Situation Awareness in the Maritime Domain

Keith Muir

Michael Babec

L3Harris Technologies

Situation Awareness in the Maritime Domain

INTRODUCTION

Central to enabling safe and unrestricted maritime trade around the world, the need to ensure security of ports, harbors and shipping continues to emerge as an increasing challenge for government agencies and commercial entities in the 21st century.

Whether it be the threat of attack by small surface vessels, divers or autonomous underwater vehicles (AUVs) from the sea or unmanned aerial vehicles (UAVs) and ground assault from ashore, ports and harbors must be equipped with next-generation technologies capable of providing authorities with advanced warning and necessary levels in situation awareness (SA).

Problem Sets

According to NATOôs Center for Maritime Research and Experimentation (CMRE), both commercial and military ports and harbors can be difficult to protect due to their significant size; amount of sea- and land-based traffic; and proximity to urban areas.

Describing how small boats have been used to attack docked ships in the past (USS Cole attack, 12 October 2000), CMRE doctrine warns how the threat of attack can come from a variety of ñsmall [and] hard-to-detect sourcesò which can complicate the task of port protection.

ñThis complex environment makes it difficult to monitor ports for hostile intent and even more challenging to develop a response that is non-lethal to the many people who are at the port and who may live, work, and recreate in the surrounding area,ò CMRE doctrine describes.

Protective measures available to government agencies and port authorities include a layered approach to cyber security; groundbreaking electro-optical and infrared (EO/IR) camera and radar solutions; as well as command and control (C2) software designed to network defensive capabilities into a Common Operating Picture (COP).

Technologies must satisfy minimum standards for both onshore and offshore critical national infrastructure (CNI) as stipulated in the Safety of Life at Sea Conventionôs 2004 International Ship and Port Facility Security (ISPS) Code.

According to the ISPS Code, which was created following the 9/11 terror attacks in the United States in 2001, government agencies and port authorities must be able to ñdetect security threats and take preventative measures against security incidents affecting port facilities used in international tradeò.

The ISPS Code describes a series of escalating Maritime Security (MARSEC) levels, which include MARSEC Level 1 (the employment of surveillance equipment to monitor restricted areas) and MARSEC Level 2 (the employment of persistent surveillance technologies).

Examples of WESCAM MX-10MS deployment include integration of the sensor onboard unmanned surface vessels (USVs), such as Zyvex Marine ôPiranhaôand the ñMarine Autonomy Surface Testbed (MAST) 13ò of the UKôs Defence Science and Technology Laboratory. The Royal Australian Navy and Australian Border Force have successfully deployed the WESCAM MX-10MS sensor onboard their Cape Class Patrol Boats to provide maritime security during border protection missions.

Having proven its ability to support the maritime security requirements of surface vessels, customers are now requesting the WESCAM MX-10MS sensors be integrated on fixed installations ashore to protect CNI as well as docked surface vessels within the port or harbor itself.

ñThere has been success in a number of areas with customers operating WESCAM MX-10MS turrets on vessels,ò Babec explained. ñOne customer, in particular, has asked to take that same payload and integrate it ashore as part of a networked tower configuration in order to overlook the ocean. We have received very good feedback for both wireless and wired operations, all of which can be integrated into a COP for enhanced SA.ò

Describing L3Harrisôextension of WESCAM MX-10MS applications beyond its more traditional defense and security marketplace, Babec also highlighted how the employment of the sensor could assist commercial shipping agencies and port authorities in reducing insurance premiums.

The WESCAM MX-10MS features a multi-spectral, multi-sensor payload suite that provides superior imaging under a wide range of illumination and atmospheric conditions. A high definition (HD) thermal imager provides the ability to see targets under no-light conditions and provides high target contrast in the day. A wide-angle HD color day camera provides surveillance, situational awareness, and target detection capability, while a narrow-angle camera provides long-range target recognition and identification capability. The imagers are supported by a gimbal that provides a full 360-degree field-of-regard and automatic scanning functions that service to minimize operator workload.

Stabilization performance is essential to optical range performance. The 4-axis architecture separates the inner axis, which performs the fast and fine motion required for super

Further, the WESCAM MX-10MS leverages L3Harrisôinvestment in high-end imaging systems by providing state-of-the-art features that significantly reduce operator workload, allowing them to focus on the target, versus the equipment. An internal inertial navigation system, consisting of an embedded GPS and inertial measurement unit coupled with an internal laser rangefinder; provide accurate and stable target geo-location. The WESCAM MX-10MS also features advanced image processing algorithms, easy-to-use, and robust auto-tracker and image blending capability.

System-of-System0.7W* 1 862422 i4(ETQ0.00000912 0 612 792 reW*nBT/F2 9 Tf1 1 0 0 1 86624 18285 Tm1 0 0 rg1 0 0 RG[S)-7ysET

Specializing in EO/IR & radar technology, public safety and military-grade tactical communications, as well as C2 software and analytical instrumentation, L3Harris stands ready to integrate WESCAM MX-10MS sensors and distributed system-of-systems approach into existing infrastructure.