Innovative Defense Technologies

Cyber Resiliency via Virtualization for Combat Systems

Virtualization has the potential to increase cyber resiliency for Navy combat systems by providing flexible system configurations that can adapt to degraded performance conditions. Vendor and combat system agnostic virtual resource management and performance analysis tools are necessary to reach this potential. Innovative Defense Technologies (IDT) designs, develops and delivers solutions that enable the rapid delivery of warfare capabilities for the DOD. A sustained competitive advantage is achieved through vendor-agnostic management of virtual resources and reliable, real-time performance assessment capability that is normalized on system events, configurable to any combat system. This technology will be applied to AEGIS and SSDS to validate the innovation by 2021, available for transition to government and contractors desiring to leverage virtualization for increased cyber resiliency.

Technology Category Alignment:
Human Computer Interfaces (HCI) for Decision Making
Assuring Effective Missions
System Interfaces & Cognitive Processes
Modeling, Simulation & Test Infrastructure

Contact:
Claire Moore
CMoore@idtus.com
(703) 522-5561
https://idtus.com/

SYSCOM: NAVSEA
Contract: N68335-19-C-0149

Booth: 19
Room: FST at NSL
Presenting: Nov 7th at 9:45 AM

WHO
SYSCOM: NAVSEA
Sponsoring Program: Program Executive Office Integrated Warfare System (PEO IWS) 1.0 – AEGIS Combat System; PEO IWS 10.0 - Ship Self Defense Systems (SSDS)
Transition Target: Future Aegis Combat System leveraging Virtualization BL (FY23+)
TPOC:
Other transition opportunities:
Examples include Ship Self Defense Systems (SSDS), Army Integrated Air & Missile Defense (IAMD), Terminal High Altitude Area Defense (THAAD), Ground Based Midcourse Defense (GMD), etc.
Notes: IDT supported the successful live-fire from the AEGIS Virtual Twin in March 2019 and continues to push how virtualization can be used tactically onboard a combat ship. In future AEGIS baselines, the need to efficiently manage the virtual builds and rotate the system under test in the virtualized environment will be required.

USS John Paul Jones (DDG 53) launches a Standard Missile (SM) 2 during a live-fire test of the ship’s Aegis weapons system on Feb. 8, 2014. US Navy Photo

WHAT
Operational Need and Improvement: Cyber resiliency, which enables a system to combat or fight through a cyber-attack, is essential in today’s cyber environment. It is paramount that systems have the ability to protect, detect, react and restore themselves after a cyber-attack, or accidental or malicious events. In computing, virtualization refers to techniques that abstract hardware from software and create virtual instantiations of systems, hardware, storage, or networks that operate independently. Use of virtualization to implement cyber resiliency capabilities can help manage a cyber-attack and will be a new capability for AEGIS and SSDS.
Specifications Required: Virtualized Combat System Resources. The solution assumes no changes are required to existing builds and therefore able to deliver this capability directly to the Navy, as an integrated software product, provided IDT has access to the certified build of the Navy or DoD system.
Technology Developed: Helm’s Wheel software, with Real-Time Risk Assessment (RRA) and Revolving Defense Attack Surface (RDAS) software components, integrated for Aegis and SSDS.
Warfighter Value: Improved cyber resiliency minimizes the time spent recovering and restoring the system from a cyber-attack and maximizing the time spent with full mission capabilities. Through distributed allocation, the ability to operate the system from different physical or logical locations reduced the impact of system degradation at any one location. Maturing this capability onboard a ship will maximize the potential for tactical use and improved cyber resiliency once combat ships are being deployed with builds run on a virtualized platform.

WHEN

<table>
<thead>
<tr>
<th>Contract Number</th>
<th>N68335-19-C-0149</th>
</tr>
</thead>
<tbody>
<tr>
<td>Milestone</td>
<td></td>
</tr>
<tr>
<td>Component proof of concept for RRA and RDAS</td>
<td>N/A</td>
</tr>
<tr>
<td>RDAS and RRA component validation in a lab environment</td>
<td>N/A</td>
</tr>
<tr>
<td>RDAS and RRA component validation in a relevant environment</td>
<td>Low</td>
</tr>
<tr>
<td>Helm’s Wheel prototype validation on AWS</td>
<td>Low</td>
</tr>
</tbody>
</table>

Projected Business Model: IDT intends to offer the Helm's Wheel capability as a software license deliverable with associated customized services in order to integrate this system resiliency capability with the target mission critical system. The primary source of revenue for Helm's Wheel will be in the associated services where the software will be offered royalty free to the government, and for a fee to industry. IDT also expects to receive development funding from specific customer sin order to add additional features to Helm's Wheel.

Company Objectives: IDT is interested in partnering with other DoD programs that have mission critical systems such as combat systems, mission control systems, and fire control systems. IDT will initially be transitioning Helm’s Wheel to NAVSEA IWS 1.0 Aegis, and NAVSEA IWS 10.0 SSDS, and would like to speak with other SYSCOM’s programs as part of the STP program and FST event to identify additional opportunities for transition.

Potential Commercial Applications: Helm’s Wheel is ideal for mission critical systems that reside on limited and/or sensitive infrastructure, where resiliency is needed. This includes power grid, oil & gas, transportation, material shipping, and commercial space markets.