The Unmanned Autonomous Systems Cyberspace Arena (UCA). A M&S Architecture and Relevant Tools for Security Issues Analysis of Autonomous System Networks

Marco Biagini[1], Sonia Forconi[1(✉)], Fabio Corona[1], Agatino Mursia[2], Lucio Ganga[2], and Ferdinando Battiati[3]

[1] NATO Modelling & Simulation Centre of Excellence, Rome, Italy
{mscoe.cd01, mscoe.cde02, mscoe.cd04}@smd.difesa.it
[2] LEONARDO Finmeccanica, Rome, Italy
{agatino.mursia, lucio.ganga}@leonardocompany.com
[3] Scuola delle Trasmissioni e Informatica, Rome, Italy
ferdinando.battiati@esercito.difesa.it

Abstract. In the framework of the modern tactical scenarios and the increasing employment of Unmanned Autonomous Systems (UAxS) in multi-battlespace domains (land, naval, air and cyberspace), the threats to the communications and networks available among the units on the battlefield are becoming ever more challenging. It thus becomes crucial to protect communications and networking of these systems from possible hostile actions aimed at jeopardizing mission execution in the Cyberspace. This paper is focused on the required properties and capabilities of a UAxS Cyberspace Arena (UCA), a simulation-based communication and networking environment where it will be possible to evaluate UAxS tactical communication solutions as well as the related countermeasures in case of cyber-attacks and in terms of their resilience and reactivity to the considered security threats.

The UCA is developed as an emerging concept to support UAxS Concept Development and Experimentation phases and its overarching architecture and related M&S tools are described, focusing on a Networks and Communications Simulator (Cyber Arena), within a Modelling and Simulation as a Services approach. In conclusion, the UCA architecture aims to demonstrate how it will be possible, in such an environment, to evaluate UAxS Security issues and challenges related to tactical communication and networking solutions in case of cyber-attacks, both in term of their resilience and reactivity to the considered security threats.

Keywords: Unmanned autonomous systems · Cyberspace · CSSE · Cyber defence

J. Hodicky (Ed.): MESAS 2016, LNCS 9991, pp. 168–175, 2016.
DOI: 10.1007/978-3-319-47605-6_13

1 Introduction

In the context of modern strategies for combat and patrol operations, tactical scenarios pose demanding challenges to the communication and networking infrastructure available among the units on the battlefield. Furthermore, during these operations the use of Unmanned Autonomous Systems (UAxS) in multi-battlespace domains such as the land, naval, air and space is becoming actual and challenging. Military decision making support systems at all levels depends essentially on the communication networks and in the case of failure might negatively influence the mission execution [14]. In the case of communication failure, the technique of Modelling and Simulation might be implemented to overcome it for a defined time [15]. It is crucial to protect communications and networking of these systems from possible hostile actions aimed at jeopardizing mission execution in the Cyberspace. Considering the Cyberspace a virtual transversal domain to the battlespace domains, this paper describes the required properties and capabilities of a UAxS Cyberspace Arena (UCA).

The UCA is being developed as an emerging concept to support UAxS Concept Development and Experimentation phases. It originates from the implementation and customization of an ongoing National (Italian) Military Research Program (PNRM), the Cyber Security Simulation Environment (CSSE). The UCA aims to provide a simulation-based communication and networking environment where it will be possible to evaluate UAxS tactical communication solutions as well as the related countermeasures in case of cyber-attacks and in terms of their resilience and reactivity to the considered security threats.

Therefore, the first section of this paper briefly illustrates main initiatives of the NATO Modelling and Simulation Centre of Excellence (M&S CoE) in the field of multi-robots simulation environment. Then the CSSE Program is introduced in the next section, in order to present its objectives and how it contributes in the international context to the studies about the problems related to cyber threats facing the communications networks (tactical or infrastructured) of military units.

In the following section the central topic of the paper is addressed. The requirements for the development of a UCA and the related modelling and simulation (M&S) tools, in terms of properties and capabilities, are described aiming at the delivery of an environment capable at investigating cyber security issues in such tactical context. The UCA concept is based on an integrated simulation environment allowing to model UAxS communication networks, the security threats typical of scenarios where they operate, as well as the related countermeasures. As result, the section illustrates the UCA overarching architecture and related M&S tools, focusing on a Networks and Communications Simulator (Cyber Arena). This architecture is developed as a possible federation of systems, like a Robot Scenario Generator and Animator (RSGA), possibly a C2 system, real and virtual Robots, exploiting heterogeneous technologies, such as Robotic Operating System (ROS), Systems in the loop (SITL) and High Level Architecture (HLA) Run-Time Infrastructure (RTI), gateways between different communication protocols within a Modelling and Simulation as a Services approach.

In the conclusions, it is stressed that the UCA architecture aims to demonstrate how it will be possible, in such an environment, to evaluate UAxS Security issues and

challenges related to tactical communication and networking solutions in case of cyber-attacks, both in term of their resilience and reactivity to the considered security threats.

2 NATO M&S Activities Supporting UAxS Concept Development and the UCA Architectural Design

The NATO M&S CoE has being involved in several initiatives regarding the UAxS concept Development and Experimentation. Following a brief overview of these initiatives to introduce the Cyber Space Arena Concept.

The Simulated Interactive Robotics Initiative (SIRI). It was a cooperative project between the M&S CoE and the US Joint Staff J6, in collaboration with a former Finmeccanica company. It was focused on interoperability issues for integrating a Multi-Robot System (MRS) in a Multinational Coalition Scenario [4]. In particular, the initiative was focused on exploring the use of National Information Exchange Model (NIEM) MilOps domain. It is an eXtensible Markup Language (XML)-based data model for message exchange in an unmanned systems environment [5]. The MRS was based on Unmanned Ground Vehicles (UGVs) and their Artificial Intelligence was based on the ROS [6]. MRS were remotely controlled by US [7].

The M&S CoE has then hosted and participated at the 3rd workshop of the CUAxS project. The workshop goal was to make tangible progress on the concept development of the CUAxS. The outcomes of this workshop were:

- the "Stratification matrix". This matrix put in relationship the level of autonomy with the type of operations (the NATO Campaign themes) and the operational functional areas, as defined in the Allied Joint Doctrine [11], or type of unit (i.e., combat, combat support, combat service support)
- the definition of the UAxS functionalities, in order to identify the possible vulnerabilities of these systems and, therefore, the countermeasures to exploit these weaknesses.

In this framework, M&S CoE proposed to design an architectural concept based on M&S tools suitable to support the CUAxS concept development and experimentation activities and the implementation of these tools to support the Concept Development Assessment Game (CDAG) wargame [3].

Following the M&S CoE participated to the meeting of the 136 Specialist Team of the Information System Technology (IST), another STO panel regarding Security Challenges for Multi-domain Autonomous and Unmanned C4ISR Systems [8]. During the workshop was given by the CoE representative the contributes to the team regarding the SIRI experience and in that occasion were put the basis for a M&S based tool to support the countering UAxS Concept Development.

In addition the M&S CoE participates to the NMSG 145 Research Task Group with a permanent representative [9]. This Tak group has the aim to operationalize the Command and Control – Simulation environments (C2SIM) interoperability standards and technologies. In particular, the M&S CoE is contributing to the development of the

recommendations for formalizing the C2SIM standard with a STANAG. The CoE involvement is as part of the subgroup who is in charge to develop the C2SIM extension for UAxS.

3 Cyber Security Simulation Environment (CSSE)

The Unmanned Autonomous Systems Cyberspace Arena project originates from the implementation and customization of an ongoing National (Italian) Military Research Program (PNRM), the Cyber Security Simulation Environment (CSSE). It arises from the need to study, through the use of advanced simulation systems, problems related to cyber threats facing the communications networks (tactical or infrastructured) of military units may be subjected engaged in. CSSE has been transposed the directions provided by the working groups (current and old) in the International arena such as:

- NATO SAS-065 (NATO C2 Maturity Model),
- SAS-085(C2 Agility)
- MSG-117 (M&S in support of Cyber Defense).

The CSSE demonstrator is an open and non-classified environment, its configurability and the ability to create and/or modify equipment models, protocols, threats and countermeasures entirely new make it a versatile tool for the institutional activities of the Italian Army School of Transmission and Computing (SCUTI).

The CSSE project objectives are:

- analyze the state of art in the fields of Modelling and Simulation and Cyber Security with a detailed focus on military networks and cyber threats;
- define and describe operational scenarios, making also reference to the outcome of NATO SAS-065 and NATO SAS-085 activities, in which operate military tactical networks subject to cyber attacks;
- define and develop a simulation architecture that will allow for building a test bed environment (demonstrator) in which attackers and defenders can exercise the scenarios, cyber threats and related countermeasures previously identified without disturbing the real operational network;
- evaluate, on the demonstrator, different situations, building a repository of reference scenarios to be used for cyber operators training;
- disseminate the results obtained from the campaign of experiments

The demonstrator architecture is open experimenting cyber issues not only on tactical networks but in general on communication networks and the Live - Constructive simulation techniques is used to evaluate state-of-the-art cyber threats and countermeasure.

The demonstrator can also be seen as one component of a future integrated system (Cyber Trainer) in which exercises are performed by several groups that operate in Red versus Blue Forces type scenarios.

4 Cyber Arena: "Communication and Networking Simulation"

Modelling and Simulation (M&S) is a key tool in supporting Unmanned Autonomous Systems (UAxS) CD&E activities and addressing associated security challenges focussing on the communications and networking protection of these systems from possible hostile actions aimed at jeopardizing mission execution in a virtual domain namely Cyberspace Arena.

4.1 Unmanned Autonomous Systems Cyberspace Arena

The Unmanned Autonomous Systems Cyberspace Arena (UCA) is an emerging concept developed to support the Unmanned Autonomous Systems (UAxS) Concept Development and Experimentation (CD&E) phases. The UCA concept is based on an integrated simulation environment to provide a simulation-based communication and networking environment to evaluate UAxS tactical communication network, the security threats typical of scenarios where they operate, the related countermeasures in case of cyber-attacks and in terms of their resilience and reactivity to the considered security threats.

In the UAxS conceptual architecture, illustrated in Fig. 1, the UCA element provides the robots communication and network simulation capability. The M&S of Communication and Networking components plays a relevant role in all simulation architecture oriented to test net-centric architectures. Performances of communication and networking component in some scenarios (i.e. in the mobile and tactical scenarios) are often unpredictable due to:

- Effects of the land orography
- Low bandwidth available
- Presence of noise (environment or intentional jamming)
- Communication and networking devices probability failure
- Low availability of communication infrastructures

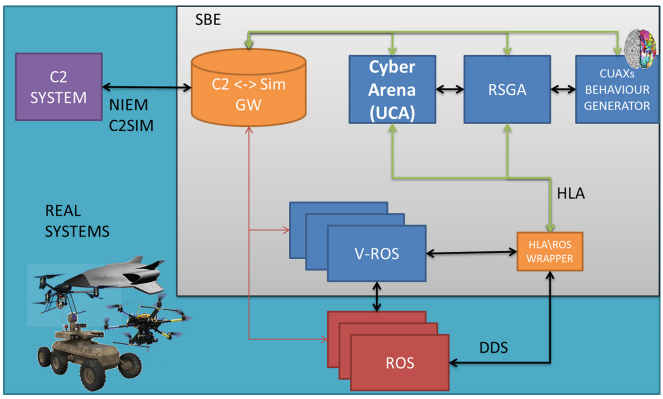

Fig. 1. Conceptual architecture of M&S tools to support the UAxS CD&E phases

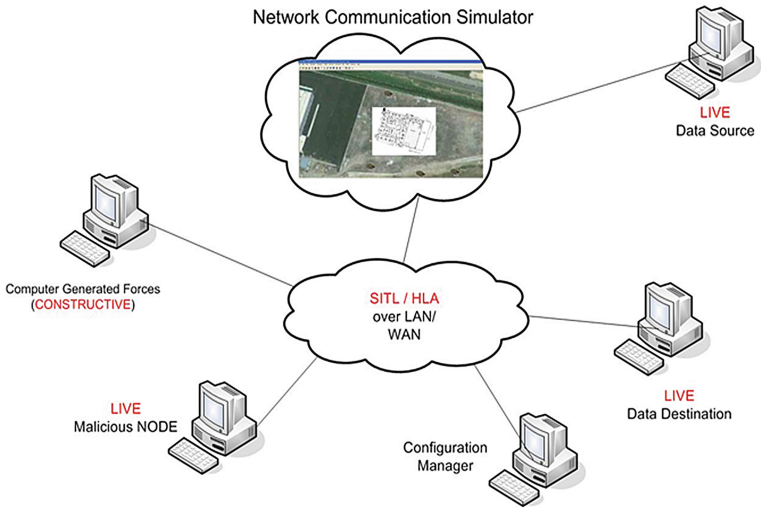

Fig. 2. The UCA components

The UCA components, illustrated in Fig. 2, are:

- Data source and Data destination represents the start point and the end point of the information exchange that will suffer the cyber attack
- Network Communication Simulator tool to provide to NATO modelling and simulation tools (OPNET) to develop, design, analyze and to verify and validate (V&V) network and communication architectures and solutions applying NATO standards (NAF)
- System-in-the-Loop (SITL) capability allows for establishing a connection "Live-Constructive" through which the real hardware and the simulation environment interact as a single unified system. This allows for:
  - Analyze effects of a simulated network on a real application
  - Utilize simulation as a traffic generator to load real network
  - Conduct stress tests on real equipment/application in an environment that simulate operational conditions
- HLA (High Level Architecture) is an architecture of "general purpose" type defined for the simulation reuse and interoperability. HLA supports the data exchange, with or without "Time Synchronization", so as other synchronization type, rescue/recovery operations, information distribution and dissemination. HLA is a IEEE international open standard that is evolving through international processes. This connectivity assures that HLA based experimental frameworks should be plug and play connected to UCA [16].
- Computer Generated Forces (CGF) is a tool with the following functions:
  - Creating and managing libraries of object (platform, sensor, weapon, etc.)
  - Scenario composition, defining the geographical location, kinematic and events.
  - Application of tools to the Mission Planning support

  - Animation of the scenario and subsequent scenario data distribution follow the standard
  - Using AI (Artificial Intelligent) tool for complex simulation.
- Malicious Node is a Kali distribution of Linux OS, it allows to launch cyber attacks both to real and simulated equipments.
- Configuration Manager is a web based application that coordinates the management of the scenarios set in the other CSSE simulators, and the management of the sessions results simulation (statistics).

The UCA architecture aims to demonstrate how is possible, in such an environment, to evaluate UAxS Security issues and challenges related to tactical communication and networking solutions in case of cyber-attacks, both in term of their resilience and reactivity to the considered security threats.

5 Conclusions

The paper illustrates the UCA emerging concept developed to support UAxS Concept Development and Experimentation phases and the possibility to evaluate UAxS tactical communication solutions as well as the related countermeasures in case of cyber-attacks. The UCA overarching architecture and related M&S tools presented is focusing on the relevant role plays by the M&S of Communication and Networking components. Also relevant aspects in the UCA field are the robots communication payload models, the robotic cyber attack models and the real systems to simulated environment interaction. The UCA architecture demonstrate how it is possible to evaluate UAxS Security issues and challenges related to tactical communication and networking solutions in case of cyber-attacks.

References

1. NATO ACT CEI CAPDEV: Autonomous Systems Countermeasures (2016). http://innovationhub-act.org/AxSCountermeasures. Accessed May 2016
2. NATO STO SAS 082: Disruptive Technology Assessment Game - Evaluation and Validation (2012). http://www.cso.nato.int/activities.aspx?pg=2&RestrictPanel=6&FMMod=0&OrderBy=0&OrderWay=2. Accessed May 2016
3. NATO STO SAS 086: Maritime Situational Awareness: Concept Development Assessment Game (CDAG) (2010). http://www.cso.nato.int/activities.aspx?pg=3&RestrictPanel=6&FMMod=0&OrderBy=0&OrderWay=2. Accessed May 2016
4. SSI Finmeccanica Company: SIRI Operational Scenario, Taranto (2015)
5. NIEM: National Information Exchange Model (2016). https://www.niem.gov/Pages/default.aspx. Accessed May 2016
6. ROS: Robotic Operating System (ROS) Documentation (2016). http://wiki.ros.org/. Accessed May 2016
7. Litwiller, S., Weber, M., Klucznik, F.: Improving robotic and autonomous system information interoperability: standardizing data exchange with XML. In: Hodicky, J. (ed.) MESAS 2014. LNCS, vol. 9055, pp. 24–39. Springer, Heidelberg (2015)

8. Byrum, F., Sidoran, J.: IST 136 Roadmap - Security Challenges for Multi-Domain Autonomous and Unmanned C4ISR Systems (Draft - unpublished). STO CSO (2016)
9. NATO STO NMSG 145: Operationalization of Standardized C2-Simulation Interoperability. STO CSO – STO activities (2016). http://www.cso.nato.int/activities.aspx?RestrictPanel=5. Accessed May 2016
10. MCDC: Policy Guidance – Autonomy in Defence Systems (2014). http://innovationhub-act.org/sites/default/files/u4/Policy%2520Guidance%2520Autonomy%2520in%2520Defence%2520Systems%2520MCDC%25202013-2014%2520final.pdf. Accessed May 2016
11. NATO Standardization Agency: Allied Joint Doctrine – AJP 1.0. NATO document, Brussels (2010)
12. Siegfried, R., Van den Berg, T., Cramp, A., Huiskamp, W.: M&S as a service: expectations and challenges. In: Fall Simulation Interoperability Workshop, Orlando, FL (USA), pp. 248–257 (2014)
13. NATO STO MSG 136: Modelling and Simulation as a Service. STO CSO – STO Activities (2016). http://www.cso.nato.int/activities.aspx?RestrictPanel=5. Accessed May 2016
14. Hodicky, J., Frantis, P.: Decision support system for a commander at the operational level. In: Dietz, J.L.G. (ed.) KEOD 2009 – Proceedings of International Conference on Knowledge Engineering and Ontology Development, Funchal – Madeira, October 2009, pp. 359–362. INSTICC Press (2009). ISBN 978-989-674-012-2
15. Hodicky, J., Frantis, P.: Using simulation for prediction of units movements in case of communication failure. World Acad. Sci. Eng. Technol. Int. J. Electr. Comput. Energ. Electr. Commun. Eng. **5**(7), 796–798 (2011)
16. Hodicky, J.: HLA as an Experimental Backbone for Autonomous System Integration into Operational Field. In: Hodicky, J. (ed.) MESAS 2014. LNCS, vol. 8906, pp. 121–126. Springer, Heidelberg (2014)