Topic: N162-115

Star Lab Corporation

Warden: Cyber Threat Anomaly Detection for Combat Systems

Star Lab's Warden is a minimally invasive technology designed specifically to detect advanced cyber threats inside unique defense compute environments, e.g., systems running customized Linux and real-time operating systems. Consisting of a lightweight sensor package, an ensemble of detectors, and an artificial neural network, Warden identifies potential cyber threats and reports them via the syslog mechanism. Warden's functionality has been prototyped, tested, and verified using realistic test and training environments for the Aegis Weapon System. Star Lab, an embedded systems security company, is dedicated to protecting devices and systems operating in open, hostile environments. Our goal is for prime contractors to integrate Warden as they modernize combat systems to defeat never-before-seen cyber-attacks.

Technology Category Alignment:

Assuring Effective Missions
Trust Foundations
Networks and Communications
Resilient Infrastructure

Contact:
Adam Fraser
adam@starlab.io
(202) 706-7027
https://starlab.io/
SYSCOM: NAVSEA
Contract: N00178-18-C-7002

Booth: 605
Room: Club Room East
Presenting: Apr 11th at 9:40 AM
Corporate Brochure: https://navystp.com/vtm/open_file?type=brochure&id=N00178-18-C-7002

Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

NAVSEA #2018-0643

Topic # N162-115

Warden: Cyber Threat Anomaly Detection for Combat Systems

Star Lab Corporation

WHO

SYSCOM: NAVSEA

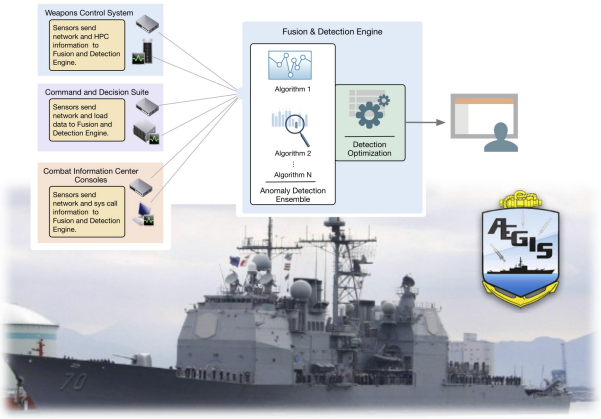
Sponsoring Program: PEO Integrated Warfare Systems (IWS) 1.0, AEGIS Integrated Combat System

Transition Target: AEGIS

TPOC:
(540)284-0035

Other transition opportunities:
Integrated Maritime, Ground, and Aerial Combat Systems

Notes: Warden is designed to use data captured by several sensor modalities such as network sniffers, logs, and load monitoring software. Warden includes a fusion and detection engine where an ensemble of detectors identifies deviations from a baseline model. Warden also includes a collection of detectors to identify deviations from baseline models. Warden's Ensemble Framework includes sensitivity controls in the form of detection optimization algorithms to reduce false positives. This is particularly important, as false alarms quickly erode operator trust.



Copyright 2018, Star Lab Corp.

WHAT

Operational Need and Improvement: Cyber-attacks against mission-critical combat systems are a growing concern across the Department of Defense. Combat systems are comprised of subsystems running customized Linux and real-time operating systems, enterprise intrusion detection systems and security products. A threat detection system is required to address gaps in weapon system security such as the inability to (1) detect undocumented attacks, (2) operate without impacting real-time constraints of modern combat systems, and (3) rapidly detect attacks while also achieving a low false positive rate.

Specifications Required: The threat detection system should be capable of being integrated with any hardware and software system. The system should provide real-time detection of imminent, undocumented cyber-attacks while also having no impact on system message latency or application performance. The system should identify cyber-attacks using data collected through network traffic, computer usage logs, and load monitoring software. False alarms should be minimized.

Technology Developed: Warden consists of a lightweight sensor package that monitors combat system behaviors, e.g., communication patterns, application performance statistics, application control-flow statistics, etc.; an ensemble of detectors to identify cyber threats, in particular, undocumented attacks delivered by the advanced persistent threat (APT); and reasoning algorithms in the form of an artificial neural network to verify malicious activity. Warden's minimally invasive sensors and efficient, highly-reliable algorithms detect attackers attempting to access or tamper with and alter combat system software/firmware, and they severely limit an attacker's freedom of maneuver if access is obtained.

Warfighter Value: Star Lab's novel technology applies anomaly detection to unique combat system operational environments for the purpose of cyber threat detection. Warden is minimally invasive allowing it to be integrated with real-time operating systems. Additionally, operators can trust that Warden will detect only real cyber threats as advanced artificial intelligence algorithms are used to reduce the occurrence of false positives. The potential of this technology is so promising Innovative Defense Technologies (IDT) has partnered with Star Lab during the Phase II to support the integration of the technology into the Aegis combat system.

WHEN

Contract Number: N00178-18-C-7002 **Ending on:** December 21, 2018

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Sensor Framework	Low	Combat system degradation no more than 1%	4	October 2018
Detection Ensemble Framework	Med	Detection within 90 seconds of attack with < 1% false positive rate	4	October 2018
Logging and User Reporting	Low	Manual evaluation by AEGIS SMEs	4	August 2018
Deployment and Configuration Interface	Low	Manual evaluation by AEGIS SMEs	5	November 2019
Transition	Med	Prototype demonstration on representative system	5	December 2019
Transition	Med	Prototype demonstration on representative system	6	December 2020

HOW

Projected Business Model: Star Lab's business goal is to license this technology to Prime integrators. Under this business model, Star Lab will provide a flexible perpetual license to its software per a pricing guide to be developed during the later stages of Phase II. Star Lab's product licensing model was purposely chosen to offer the lowest total cost of ownership (TCO) for our customers, compared to the cost of hiring, developing, and maintaining internal security solutions. Unlike many software vendors who are only interested in making a quick sale, Star Lab develops long-term relationships with its customers, typically becoming a trusted security partner across a number of product lines and corporate initiatives. Additionally, Star Lab will offer product support for training, tailoring, integration, and deployment. Star Lab utilizes a straightforward pricing rate per hour for professional support and works with customers to estimate the time needed to transition from initial concept to production deployment.

Company Objectives: In the short term, Star Lab will integrate and transition Warden through its partnership with IDT. During the Phase II and possible Phase III, Star Lab will demonstrate and validate this technology through seminal test events using existing (potentially augmented) system integration test procedures within a test environment provided by IDT. Long-term objectives include leveraging existing anti-tamper / cybersecurity programs across the DoD to developed numerous strategic partnerships with key DoD Prime integrators. Collectively, these efforts strengthen the company's commercialization strategy and provide Star Lab with the proper foundation to bring this novel solution to a wide range of markets.

Potential Commercial Applications: In addition to the defense industry, Warden can be leveraged to protect mission-critical or safety-critical systems in the information technology (IT), manufacturing, industrial, and medical sectors. These systems, like defense systems, are critical to the American way of life. Novel capabilities are desired to prevent costly, and even life-endangering impacts of cyber attacks, from adversaries that leverage undocumented attacks.

Contact: Adam Fraser, COO
adam@starlab.io 202-706-7027

Topic: N152-096

QuickFlex, Inc.

FlexDuo - An FPGA Accelerated, Flexible Execution Mission Processing

FlexDuo distributed mission processing computer architecture provides reconfigurable FPGA capability to advanced avionics architectures. This capability allows for the ability to perform high speed video processing in support of advanced architectures while also dynamically securing unsecure networks via integrated security. Simultaneously, FlexDuo supports current and future high-speed, high-power hardware and more video-intensive processing. Initially targeting V22 Osprey, AH- 1Z, and UH-1Y helicopters as a rapid acquisition path to securely insert true commercial off-the-shelf hardware into military applications. FlexDuo's innovative approach helps future-proof systems while reducing cost by minimizing the use of preloaded FPGA-based architectures or specific chips, providing software portability, integration and upgrades via standards-based interfaces, and miniaturization. QuickFlex provides products and services in development of and support of high-performance, state-of-the-art, reconfigurable systems and circuit solutions, novel security protections, fault tolerant solutions, and sophisticated decision engines for embedded, desktop, and networking technologies. FlexDuo technology is anticipated to be a spiral integration into rotorcraft and airframe avionics.

Technology Category Alignment:

Advanced Computing/Software Development
Trust Foundations
Advanced Electronic Protection Techniques and Technology

Contact:
Sally Draper
sdraper@quickflex.com
(210) 824-2348
http://www.quickflex.com
SYSCOM: NAVAIR
Contract: N68335-17-C-0388

Booth: 603
Room: Club Room East
Presenting: Apr 11th at 9:10 AM

Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.
NAVAIR 2018-833

Topic # N152-096
FlexDuo - An FPGA Accelerated, Flexible Execution Mission Processing
QuickFlex, Inc.

WHO

SYSCOM: NAVAIR

Sponsoring Program: PMA 275 V22 Osprey Program and PMA 276 H-1 Helicopter Program

Transition Target: V22 Osprey, AH-1Z and UH-1Y Helicopters

TPOC:
(301)342-5690

Other transition opportunities: The FlexDuo distributed mission computing technology is ideal for other new or retrofitted Navy and DoD (attack) rotorcraft and fixed wing aircraft, as well as civil air systems. The architecture could also potentially be utilized for securing systems, radar applications, and/or basically anywhere Field Programmable Gate Arrays (FPGAs) that need to be secured or networked are installed.

US Navy Image 180204-N-XK809-047, available at https://www.navy.mil/management/photodb/photos/180204-N-XK809-047.JPG

Notes: FlexDuo's versatile multi-node design will enable it to be scaled for use on a variety of aircraft and other systems, providing further cost savings and enhancing its commercialization potential. The state-of-the-art FlexDuo approach helps future-proof systems, while providing a more cost effective, high performance, fault tolerant architecture designed for next generation, increasingly computationally intensive algorithms.

WHAT

Operational Need and Improvement: To replace centralized mission computer/processing, the Navy needs a more cost effective, flexible, distributed architecture supporting current/future high speed/high power hardware and more video intensive processing with increased mission computing fault tolerance. As a team member of three companies, QuickFlex is performing offload of Central Processing Unit (CPU)/Graphics Processing Unit (GPU) functions and dynamic securing of the network.

Specifications Required: Overall team goals: maintain full situational awareness (S/A) across 4 Extended Graphics Array/High Definition (XGA/HD) (720 & 1080p) displays & processing maps, digital video, & sensor data, even if loose up to 50% of Processing Nodes. Architecture should have singular nodal processing system of at least 3 nodes with documented expandability limit, reduced unit cost 20% or less, & include new, higher speed systems (i.e., Ethernet). QuickFlex goal: provide secure, flexible high-performance distributed processing architecture.

Technology Developed: FlexDuo's defining feature is the ability to sub-divide a software (SW) workload between groups of SW processors & hardware (HW) acceleration components and at runtime dynamically allocate these tasks between constituent components, taking into account possibility of HW being destroyed, lost, or compromised when making the dynamic allocation. FlexDuo implementation will consist of a collection of FPGA-accelerated Processing Nodes (PNs) with capability to react to lost PNs & automatically restore their associated functionality. Lost or failing PNs are detected by SW developed by another team member. To accommodate various functions, FlexDuo provides a flexible execution model: functions may run on CPU or be implemented on FPGA & GPU resources for HW acceleration. FlexDuo uses compliant Real Time Operating System (RTOS) to guarantee functions will not interfere with each other when running on CPU. FlexDuo uses innovative techniques to compartmentalize functions for individual unit testing, increasing overall system reliability while removing need to exhaustively test & certify every possible permutation of simultaneous process allocations.

Warfighter Value: Supports mission success/safety: provides operators with full system functionally even in event of node failure while providing increased S/A, more real-time comprehensive video & other feeds. Reduces costs: minimizes use of aviation specific chips, provides SW portability, integration & upgrades via standards-based interfaces, miniaturization, & performance hedge against obsolescence.

WHEN

Contract Number: N68335-17-C-0388 **Ending on:** June 20, 2018

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Phase II Base	N/A	Submitted Architecture and Design Documentation Version 1, including unclassified analysis of FlexDuo architecture security requirements.	4+	June 2018
Phase II Base	N/A	Submitted User Guide and Read Me First Version 1 for implementation of the FlexDuo technologies.	4+	June 2018
Phase II Base	N/A	Finalized FlexDuo initial infrastructure software using selected board, operating system, and necessary driver(s) for communication; submitted FlexDuo Software Code Version 1 and software video demonstration.	3+	June 2018
Phase II Option I	N/A	Demonstrate FlexDuo Architecture on Processing Node demonstration and development platform incorporating Key FPGA technology, Fault Tolerance, Security, Networking, and other aspects of software and firmware design	6+	December 2019
Phase II Option II	Med	If Option II exercised, finalize Testing and Integration, finalize Demonstration and Development Platform, provide higher fidelity prototype and technical readiness level (TRL).	7+	December 2020

HOW

Projected Business Model: QuickFlex expects to use the direct sales model, with profits derived from product licensing sales, training, maintenance agreements, and engineering services contracts. Agreements are expected to include standard, yet customized, software licensing and maintenance agreements, with engineering research and development (R&D) and other services at industry rates. Depending upon customer needs, FlexDuo technologies can be customized for various environments using QuickFlex engineering R&D services.

Company Objectives: QuickFlex is proud to support our valued U.S. Federal Government (e.g., DoD, NASA, DoE, and others), DoD contractor, and other customers. QuickFlex and its experts have a proven record of successful product development from concept generation through deployment, supporting all phases of the product life cycle including: Qualifications (Flight), Certifications, Radiation Testing, Manufacturing, Support, and Upgrades. QuickFlex provides products and services in the development and support of high-performance, state-of-the-art, reconfigurable systems and circuit solutions, novel security protections, fault tolerant solutions, and sophisticated decision engines for embedded, desktop, and networking technologies. With current focus on leveraging QuickFlex's technologies and expertise to create secure, fault tolerant distributed mission computing, secure mobile-ad-hoc network (MANET)/fixed network technologies, and Cyber Security and Anti-Tamper solutions, QuickFlex's innovations are applicable for systems of all sizes. QuickFlex is continuing its long term goals of providing more standardized, broadly applicable, readily customizable technologies to help deliver lower non-recurring engineering (NRE), faster-time-to-deployment, reduced risks to programs, and increased product life.

Potential Commercial Applications: Beyond the DoD, FlexDuo can bring value to various National Critical Infrastructure (NCI) industries, such as the energy sector. Other sectors include oil and gas drilling and "smart factory" manufacturing where FlexDuo's capabilities make it a first-rate choice for more harsh manufacturing environments.

Contact: Sally Draper, President and CEO
sdraper@quickflex.com (210)824-2348

Topic: N161-070

BlueRISC, Inc.

Retrofitting Code into Embedded Binaries

For the last 15+ years, BlueRISC, Inc. has provided next generation system assurance and cyber security products and solutions for government and private industry. ThreatSCOPE Code Injection (CI) is a binary-level, vulnerability analysis toolkit (i.e. no source code required) enabling automated insertion of code into embedded executables/firmware. It provides vulnerability and performance guidance for the insertion of generic and cyber-hardening codes via an interactive GUI. ThreatSCOPE CI is directly applicable to a number of military and commercial embedded systems including unmanned systems (e.g. drones), avionics, industrial control systems as well as legacy embedded systems. ThreatSCOPE CI has been validated on real-world embedded firmware (e.g. Apache web server, avionics OFP) and shown to enable the patching of identified vulnerabilities (e.g. Heartbleed). We seek to license to large system integrators and integrate into Navy software assurance flows.

Technology Category Alignment:

Fixed Wing Vehicles (includes UAS)
Advanced Computing/Software Development
Trust Foundations
Integrating Architecture and Capability Demonstrations
Unmanned Ground and Sea Vehicles

Contact:
Kristopher Carver
kris@bluerisc.com
(413) 359-0599
https://www.bluerisc.com/
SYSCOM: ONR
Contract: N68335-17-C-0453

Booth: 607
Room: Club Room East
Presenting: Apr 11th at 9:30 AM
Corporate Brochure: https://navystp.com/vtm/open_file?type=brochure&id=N68335-17-C-0453

Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.
ONR Approval #43-4388-18

Topic # N161-070
Retrofitting Code into Embedded Binaries
BlueRISC, Inc.

WHO

SYSCOM: ONR

Sponsoring Program: ONR Code 31

Transition Target: Resilient Hull/Infrastructure Mechanical & Electrical Security (RHIMES)

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

Other transition opportunities: UAS's, Avionics, Critical infrastructure. In general, Navy and Department of Defense (DoD) programs with embedded software assurance and/or information assurance requirements.

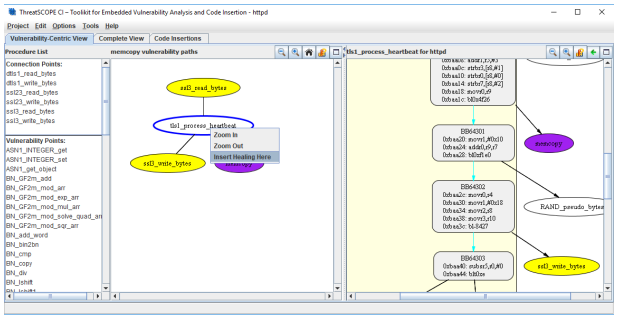


Image courtesy of BlueRISC, Inc., Copyright 2018,

Notes: This image depicts the ThreatSCOPE Code Injection (CI) toolkit. On the left is a list of procedures/functions, extracted directly from an embedded executable, that contain vulnerability-relevant artifacts. The center panel shows a visualization of an identified exploitable path with the option to perform automated code insertion on this path. The right panel shows a detailed control-flow graph view of the selected procedure/function - fine-grain code insertion is possible in this panel. Upon insertion of the cyber hardening code via the user interface, the toolkit automatically generates an updated executable/image containing the inserted code and provides this as an output.

WHAT

Operational Need and Improvement: Effectively securing the growing array of embedded devices in use on military platforms is a critical challenge. Furthermore, embedded devices play a central role in critical infrastructure and control key mechanical systems in the industrial, energy, and transportation sectors. In such applications, errors and vulnerabilities in the software running on these devices can have devastating impacts due to their ability to cause failures in the physical world. ThreatSCOPE CI not only performs an automated vulnerability characterization of these embedded software components, without the requirement of source code, but also enables the user of the tool to insert functionality into the software for the purpose of cyber-hardening or otherwise (e.g. new functionality in legacy systems, etc.).

Specifications Required: Critical embedded systems must be hardened against cyber-attack. For many of these systems (e.g. legacy), source code and/or a relevant development environment is not easily obtainable. Additionally, the insertion of codes (for cyber-hardening or otherwise) can have an impact on performance which must be managed.

Technology Developed: ThreatSCOPE Code Injection (CI) is a binary-level, vulnerability analysis toolkit (i.e. no source code required) enabling automated insertion of code into embedded executables/firmware. It provides vulnerability and performance guidance for the insertion of generic and cyber-hardening codes via an interactive GUI. The tool ensures that the inserted code operates within the existing constraints of the embedded software maintaining intended functionality while minimizing performance overhead. ThreatSCOPE CI has been validated on real-world embedded firmware (e.g. Apache web server, avionics Operational Flight Program - OFP) and shown to enable the patching of identified vulnerabilities (e.g. Heartbleed).

Warfighter Value: ThreatSCOPE CI enables vulnerability analysis and cyber hardening of embedded software without the requirement of source code. The solution is directly applicable to a number of military and commercial embedded systems including unmanned systems (e.g. drones), avionics, industrial control systems as well as legacy embedded systems. ThreatSCOPE CI will give warfighter's assurance that mission-critical embedded systems can be hardened against malicious cyber-attacks while maintaining operational mission functions.

WHEN

Contract Number: N68335-17-C-0453 **Ending on:** October 31, 2019

Milestone	Risk Level	Measure of Success	Ending TRL	Date
SBIR Phase I proof-of-concept prototype demonstration	N/A	Proof-of-concept vulnerability analysis and cyber hardening via code injection in vulnerable Apache Web Server embedded executable	5	1st QTR FY17
ThreatSCOPE CI vulnerability characterization and generic code insertion support	Low	Prototype toolkit validated through test and evaluation	6	3rd QTR FY19
ThreatSCOPE CI UAS Demonstration	Med	Cyber hardening while maintaining functional correctness on a relevant embedded system application	7	1st QTR FY20
ThreatSCOPE CI Avionics OFP Demonstration	Med	Cyber operational requirements met in developmental test and evaluation of avionics system	8	1st QTR FY21
Transition solution into Navy/DoD program(s) and/or commercial offering	Med	Cyber operational requirements met in operational test and evaluation	9	1st QTR FY22

HOW

Projected Business Model: Since 2002, BlueRISC has worked with the government to provide innovative solutions to cutting-edge problems in the cyber-security space. BlueRISC will license the ThreatSCOPE CI toolkit to large system integrators for utilization with Navy and DoD platforms, such as unmanned aircraft, avionics systems and embedded control systems. BlueRISC will provide users with full documentation, as well as example use-cases, on how to use the ThreatSCOPE CI toolkit. BlueRISC has commercialized toolkits resulting from SBIR efforts in the past and will leverage its existing online and licensing infrastructure. These toolkits have been sold worldwide in more than 15 countries.

Company Objectives: Binary-level compilation, exploitability analysis and cyber-hardening are core competencies of BlueRISC, making this Navy effort align directly with its corporate direction. BlueRISC's expertise and relationships in these domains will ensure the success of the solution beyond this SBIR Phase II effort. BlueRISC will employ a multi-pronged strategy, via existing partnerships in the defense space, to transition the ThreatSCOPE CI toolkit to Navy programs as well as the broader DoD market. BlueRISC will also leverage existing relationships in the industrial control space (specifically the energy sector) to commercialize the tool outside of the government.

Potential Commercial Applications: ThreatSCOPE CI is expected to further the software assurance field by enabling the retrofitting of embedded firmware with cyber hardening codes at exploitability relevant locations. The project is an ideal fit for BlueRISC and will provide a strong opportunity to not only target government programs but to also transition the technology to the commercial sector, specifically targeting embedded systems. BlueRISC will target embedded systems in the commercial space (e.g. drones, Internet-of-Things - IoT, Industrial Control Systems - ICS, etc.) via a cloud-based rental model enabling broader adoption in an easy-to-use and cost-effective manner.

Contact: Kristopher Carver, Technical Director
kris@bluerisc.com (413) 359-0599

Topic: N161-068

JPAnalytics LLC

The Modular Clandestine Communications System (MCCS)

JPAnalytics' Modular Clandestine Communications System (MCCS) is an underwater acoustic communications system capable of delivering reliable communications in challenging environments while being virtually undetectable by adversaries. JPAnalytics lives by the motto "Where Data, Theory and Analysis Create Innovative Solutions" to harness its expertise in signal processing, underwater acoustics, communications and embedded systems and develop paradigm-shifting solutions in underwater acoustic communications and detection. The MCCS addresses extensive needs in undersea vehicles, weapons and sensors. Its proprietary processing algorithms and modular signal, software and hardware architectures enable robust operation in challenging environments and efficient system optimization to satisfy user requirements and constraints. The MCCS has been extensively tested with field data and analyzed by independent organizations. JPAnalytics is looking for visionary customers and innovative and resourceful partners.

Technology Category Alignment:

Scalable Teaming of Autonomous Systems
Networks and Communications
Unmanned Ground and Sea Vehicles
Acoustic, Seismic and Magnetic

Contact:
Dr. James Preisig
jpreisig@jpanalytics.com
(508) 986-9425
http://jpanalytics.com/
SYSCOM: ONR
Contract: N68335-17-C-0550

Booth: 609
Room: Club Room East
Presenting: Apr 11th at 9:20 AM

Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

ONR Approval #43-4388-18

Topic # N161-068

The Modular Clandestine Communications System (MCCS)

JPAnalytics LLC

WHO

SYSCOM: ONR

Sponsoring Program: Forward-Deployed Energy and Communication Outpost (FDECO)

Transition Target: Forward-Deployed Nodes, UUVs, Sensors and Weapons

TPOC:
Dr. Robert Headrick
bob.headrick@navy.mil

https://www.onr.navy.mil/en/About-ONR/History/tales-of-discovery/remus

Other transition opportunities: MCCS provides a reliable and clandestine (Low Probability of Detection or LPD) communications capability for underwater platforms. Communications between manned platforms, between manned and unmanned platforms and between unmanned platforms are all supported. Any scenario where clandestine acoustic communications is needed between undersea platforms is a transition opportunity for MCCS. JPAnalytics desires to work with transition partners with the vision and desire to exploit the capabilities of MCCS to create new capabilities for our nation's warfighters.

Notes: The MCCS will enable reliable and clandestine mission critical communications for the Mk 18 Mod 2 Kingfish shown here and future generations of unmanned undersea vehicles, sensors and weapons.

WHAT

Operational Need and Improvement: The use of distributed and small manned and unmanned undersea platforms is an important component of current and future operations. Communications between the distributed platforms necessary to maintain cross-platform coordination, situational awareness and positive operational control is often required in these operations. Currently, this typically relies on commercial modems that employ fairly high source levels and/or readily recognizable acoustic signals. However, for many missions the probability of success relies on maintaining a stealthy posture. A reliable, robust and clandestine undersea communications capability that is adaptable to diverse environments, platforms and operational constraints and requirements is needed to insure the future viability of these missions.

Specifications Required: To develop an acoustic communications system employing stealthy (covert, LPD) techniques for sending information through ocean acoustic channels at modest to moderate bit rates (100s of bits per second) over ranges of 1 to 10 km.

Technology Developed: The MCCS core technologies are modular signal, algorithm and hardware architectures that enable efficient system optimization and implementation to meet user needs. The modular signal architecture integrates a unique "featureless" signal set with error correction coding that reliably transmits information at very low SNRs and is difficult for an adversary to detect. The modular signal processing algorithm architecture integrates a two-stage adaptive signal detection, synchronization, and demodulation algorithm with an efficient decoding structure and enables efficient implementation on low-power processors. The modular hardware architecture combines COTS embedded processing modules with customized "wet-end" hardware to allow the use of state-of-the-art low-power processing technology in parallel with "wet-end" system optimization for specific applications.

Warfighter Value: JPAnalytics' Modular Clandestine Communications System (MCCS) provides a reliable underwater acoustic communications capability to the warfighter in challenging environments while being virtually undetectable by adversaries. This will increase the probability of success of the missions discussed above under "Operational Need". The modular signal and processing structure enables the MCCS to automatically update itself or be easily updated by an end user to better maintain an LPD posture and to adjust to changing operational constraints and requirements.

WHEN

Contract Number: N68335-17-C-0550

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Demonstrate MCCS Core Stage 1 algorithm running on COTS embedded processor. Demonstrate low counter detection vulnerability of MCCS signal set.	N/A	Algorithm running and providing accurate results. Signals satisfy user LPD metrics.	4	3rd QTR FY18
Demonstrate entire MCCS received signal processing chain running in real-time on COTS embedded processor.	Low	COTS processing card satisfying SWaP constraints and numerically accuracy of embedded algorithms comparable with that of off-line algorithms.	4	2nd QTR FY19
Demonstrate MCCS implemented on COTS embedded processor reliably demodulating signals under operational conditions.	Low	Message success rate exceeding user defined threshold in operational conditions.	5	3rd QTR FY19
Demonstrate communications to and from a selected operational platform over desired operational ranges.	Med	Message success rate exceeding user defined threshold in operational conditions.	6	4th QTR FY20

HOW

Projected Business Model: JPAnalytics will pursue Phase II Option and Subsequent Phase II funding to transition the prototype system developed with the Phase II Base funding to application-specific, deployment-ready systems. Once this is done, JPAnalytics will consider three primary methods of transition. These are to license MCCS processing algorithms and optimized signal sets and array configurations to prime contractors to integrate into their systems, to provide programmed embedded processing chips to acoustic modem manufacturers, and to produce board sets, arrays and transducers for direct sale to end users or system integrators. Both one-time and subscription-based licenses will be considered.

JPAnalytics plans to retain the sole right to modify MCCS signal sets optimized for end-user applications and approval rights for the transmit transducers and receive hydrophone arrays used with the system. JPAnalytics will also offer to customers hydrophone array and wet-end electronics design services to enable them to maximize overall system performance.

Company Objectives: JPAnalytics lives by the motto "Where Data, Theory and Analysis Create Innovative Solutions" to harness its expertise in signal processing, underwater acoustics, communications and embedded systems and develop paradigm-shifting solutions in underwater acoustic communications and detection. Our work is always guided by the harsh task master of reliable operation in the real-world environments in which our nation's forces must operate. Our objective is to identify challenging candidate applications and needs, develop new core technological capabilities and rapidly and efficiently transition those capabilities into solutions that meet the needs of our customers. JPAnalytics is looking for visionary customers and innovative and resourceful partners with whom it can work to achieve this objective.

Potential Commercial Applications: The MCCS signal structure and detection methodology is useful and applicable in any applications where communications occurs at very low signal-to-noise ratios and in dynamic multipath environments.

Contact: Dr. James Preisig, President
jpreisig@jpanalytics.com (508) 986-9425