee premium (including dependent coverage)
- 401K retirement plan
- Generous PTO and paid holidays

apply now

Career Opportunities

ALTIX

Direct Imaging & Contact Printers

Sales Technical Engineer

ALTIX, a French company, designs, manufactures, markets and services exposure equipment for the printed circuit board, flexible circuit, metal etching, touch panel and other industries. The U.S. subsidiary, focused on the sale and service of Altix equipment in North America, is looking for a sales technical engineer to support their growth.

Responsibilities

- Promote Altix's products by visiting customers
- Serve as a technical lead & product expert to provide technical recommendations to customers
- Gather on-the-ground market intelligence through customer contact
- Ensure sustainable growth in sales, profits, and market presence
- Develop new business and achieve targets for market penetration, sales and profit
- Manage sales partners

Skills & Qualifications

- Minimum 2 to 5 years' experience in sales for capital equipment in the PCB market or related industries
- Business development and marketing background preferred
- 5+ years' North American business leadership experience in related field
- Strong leadership, decision-making and communication skills.
- Proficiency in standard computer software applications such as Microsoft Office
- Excellent written and oral communication skills
- Willingness to travel within the US, Canada and to France for training

Email contact: sylvain.dromaint@altix.us

apply now

CHEMCUT

Director of Operations

State College, PA

Chemcut Corp., a world leader in wet processing equipment for the manufacture of printed circuit boards and chemical etching of various metals, is seeking a Director of Operations.

Objectives of the Role:

- Collaborate with the CEO in setting and driving organizational vision, operational strategy, and hiring needs.
- Oversee manufacturing operations and employee productivity, building a highly inclusive culture ensuring team members thrive and organizational outcomes are met.
- Directly oversee manufacturing operations, production planning, purchasing, maintenance & customer service (product support) and partner with the CEO and controller on sales management to budget for sufficient investment capital to achieve growth targets.
- Aggressively manage capital investment and expenses to ensure the company achieves investor targets relative to growth and profitability.

Qualifications:

- Bachelor's degree in mechanical, electrical, or related fields
- 5+ years' experience in leadership positions
- Leadership skills, with steadfast resolve and personal integrity
- Understanding of advanced business planning and regulatory issues
- A solid grasp of data analysis and performance metrics
- Ability to diagnose problems quickly and have foresight into potential issues

Preferred Qualifications:

- Master's degree in business or related field
- International business experience

To apply, please submit a cover letter and resume to hr@chemcut.net

apply now

Career Opportunities

ventec INTERNATIONAL GROUP 騰輝電子

European Product Manager
Taiyo Inks, Germany

We are looking for a European product manager to serve as the primary point of contact for product technical sales activities specifically for Taiyo Inks in Europe.

Duties include:
- Business development & sales growth in Europe
- Subject matter expert for Taiyo ink solutions
- Frequent travel to targeted strategic customers/OEMs in Europe
- Technical support to customers to solve application issues
- Liaising with operational and supply chain teams to support customer service

Skills and abilities required:
- Extensive sales, product management, product application experience
- European citizenship (or authorization to work in Europe/Germany)
- Fluency in English language (spoken & written)
- Good written & verbal communications skills
- Printed circuit board industry experience an advantage
- Ability to work well both independently and as part of a team
- Good user knowledge of common Microsoft Office programs
- Full driving license essential

What's on offer:
- Salary & sales commission--competitive and commensurate with experience
- Pension and health insurance following satisfactory probation
- Company car or car allowance

This is a fantastic opportunity to become part of a successful brand and leading team with excellent benefits. Please forward your resume to **jobs@ventec-europe.com.**

apply now

MacDermid Alpha ELECTRONICS SOLUTIONS

R&D Scientist III
Orange, CT

Job Description: The scientist will be a leader in technology for plating chemistry development, electrolytes, and additives. The position is hands-on, where the ideal candidate will enjoy creating and testing new aqueous plating processes and materials to meet the most demanding semiconductor applications related to Wafer-Level Packaging and Damascene. The qualified candidate will work as part of the R&D team while interacting with scientists, product management, and application engineers to commercialize new products for the advanced electronic solution business.

apply now

Technical Marketing Specialist
Waterbury, CT

This position provides information from the product team to the marketing communications team. It is a multifunctional role that requires some experience within electronics manufacturing supply chain or knowledge of how electronic devices are manufactured, specifically PCBs, semiconductors, and the chemical processes utilized therein. The primary function of this role is to help in the generation of product marketing collateral, but also includes assisting in tradeshow content development, advertising, and launches.

apply now

Career Opportunities

KYZEN
Where Science and Care Converge.

Regional Manager
Midwest Region

General Summary: Manages sales of the company's products and services, Electronics and Industrial, within the States of IL, IN & MI. Reports directly to Americas Manager. Collaborates with the Americas Manager to ensure consistent, profitable growth in sales revenues through positive planning, deployment and management of sales reps. Identifies objectives, strategies and action plans to improve short- and long-term sales and earnings for all product lines.

DETAILS OF FUNCTION:
- Develops and maintains strategic partner relationships
- Manages and develops sales reps:
  - Reviews progress of sales performance
  - Provides quarterly results assessments of sales reps' performance
  - Works with sales reps to identify and contact decision-makers
  - Setting growth targets for sales reps
  - Educates sales reps by conducting programs/seminars in the needed areas of knowledge
- Collects customer feedback and market research (products and competitors)
- Coordinates with other company departments to provide superior customer service

QUALIFICATIONS:
- 5-7+ years of related experience in the manufacturing sector or equivalent combination of formal education and experience
- Excellent oral and written communication skills
- Business-to-business sales experience a plus
- Good working knowledge of Microsoft Office Suite and common smart phone apps
- Valid driver's license
- 75-80% regional travel required

To apply, please submit a COVER LETTER and RESUME to: Fernando Rueda, Americas Manager

fernando_rueda@kyzen.com

apply now

pluritec®
MACHINES FOR PRINTED CIRCUIT BOARDS

Field Service Engineer
Location: West Coast, Midwest

Pluritec North America, ltd., an innovative leader in drilling, routing, and automated inspection in the printed circuit board industry, is seeking a full-time field service engineer.

This individual will support service for North America in printed circuit board drill/routing and x-ray inspection equipment.

Duties included: Installation, training, maintenance, and repair. Must be able to troubleshoot electrical and mechanical issues in the field as well as calibrate products, perform modifications and retrofits. Diagnose effectively with customer via telephone support. Assist in optimization of machine operations.

A technical degree is preferred, along with strong verbal and written communication skills. Read and interpret schematics, collect data, write technical reports.

Valid driver's license is required, as well as a passport, and major credit card for travel.

Must be able to travel extensively.

apply now

Career Opportunities

American Standard Circuits

Creative Innovations In Flex, Digital & Microwave Circuits

Wet Process Engineer

ASC, the largest independent PCB manufacturer in the Midwest, is looking to expand our manufacturing controls and capabilities within our Process Engineering department. The person selected will be responsible for the process design, setup, operating parameters, and maintenance of three key areas—imaging, plating, etching--within the facility. This is an engineering function. No management of personnel required.

Essential Responsibilities

Qualified candidates must be able to organize their own functions to match the goals of the company.

Responsible for:

- panel preparation, dry film lamination, exposure, development and the processes, equipment setup and maintenance programs
- automated (PAL line) electrolytic copper plating process and the equipment setup and maintenance programs
- both the cupric (acid) etching and the ammoniacal (alkaline) etching processes and the equipment setups and maintenance programs

Ability to:

- perform basic lab analysis and trouble-shooting as required
- use measurement and analytical equipment as necessary
- work alongside managers, department supervisors and operators to cooperatively resolve issues
- effectively problem-solve
- manage multiple projects concurrently
- read and speak English
- communicate effectively/interface at every level of the organization

Organizational Relationships

Reports to the Technical Director.

Qualifications

Degree in Engineering (BChE or I.E. preferred). Equivalent work experience considered. High school diploma required. Literate and functional with most common business software systems MS Office, Excel, Word, PowerPoint are required. Microsoft Access and basics of statistics and SPC a plus.

Physical Demands

Exertion of up to 50 lbs. of force occasionally may be required. Good manual dexterity for the use of common office equipment and hand tools.

- Ability to stand for long periods.

Work Environment

This position is in a manufacturing setting with exposure to noise, dirt, and chemicals.

Click on 'apply now' buttton below to send in your application.

apply now

Career Opportunities

Manncorp™

SMT Field Technician
Hatboro, PA

Manncorp, a leader in the electronics assembly industry, is looking for an additional SMT Field Technician to join our existing East Coast team and install and support our wide array of SMT equipment.

Duties and Responsibilities:
- Manage on-site equipment installation and customer training
- Provide post-installation service and support, including troubleshooting and diagnosing technical problems by phone, email, or on-site visit
- Assist with demonstrations of equipment to potential customers
- Build and maintain positive relationships with customers
- Participate in the ongoing development and improvement of both our machines and the customer experience we offer

Requirements and Qualifications:
- Prior experience with SMT equipment, or equivalent technical degree
- Proven strong mechanical and electrical troubleshooting skills
- Proficiency in reading and verifying electrical, pneumatic, and mechanical schematics/drawings
- Travel and overnight stays
- Ability to arrange and schedule service trips

We Offer:
- Health and dental insurance
- Retirement fund matching
- Continuing training as the industry develops

apply now

INSULECTRO

Are You Our Next Superstar?!

Insulectro, the largest national distributor of printed circuit board materials, is looking to add superstars to our dynamic technical and sales teams. We are always looking for good talent to enhance our service level to our customers and drive our purpose to enable our customers to build better boards faster. Our nationwide network provides many opportunities for a rewarding career within our company.

We are looking for talent with solid background in the PCB or PE industry and proven sales experience with a drive and attitude that match our company culture. This is a great opportunity to join an industry leader in the PCB and PE world and work with a terrific team driven to be vital in the design and manufacture of future circuits.

apply now

Career Opportunities

Printed Circuits

Printed Circuits, a fast-growing printed circuit board fabricator, offers:

- Excellent opportunities for advancement and growth
- Dynamic manufacturing environment
- Excellent health, dental and other benefits
- Annual profit-sharing plan
- Signing bonus
- Additional incentives at the leadership level
- Clean facility with state-of-the-art manufacturing equipment
- Highly collaborative corporate and manufacturing culture that values employee contributions

Laminator Technician

Nature of Duties/Responsibilities

- Layup cover lay
- Layup rigid flex
- Layup multilayer/CU core boards
- Oxide treat/cobra treatment of all layers/CU cores
- Shear flex layer edges
- Rout of machine panel edges and buff
- Remove oxide/cobra treatment (strip panels)
- Serialize panels
- Pre-tac Kapton windows on flex layers (bikini process)
- Layup Kapton bonds
- Prep materials: B-stage, Kapton, release sheet
- Breakdown: flex layers, and caps
- Power scrub: boards, layers, and caps
- Laminate insulators, stiffeners, and heatsinks
- Plasma cleans and dry flex layers B-stage (Dry)
- Booking layers and materials, ready for lamination process
- Other duties as deemed necessary by supervisor

Education/Experience

- High school diploma or GED
- Must be a team player
- Must demonstrate the ability to read and write English and complete simple mathematical equations
- Must be able to follow strict policy and OSHA guidelines
- Must be able to lift 50 lbs
- Must have attention to detail

Wet Process/Plating Technician

Position is 3rd shift (11:00PM to 7:30AM, Sunday through Friday)

Purpose

To carry out departmental activities which result in producing quality product that conforms to customer requirements. To operate and maintain a safe working environment.

Nature of Duties/Responsibilities

- Load and unload electroplating equipment
- Fasten circuit boards to racks and cathode bars
- Immerse work pieces in series of cleaning, plating and rinsing tanks, following timed cycles manually or using hoists
- Carry work pieces between departments through electroplating processes
- Set temperature and maintains proper liquid levels in the plating tanks
- Remove work pieces from racks, and examine work pieces for plating defects, such as nodules, thin plating or burned plating
- Place work pieces on racks to be moved to next operation
- Check completed boards
- Drain solutions from and clean and refill tanks; fill anode baskets as needed
- Remove buildup of plating metal from racks using chemical bath

Education and Experience

- High school diploma or GED required
- Good organizational skills and the ability to follow instructions
- Ability to maintain a regular and reliable attendance record
- Must be able to work independently and learn quickly
- Organized, self-motivated, and action-oriented, with the ability to adapt quickly to new challenges/opportunities
- Prior plating experience a plus

apply now

Career Opportunities

MivaTek Global

Field Service Technician

MivaTek Global is focused on providing a quality customer service experience to our current and future customers in the printed circuit board and microelectronic industries. We are looking for bright and talented people who share that mindset and are energized by hard work who are looking to be part of our continued growth.

Do you enjoy diagnosing machines and processes to determine how to solve our customers' challenges? Your 5 years working with direct imaging machinery, capital equipment, or PCBs will be leveraged as you support our customers in the field and from your home office. Each day is different, you may be:

- Installing a direct imaging machine
- Diagnosing customer issues from both your home office and customer site
- Upgrading a used machine
- Performing preventive maintenance
- Providing virtual and on-site training
- Updating documentation

Do you have 3 years' experience working with direct imaging or capital equipment? Enjoy travel? Want to make a difference to our customers? Send your resume to N.Hogan@MivaTek.Global for consideration.

More About Us

MivaTek Global is a distributor of Miva Technologies' imaging systems. We currently have 55 installations in the Americas and have machine installations in China, Singapore, Korea, and India.

apply now

eptac

TRAIN. WORK SMARTER. SUCCEED.

Become a Certified IPC Master Instructor

Opportunities are available in Canada, New England, California, and Chicago. If you love teaching people, choosing the classes and times you want to work, and basically being your own boss, this may be the career for you. EPTAC Corporation is the leading provider of electronics training and IPC certification and we are looking for instructors that have a passion for working with people to develop their skills and knowledge. If you have a background in electronics manufacturing and enthusiasm for education, drop us a line or send us your resume. We would love to chat with you. Ability to travel required. IPC-7711/7721 or IPC-A-620 CIT certification a big plus.

Qualifications and skills

- A love of teaching and enthusiasm to help others learn
- Background in electronics manufacturing
- Soldering and/or electronics/cable assembly experience
- IPC certification a plus, but will certify the right candidate

Benefits

- Ability to operate from home. No required in-office schedule
- Flexible schedule. Control your own schedule
- IRA retirement matching contributions after one year of service
- Training and certifications provided and maintained by EPTAC

apply now

Career Opportunities

The Test Connection, Inc.

Rewarding Careers

Take advantage of the opportunities we are offering for careers with a growing test engineering firm. We currently have several openings at every stage of our operation.

The Test Connection, Inc. is a test engineering firm. We are family owned and operated with solid growth goals and strategies. We have an established workforce with seasoned professionals who are committed to meeting the demands of high-quality, low-cost and fast delivery.

TTCI is an Equal Opportunity Employer. We offer careers that include skills-based compensation. We are always looking for talented, experienced test engineers, test technicians, quote technicians, electronics interns, and front office staff to further our customer-oriented mission.

Associate Electronics Technician/ Engineer (ATE-MD)

TTCI is adding electronics technician/engineer to our team for production test support.

- Candidates would operate the test systems and inspect circuit card assemblies (CCA) and will work under the direction of engineering staff, following established procedures to accomplish assigned tasks.
- Test, troubleshoot, repair, and modify developmental and production electronics.
- Working knowledge of theories of electronics, electrical circuitry, engineering mathematics, electronic and electrical testing desired.
- Advancement opportunities available.
- Must be a US citizen or resident.

apply now

Test Engineer (TE-MD)

In this role, you will specialize in the development of in-circuit test (ICT) sets for Keysight 3070 (formerly HP) and/or Teradyne (formerly GenRad) TestStation/228X test systems.

- Candidates must have at least three years of experience with in-circuit test equipment. A candidate would develop and debug our test systems and install in-circuit test sets remotely online or at customer's manufacturing locations nationwide.
- Candidates would also help support production testing and implement Engineering Change Orders and program enhancements, library model generation, perform testing and failure analysis of assembled boards, and other related tasks.
- Some travel required and these positions are available in the Hunt Valley, Md., office.

apply now

Sr. Test Engineer (STE-MD)

- Candidate would specialize in the development of in-circuit test (ICT) sets for Keysight 3070 (formerly Agilent & HP), Teradyne/ GenRad, and Flying Probe test systems.
- Strong candidates will have more than five years of experience with in-circuit test equipment. Some experience with flying probe test equipment is preferred. A candidate would develop, and debug on our test systems and install in-circuit test sets remotely online or at customer's manufacturing locations nationwide.
- Proficient working knowledge of Flash/ISP programming, MAC Address and Boundary Scan required. The candidate would also help support production testing implementing Engineering Change Orders and program enhancements, library model generation, perform testing and failure analysis of assembled boards, and other related tasks. An understanding of stand-alone boundary scan and flying probe desired.
- Some travel required. Positions are available in the Hunt Valley, Md., office.

Contact us today to learn about the rewarding careers we are offering. Please email resumes with a short message describing your relevant experience and any questions to careers@ttci.com. Please, no phone calls.

We proudly serve customers nationwide and around the world.

TTCI is an ITAR registered and JCP DD2345 certified company that is NIST 800-171 compliant.

apply now

Career Opportunities

YOUR JOB AD HERE

For information, please contact:
BARB HOCKADAY
barb@iconnect007.com
+1 916.365.1727 (PACIFIC)

I-Connect007
GOOD FOR THE INDUSTRY

ARLON
ELECTRONIC MATERIALS

Arlon EMD, located in Rancho Cucamonga, California, is currently interviewing candidates for open positions in:

- **Engineering**
- **Quality**
- **Various Manufacturing**

All interested candidates should contact Arlon's HR department at 909-987-9533 or email resumes to careers.ranch@arlonemd.com.

Arlon is a major manufacturer of specialty high-performance laminate and prepreg materials for use in a wide variety of printed circuit board applications. Arlon specializes in thermoset resin technology, including polyimide, high Tg multifunctional epoxy, and low loss thermoset laminate and prepreg systems. These resin systems are available on a variety of substrates, including woven glass and non-woven aramid. Typical applications for these materials include advanced commercial and military electronics such as avionics, semiconductor testing, heat sink bonding, High Density Interconnect (HDI) and microvia PCBs (i.e. in mobile communication products).

Our facility employs state of the art production equipment engineered to provide cost-effective and flexible manufacturing capacity allowing us to respond quickly to customer requirements while meeting the most stringent quality and tolerance demands. Our manufacturing site is ISO 9001: 2015 registered, and through rigorous quality control practices and commitment to continual improvement, we are dedicated to meeting and exceeding our customers' requirements.

For additional information please visit our website at www.arlonemd.com

apply now

Career Opportunities

U.S. CIRCUIT

Plating Supervisor

Escondido, California-based PCB fabricator U.S. Circuit is now hiring for the position of plating supervisor. Candidate must have a minimum of five years' experience working in a wet process environment. Must have good communication skills, bilingual is a plus. Must have working knowledge of a plating lab and hands-on experience running an electrolytic plating line. Responsibilities include, but are not limited to, scheduling work, enforcing safety rules, scheduling/maintaining equipment and maintenance of records.

Competitive benefits package.
Pay will be commensurate
with experience.

Mail to:
mfariba@uscircuit.com

apply now

APCT
Passion | Commitment | Trust

APCT, Printed Circuit Board Solutions: Opportunities Await

APCT, a leading manufacturer of printed circuit boards, has experienced rapid growth over the past year and has multiple opportunities for highly skilled individuals looking to join a progressive and growing company. APCT is always eager to speak with professionals who understand the value of hard work, quality craftsmanship, and being part of a culture that not only serves the customer but one another.

APCT currently has opportunities in Santa Clara, CA; Orange County, CA; Anaheim, CA; Wallingford, CT; and Austin, TX. Positions available range from manufacturing to quality control, sales, and finance.

We invite you to read about APCT at APCT.com and encourage you to understand our core values of passion, commitment, and trust. If you can embrace these principles and what they entail, then you may be a great match to join our team! Peruse the opportunities by clicking the link below.

Thank you, and we look forward to
hearing from you soon.

apply now

Career Opportunities

BLACKFOX
Premier Training & Certification

IPC Instructor

Longmont, CO; Phoenix, AZ; U.S.-based remote

Independent contractor, possible full-time employment

Job Description

This position is responsible for delivering effective electronics manufacturing training, including IPC Certification, to students from the electronics manufacturing industry. IPC instructors primarily train and certify operators, inspectors, engineers, and other trainers to one of six IPC Certification Programs: IPC-A-600, IPC-A-610, IPC/WHMA-A-620, IPC J-STD-001, IPC 7711/7721, and IPC-6012.

IPC instructors will conduct training at one of our public training centers or will travel directly to the customer's facility. A candidate's close proximity to Longmont, CO, or Phoenix, AZ, is a plus. Several IPC Certification Courses can be taught remotely and require no travel.

Qualifications

Candidates must have a minimum of five years of electronics manufacturing experience. This experience can include printed circuit board fabrication, circuit board assembly, and/or wire and cable harness assembly. Soldering experience of through-hole and/or surface-mount components is highly preferred.

Candidate must have IPC training experience, either currently or in the past. A current and valid certified IPC trainer certificate holder is highly preferred.

Applicants must have the ability to work with little to no supervision and make appropriate and professional decisions.

Send resumes to Sharon Montana-Beard at sharonm@blackfox.com.

apply now

American Standard Circuits
Creative Innovations In Flex, Digital & Microwave Circuits

CAD/CAM Engineer

Summary of Functions

The CAD/CAM engineer is responsible for reviewing customer supplied data and drawings, performing design rule checks and creating manufacturing data, programs, and tools required for the manufacture of PCB.

Essential Duties and Responsibilities

- Import customer data into various CAM systems.
- Perform design rule checks and edit data to comply with manufacturing guidelines.
- Create array configurations, route, and test programs, penalization and output data for production use.
- Work with process engineers to evaluate and provide strategy for advanced processing as needed.
- Itemize and correspond to design issues with customers.
- Other duties as assigned.

Organizational Relationship

Reports to the engineering manager. Coordinates activities with all departments, especially manufacturing.

Qualifications

- A college degree or 5 years' experience is required. Good communication skills and the ability to work well with people is essential.
- Printed circuit board manufacturing knowledge.
- Experience using CAM tooling software, Orbotech GenFlex®.

Physical Demands

Ability to communicate verbally with management and coworkers is crucial. Regular use of the telephone and e-mail for communication is essential. Sitting for extended periods is common. Hearing and vision within normal ranges is helpful for normal conversations, to receive ordinary information and to prepare documents.

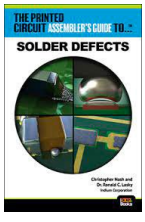
apply now

WATCH AND LEARN

Predicting Reliability in Electronics

In this engaging, 11-part micro webinar series, topic experts Graham Naisbitt and Chris Hunt examine the history of the influences of electrochemical migration (ECM) and the evolving use of Surface Insulation Resistance (SIR) testing that has been developed over the past 25 years by GEN3 and its association with the British National Physical Laboratory. GEN3 and NPL have created the standard that has now been in widespread use around the world since the turn of the millennium.

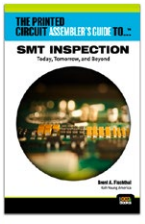
I-007e Books: The Printed Circuit Assembler's Guide to...



Solder Defects

by Christopher Nash and Dr. Ronald C. Lasky, Indium Corporation

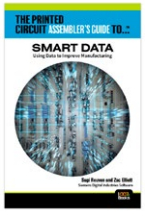
This book is specifically dedicated to educating the printed circuit board assembly sector and serves as a valuable resource for people seeking the most relevant information available.



SMT Inspection: Today, Tomorrow, and Beyond

by Brent Fischthal, Koh Young America

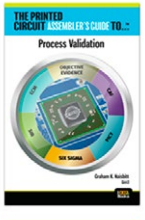
An in-depth insight into new and exciting true 3D inspection technology is provided in this book, along with a look into the future of leveraging big data management and autonomous manufacturing for a smarter factory.



Smart Data: Using Data to Improve Manufacturing

by Sagi Reuven and Zac Elliott, Siemens Digital Industries Software

Manufacturers need to ensure their factory operations work properly, but analyzing data is simply not enough. Companies must take efficiency and waste-reduction efforts to the next phase using big data and advanced analytics to diagnose and correct process flaws.



Process Validation

by Graham K. Naisbitt, Gen3

This book explores how establishing acceptable electrochemical reliability can be achieved by using both CAF and SIR testing. This is a must-read for those in the industry who are concerned about ECM and want to adopt a better and more rigorous approach to ensuring electrochemical reliability.

Advanced Manufacturing in the Digital Age

by Oren Manor, Siemens Digital Industries Software

A must-read for anyone looking for a holistic, systematic approach to leverage new and emerging technologies. The benefits are clear: fewer machine failures, reduced scrap and downtime issues, and improved throughput and productivity.

Our library is open 24/7/365. Visit us at: I-007eBooks.com

PUBLISHER: **BARRY MATTIES**
barry@iconnect007.com

MANAGING EDITOR: **NOLAN JOHNSON**
(503) 597-8037; nolan@iconnect007.com

ASSOCIATE EDITOR: **MICHELLE TE**
michelle@iconnect007.com

TECHNICAL EDITOR: **PETE STARKEY**
+44 (0) 1455 293333; pete@iconnect007.com

TECHNICAL EDITOR: **PATTY GOLDMAN**

CONTRIBUTING TECHNICAL EDITOR: **HAPPY HOLDEN**
(616) 741-9213; happy@iconnect007.com

CONTRIBUTING TECHNICAL EDITOR: **DAN FEINBERG**
baer@iconnect007.com

SALES MANAGER: **BARB HOCKADAY**
(916) 365-1727; barb@iconnect007.com

MARKETING SERVICES: **TOBEY MARSICOVETERE**
(916) 266-9160; tobey@iconnect007.com

PRODUCTION MANAGER: **SHELLY STEIN**
shelly@iconnect007.com

MAGAZINE LAYOUT: **RON MEOGROSSI**

AD DESIGN: **SHELLY STEIN, MIKE RADOGNA, TOBEY MARSICOVETERE**

CREATIVE TECHNOLOGIST: **BRYSON MATTIES**

COVER: **SHELLY STEIN**

COVER IMAGE: **SHELLY STEIN**

SMT007 MAGAZINE

SMT007 MAGAZINE®
is published by BR Publishing, Inc.,
942 Windemere Dr. NW, Salem, OR 97304

July 2022, Volume 37, Number 7
SMT007 MAGAZINE is published monthly,
by BR Publishing, Inc.

ADVERTISER INDEX


Problems solved!
PCBOO7 MAGAZINE
APRIL 2022
EDUCATION
Attend a conference.
Take a workshop.
Become certified.
PCBOO7 MAGAZINE
MAY 2022
GOLDEN ROI OPPORTUNITIES
Cybersecurity & Counterfeiti
PCBOO7 MAGAZINE
PLATING
DESIGNOO7 MAGAZINE
APRIL 2022
DESIGNOO7 MAGAZINE
MAY 2022
Designing in a Vacuum
DESIGNOO7 MAGAZINE
JUNE 2022
DWM
DESIGN WITH MANUFACTURING
SMTOO7 MAGAZINE
JUNE 2022
COLLABORATION
AND PARTNERSHIPS
SMTOO7 MAGAZINE
JULY 2022
SECURITY
TRIPLE WORD SCORE
TRIPLE LETTER THREAT
SUBSCRIBE NOW