Secured Architecture for Unmanned Surface Vehicle Fleets Management and Control

Pedro Merino Laso
French Maritime Academy (ENSM)
38, rue Gabriel Péri BP 90303
44103 Nantes Cedex 04, France
pedro.merino-laso@supmaritime.fr

David Brosset
Naval Academy Research Institute
Ecole navale - CC 600 F29240
Brest Cedex 9, France
david.brosset@ecole-navale.fr

Marie-Annick Giraud
SOFRESUD
777 Avenue de Bruxelles
83500 La Seyne sur Mer, France
marie-annick.giraud@sofresud.com

***Abstract*—Cyber-physical systems contribute to building new infrastructure in the modern world. These systems help realize missions reducing costs and risks. The seas being a harsh and dangerous environment are a perfect application of them. Unmanned Surface vehicles (USV) allow realizing normal and new tasks reducing risk and cost i.e. surveillance, water cleaning, environmental monitoring or search and rescue operations. Also, as they are unmanned vehicles they can extend missions to unpleasing and risky weather conditions. The novelty of these systems makes that new command and control platforms need to be developed. In this paper, we describe an implemented architecture with 5 separated levels. This structure increases security by defining roles and by limiting information exchanges.**

***Index Terms*—USV, cyber-physical systems, SCADA, security, control system**

I. Introduction

Nowadays, maritime transportation is the preferred mean of transport for most of merchandise. In the European Union, 76.1% of transported goods is made by seas, which represents 50.6% of the value of its trade [1]. However, aerial transportation is preferred for merchandizes with high value/weight ratio. But there exist other important maritime assets like energy, communication and fishing. Ships, ports communication systems and different types of buildings compose the needed infrastructure to accomplish these goals.

All these structures represent an important, strategic and economic value. A failure or a successful attack would have vital implications caused by dysfunctions of i.e. water supply, public health and energy. For this reason, they are often considered as critical infrastructure.

Particularly, the seas are a harsh environment where the laws are sometimes not respected. Nowadays, pirate attacks represent an actual risk of naval security that implies these assets and crew members. Environmental disasters also need particular attention. Cyber-physical systems are used in SCADA systems to control and survey procedures, which extends the attack surface to cyberspace. SCADA systems can be integrated in Unmanned Vehicles (UV) to automatize dangerous tasks.

The project Sea4M, coordinated by SOFRESUD, is supported by the French Environment & Energy Management Agency (ADEME) in the frame of the Future Investments Programme.

The particularities of UV make that new architectures need to be developed. Sea4M [2] project looks for building a whole architecture of command and control of heterogeneous Unmanned Surface Vehicles (USV) with multi-mission purposes. This architecture needs to be capable of coordinating cooperative missions of semi-autonomous vessels where multiple roles need to be considered in decision-making and control processes.

The paper is organized as follows. First, a short related work section introduces some research about the security of drones and SCADA systems. The third section presents the new developed architecture. This architecture is based on five different levels. Section 4 explains main security measures. Finally, a conclusion lists the main benefits of the architecture and gives some perspectives.

II. Related Work

In many cases, autonomous systems are the best option to use to supervise and control sensitive systems. To survey and protect these assets, multiple systems are deployed as aerial drones (UAV), unmanned surface vehicles (USV) and SCADA systems. All these protection systems also become critical if they aim to protect critical infrastructure.

USV are nowadays an important field of research due to its low cost and wide applications [3]. Typical examples of their applications are environmental monitoring [4], surveillance [5] and underwater mapping [6].

Sometimes, novelty USV projects reuse existing control software for other unmanned vehicles as UAV [7]. In this case the chosen solution was Monitor Planner, that allows a fast developing of a global solution. However, maritime navigation has different characteristics and uses different information sources. For example, waves can block camera views and pilots use a compass and radar to compensate this disadvantage. There also exists adapted solutions to control semi-autonomous USV [8]. All considerations for maritime navigation have been taken into account. On the other hand, these systems do not consider different roles and tasks that exist in reality. That is, their focus is on control software without paying attention to commandment chain.

SCADA systems that equipped UV can also be vulnerable. The security of these systems is more and more addressed

by the scientific community because of their presence in numerous critical systems. The studies concern both anomaly detection and security properties modelling [9]–[11].

III. Proposed Architecture

In Sea4M project, we have chosen to conceive an architecture with five separate levels. ISA-95 industrial standard has inspired this approach [12]. This standard defines abstract levels going from 0 to 4 with different objectives.

Each level has a particular role which allows isolating tasks to increase security. Thin communications are needed between these levels but they can be easily protected due to this size and known structure. Other measures such as encryption and whitelisting will be used. Also, most of interchanged information does not involve confidentiality risks because it concerns public data i.e. AIS positions and RADAR detections.

Fig. 1 shows the defined levels: USVs, exploitation centre, operational centre and management. Centres are physically isolated increasing security and flexibility.

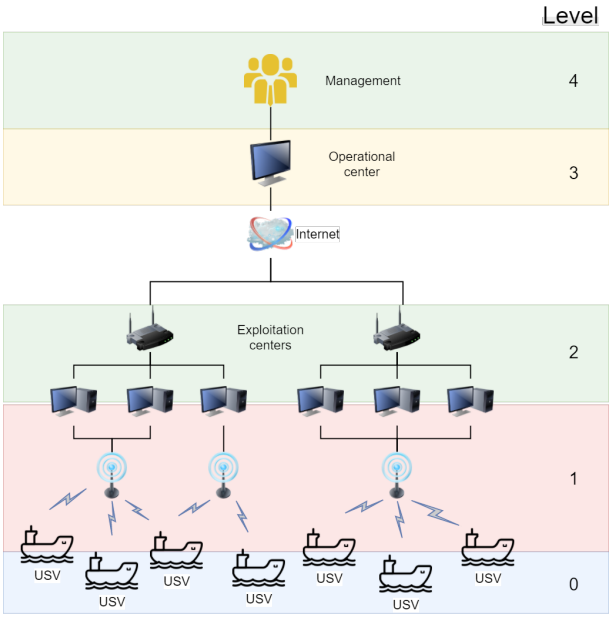

Fig. 1. Architecture schema with levels.

A. Level 4: Management

Management plan strategies and fix objectives. For that, they handle budgets and company resources to achieve them. In our application, they define the engaged means (people and USVs), objectives and priorities.

B. Level 3: Operational Centre

Operational centre receives orders and limitations from management centre. Centre plans specific missions based on this information. To specify the details of the mission they have an overview of the whole fleet of USV and external information as port data. Also, they have access to real-time data from the exploitation region that is observed by AIS and RADAR systems installed in different observation points.

Finally, they assign missions to exploitation centres. Due to isolation between centres to prevent security risks, level 3 should also coordinate operations if a mission engages more than one of those centres.

Another important mission is to survey that exploitation centres realize the assigned tasks as planned. That is necessary because they usually adapt missions during their execution in order to adapt them to variable conditions.

C. Level 2: Exploitation Centre

Exploitation centres monitor and perform missions described by operational centre. As USVs are semi-autonomous, in practice they monitor the vessels and for instances, they take control in difficult circumstances. They also monitor the state of the system to detect maintenance needs or problems that can impact on the mission. Each exploitation centre has an assigned fleet that cannot be controlled and monitored by other centres.

D. Level 1: SCADA (Automatism and Sensors)

SCADA systems comprise all systems that allow communicating, controlling and monitoring USVs. That is, the exploitation centre equipment that send and receive commands from USVs and inboard USV systems. Three groups of subsystems are included in this level: automatisms, sensors and communication systems. Among the most used sensors there are RADAR systems, GPS and LIDAR while the most common automatisms are the rudder and the motor. As USVs are heterogeneous, several embedded equipments are present in each vessel i.e. adapted rescue materials.

E. Level 0: Physic

Even though whole system has hardware components to simplify, we only consider USVs as physical part of the system because it is the part that interacts with physical world. So, all the embedded systems listed in previous subsection are considered at this level when they are seeing as material components.

IV. Security Measures

To secure the platform, different measures have been taken into account. Mainly, this protection consists of role-based tasks, physical and network isolation, secured connections and limitations on communications.

First, each level has defined roles as described in previous section. No other level can accomplish different tasks that those assigned. That is, level 4 communicates available means and objectives to be accomplished to level 3. Level 3 plans specific missions based on this limitations and order to level 2 to realize them. Level 2 monitor and control drones thanks to the sensors and actuators present on the USVs.

Second, each level and centre are physically distant. This isolation allows implementing resilient measures i.e. backup centre if first one is impacted. Also, computer networks are isolated to prevent intrusions.

Third, only verified systems can belong to the system thanks to whitelisting protection. Also, encrypted communications are

preferred in all exchanges. When that is not possible i.e. phone calls between levels 3 and 4, authentication protocols are used.

Finally, information exchanges are limited. Only two connected levels can communicate. To avoid espionage and attacks propagation, if multiple centres exist on the same level they can't send information between them. Also exchanged information are limited to the interests of each level i.e. level 4 receive a report of realized mission but it cannot visualize operation data as USV position.

V. Conclusion and Future Work

In this paper, we have presented the architecture of a novel system to control and manage USV fleets. Naval missions engage heterogeneous systems with a specific commandment chain. As USV operating processes are vulnerable in different manners, the implemented solution gives a vital importance to security.

Sea4M project has developed this architecture based on security by design principles. Five different levels allow separating systems, roles and tasks. Each level realizes limited operations with thin connections with other levels. Also, each level applies specific security measures chosen for its particularities.

Future works concern the development of an adapted Human Computer Interface (HCI) and a validation experiment in real context and missions. Also, a further security analysis will be performed for specific equipment and technologies.

Acknowledgment

The authors thank the members of the Sea4M project for their support and advice given during the writing of this article.

References

[1] European Commission, "Eu transport in figures. statistical pocketbook 2017.," tech. rep., European Union, 2017.

[2] (2018, Apr.) Sea4M summary sheet. [Online]. Available: http://www.ademe.fr/sites/default/files/assets/documents/sea4m_fiche_laureat.pdf

[3] Z. Liu, Y. Zhang, X. Yu, and C. Yuan, "Unmanned surface vehicles: An overview of developments and challenges," *Annual Reviews in Control*, vol. 41, pp. 71–93, 2016.

[4] C. Powers, R. Hanlon, and D. G. Schmale, "Tracking of a fluorescent dye in a freshwater lake with an unmanned surface vehicle and an unmanned aircraft system," *Remote Sensing*, vol. 10, no. 1, p. 81, 2018.

[5] S. Shriyam, B. C. Shah, and S. K. Gupta, "Decomposition of collaborative surveillance tasks for execution in marine environments by a team of unmanned surface vehicles," *Journal of Mechanisms and Robotics*, vol. 10, no. 2, p. 025007, 2018.

[6] B. Metcalfe, B. Thomas, A. Treloar, Z. Rymansaib, A. Hunter, and P. Wilson, "A compact, low-cost unmanned surface vehicle for shallow inshore applications," in *Intelligent Systems Conference (IntelliSys), 2017*, pp. 961–968, IEEE, 2017.

[7] J. Villa, J. Paez, C. Quintero, E. Yime, and J. Cabrera, "Design and control of an unmanned surface vehicle for environmental monitoring applications," in *Robotics and Automation (CCRA), IEEE Colombian Conference on*, pp. 1–5, IEEE, 2016.

[8] G. A. Osga and M. R. McWilliams, "Human-computer interface studies for semi-autonomous unmanned surface vessels," *Procedia Manufacturing*, vol. 3, pp. 982–989, 2015.

[9] Rafael Ramos Regis Barbosa. Anomaly detection in scada systems-a network based approach. 2014.

[10] Pedro Merino Laso, David Brosset, and John Puentes. Analysis of quality measurements to categorize anomalies in sensor systems. In *Computing Conference, 2017*, pages 1330–1338. IEEE, 2017.

[11] Jiexin Zhang, Shaoduo Gan, Xiaoxue Liu, and Peidong Zhu. Intrusion detection in scada systems by traffic periodicity and telemetry analysis. In *Computers and Communication (ISCC), 2016 IEEE Symposium on*, pages 318–325. IEEE, 2016.

[12] I. S. of Automation, "Ansi/isa-95," 1995.