August 2024

NAVY SBIR TRANSITION PROGRAM SPOTLIGHT

Company: Amida Technology Solutions, Inc.
Website: www.amida.com

POC: Peter L. Levin, PhD
Phone: 617-921-0471

Address: 900 19th Street NW, Suite 203
Washington, District of Columbia 20006

Amida's breakthrough AI-powered cybersecurity tool for detecting vulnerabilities in semiconductor devices builds assurance for custom microelectronics users

By Amie Alscheff

Through a Navy SBIR contract, Amida Technology Solutions, Inc. (Amida) has developed a breakthrough software tool suite that can detect cyber vulnerabilities on chips during their design, test, production, and operation. Amida's technology dramatically improves the assurance of custom microelectronic components (CMCs). For its breakthroughs in artificial intelligence (AI) and graph theory, Amida has been awarded six patents to date and has further patent applications pending.

The SBIR project, a first for Amida, was an unusual undertaking for the company, says co-founder and CEO, Peter L. Levin. Amida is primarily a data management company. Its core competency is the design and implementation of applications that help government and commercial organizations securely exchange sensitive information. "A more typical customer might be a health system, such as Veterans Affairs, where they're looking for advanced analytics, like how certain kinds of medicines or therapies might work. We're looking for pathologies or vulnerabilities in patient cohorts that might not be seen using conventional analytical techniques," says Levin.

When Levin, who has a background in semiconductor device physics and semiconductor device design, saw the Navy's solicitation he realized that the advanced analytics Amida uses in other sectors could be applied to microelectronics as well. "On the surface it looks like there wouldn't be much overlap," Levin recalls. Before submitting a response to the solicitation, he reached out to the technical point of contact to confirm that the Navy would be interested in his white paper. "It turns out that the ability to expose and reveal cybersecurity vulnerabilities in microelectronic devices is based upon a mathematical construct—a mathematical foundation, if you like—that is remarkably similar to the work Amida does. In many respects it's just two different applications of the same underlying data management and theoretical frameworks that we've built the entire company on.

"We were brand new to SBIR and we were just incredibly lucky. This topic in particular was ferociously competitive and we were just delighted that we won."

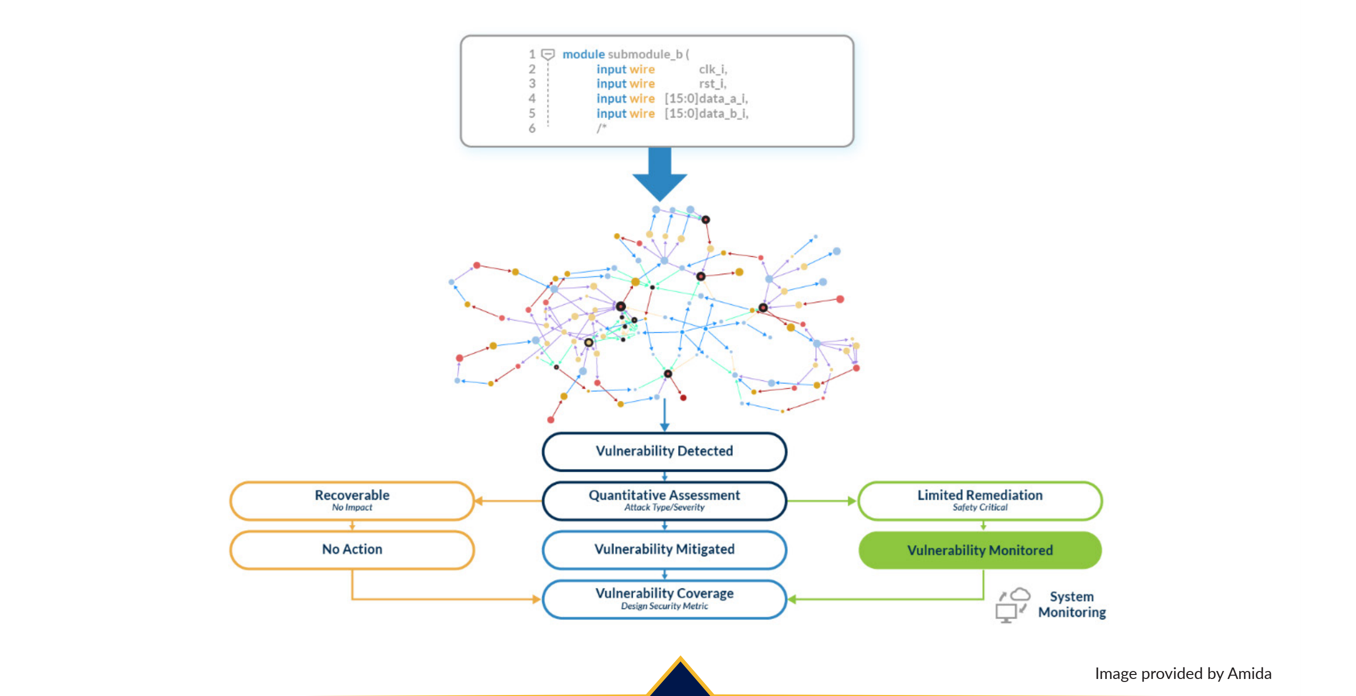
Amida's SBIR work began in 2017, sponsored by the Navy's Government Equipment Management program within NAVSEA's Team Ships. As part of the Phase II award, in 2022, Amida opted to participate in Navy STP. "It was very collaborative, very cooperative," says Levin. "We appreciated very much the engagement and the introductions."

The platform Amida developed during the Phase II addresses security concerns at the design level by comprehensively exploring the behavioral model for vulnerabilities using Amida's patented graph-based technique. For completed systems, Amida's platform also includes in-silicon surveillance instruments that in future could enable attack detection, identification, and remediation in the field.

The tool can be applied to any digital component, including field programmable gate arrays (FPGAs) and application-specific integrated circuits (ASICs), from simulation through sign-off, to manufacturing test and system deployment. It discovers embedded and genetic anomalies, as well as externally triggered intrusions and manipulations. While it was developed for the Department of Defense (DoD), Amida's technology can also be used in the commercial microelectronics industry as "fundamentally the same technology," according to Levin.

In designing the software, Amida anticipated that customers may want to integrate it with the other systems they're already using. "It's a standalone product if that's how you want to use it, and it also seamlessly integrates with other applications in the semiconductor supply chain. It works perfectly well either way," says Levin.

Amida's cybersecurity tool suite is featured on the Tradewind Solutions Marketplace, an Other Transaction Authority (OTA) sponsored by the DoD's chief data and artificial intelligence officer. Launched in November 2022, the Tradewinds Solutions



```
module submodule_b (
        input wire          clk_i,
        input wire          rst_i,
        input wire    [15:0]data_a_i,
        input wire    [15:0]data_b_i,
        /*
```

Image provided by Amida

Amida's software tool suite detects cyber vulnerabilities on chips, improving security assurance for CMCs.

Marketplace provides a venue for DoD organizations to discover and procure analytics, digital, and AI/machine learning capabilities solutions through rapid acquisition procedures. Technologies showcased within the marketplace must pass through intense competitive assessment procedures which satisfy the competition requirements of the Federal Acquisition Regulation (FAR), the Defense Federal Acquisition Regulation Supplement (DFARS), and the statutes, policies, and guidance applicable to the DoD's OTAs.

Amida's cybersecurity tool suite is available currently as a complete and usable product, but Levin is hoping to "extend the roadmap" of the company's Phase II work with additional SBIR awards, whether that be a Phase II.5 added to the existing project or a Phase III award from a program interested in using the technology for specific microelectronic devices, especially those used in national security. The current product is used pre-synthesis to evaluate the device for vulnerabilities before manufacturing; further developments would allow the tool to be used post-synthesis on the physical device, along with additional enhancements.

"We've been able to demonstrate the effectiveness of this new approach to microelectronic security on several microprocessor designs. What we're hoping to accomplish with further funding is more and better. By more we mean more microprocessors and other kinds of application-specific integrated circuits (ASICs). The more we run through this new algorithm, the better we'll be able to expose more vulnerabilities that cannot be seen with conventional methods. It's a pretty extensive library. It would be hard, I think, for an adversary to get through. But as is always the case in cyber, you don't know what you don't know, and so we would want to use further funding to extend the coverage of the AI-based anomaly and vulnerability detection that we got patented last year and that we've already made," Levin explains.

"The reason that we're still very persistent about finding the right partner inside the government is that if you know where the vulnerability is—if you know how your adversary is going to manipulate or attack you—you can actually soften the blow. In addition to trying to prevent what's going to happen, you can also be prepared for what could happen if an ideological adversary starts tampering with your microelectronics. Knowing what, where, and how allows you to be prepared once you've made the chip. Using our technology, you're not flying blind. You've got visibility into what's happening and the possibility that you can repair it in flight."

Amida is a software and technology services company that develops and configures data resources for government and commercial clients. Amida creates and manages solutions that enable the reliable exchange of sensitive information, from conception through deployment. For further information, see www.amida.com.

Amida

Data-Driven Success