SEMICONDUCTOR ENGINEERING (/)
DEEP INSIGHTS FOR THE TECH INDUSTRY

MANUFACTURING, PACKAGING & MATERIALS (/CATEGORY-MAIN-PAGE-MANUFACTURING/)

Industry Pushes For Fab Tool Security Standards

Vulnerabilities from old equipment plus huge value of data makes chip manufacturers a potential target.

SEPTEMBER 17TH, 2020 - BY: **MARK LAPEDUS (HTTPS://SEMIENGINEERING.COM/AUTHOR/MARK-LAPEDUS/)**

The semiconductor industry is developing new cybersecurity standards for fab equipment in an effort to protect systems from potential cyberattacks, viruses, and IP theft.

Two new standards are in the works, which are being formulated under the auspices of the SEMI trade group with leadership from chipmakers and others. Led by Intel and Cimetrix, the first standard deals with malware-free equipment integration measures. TSMC and the Industrial Technology Research Institute (ITRI) are spearheading the other standard, which addresses the security requirements and guidelines for computer operating systems and other technologies in fab equipment. In both cases, the industry faces some hurdles for implementing fab tool security standards.

These standards have been in the works for some time, but the industry is accelerating them as cyberthreats increase. Chipmakers have put the security measures in place to protect their internal IT systems and fabs. The goal is to prevent malicious attacks, service disruptions, and IP theft, any of which would have an impact on revenue.

Still, cyberattacks are on rise against businesses, governments, and individuals. The semiconductor industry isn't insulated from these threats, although it's hard to quantify the numbers or success rates. But since July of 2020, Tower Semiconductor and X-Fab separately have been hit with cyberattacks.

"This is a growing problem," said Chad Duffy, global product manager at CyCraft, a Taiwan-based cybersecurity technology company. "It's also important to know that these sorts of things can be stopped."

Needless to say, it's essential to have security measures in the IT organization as well as the fab. In a fab, chipmakers may have a multitude of IC production equipment, which are all connected in a network. But because much of the equipment is not brand new, a large percentage of the tools may incorporate computers with outdated operating systems and older ports.

For chipmakers, that's a major cause of concern. Fab equipment with older computer operating systems and network ports are potentially vulnerable to attacks, according to the SEMI fab tool security standard documents. Potentially, malware or malicious software could use security exploits to attack equipment, causing the systems to crash.

It also could be used to attack the hugely valuable and competitive IP of foundries and packaging houses, as well as their customers. Nearly all chipmakers use third-party foundry and packaging services, and much of that involves highly proprietary GDSII data. In addition, the foundry processes themselves are extremely valuable.

This is where the two SEMI standards fit in. They don't deal with the IT systems within a corporation, but rather it specifically addresses standards and guidelines for fab equipment. "The semiconductor equipment market is worth over $60 billion each year, and semiconductors themselves are among the world's most valuable products. So, it's critical to identify risk-based measures to protect manufacturing technology, intellectual property, and operations from cybersecurity threats," said Ryan Bond, a software engineer in the Equipment Integration group at Intel, and the co-chair of the SEMI malware-free software delivery task force. "Highly automated semiconductor fabs operate as a network of equipment from different suppliers. After reports that some companies experienced disruption of their operations due to cybersecurity attacks, the industry decided it was time to act to improve consistency of security with a standards-based approach to securing the fab network. No standard exists today that is shared across different companies. By bringing a set of standards to the table, both device makers and equipment vendors benefit from clear expectations, resulting in reduced risk and improved security."

Nonetheless, the industry is in various stages of formulating two standards. They are:

- SEMI Draft Document 6566, Specification for Malware-Free Equipment Integration. This standard defines protocols for pre-shipment scans of equipment. It also addresses support for file transfers, maintenance patches, and component replacement.
- SEMI Draft Document 6506, Specification for Cybersecurity of Fab Equipment. This standard defines the security requirements and guidelines for fab equipment. The 6506 spec is in the ballot stage, while 6566 is targeted for possible ratification in 2021.

Growing threats

Cyberattacks aren't new. Starting in the 1970s, computer hackers with malicious intent began to surface. Then, in 2010, industrial cyberattacks gain notoriety with Stuxnet, which was a computer worm designed to sabotage Iran's nuclear facilities.

In 2017, the infamous WannaCry ransomware attack surfaced. A cryptoworm attacked systems running Microsoft Windows by encrypting data. The goal was to demand ransom payments. Ransomware is still problematic.

Over time, cyberattacks have escalated. In a recent report, McAfee saw an average of 375 new threats per minute in just the first quarter of 2020. The company also found a surge of cybercriminals exploiting the COVID-19 pandemic through phishing campaigns and malware. Nearly 47% of all security incidents took place in the United States, according to McAfee.

"One of the bigger trends that has emerged in the past five years is more of the systematic operations of these hacking groups. A lot of them have government sponsors and government funding," CyCraft's Duffy said. "The main thing to look at is not just the amount of the attacks. It's also the sophistication of the attacks."

To stay ahead in the cyber game, security vendors are developing next-generation detection and response tools for organizations. "Current security products and services roughly break down into prevention, detection, and response delivered in multiple layers on the network and endpoints. Prevention is about blocking known and highly suspicious

threats, whereas detection and response are about finding new or more sophisticated threats and removing them," Duffy said.

CyCraft and others use AI-based detection and response technologies. "One is the idea of managed detection and response. We have prevention, as well. Hackers use any sort of known or suspicious tools. We can block that immediately. That happens on the endpoints and on the network," Duffy said.

Each industry faces a number of security challenges. For example, chipmakers operate fabs on a 24/7 basis and can ill afford a work stoppage. A potential cyberattack could disrupt operations. There are other issues as well.

"IT security is becoming more important than ever, especially given our accelerated digital transformation and increasing reliance on communication technologies, as a result of the Covid pandemic. It's an imperative for companies to protect their intellectual property and sensitive information," said Amy Leong, senior vice president at FormFactor (https://semiengineering.com/entities/formfactor/).

Generally, the semiconductor industry has recognized the problem. For example, many Taiwan-based chipmakers have implemented the latest security technologies. "A lot of the major ones have jumped on detection and response tools," Duffy said. "This is already something that's gone on for the past two years."

Those efforts have not completely solved the problem. In 2018, for example, TSMC was the victim of a virus that impacted computer systems and fab tools in Taiwan. The virus was caused by a "misoperation" during the software installation process for a new tool, according to TSMC. This caused the virus to spread once the tool was connected to the network. The problem was quickly fixed and no confidential information was compromised.

Last year, Taiwan experienced an onslaught of cyberattacks, or so-called advanced persistent threat (APT) attacks, from various parties. It's unclear how successful these attacks were in Taiwan.

In July of 2020, German foundry vendor X-Fab was the target of a ransomware cyberattack. Following the event, X-Fab's IT systems and manufacturing sites were halted. The company resumed operations days after the attack with little material impact.

Then, in September of 2020, Tower Semiconductor suffered a cyberattack. Four days later, Tower resumed operations. Customer data remained protected during the event, according to Tower.

Cyberattacks are malicious. The COVID-19 pandemic has exacerbated the situation. Earlier this year, the pandemic struck, forcing a large percent of the world's population to work at home. Some companies are equipped to manage remote and secure workforces, but others are not.

This presents a challenge in the semiconductor industry. Typically, a fab is managed by on-site personnel. Chipmakers also can use remote diagnostic tools to monitor the equipment in the plant. From February to April 2020, the use of software for remote diagnosis among chipmakers more than doubled, according to SEMI. That remained at record-high levels in May and June, according to SEMI.

"There is a benefit for remote monitoring and remote diagnosis, particularly during COVID," said Aki Fujimura, CEO of D2S (https://semiengineering.com/entities/d2s/). "But there is no question that anything exposed to the external network is constantly under attack. Typically, hackers try to get in anywhere. Then, once in, they could hack layer-by-layer to anything that a machine is connected to."

The standards

Generally, semiconductor vendors have implemented security measures within their respective IT organizations and fabs.

"Every fab deploys processes, access controls and security controls to reduce the risk of cybersecurity threats to the fab network," Intel's Bond said. "Today, each company imposes their own set of rules on equipment vendors outlining how to best mitigate cybersecurity risks in their networks."

For example, many chipmakers ban the use of USB memory sticks within the fab. "Many fabs and mask shops prohibit cell phones and other devices that have communication capability," D2S' Fujimura said. "This is inconvenient for servicing or diagnosing trouble with experts within the company and its vendors, but this is considered necessary to maintain the required level of security."

Nonetheless, the industry has begun to take security more seriously. In 2018, TSMC initiated an effort to develop at least one fab equipment security standard.

At that time, TSMC outlined the challenges in a presentation. First, a chipmaker might have several fabs. Each fab consists of a datacenter, host systems, and equipment. The equipment and systems are connected in a network, which must be secure.

A large chipmaker might have 1,500 individual fab tools from 75 different vendors, according to TSMC. In some cases, a tool might have 8 computers integrated into the system. The computers run different operating systems. Some 30 operating system types may exist in fabs.

A computer operating system in a given tool has an average lifecycle from 4 to 6 years. From 1995 to 2018, more than 20 versions of those operating systems became outdated or reached the end-of-service (EOS), according to a SEMI security standard document. On average, 1 to 2 operating system types will become EOS per year, according to SEMI. Worse, some tools may lack update patches to fix potential vulnerabilities.

All told, there are potential threats for any EOS operating system or older ports in tools that cannot be upgraded to prevent viruses and hackers from attacking the network.

With these and other issues in mind, the industry is calling for standards, which could reduce risk and improve security. "Globalization of technology design, development, manufacturing and distribution have created an environment of complicated supply chains," Intel's Bond said. "The work being done to mitigate cybersecurity risks in the fabs is an important piece, but there is also a growing need to provide assurances of platform integrity in every stage."

To address these issues, two standards are being proposed. The first one, called SEMI Draft Document 6566, is targeted to prevent equipment suppliers from inadvertently introducing or spreading malware in the fab network. "The standard refers equipment suppliers to respected third-party organizations for information about existing vulnerabilities and best-known practices on hardening systems, which they can use to evaluate against their equipment," Bond said. "The standard does not target any one specific operating system, software, or networking component, but instead provides an infrastructure and process that can be applied to any computing device within the equipment."

The second standard, called SEMI Draft Document 6506, hopes to establish several guidelines in the following areas:

- Fab tool computer operation system security.
- Network security (e.g. restricted TCP/UDP ports, avoid using high-risk vulnerable ports like TCP/445).

- End-point protection.
- Security monitoring.

Implementing standards

While the semiconductor industry has laid out a strong case to implement fab equipment security standards, some challenges and issues remain. Implementing security standards isn't as simple as it sounds.

"In general for cybersecurity, physical security is most important. This includes the network to which the computer is connected to," D2S' Fujimura said. "So fabs and mask shops carefully determine the tradeoff between accessibility for operational control and convenience versus the threat of a potential breach. In many cases the network on which the equipment resides is physically separated from any machine that has access to the office network, for example, and is also physically separated from any machine that has access to the external world."

There are other issues. Upgrading tools with the latest operating system software is easier said than done. And implementing new standards takes time and money. Larger fab tool vendors may have the resources to address the issues. Smaller vendors with limited resources may not.

The same is true for chipmakers. Intel, Samsung, TSMC, and others may have the resources to help tool vendors here. Other chipmakers may lack the necessary resources.

"Setting the standards for the OS is a difficult thing," CyCraft's Duffy said. "If you set these standards, is it something that vendors are really going to be able to do? On the other hand, some vendors have jumped ahead of that. They are not waiting for this standard. They are jumping ahead and getting these tools in place ahead of time."

Some are ahead of the curve. "The importance of security amongst capital equipment in fabs can't be understated. Customers expect high utilization rates for Teradyne equipment and can't afford to have their production plans interrupted by preventable security vulnerabilities or operating system obsolescence. While underlying silicon processes and software technologies continue to evolve at a rapid pace, capital equipment must similarly evolve to ensure maximum productivity," said Mark Kahwati, director of product marketing at Teradyne. "On the surface, the proposed standards do not present particular implementation challenges. In fact, many of Teradyne's product lines already implemented many of the elements highlighted in the standards several years ago. The most notable challenge is associated with maintaining the security of the underlying OS technology. Capital equipment typically has lifetimes which are a factor of 3–4 that of the OS technology. Success on this front requires working with OS technology partners to extend support and security for these OS platforms."

Security is important for fab tool vendors, but it's not the only consideration when developing new equipment or upgrading existing ones. Developing new tools is especially complicated. It takes several years and millions of dollars to develop new tools.

The process starts when a tool maker defines a new system. Then, an equipment maker procures components for the system. The more sophisticated fab tools incorporate more than 50,000 parts from dozens of suppliers. Chambers, pumps, RF generators, seals and valves are among the key components in a tool.

Fab tools also incorporate computers with operating system software. Vendors want to integrate tools with the latest software with security in mind.

In a tool, every component and software program is important. If a component is faulty, the system won't perform up to spec or may require an inordinate amount of maintenance.

Nonetheless, fab tool vendors tend not to discuss their internal equipment R&D efforts, particularly their sensitive security software technologies.

In one recent presentation, though, an executive from TEL provided some insights on the evolution and development of fab equipment from an Industry 4.0/smart manufacturing perspective and where security fits in here.

In many cases, today's fab tools incorporate new capabilities, virtual metrology and tool connectivity in and outside the fab. Virtual metrology (https://semiengineering.com/knowledge_centers/manufacturing/process/metrology/) is a way to predict the properties of a process using sensor data and/or machine learning.

"Now, we're really into what's called a cyber physical world. And what that means is we're creating models around physical behaviors that occur within our equipment, around materials, and our processes," said Ben Rathsack, vice president and deputy general manager of TEL America (https://semiengineering.com/entities/tel/), during the presentation.

At a high level, TEL breaks down the cyber physical world into four parts. "The first is analytics and intelligence. The next is getting into the advanced production methods and your productivity, yield and things like that," Rathsack said. "The third bucket is about data computing, power, and connectivity. If you think about data, the amount of data that you're collecting from your tools or from your production line is staggering. And then the question is the connectivity and how to do that securely."

The fourth one involves human machine interaction. "As you create these models, how do humans interact with that. How do they make judgments based on that?" Rathsack said.

Conclusion

Unfortunately, cyberattacks are here to stay and are increasing. COVID-19 has made the problem worse.

Obviously, security is important for industries, governments, and individuals. Fortunately, the IC industry is aware of the issues and is addressing it. The challenge is to stay one step ahead of the game.

TAGS: CIMETRIX (HTTPS://SEMIENGINEERING.COM/TAG/CIMETRIX/) CYBERATTACKS (HTTPS://SEMIENGINEERING.COM/TAG/CYBERATTACKS/) CYBERSECURITY (HTTPS://SEMIENGINEERING.COM/TAG/CYBERSECURITY/) CYCRAFT (HTTPS://SEMIENGINEERING.COM/TAG/CYCRAFT/) D2S (HTTPS://SEMIENGINEERING.COM/TAG/D2S/) FORMFACTOR (HTTPS://SEMIENGINEERING.COM/TAG/FORMFACTOR/) INTEL (HTTPS://SEMIENGINEERING.COM/TAG/INTEL/) IP (HTTPS://SEMIENGINEERING.COM/TAG/IP/) ITRI (HTTPS://SEMIENGINEERING.COM/TAG/ITRI/) MALWARE (HTTPS://SEMIENGINEERING.COM/TAG/MALWARE/) SAMSUNG (HTTPS://SEMIENGINEERING.COM/TAG/SAMSUNG/) SECURITY (HTTPS://SEMIENGINEERING.COM/TAG/SECURITY/) SEMI (HTTPS://SEMIENGINEERING.COM/TAG/SEMI/) SEMICONDUCTOR (HTTPS://SEMIENGINEERING.COM/TAG/SEMICONDUCTOR/) SEMICONDUCTOR EQUIPMENT (HTTPS://SEMIENGINEERING.COM/TAG/SEMICONDUCTOR-EQUIPMENT/) STANDARDS (HTTPS://SEMIENGINEERING.COM/TAG/STANDARDS/) STUXNET (HTTPS://SEMIENGINEERING.COM/TAG/STUXNET/) TEL (HTTPS://SEMIENGINEERING.COM/TAG/TEL/) TOWER SEMICONDUCTOR (HTTPS://SEMIENGINEERING.COM/TAG/TOWER-SEMICONDUCTOR/) TSMC (HTTPS://SEMIENGINEERING.COM/TAG/TSMC/) X-FAB (HTTPS://SEMIENGINEERING.COM/TAG/X-FAB/) X-FAB SILICON FOUNDRIES (HTTPS://SEMIENGINEERING.COM/TAG/X-FAB-SILICON-FOUNDRIES/)

Mark LaPedus **(all posts) (https://semiengineering.com/author/mark-lapedus/)**

Mark LaPedus is Executive Editor for manufacturing at Semiconductor Engineering.