Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.
NAVSEA #2022-0365

Topic # N171-054
Cyber Threat Insertion and Evaluation Technology for Navy Ship Control Systems
Amida Technology Solutions, Inc.

WHO

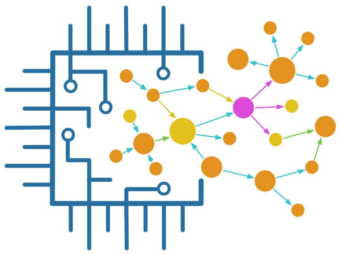
SYSCOM: NAVSEA

Sponsoring Program: Team Ships, Government Equipment Management

Transition Target: Navigational systems, surveillance systems, and targeting systems

TPOC: (215) 897-8297

Other Transition Opportunities: Industrial controllers, infrastructure controllers, information processing systems, communication systems, embedded devices, durable medical equipment



Copyright 2022 Amida Technology Solutions Inc.

Notes: This technology characterizes the threats and risks to custom microelectronic components (CMCs). Conventional approaches are platform-specific and rely on formal methods. Our solution reveals hidden vulnerabilities using a novel representation of the register-transfer-level (RTL) that graphically models the connections between signal and state. We have also developed a comprehensive suite of compact and self-tuning surveillance instruments and AI/ML monitors that detect anomalous behavior on deployed devices. The tool is fully applicable to field programmable gate array (FPGA)-based systems, as well as new, application-specific, integrated circuits (ASICs). The principal investigators are well-known for their prior contributions to cybersecurity and semiconductor test, while the board and senior advisors are similarly recognized for their work in national security.

WHAT

Operational Need and Improvement: The Navy and NSA have expressed the need for a structured approach to CMC assurance and risk assessment. We have developed a novel Design for Security and Trust (DFST) methodology that ensures CMCs are hardened to cybersecurity risks and capable of self-tuning operational surveillance. This new and patented technology allows manufacturers, integrators, and system architects to construct platforms that can automatically detect and identify chip-level cyberattacks in real time using embedded instrumentation and Machine Learning (ML) models. It addresses cybersecurity concerns across the entire CMC supply chain, from inception to fabrication, with: (1) analysis of the RTL for vulnerabilities, (2) embedded security in the hardware development life cycle (HDLC), (3) assurance of the integrity and performance of semiconductor devices during their design, and (4) verification that products are secure.

Specifications Required: Navy sought development of a hardware/software solution capable of running many tests using combinations of defense methodologies.

Technology Developed: Amida has developed a set of new analysis and evaluation tools that secure CMC-based devices. Pre-silicon, it identifies structural vulnerabilities to signal and state. In emulation and post-silicon, it uses sophisticated predictive analysis processes to identify behavioral anomalies, emulate the effects of attacks, and train ML models to recognize similar attack behaviors. Unlike current hardware security approaches that are primarily formal and forensic, this technology identifies likely attack vectors prior to device fabrication, integration, and field deployment.

Warfighter Value: Devices secured by our DFST methodology are cyber-hardened to be more resistant to new and unknown cyberattacks, including RTL-based zero-days. Instrumentation embedded into CMCs allows users and administrators to monitor system cyberhealth in real time and be notified with attribution and mitigation details upon observation of attack behavior within the chip.

WHEN

Contract Number: N68335-19-C-0259 **Ending on:** Jul 22, 2022

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Demonstration of full DFST methodology prototype	N/A	Conducted a full test of the prototype DFST design loop, created and analyzed a realistic design. Tested ML models to detect novel hardware attacks.	5	4th QTR FY21
Completed MVP of our vulnerability analysis software product	N/A	Evaluated a commercial core. Explored and reported design vulnerabilities for an industry partner.	6	3rd QTR FY22
Cybersecurity vulnerability and instrument design tool	Low	Collection of real-time data from a CMC or FPGA-based device to train attack recognition through machine learning.	7	3rd QTR FY23
Release of attack emulation and characterization software for intrusion recognition model training	Low	Generally available real-time monitoring and attack-behavior recognition system. Fully productized software will be integrated into devices during system assembly.	7	3rd QTR FY24
Deployment of hardware-monitoring and attack-recognition appliance alongside evaluated component	Medium	An integrated software product for system evaluation and characterization. The attack-behavior recognition system will provide real-time surveillance. We will deploy the hardware assurance platform in a real-world system.	7	3rd QTR FY25

HOW

Projected Business Model: The product will be licensed to the end user. The pre-silicon design review will require limited training; we are also prepared to offer design evaluation as a service. This is a software solution, so there are no manufacturing considerations at this time. The post-silicon tool is also a software product and will be integrated into a system-administration dashboard. We will leverage DoD connections to identify additional target platforms and programs that are currently developing or updating CMC-based solutions. We will simultaneously increase awareness of our hardware assurance software products within the CMC design and manufacturing community. Additionally, we will continue ongoing research and development efforts to productize novel threat-modeling and recognition technologies.

Company Objectives: Use tools and services to identify and support DoD programs that rely on CMC-based systems. Develop relationships with industrial microelectronics providers and design organizations to apply the novel analysis and evaluation techniques to real-world CMC designs. Continue to develop commercially available software products, based on the prototype technology, that we can sell – directly or through channel partnerships – to microelectronics providers.

Potential Commercial Applications: We have productized the DFST technology as individual software components that will be available for purchase either as standalone modules or as a complete software suite. Semiconductor design groups, intellectual property (IP) vendors, and custom system integrators are target customers for the RTL vulnerability analysis tool that is currently available. Future software releases will productize instrument insertion, autonomous detection, and real-time monitoring solutions.

Contact: Peter L. Levin, PhD, Co-Founder & CEO
peter@amida.com (617) 921-0471