A Verification, Validation and Accreditation Process for Autonomous Interoperable Systems

Alberto Tremori, Pilar Caamaño Sobrino, Arnau Carrera Viñas, Giovanni Luca Maglione, David Solarna, Robert Been, and Thomas Mansfield(✉)

NATO STO Centre for Maritime Research and Experimentation, 400 Viale San Bartolomeo, La Spezia, Italy
{alberto.tremori,pilar.caamano,arnau.carrera,giovanni.maglione, david.solarna,robert.been,thomas.mansfield}@cmre.nato.int

Abstract. Navies, Industries and Research are investigating how to move to future mine counter measure operations where of multiple autonomous underwater vehicles work collaboratively with minimal human interaction. Modelling and simulation is proving to be a capable support to test autonomy by the adoption, in particular, on interoperable environments that may comprise of models, hardware and software-in-the-loop. Industry and NATO standards exist for federated simulation but the standards do not provide detailed guidance to carry out lean, comprehensive and consistent design, development and testing of distributed simulation for autonomy.

This paper presents a methodological framework and identifies process steps that support users in the design and development and allow development teams to carry out efficient verification, validation and accreditation activities on distributed simulation systems. The framework has been designed to be lean and efficient while producing outputs that comply fully with existing industry standard approaches.

The presented framework has been demonstrated on a distributed modelling and simulation system in a representative underwater environment.

Keywords: Verification and Validation · Acrediation · Mine Countermeasure Autonomous underwater vehicles · Modelling and simulation

1 Introduction

Multiple Autonomous Underwater Vehicles (AUVs) may be used to provide maritime Mine Countermeasure (MCM) capabilities [1, 2]. Typical mission scenarios require a range of AUV's with a variety of sensors to work collaboratively with limited human interaction. During these scenarios a wide range of autonomous interactions are likely to occur, each affected by a complex set of variable parameters.

At each stage of development, from conceptual design to the verification, validation and accreditation (VV&A) stage, techniques are required to visualize, analyze and document the performance of the system. The federated, distributed environment under test may consist of either models, hardware-in-the-loop and/or software-in-the-loop [3].

J. Mazal (Ed.): MESAS 2017, LNCS 10756, pp. 314–323, 2018.
https://doi.org/10.1007/978-3-319-76072-8_22

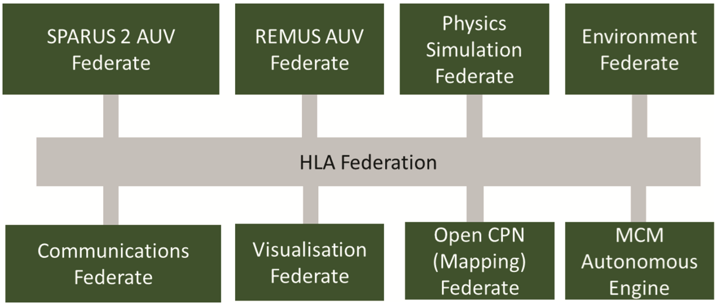

Fig. 1. Typical MCM simulation federation.

While high level industry standards exist for the VV&A of federated simulation environment, no detailed processes exist to guide the user through the process of VV&A for the type of distributed system required for the development of interoperable, autonomous systems. The lack of low level processes and guidance prevents the consistent execution of lean yet comprehensive test procedures.

Due to the complexity of the system interactions in a distributed hybrid federation that is simulating interactions between autonomous systems, innovative new low level processes and supporting procedures are required to allow consistent results to be obtained in the test of all federated simulation environments [4]. This process is required to guide the system VV&A stakeholders through all relevant phases of the development lifecycle.

This paper presents an innovative framework for the VV&A of distributed, hybrid Modelling and Simulation (M&S) federations. It allows an increased understanding of the hardware and software under test by combining it within operationally relevant live-virtual-constructive scenarios. The proposed framework enables this capability with a lean and efficient framework which complies with the latest Institute of Electrical and Electronic Engineers (IEEE) standards and industry best practices for VV&A [5, 6] as well as NATO Verification and Validation (V&V) guidance [7, 8].

This paper is structured as follows; Sect. 2 describes the structure of existing industry standard guidance for M&S VV&A activities. It also provides further information about a typical M&S federation and describes a typical MCM scenario with cooperating AUVs. Section 3 describes the proposed framework, detailing the procedural advice and the content of the document deliverables. The results of a practical system demonstration is discussed in Sect. 4. Section 5 presents the planned future work and Sect. 6 discusses the main conclusions.

2 Existing Modelling and Simulation Architecture

2.1 Example of a Federated M&S Environment

To allow the simulation of interoperable, autonomous systems required for operations such as MCM, a High Level Architecture (HLA) federation is composed. An example HLA federation is shown in Fig. 1.

Each federation represents a sub-system of the final mission environment. The federates exists throughout the development lifecycle of the system. Initially, the federation is likely to exist of behavioural models which allow the anticipated performance of the complete system to be developed and understood. If the system is being developed by multiple teams, these federates by be located at individual geographic locations.

As the development lifecycle progresses and the maturity of the federates grows, these behavioural models may be replaced by either software-in-the-loop or hardware-in-the-loop. Work has been carried out to generate a bridge between HLA and hardware-in-the-loop through a Robotic Operating System [9]. The inclusion of hardware-in the loop enables work carried out on federation VV&A activities to also provide evidence towards the system level verification and validation (V&V).

The ability to increase the robustness, consistency and efficiency of the VV&A activities is crucial to the success of all stages of the system lifecycle.

2.2 Existing M&S V&V Guidance

The Institute of Electrical and Electronic Engineers (IEEE) provides high level guidance for simulation development and VV&A activities for federated simulation environments. Guidance is provided in the IEEE standard for Recommended Practice for Verification, Validation and Accreditation Development and Execution Process in IEEE standard 1516.4-2007 [5]. To complement the IEEE guidance, a further recommended Practice for Distributed Simulation Engineering and Execution Process (DSEEP) is detailed in IEEE standard 1730-2010 [6]. These IEE documents provide the high level guidance for the VV&A activities that should be carried out and, when used together, result in the generation of a DSEEP report. In addition to these standards, NATO M&S verification and validation activities commonly follow the Generic Methodology for Verification and Validation [8].

For many MCM M&S activities, standardized VV&A procedures can be found in the military standard for the Documentation of Verification, Validation and Accreditation for Models and Simulations [10].

A summary of the current processes and procedures for M&S VV&A can be seen in Fig. 2.

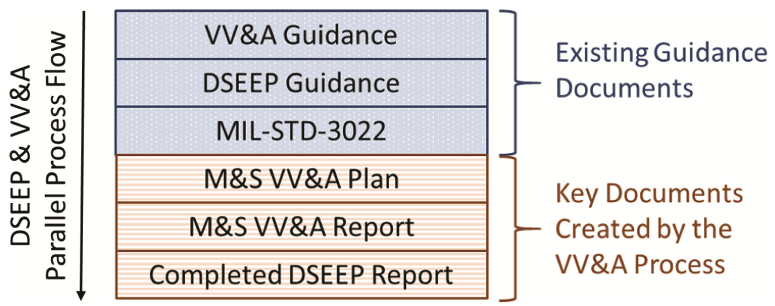

Fig. 2. Existing guidance and procedures for M&S VV&A.

The high level guidance provided in the existing guidance documents is targeted at supporting federated systems and the key deliverable, the DSEEP report, is structured to support the development of these systems. The lower level MIL-STD guidance [10] is not specifically aimed at federated systems. Following the low level processes for the VV&A of a federated, distributed and hybrid system may not result in the consistent achievement of lean and comprehensive VV&A goals. The lack of consistency can be seen in the generated VV&A plans and reports.

This paper provides a framework that replaces the low level procedures document [10] with procedures and templates that will produce a more consistent VV&A outcome for federated and distributed simulation environments.

3 Improved VV&A Procedures for Federated Simulations

This paper presents improvements to the existing VV&A processes to provide increased consistency, robustness and efficiency when applied to federated systems. The proposed processes produce deliverables that are consistent with the IEEE VV&A and DSEEP standards [5, 6]. A summary of the improvements made and the documents generated can be seen in Fig. 3.

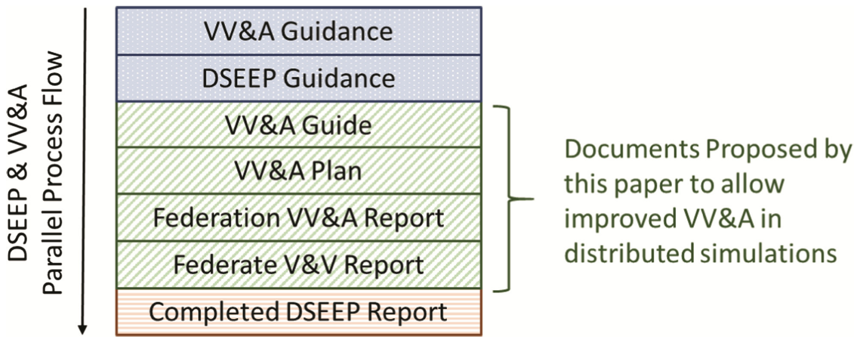

Fig. 3. Summary of the changes made to support distributed simulations.

The proposed process structure has been formed by four key documents; one guides and three templates. These documents have been produced to conceptually and methodologically guide all relevant stakeholders, including the development team, the V&V and Accreditation agents through the entire life cycle, from the definition of the end user needs to the Acceptance assessment. This framework was defined according to the specific characteristics of a federated architecture and has been designed to provide a lean, efficient process.

The four key documents generated by the process are divided into two levels. The two levels and the content of the five key documents are described in further detail in the remainder of this section.

- **Federation level:** VV&A Guide, VV&A Plan Template and VV&A Report Template

- **Federate level:** V&V Report Template.

The **Federation VV&A Guide** aims to guide the reader during the application of VV&A standards and the production of the different parts of the VV&A document. In particular the document contains the information related to the temporal execution of the VV&A phases, the explanation of the activities in each phases and their link to the VV&A document template.

The **Federation VV&A Template** contains a template of the document prescribed by the IEEE 1516.4 Standard for the VV&A. It is structured to be coupled with the VV&A guide; specifically the document template contains the structure of chapters and paragraphs, together with examples of texts, tables and figures to be produced during the VV&A activities for a Federation. Each VV&A guide phase contains links to the template in order to facilitate the document editing process.

The Federation VV&A Template is further divided into four main sections: First is the **M&S Description**, **Accreditation Plan** and the **V&V Plan**. Following this a template for the federation **V&V and Accreditation reports** are presented.

- **M&S Description** section is devoted to the identification of the characteristic of the federation, including goals, requirements, acceptability criteria, conceptual model, federation design, and FOM.
- **Accreditation** and **V&V Plans** are devoted to planning the Accreditation and V&V activities. These sections include the description of the methodology as well as the specific tasks with related techniques and responsibilities. The V&V plan also includes the activities related to the single federate V&V and the referent for validating the federation.
- **V&V Reports** and **Accreditation Reports** contain the results of the activities planned in the previous sections and their outcomes. The final product of the VV&A process is the Accreditation and Acceptance Assessment in the Accreditation Report, in which the recommendations for the user are identified.

Finally, the **Federate V&V Document** template serves as guidance for the single federate documentation for V&V purpose. The document includes the description of federate goals and the entities published during the federation execution. A core part of this document is the definition of the data exchange model which includes objects and interactions published/subscribed by the federate in the federation.

The guidance in both the VV&A guide and the VV&A Template should contain a bias that aims to carry out federation testing where possible. This bias in the reporting of tests will typically result in the majority of the test report being produced at federation level. The relationship between the federation and federate test reports and a single test plan can be seen in Fig. 4.

The templates and guidance notes presented in this paper have been produced and used to harmonize development, VV&A and system level V&V efforts.

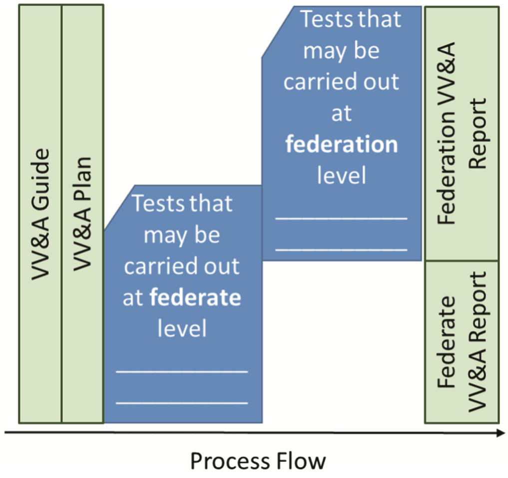

Fig. 4. Differentiation of the federate and federation test report contents.

4 Practical Framework Demonstration

Following the creation of the presented guidance documents and templates, the initial phases of the DSEEP/VV&A process have been carried out in a federated, distributed environment that simulates the interactions between several AUVs in an MCM scenario.

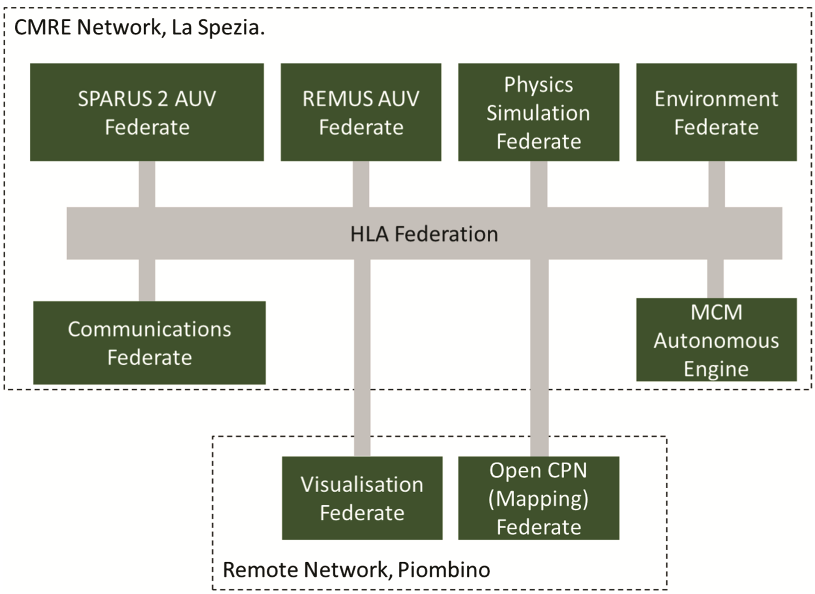

Fig. 5. Distributed test environment.

To provide a practical example of the process presented in this paper, a VV&A test exercise was demonstrated at a recent a maritime robotics event. In September 2017, an academic robotics event was held in Piombino, Italy. During the exhibition the integration a distributed federation was created between the robotics event and the NATO Centre for Maritime Research and Experimentation (CMRE), La Spezia, Italy. A topology of the federate structure can be seen in Fig. 5.

The infrastructure was composed of a network at CMRE, La Spezia, known as the CMRE Network and one laptop in the Piombino event, known as the Remote Network. The remote group of simulation federates were composed by the Visualization and the Open CPN (Mapping) Federate. These federates were situated in the mobile network. Figure 6 depicts the topology of the network utilized for the demonstration. It is possible to identify the two groups of systems as long with the list of entities composing the two groups.

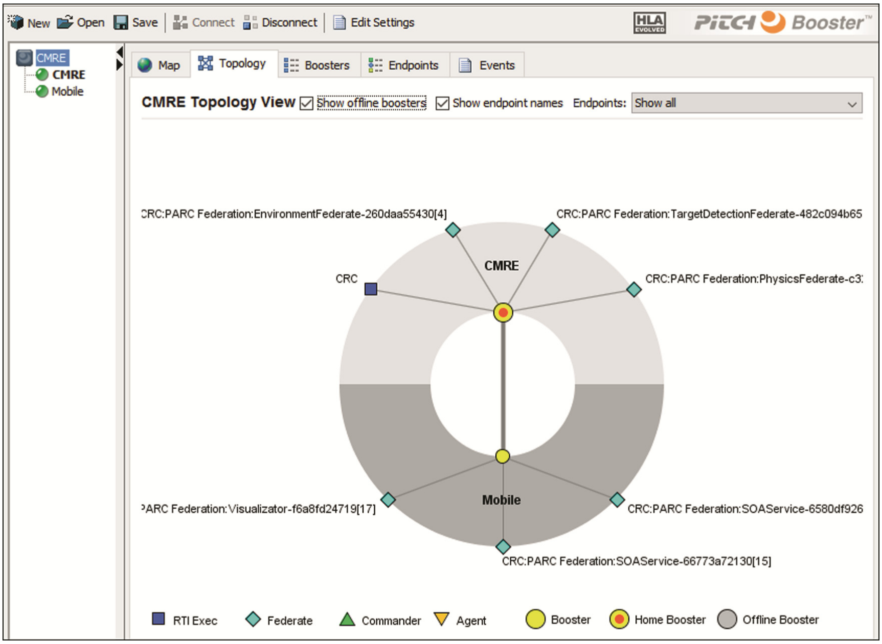

Fig. 6. Demonstration network topology.

The demonstration performed in order to test the successful connection can be split into three main steps. The first step was to define the mission area and the seafloor coverage using the Environment Federate at CMRE. The second step consisted of randomly placing 100 targets in the defined area using the Target Detector at CMRE. Finally the Visualization Federate at the remote site in Piombino received all this information and represented the virtual environment accordingly.

During the test, the security of the distributed network was required to comply with the NATO Security Committee Management Directive in CIS Security [11]. This has been achieved, despite using an open internet connection, by using a virtual private network from a secure asset at Piombino to the La Spezia site.

The simulation was successfully carried out and demonstrated the concept of using an M&S framework for conducting V&V activities on systems in distributed locations.

5 Future Work

The presented VV&A framework is currently being implemented in support of maritime MCM operations at CMRE, La Spezia. Preliminary federation and federate level objectives along with their related acceptability criteria have been identified based on final user needs. The final user will be involved further in the accreditation for further refinements.

In addition to the execution of the proposed framework, the M&S team is currently also working on the preliminary integration of HTC Vive [12] Virtual Reality Headsets into the current MCM scenario. The aim of this capability is to augment the operational capability and to support operators in missions that include autonomous systems as demonstrated in Fig. 7.

Fig. 7. Preliminary test with user exploring a 3D virtual operational area by HTC Vive.

The preliminary tests demonstrate the powerful potential of having the user fully immersed in the operational scenario, providing fruitful insight on the management of the operations and may further aid the execution of system level V&V activities. This use case will provide an ideal additional test case for the VV&A framework where complex user requirements will need to be tested and evidence collected.

6 Conclusions

The use of federated simulation environments allows encouraging opportunities to aid the development of autonomous systems throughout their development lifecycle, from initial design to final V&V testing. To allow the benefits of federated M&S environments to be realized, improved consistency and efficiency of the support provided needs to be supported.

Widely adopted high level IEEE Standards exist that encourage successful VV&A activities in federated simulation environments. While high level guidance exists, there is still scope for diverging lower level approaches that can lead to varying levels of VV&A efficiency, quality and clarity.

This paper has provided a framework for the implementation of a standardized low level methodology to increase the consistency of low level VV&A activities. These low level guides and templates are targeted at distributed federations that may be formed of models, hardware or software-in-the-loop. This methodology has been demonstrated to provide VV&A evidence in a distributed federation.

This proposed guidance will improve the consistency and efficiency of M&S federations in the support of autonomous system development. The approach could be used in future to support not only low level VV&A activities but, as system complexity and the number of performance variables increases, system level V&V evidence collection.

References

1. Pinto, J., Ribeiro, M., Giodini, S., L'Hoir, P., Braga, A., Sartore, A., Giron-Sierra, J.M., Sousa, J.: Network enabled cooperation of autonomous vehicles: a communications perspective. In: IEEE OCEANS 2017, Aberdeen, UK (2017)
2. Sariel, S., Erdogan, N., Balch, T.: Naval mine coutermeasure missions. IEEE Robot. Autom. Mag. **15**(1), 45–52 (2008)
3. Hodicky, J.: HLA as an experimental backbone for autonomous system integration into operational field. In: MESAS 2014: Modelling and Simulation for Autonomous Systems, Rome, Italy (2014)
4. Hodicky, J.: Standard to support military autonomous system life cycle. In: International Conference on Mechnatronics 2017, Brno, Czech Republic (2017)
5. IEEE: Recommended practice for verification, validation, and accreditation of a federationan overlay to the high level architecture federation development and execution process. In: EEE Std. 1516.4-2007, pp. 1–76 (2007)
6. IEEE: IEEE recommended practice for distributed simulation engineering and execution process (DSEEP). In: EEE Std. 1730-2010. IEEE (2011)
7. Ruiz, J., Behner, H., Herzog, R., Hodicky, J., Vrieler, S., Lofstrand, B.: Towards a new NATO certification capability for HLA interoperability. In: SISO Simulation Innovation Workshop, Orlando, USA (2016)
8. Roza, M., Sebalj, D., Voogd, J.: The generic methodology for verification and validation support acceptance of models, simulations and data. The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology 10(4), pp. 347–365 (2012)

9. Carrera, A., Tremori, A., Cammano, P., Been, R., Bruzzone, A.G.: HLA Interoperability for ROS-based autonomous systems. In: International Workshop on Modelling and Simulation for Autonomous Systems (2016)
10. United States Department of Defense: Department of Defense Standard Practice - Documentation of Verification, Validation and Accreditation (VV&A) for Models and Simulations. MIL-STD-3022, US, January 2008
11. NATO Security Committee: Management Directive on CIS Security, AC/35-D/2005-REV3, NATO, 12th October 2015
12. HTC: HTC Vive, Virtual Reality Headset (2016). https://www.vive.com/eu/