Monday, March 2, 2020
10:00 a.m. – 10:20 a.m.
Achieving Cyber Resiliency: Protecting the Controls Impacting Weapons

Ed Suhler
Vice President, OT Cybersecurity Implementation Services
Mission Secure, Inc.

Abstract:
Shipborne command and control, systems, and weapon platforms offer unique challenges for cybersecurity. First, operators must overcome all of the problems of protecting operational technology (OT) systems that share commonalities with industrial control systems (ICS). But, operating within some of the most cyber-contested areas in the world, these assets also need to function independently in non-connected environments. In assessing these cyber challenges, where are their potential impacts most dire? Directly inside the cyber-physical systems themselves and in the processes they control.

Addressing the cyber threats where they are most catastrophic is where cybersecurity needs to begin. Traditional cybersecurity approaches protect critical systems by layering barriers in front of potential adversaries to try to keep them at bay. We propose a new type of cybersecurity, one that assumes a determined adversary will gain access. Therefore, cyber-physical systems should not just be protected from intruders but, more importantly, resilient to potential cyber threats and attacks.

Put cyber protections in the physical processes we rely on to ensure mission execution—navigation; propulsion; hull, mechanical and electrical (HM&E); combat and weapons; and aviation controls. This method should include monitoring and protection capabilities spanning both the entire IT network as well as the control systems that sit on those networks and control the physical processes.

A new generation of technology exists to address these cyber challenges in both joint and connected ship-to-shore applications and in applications where the ship needs protections when running independently or non-connected to shore-based systems. Mission Secure's EagleEye Platform was purpose-built to address these challenges. Using comparative analysis and change detection between the digital command and control signaling (operator activity; Ethernet, TCP/IP, or serial) and the raw physical analog signals (physical component activity; 24 VDC, 4-20 mA) with system awareness provided at the network traffic level, the MSi EagleEye Platform provides operators unprecedented insight and protection from the individual component level (Level 0) throughout the vessel ICS ecosystem to the network traffic layer (Level 3).

The MSi Platform is effectively a new ICS cybersecurity solution adding network traffic monitoring and activity correlation, an in-line fail-safe industrial firewall, and operator interface with automated component setup features. Similar to a missile warning system (MWS) on a tactical aircraft, the MSi EagleEye Platform can continuously monitor for cyber threats—even zero-day attacks, compromised supply chain components, or active attack—prevent potential cyber attacks, alert appropriate personnel, and provide initial threat information, even automatically restore firmware to a gold standard. The patented MSi Platform is the 21st century's cyber warning system integrated with threat inoculation for cyber-physical systems—from the IT network down to Level 0 field devices.

A proven, commercially deployed industrial control system (ICS) cybersecurity solution, the MSi EagleEye Platform has immediate and substantial defense applications for protecting Navy platforms and systems, including vessels, aircraft, and shore-based facilities such as shipyards, manufacturing plants, and power or distribution utilities.