Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.
ONR Approval #43-3252-17

Topic # N15A-T022
Embedded Architecture for Cyber-resilience (EAC)
Charles River Analytics Inc.

WHO

SYSCOM: ONR

Sponsoring Program: ONR Code 31

Transition Target: Unmanned Aircraft Systems or security-critical cyber-physical systems

TPOC:
Dr. Daniel Koller
daniel.koller@navy.mil

Photo courtesy of U.S. Navy, 131031-N-SW486-022.JPG

Other transition opportunities:
Product may be integrated into the Navy's embedded control systems for various ship-board naval applications or any number of military and commercial systems that must defend cyber physical systems from attack such as satellite (e.g. CubeSat), unmanned underwater vehicles, weapons systems, ISR platforms, avionics, and industrial control systems.

Notes: As an example of an alternate SBIR transition path successfully pursued on another program, Charles River developed a tool to guide the war¬fighter through a formalized approach to assessing, analyzing, and forecasting human behavior (Contract Number FA8650-04-C-6403). The tool eventually underwent a successful Military Utility Assessment in 2008 and an Extended User Assessment with a Joint agency; it is now in use by DoD war¬fighters worldwide.

WHAT

Operational Need and Improvement: Navy warfighters rely heavily on critical real-time cyber-physical systems to successfully complete mission objectives. As these systems become more interconnected, they are also more vulnerable to cyber-attacks by malicious adversaries. Fielded cyber-physical control systems must be resilient to faults caused by cyber-attacks as well as transient failures, because a successful attack on key control systems could result in physical catastrophic consequences for the mission and personnel. Therefore, these systems need to be extended with capabilities to (1) prevent faults affecting individual system software components from spreading throughout the entire system; (2) detect system compromises and determine which software components are affected; and (3) recover compromised components to a trusted state upon detection of faults without adversely affecting overall real-time system performance.

Specifications Required: Real-time control systems must provide predictable response times for real-time tasks. Cyber-physical systems can tolerate transient loss of control signals (i.e., software operation) for a limited amount of time as allowed by physical system properties and laws of physics, and fault tolerance capabilities must take such physical tolerance characteristics into account.

Technology Developed: We are developing an Embedded Architecture for Cyber-resilience (EAC) to protect cyber-physical systems from cyber threats, ensuring fault isolation for both system- and application-level software components and using novel machine learning algorithms to detect, locate, and automatically recover from compromises due to cyber-attacks. Early versions of EAC have successfully detected component faults and predictably and efficiently recovered from these faults to achieve mission success.

Warfighter Value: EAC is directly applicable to a number of military and commercial systems including satellites (e.g. CubeSat), avionics, unmanned systems, and industrial control systems. EAC will give warfighters assurance that mission-critical information and control systems will continue to operate in the presence of malicious cyber-attacks without disrupting mission activities.

WHEN

Contract Number: N68335-17-C-0153 **Ending on:** January 16, 2019

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Design and evaluate proof-of-concept prototype	N/A	Proof of concept of fault detection algorithms and recovery mechanism	3	November 2016
Develop and evaluate full-scope prototype in simulated environment	Med	Performance evaluation of fault resilience mechanisms	5	January 2019
Field test prototype on Navy platform in an operational scenario	High	Performance requirements met in an operational scenario	7	July 2020
Transition technology into FNC Program and/or integrate with commercial platform	Med	Operational requirements met in developmental test and evaluation	8	April 2021

HOW

Projected Business Model: Charles River has over 30 years of steady growth providing innovative, cost-effective solutions through intelligent systems R&D. Over 100 Charles River projects have produced a wealth of advanced-technology prototype software that can facilitate the rapid integration of critical technology into operational systems. Charles River will license EAC technology to large system integrators and integrate into Navy platforms, such as unmanned aircraft and embedded control systems. Once integrated, Charles River will provide users with full documentation on how to use features of EAC. For example, we have licensed our VisionKit ®, partly funded by DoD and NASA SBIRs, to developers of image and video analysis solutions.

Company Objectives: Cyber security, system resilience, and machine learning are core business areas for Charles River, making the success of this effort fall squarely within our corporate interests and competencies. Charles River expertise will ensure the success of the innovations developed under the EAC program beyond the STTR contract. In particular, Charles River plans to pursue a multi-part plan to transition this technology to the U.S. Navy and other U.S. Government customers, as well as provide benefits to commercial markets and customers seeking to enhance security and resilience of IT systems.

Potential Commercial Applications: We expect the full-scope EAC to have immediate and tangible benefits for a number of commercial systems that rely on defending cyber physical systems from attacks. In particular, EAC will help defend commercial satellite, avionics, and industrial control systems from attacks and enable them to fight through the effects of the attacks with minimal disruptions. Augmenting commercial avionics control systems with EAC will enable users to securely execute mission-critical applications.

Contact: Curt Wu, Chief Software Engineer
cwu@cra.com (617) 491-3474 x564