Annals of DAAAM for 2010 & Proceedings of the 21st International DAAAM Symposium, Volume 21, No. 1, ISSN 1726-9679
ISBN 978-3-901509-73-5, Editor B. Katalinic, Published by DAAAM International, Vienna, Austria, EU, 2010
Make Harmony Between Technology and Nature, and Your Mind will Fly Free as a Bird
Annals of DAAAM International

COMMAND AND CONTROL ARCHITECTURE FOR MARITIME SAFETY INTEGRATED SYSTEMS

CATA, M[arian]; POPA, C[atalin] & BEIZADEA, H[aralambie]

Abstract: *This paperwork is approaching the various aspects of intelligent command and control systems used in maritime domain protection. The goal of paper research is to find out and finally to propose, some practical solutions that would effectively reduce the risks and the vulnerabilities within commercial shipping informational management, in particular with application in Constanta harbour activity. Thus, as a first step in the research demarche, the paper is disseminating the particular characteristics and features for the command and control architecture, detailing the functional hierarchy, and the physical and operational architectures, in order to provide a sufficient protection and security in maritime area.*

Key words: *systems engineering, maritime security*

1. INTRODUCTION

Maritime Domain Protection (MDP) systems must provide command and control coherent functions for critical decision-making support, in case of authority's activities for coast, port and waterways management. The systems should provide port safety monitoring prior vessels activity, in order to control ports entry and inland waterways acces, by integrating data systems, connected to a large rank of sensors and other data sources, performing specific further functions as: processing, storage, display and dissemination. Therefore, these systems should provide various safety port functions as: detection, classification and tracking of approaching objects. In this respect, automatic Identification System (AIS) technology is able to provide situational awareness based on positive identification of approaching vessels. Rule-based software can be configured to identify situations that are out of the rank or norm and further to provide alarms in order to alert commanding port authorities. Warnings and alarms can be set up to warn trained operators when a ship is unidentifiable or when approaching unsafe waters. When disaster occurs, the system provides support to search and rescue and emergency response teams as well. Automated reports facilitate the coordination and planning of resources, movement histories and schedules, intelligence and customs clearance information.

2. ARCHITECTURAL MODEL

Some authors (Maier & Rechin, 2000) provide an architectural views methodology and others (Buede, 2009) an architectural model with tree views: functional, physical and operational. The functional architecture describes what the system must do, under what conditions it must perform these functions and how the achievement of these functional capabilities is met using appropriate metrics. The physical architecture represents partitioning of physical resources, specifically the technological components and subsystems, which must be synthesized into an integrated grand system that performs the system's functions. The operational architecture maps the physical architecture and its resources to the system functions in a manner suitable for quantitative analysis within a discrete-event simulation or other suitable simulation or analytical modeling tool (McCarthy C. et al., 2006). The Maritime Domain Protection physical architecture can combine several separate systems into an integrated architecture model. Such models can be fully functioning for commercial shipping in Constanta harbour, as it has been shown in bellow figure.

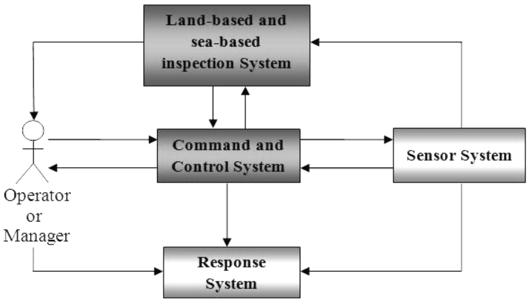
Land-based and sea-based inspection System
Command and Control System
Sensor System
Operator or Manager
Response System

Fig. 1. The proposal for a MDP physical architecture

3. FEATURES OF A MARITIME C2 SYSTEM

A modern maritime command and control system must provide multiple features that can be grouped in five classes (Lockheed Martin Corporation, 2010):

Open Architecture:

- distributed processing allows simplified modification or upgrading of system equipment as technology evolves;
- operate on the latest Windows or UNIX platforms;
- standard industry interfaces are used throughout the design, permitting easy expansion of the equipment;
- system architecture supports networking to additional control centres or operator workstations;
- Interface Adapter Units accommodate in the addition of radars, cameras and communications equipment;

Object Oriented Rule-Based System:

- provides rule base for workstation operator tasking;
- vessel and target movements are automatically processed applying expert tactical knowledge, safety and security rules and standard operating procedures, providing automated decision aids;
- operators can routinely re-define safety, security and surveillance zones based on dynamic conditions;
- watchstanders can be alerted to evolving situations of special interest, ensuring continuous, comprehensive management of safety and security and traffic coordination;

Fused Data Display:

- All fused-track data is available to each operator workstation or selectable by type of sensor source, to create the single best view of the situation.
- Track data from all sources are displayed on a single screen within each operator workstation.
- The Area of Interest can be sectored to any configuration.
- many picture-in-picture views that can be displayed for discrete track views.

Database Linked to Workstation Displays:

- vessel attributes are dynamically associated with the vessel track on the geographic display;
- ship movement and target information forms are readily completed with minimum data entry;
- real-time displays are available for all categories of data.
- vessel data are consistent between operator workstations, stand alone PCs and any external users;
- the full relational database interfaces to external sources to facilitate updating and exchange;

Sensor Data Sharing:

- data from multiple sources can be simultaneously displayed on all operator workstations;
- fewer operators are required to manage a geographic area;
- sharing allows fusion of data from various sensors, including radar and electro-optic sensor fusion;
- maximum flexibility provides additional robustness for sensitive national security related functions.

4. SOFTWARE ARCHITECTURE

The proposed architecture for the C2 system is based on:

(1) **Open standards**: to assure the interoperability level, communication protocols and data representation.

(2) **Modules:** the system is built from modules that contain services and have a lot of important characteristics like reuses capacity and autonomy

(3) **SOA:** the modules must provide services and consume services provided by other modules. SOA architecture offers characteristics like reuses, scalability, flexibility and interoperability.

(4) **Distributed system:** The most important characteristic of the distributed architecture in this case is possibility to dislocate modules in various geographic regions.

The software architecture is defined on a layers model and is divided in two main layers: “Module” and “Service Bus”, like it has been underpinned in figure no. 2.

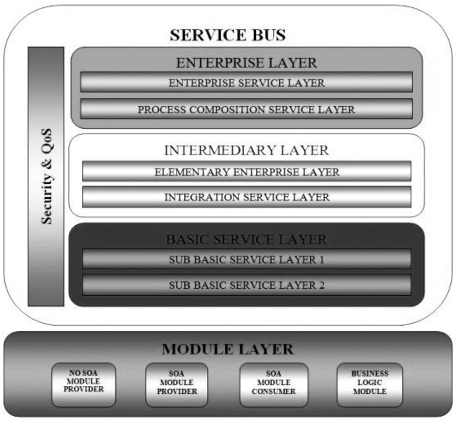

Fig. 2. The proposed model of a modular architecture

4.1 “Module” layer

This software components layer contains modules that implement a service consumer or a service provider. The modules use a bus to provide or consume services in the same time.

4.2 “Service Bus” layer

This bus is an abstract concept used to explain what a module have the communication possibility with all the system only by this way. In fact, one module interactions with different layers from bus for realize his scope: provide or consume services. These layers are:

(1) **Basic Service Layer**: this logical layer may contain a series of sublevels named Sub-Basic Service Layers. Each of these sublevels can correspond for a special technology.

(2) **Intermediary Layer**: this layer is divided in two sub-layers for a better understanding of the architecture. The base layer is named Integration Service Layer and is responsible with the integration of the different technologies (and with data normalization) of the Basic Service Layer to supply them to the superior level (Elementary Enterprise Service Layer). To achieve this, the Integration Service Layer must contain a series of adaptors which allow that any layer’s service can be adapted in the Elementary Enterprise Service Layer. Also, the Integration Layer contains an agent for each sub-layer that supply coordination and synchronisation of the booths layers (SBSL and EESL). The superior layer, named Elementary Enterprise Service Layer, contains services directly developed in this layer, I/O services delivered by Basic Service Layer. These services are considered to be the high precision for the superior levels. EESL is a Web Service level based on SOA technology.

(3) **Enterprise Layer**: like the Intermediary Layer, this is also divided in two sub-layers in order to define the understanding. The goal of the Process Composition Service Layer is to create the business processes using the elementary services which are provided by the Elementary Enterprise Service Layer. This layer embeds the complexity of the service, implements the business process and provides the maintenance of the process state. The Enterprise Service Layer contains services for representation of the business macro-processes. This layer provide a very complex service formed by a different elementary services supplied by the inferior layers. Practically, the simple services will be aggregated to supply a service that is considerate complete and that is also realising a macro-functionality.

(4) **Security and Quality of Service Layer**: the mission of this layer is to coordinate and modify the security levels which are implemented by each Sub-Basic Service Layer and especially by the Elementary Enterprise Service Layer. Also, this layer provides a very clear quality of the service.

5. CONCLUSIONS

The requirements of an increased security for port operations ask for revolutionary C2 decision-making technologies dinnamicly designed for the operators and managers, in order to guarantee a rapid situational understanding and control. The proposed architecture is a major step for building a coherent informational system on regional level, in order to assure an efficient port management and control. The research team intend to develop this concept and to interfere with the economic environment in order to get a further valoriziation of proposed concepts.

6. REFERENCES

Buede, D. (2009) *The engineering design of systems*, John Wiley and Sons, (2nd Ed.), New York, ISBN 0-471-28225-1

Maier, M.W.; Rechin E. (2000) *The art of systems architecting*, CRC Press, (2nd Ed.), New York, ISBN 0-8493-0440-7

McCarthy, C.; Russ, W.; Vaidyanathan, R.; Paulo, E.P. (2006) *An Integrated Systems Architecture to Provide Maritime Domain Protection*, JDMS: The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, Volume 3, Number 2

*** (2010) http://www.lockheedmartin.com - Lockheed Martin Corporation, *Coastal and Border Surveillance - Integrated Systems for Monitoring Ports, Coastlines and Land Borders, Accessed on: 2010-08-14*

*** (2010) http://www.lockheedmartin.com - Lockheed Martin Corporation, *Maritime Safety, Security & Surveillance - Integrated systems for monitoring ports, waterways and coastlines, Accessed on: 2010-08-14*