Cyber Security for Aviation Weapon Systems

Submitted by Katie Dey on Tue, 03/06/2018 - 11:55am. Contributor:
David Burke

BIO

David A. Burke, Ph.D., joined Naval Air Systems Command (NAVAIR) in 2010 as part of the Air Vehicle Modification & Instrumentation (AVMI) Division. Transitioning to support the Common Systems Integration (CSI) Office in 2011, he was tasked with improving the interoperability of Navy Unmanned Aerial Systems to better meet warfighter needs. As the technical lead for the CSI office Dr. Burke stood up and chaired the Naval UAS Interface Control Working Group (ICWG), a collaborative effort between the Navy and industry partners to develop Naval Interoperability Profiles (NIOPs). Dr. Burke was also heavily involved in NATO UAS Interoperability efforts including being the chairman for NATO STANAG 4586, the NATO UAS command and control standard. In 2014 NAVAIR Cyber Warfare Detachment (CWD) was established to guide NAVAIR in how to address emerging cyber threats to military weapons systems and Dr. Burke was chosen as its Technical Director, leading all technical development efforts. In June 2017, Dr. Burke was selected to a Senior Leadership (SL) position as Director of the CWD where he leads the development of overarching cyber warfare technical strategy, processes and capabilities within NAVAIR, and is the primary point of contact for technical exchanges both within NAVAIR and with external agencies.

Dr Burke graduated from North Carolina State in 2004 with BS degrees in Computer Engineering, Electrical Engineering, and Computer Science; in 2007 with MS degree in Computer Engineering; and in 2010 with Ph. D. in Aerospace Engineering. He also holds a graduate certificate in Cyber Warfare from Naval Postgraduate School.

ABSTRACT

Naval aviation is a complex mix of IT (information technologies) and OT (operational technologies) operating in some of the most challenging environments around the globe. Nearly all are heavily reliant on software and processing hardware. From military aircraft and missiles to support equipment and logistics/maintenance environments, these unique embedded systems, diverse missions and varying strategic environments make standard cybersecurity processes difficult to apply, and consequently drive new methods for establishing robust cybersecurity postures. The Naval Air Systems Command (NAVAIR) is the acquisition arm for Naval Aviation and responsible for the cybersecurity posture of these military systems. As such, NAVAIR is applying engineering rigor to the cybersecurity process. This talk discusses some of the general challenges and opportunities including where development science would be helpful for embedded aviation systems.

Slides for this presentation are unavailable. Please see below the publicly releasable NAVAIR report on Controls Applicability Assessment For Naval Aviation Weapon Systems.

Other available formats:

Cyber Security for Aviation Weapon Systems
Switch to normal viewerSwitch to experimental viewer

Presentation Presentations