ABSTRACT for the 2015 ISA WWAC Symposium

Demystifying Government-Validated Solutions

Navy Case Study Shows How Critical Infrastructure and Facilities Can Benefit

Frank Ignazzitto[1]*

[1]Ultra Electronics, 3eTI, 9715 Key West Avenue, Suite 500, Rockville, MD 20850
(*Email: frank.ignazzitto@ultra-3eti.com and Phone: 800-449-3384)

SUBMISSION TYPE

30 minute presentation

KEYWORDS

Department of Defense, Malware, Security, SCADA Networks, Information Asssurance

ABSTRACT

The federal government and Department of Defense (DoD) facilities require resilient networks that assure availability of critical assets to support US armed forces at home and abroad. Current mandates provide significant incentives for these agencies to build more efficient and resilient systems that consume less energy and are protected from disasters, accidents and attacks.

With recent reports of Havex, Black Energy and other malware variants targeting industrial control systems and SCADA operations, facility managers are intensely concerned about providing industrial controls systems security for buildings and utility systems. Many of these include an array of legacy components that cannot be equipped individually with modern or advanced security software. This presentation will focus on a case study of the Navy's Enterprise Industrial Controls System (EICS) deployment for military-grade protection of both physical and cyber aspects, as well as analysis, modeling and prediction capabilities for building systems.

Using a base-wide wired and wireless network that scales and extends across 15-plus bases, the system provides an advanced cyber-secure framework for an optimized industrial controls system (ICS) that seamlessly blends direct digital controls (DDC) and SCADA networks into a single, cohesive installation with command and control management. The platform also provides a video surveillance for comprehensive critical-infrastructure protection. All components adhere to the DoD instruction on information assurance (IA) implementation and FISMA (Federal Information Security Management Act) requirements. The EICS solution is a foundational system through which the Navy complies with congressional mandates to securely reduce energy consumption. It has been independently tested for vulnerability mitigation, and further allows energy managers operational flexibility that is compliant with DoD-grade IA.

The presentation will outline how similar approaches and architectures can be directly applied for industrial critical-infrastructure applications. It will show that comprehensive and fully validated security

systems can improve performance and extend security beyond the firewall without negatively impacting operations, schedules, workflows or budget.

ABOUT THE AUTHOR

Frank Ignazzitto, *Vice President of Marketing for Ultra Electronics, 3eTI, brings more than 30 years of technology and management experience to industrial and government decision makers tasked with managing highly complex networks and security systems. With a background that spans military service, international business management, and start-up business execution, his career has focused most recently on business leadership in the defense and energy industries. Mr. Ignazzitto has dedicated the last 15 years driving new technology adoption with the Department of Defense, the intelligence community, Homeland Security and many other federal agencies. His diverse technology experience includes human-machine interface, electro-optical nanotechnology and advanced fuel cell systems in addition to 14 years in the oil and gas sector. After earning his BS in Engineering at the United States Military Academy, West Point, Mr. Ignazzitto served as an officer in the Air Defense branch of the US Army. Contact: frank.ignazzitto@ultra-3eti.com.*