NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(MSG-136)TP/829

www.sto.nato.int

STO TECHNICAL REPORT **TR-MSG-136-Part-II**

MSaaS Concept and Reference Architecture Evaluation Report

(Rapport d'évaluation du concept et de l'architecture de référence de MSaaS)

Evaluation Report of NATO MSG-136.

Published May 2019

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(MSG-136)TP/829

www.sto.nato.int

STO TECHNICAL REPORT **TR-MSG-136-Part-II**

MSaaS Concept and Reference Architecture Evaluation Report

(Rapport d'évaluation du concept et de l'architecture de référence de MSaaS)

Evaluation Report of NATO MSG-136.

The NATO Science and Technology Organization

Science & Technology (S&T) in the NATO context is defined as the selective and rigorous generation and application of state-of-the-art, validated knowledge for defence and security purposes. S&T activities embrace scientific research, technology development, transition, application and field-testing, experimentation and a range of related scientific activities that include systems engineering, operational research and analysis, synthesis, integration and validation of knowledge derived through the scientific method.

In NATO, S&T is addressed using different business models, namely a collaborative business model where NATO provides a forum where NATO Nations and partner Nations elect to use their national resources to define, conduct and promote cooperative research and information exchange, and secondly an in-house delivery business model where S&T activities are conducted in a NATO dedicated executive body, having its own personnel, capabilities and infrastructure.

The mission of the NATO Science & Technology Organization (STO) is to help position the Nations' and NATO's S&T investments as a strategic enabler of the knowledge and technology advantage for the defence and security posture of NATO Nations and partner Nations, by conducting and promoting S&T activities that augment and leverage the capabilities and programmes of the Alliance, of the NATO Nations and the partner Nations, in support of NATO's objectives, and contributing to NATO's ability to enable and influence security and defence related capability development and threat mitigation in NATO Nations and partner Nations, in accordance with NATO policies.

The total spectrum of this collaborative effort is addressed by six Technical Panels who manage a wide range of scientific research activities, a Group specialising in modelling and simulation, plus a Committee dedicated to supporting the information management needs of the organization.

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS System Analysis and Studies Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These Panels and Group are the power-house of the collaborative model and are made up of national representatives as well as recognised world-class scientists, engineers and information specialists. In addition to providing critical technical oversight, they also provide a communication link to military users and other NATO bodies.

The scientific and technological work is carried out by Technical Teams, created under one or more of these eight bodies, for specific research activities which have a defined duration. These research activities can take a variety of forms, including Task Groups, Workshops, Symposia, Specialists' Meetings, Lecture Series and Technical Courses.

The content of this publication has been reproduced directly from material supplied by STO or the authors.

Published May 2019

ISBN 978-92-837-2155-0

Table of Contents

List of Figures

List of Tables

List of Acronyms

AMSP	Allied Modelling and Simulation Publication
C2	Command and Control
C3	Consultation, Command and Control
COI	Community of Interest
CWIX	Coalition Warrior Interoperability Exercise
DMAO	DSEEP Multi-Architecture Overlay
DSEEP	Distributed Simulation Engineering and Execution Process
FEAT	Federation Engineering Agreements Template
HLA	High Level Architecture
IT	Information Technology
M&S	Modeling and Simulation
MoE	Measure of Effectiveness
MoP	Measure of Performance
MSaaS	M&S as a Service
MSaaS-EP	MSaaS Engineering Process
OCD	Operational Concept Document
RA	Reference Architecture
SDT	Service Description Template
V&V	Verification and Validation

MSG-136 Membership List

CO-CHAIRS

Dr. Robert SIEGFRIED
aditerna GmbH
GERMANY
Email: robert.siegfried@aditerna.de

Mr. Tom VAN DEN BERG
TNO Defence, Security and Safety
NETHERLANDS
Email: tom.vandenberg@tno.nl

MEMBERS

LtCdr Tevfik ALTINALEV
Turkish Navy
TURKEY
Email: taltinalev@hotmail.com

Mr. Gultekin ARABACI
NATO JFTC
POLAND
Email: gultekin.arabaci@jftc.nato.int

Mr. Anthony ARNAULT
ONERA
FRANCE
Email: anthony.arnault@onera.fr

Col Thierry BELLOEIL
NATO ACT
UNITED STATES
Email: thierry.belloeil@act.nato.int

Dr. Michael BERTSCHIK
DEU Bundeswehr
GERMANY
Email: MichaelBertschik@bundeswehr.org

LtCol Dr. Marco BIAGINI
NATO M&S Centre of Excellence
ITALY
Email: mscoe.cde01@smd.difesa.it

Mr. Maxwell BRITTON
Department of Defence
AUSTRALIA
Email: maxwell.britton1@defence.gov.au

Dr. Solveig BRUVOLL
Norwegian Defence Research Establishment
NORWAY
Email: solveig.bruvoll@ffi.no

Dr. Pilar CAAMANO SOBRINO
CMRE
ITALY
Email: Pilar.Caamano@cmre.nato.int

Prof. Dr. Erdal CAYIRCI
Research Center for STEAM
TURKEY
Email: erdal@dataunitor.com

Mr. Turgay CELIK
MILSOFT Software Technologies
TURKEY
Email: tcelik@milsoft.com.tr

LtCol Roberto CENSORI
NATO M&S CoE
ITALY
Email: mscoe.ms08@smd.difesa.it

Maj Fabio CORONA
NATO M&S Centre of Excellence
ITALY
Email: mscoe.cde04@smd.difesa.it

Dr. Anthony CRAMP
Department of Defence
AUSTRALIA
Email: anthony.cramp@dst.defence.gov.au

Mr. Raphael CUISINIER
ONERA
FRANCE
Email: raphael.cuisinier@onera.fr

Mr. Efthimios (Mike) DOUKLIAS
Space and Naval Warfare Systems Center Pacific
UNITED STATES
Email: mike.d.douklias@navy.mil

Ing Christian FAILLACE
LEONARDO S.p.a.
ITALY
Email: christian.faillace@leonardocompany.com

Dr. Keith FORD
Thales
UNITED KINGDOM
Email: keith.ford@uk.thalesgroup.com

LtCol Stefano GIACOMOZZI
General Defence Staff
ITALY
Email: mscoe.ds02@smd.difesa.it

Mr. Sabas GONZALEZ GODOY
NATO ACT
UNITED STATES
Email: Sabas.Gonzalez@act.nato.int

Ms. Amy GROM
Joint Staff J7
UNITED STATES
Email: amy.m.grom.civ@mail.mil

Mr. Yannick GUILLEMER
French MoD
FRANCE
Email: yannick.guillemer@intradef.gouv.fr

Dr. Jo HANNAY
Norwegian Defence Research Establishment (FFI)
NORWAY
Email: jo.hannay@ffi.no

Mr. Andrew HOOPER
MOD
UNITED KINGDOM
Email: andy.hooper321@mod.uk

Mr. Willem (Wim) HUISKAMP
TNO Defence, Security and Safety
NETHERLANDS
Email: wim.huiskamp@tno.nl

Dr. Frank-T. JOHNSEN
Norwegian Defence Research Establishment (FFI)
NORWAY
Email: frank-trethan.johnsen@ffi.no

LtCol Jason JONES
NATO M&S CoE
ITALY
Email: mscoe.dr02@smd.difesa.it

Lt Angelo KAIJSER
Dutch Ministry of Defence
NETHERLANDS
Email: AJ.Kaijser@mindef.nl

Mr. Daniel KALLFASS
EADS Deutschland GmbH/CASSIDIAN
GERMANY
Email: daniel.kallfass@airbus.com

Col Robert KEWLEY
West Point
UNITED STATES
Email: Robert.Kewley@usma.edu

LtCol Gerard KONIJN
Dutch Ministry of Defence
NETHERLANDS
Email: gerard.konijn@gmail.com

Mr. Niels KRARUP-HANSEN
MoD DALO
DENMARK
Email: nkh@mil.dk

Mr. Vegard Berg KVERNELV
Norwegian Defence Research Establishment (FFI)
NORWAY
Email: vegard.kvernelv@ffi.no

Capt Peter LINDSKOG
Swedish Armed Forces
SWEDEN
Email: peter.j.lindskog@mil.se

Mr. Jonathan LLOYD
Defence Science and Technology Laboratory (Dstl)
UNITED KINGDOM
Email: jplloyd1@dstl.gov.uk

Mr. Jose-Maria LOPEZ RODRIGUEZ
Nextel Aerospace, Defence and Security (NADS)
SPAIN
Email: jmlopez@nads.es

Mr. Rene MADSEN
IFAD TS A/S
DENMARK
Email: Rene.Madsen@ifad.dk

Ms. Sylvie MARTEL
NCIA
NETHERLANDS
Email: Sylvie.Martel@ncia.nato.int

Mr. Gregg MARTIN
Joint Staff J7
UNITED STATES
Email: gregg.w.martin.civ@mail.mil

Mr. Jose Ramon MARTINEZ SALIO
Nextel Aerospace, Defence and Security (NADS)
SPAIN
Email: jrmartinez@nads.es

LtCdr Mehmet Gokhan METIN
Navy Research Centre
TURKEY
Email: m_gokhan_metin@yahoo.com

Mr. Aljosa MILJAVEC
MoD, Slovenian Armed Forces
SLOVENIA
Email: Aljosa.Miljavec@mors.si

Mr. Brian MILLER
U.S. Army
UNITED STATES
Email: brian.s.miller116.civ@mail.mil

Dr. Katherine MORSE
John Hopkins University/APL
UNITED STATES
Email: Katherine.Morse@jhuapl.edu

LtCol Ales MYNARIK
NATO JCBRN Defence COE
CZECH REPUBLIC
Email: mynarika@jcbrncoe.cz

Mr. Rick NEWELL
JFTC
POLAND
Email: rick.newell@jftc.nato.int

Mr. Jeppe NYLOKKE
IFAD TS A/S
DENMARK
Email: jeppe.nylokke@ifad.dk

Mr. Robbie PHILIPPS
Lockheed Martin Corporation
AUSTRALIA
Email: robbie.phillips@lmco.com

Mr. Marco PICOLLO
Finmecanica
ITALY
Email: marco.picollo@finmeccanica.com

Dr. LtCol (Ret) Dalibor PROCHAZKA
University of Defence
CZECH REPUBLIC
Email: dalibor.prochazka@unob.cz

Mr. Tomasz ROGULA
NATO Joint Force Training Centre
POLAND
Email: tomasz.rogula@jftc.nato.int

Dr. Martin ROTHER
IABG mbH
GERMANY
Email: rother@iabg.de

Mr. Angel SAN JOSE MARTIN
NATO ACT
UNITED STATES
Email: Angel.SanJoseMartin@act.nato.int

Maj Alfio SCACCIANOCE
NATO M&S CoE
ITALY
Email: mscoe.cde05@smd.difesa.it

LtCol Wolfhard SCHMIDT
JFTC
POLAND
Email: wolfhard.schmidt@jftc.nato.int

Mr. Barry SIEGEL
SPAWAR Systems Center – Pacific
UNITED STATES
Email: Barry.Siegel@navy.mil

Mrs. Louise SIMPSON
Thales
UNITED KINGDOM
Email: louise.simpson@uk.thalesgroup.com

Mr. Neil SMITH
UK MoD Dstl
UNITED KINGDOM
Email: nsmith@dstl.gov.uk

Mr. Per-Philip SOLLIN
Pitch Technologies AB
SWEDEN
Email: per-philip.sollin@pitch.se

Dr. Ralf STÜBER
CPA ReDev mbH
GERMANY
Email: stueber@supportgis.de

Capt Colin TIMMONS
Department of National Defence
CANADA
Email: colin.timmons@forces.gc.ca

Maj Dennis VAN DEN ENDE
Ministry of Defence
NETHERLANDS
Email: d.vd.ende@mindef.nl

Mr. Martin Dalgaard VILLUMSEN
IFAD TS A/S
DENMARK
Email: Martin.Villumsen@ifad.dk

Mr. Brian WARDMAN
Dstl Portsdown West
UNITED KINGDOM
Email: bwardman@dstl.gov.uk

Mr. Andrzej WNUK
Joint Warfare Centre
NORWAY
Email: andrzej.wnuk@jwc.nato.int

ADDITIONAL CONTRIBUTORS

Mr. Andy BOWERS
US Joint Staff J7
UNITED STATES
Email: francis.bowers@gdit.com

Mr. Brent MORROW
US Military Academy
UNITED STATES
Email: Brent.Morrow@usma.edu

Mr. Cory SAYLES
Lockheed Martin
UNITED STATES
Email: Cory.d.sayles@lmco.com

Mr. Roy SCRUDDER
The University of Texas at Austin
UNITED STATES
Email: roy.scrudder@arlut.utexas.edu

Mr. Dennis WILDE
European IAD Centre
UNITED STATES
Email: dennis.wilde@us.af.mil

MSaaS Concept and Reference Architecture Evaluation Report

(STO-TR-MSG-136-Part-II)

Executive Summary

NATO and nations use simulation environments for various purposes, such as training, capability development, mission rehearsal and decision support in acquisition processes. Consequently, Modelling and Simulation (M&S) has become a critical capability for the alliance and its nations. M&S products are highly valuable resources and it is essential that M&S products, data and processes are conveniently accessible to a large number of users as often as possible. However, achieving interoperability between simulation systems and ensuring credibility of results currently requires large efforts with regards to time, personnel and budget.

Recent developments in cloud computing technology and service-oriented architectures offer opportunities to better utilize M&S capabilities in order to satisfy NATO critical needs. M&S as a Service (MSaaS) is a new concept that includes service orientation and the provision of M&S applications via the as-a-service model of cloud computing to enable more composable simulation environments that can be deployed and executed on-demand. The MSaaS paradigm supports stand-alone use as well as integration of multiple simulated and real systems into a unified cloud-based simulation environment whenever the need arises.

NATO MSG-136 ("Modelling and Simulation as a Service – Rapid deployment of interoperable and credible simulation environments") investigated the new concept of MSaaS with the aim of providing the technical and organizational foundations to establish the Allied Framework for M&S as a Service within NATO and partner nations. The Allied Framework for M&S as a Service is the common approach of NATO and nations towards implementing MSaaS and is defined by the following documents:

- Operational Concept Document (OCD);
- Technical Reference Architecture and associated volumes; and
- Governance Policies.

This document contains the Evaluation Report that provides an assessment of independent review on MSaaS. It provides an overview of all results and makes recommendations for incorporation into the MSG-136 Final Report.

Rapport d'évaluation du concept et de l'architecture de référence de MSaaS

(STO-TR-MSG-136-Part-II)

Synthèse

L'OTAN et les pays membres utilisent les environnements de simulation à différentes fins, telles que la formation, le développement capacitaire, l'entraînement opérationnel et l'aide à la décision dans les processus d'acquisition. Par conséquent, la modélisation et simulation (M&S) est devenue une capacité cruciale pour l'Alliance et ses pays membres. Les produits de M&S sont des ressources extrêmement précieuses ; il est essentiel que les produits, données et procédés de M&S soient facilement accessibles à un grand nombre d'utilisateurs aussi fréquemment que possible. Toutefois, l'interopérabilité entre les systèmes de simulation et la crédibilité des résultats ne sont pas encore acquises et nécessitent beaucoup de temps, de personnel et d'argent.

Les évolutions récentes du cloud informatique et des architectures orientées service offrent l'occasion de mieux utiliser les capacités de M&S afin de répondre aux besoins cruciaux de l'OTAN. La M&S en tant que service (MSaaS) est un nouveau concept qui inclut l'orientation service et la fourniture d'applications de M&S via le modèle « en tant que service » du cloud informatique, dans le but de proposer des environnements de simulation plus faciles à composer et pouvant être déployés et exécutés à la demande. Le paradigme du MSaaS permet aussi bien une utilisation autonome que l'intégration de multiples systèmes simulés et réels au sein d'un environnement de simulation dans le cloud, chaque fois que le besoin s'en fait sentir.

Le MSG-136 de l'OTAN (« Modélisation et simulation en tant que service (MSaaS) – Déploiement rapide d'environnements de simulation crédibles et interopérables ») a étudié le nouveau concept de MSaaS afin de fournir les bases techniques et organisationnelles permettant d'établir le « cadre allié de M&S en tant que service » au sein de l'OTAN et des pays partenaires. Le cadre allié de M&S en tant que service est la démarche commune de l'OTAN et des pays visant à mettre en œuvre la MSaaS. Il est défini dans les documents suivant :

- Document de définition opérationnelle ;
- Architecture de référence technique (incluant la communication du service, le processus d'ingénierie et la documentation d'expérimentation) ; et
- Politiques de gouvernance.

Ce document contient le rapport d'évaluation issu de l'examen indépendant de la MSaaS. Il donne une vue d'ensemble des résultats et émet des recommandations à incorporer dans le rapport final du MSG-136.

Chapter 1 – PURPOSE OF EVALUATION

1.1 PURPOSE

The purpose of the evaluation is to determine if the MSaaS concept offers both feasible and tangible improvement to the establishment of synthetic training environments as a service. The evaluation process will employ qualitative and quantitative methods to determine and measure value.

The purpose of the evaluation is also to support the continuation of investigation and development by providing specific evidence based analysis of:

- Technical feasibility;
- Challenges and workarounds;
- Potential solutions; and
- Realized benefits.

Recommendations will also be made to extend the topic area for further investigation by the NMSG.

The purpose with the evaluation is also to share and grow knowledge of the program. It is important to understand what MSaaS is, how it contributes to the military simulation user community, and how early adopters can utilize the technologies and methodologies investigated by MSG-136. Further implementation by a broader user base will suit to expose any potential limitations of the approach and technologies, and thereby support the continued development of community knowledge and the growing robustness of the MSaaS concepts.

The evaluation also aims to examine validation of the operational concepts proposed for specific stakeholders. Concept descriptions are anticipated to be complete and fully understandable from the stakeholder perspective. The MSaaS use cases are expected to improve upon or compliment current work processes of the various stakeholders. The evaluation will identify any gaps or deviations that may require further investigation.

1.2 SCOPE

M&S products are highly valuable to NATO and military organizations, and it is essential that M&S products, data and processes are conveniently accessible to a large number of users as often as possible. Therefore, a new “M&S ecosystem” is required where M&S products can be more readily identified and accessed by a large number of users to meet their specific requirements. This “as a Service” paradigm has to support stand-alone use as well as integration of multiple simulated and real systems into a unified simulation environment whenever the need arises. The combination of service-based approaches hereby referred to as “Modelling and Simulation as a Service” (MSaaS) is considered to be a very effective approach for composing next generation simulation systems. NATO MSG-136 (“Modelling and Simulation (M&S) as a Service – “Rapid deployment of interoperable and credible simulation environments”), was tasked to investigate, propose and evaluate standards, agreements, architectures, implementations, and cost-benefit analysis for incremental implementation of a permanently available, flexible, service-based eco-system to provide more cost effective availability of M&S products, data and processes to a large number of users on-demand.

Chapter 2 – EVALUATION METHODOLOGY

2.1 APPROACH

The approach to the evaluation of MSaaS includes the following activities:

1) Question Preparation

a) Review the MSaaS Operational Concept Document (OCD) and identify the desired effects intended to be achieved when MSaaS is implemented.

b) Elaborate these effects as system and/or capability Measures of Effectiveness (MoE).

c) Prioritize the relative importance of the MoEs and establish an MSaaS hierarchy of needs. Refine the definition of the most significant MoEs that will guide the conceptual development of MSaaS.

d) Generate a set of questions for each MoE, which through collection of responses, will aim to verify stakeholder needs, and support validation of the MSaaS concept.

e) Trace all questions to the respective sections within the MSaaS document set; including the OCD, Reference Architecture (RA), governance document (AMSP-02) and Service Description Template (SDT).

f) Determine suitable Measures of Performance (MoPs) to be utilized in future verification tests and performance specification.

g) Affiliate each of the questions to specific roles within the Technical, Military and Government M&S community of interest, so questions can be directed to the right audience.

h) Expand on questions that are too general, to ensure more specificity.

i) Rank the questions in order of importance, and by MoE, to establish a prioritized short list for the questionnaire.

j) Consult the Experimentation plan of events to identify optimum opportunities to interview individuals and collect general feedback during the question and answer panels/forums.

2) Gather Feedback

a) Identify key challenges and recommendations from the CWIX Final Reports.

b) Conduct a Capability / Technology Taxonomy workshop within MSG-136 to identify and rank the most important service needs and technical readiness levels.

c) Record questions raised by presentation and demonstration audiences at key events.

d) Interview the technical team responsible for implementing the MSaaS prototype demonstrators to identify benefits, limitations, and any issues.

e) Gather feedback from stakeholders through interviews and email questionnaires.

3) Perform Analysis

a) Categorize all questions and feedback in accordance with the defined MoEs.

b) Analyze the relative importance of the MoEs, and any newly identified quality measures.

c) Analyze and identify any significant issues in the CWIX events that can be addressed with MSaaS capability requirements and/or experiments in the future.

d) Provide discussion of the key Measures of Effectiveness based on analysis of the results of the evaluation.

4) Provide Recommendations

a) Provide a summary list of recommendations for the MSG-136 members to consider in future MSaaS research, concept development and experimentation.

2.2 SELECTION OF EVALUATION TEAM

The Software Engineering Institute recommended best practice for software architecture evaluation identifies the following requirements for team members:

- The team must be perceived by the development project as impartial, objective, and respected. The team must be seen as being composed of people appropriate to carry out the evaluation, so that the project personnel will not regard the evaluation as a waste of time, and so that the team's conclusions will carry weight.
- The team should include people highly fluent in architecture and architectural issues and be led by someone with solid experience in designing and evaluating projects at the architectural level.
- The team should include at least one operational domain expert – someone who has experience as an end user of systems in the area being evaluated.
- The team should include at least one system domain expert – someone who has built systems in the area being evaluated.
- Applicable domain knowledge is crucial and must be available from consultants to the team, if not resident on the team itself.
- Access to the design documents, any working prototypes, or source code if available.
- Knowledge of the evaluation criteria, such as might be represented by a performance engineer, if not resident on the team itself.
- Support staff will be needed to assist in review process logistics and report generation.

For the purposes of the MSaaS Evaluation, the team members shown in Table 2-1 were allocated from MSG-136.

Table 2-1: Members of MSG-136 Evaluation Team.

Name (Nationality)	Domain Expertise	Evaluation Role
Peter Lindskog (SWE)	Military Training and Simulation Operations	Evaluation Objectives, Measures of Effectiveness, Questionnaire Design and Analysis, Operational Recommendations
Rob Phillips (AUS)	Simulation Systems Architecture, Engineering, Integration and Test	Evaluation Methods, Architecturally Significant Requirements, Scenario Design and Analysis, Data Collection, Architecture Recommendations
Anthony Arnault (FRA)	Military Training and Simulation Acquisitions	Measures of Effectiveness, Questionnaire Design, Acquisition Community Advocacy, Business Model Analysis

Name (Nationality)	Domain Expertise	Evaluation Role
Jon Lloyd (GBR)	Military Training and Simulation Capability Research and Development	Simulation Services Technology Assessment, Technology Road-mapping, R&D Gap Analysis

2.3 SELECTION OF QUALITATIVE MEASURES

During Meeting #6 held at Stavanger, Norway in June of 2016, a survey was conducted across ten members of the MSG-136 working group. Each participant was asked the following two questions:

1) In no particular order, what are the five most important benefits that MSaaS is anticipated to provide you or your home country users?
2) In no particular order, what are the five most significant barriers to achieving MSaaS from your or your country user's point of view?

The responses for question 1 were categorized into either system benefits or capability benefits as shown in Table 2-2.

Table 2-2: Survey Responses (Question 1).

Key System Benefits	Key Capability Benefits
Affordability (7)	Improved Interoperability (3)
Flexibility (4)	Increased Functionality (2)
Coherence (3)	Increased Accessibility (2)
Reusability (2)	On Demand (3)
Earlier Runtime	Reduced Manpower (2)
Scalability	Increased Maintainability
Modularity	Increased Availability
Composability	Commonality
Open Source	Increased Usability
Load Balancing	Improved Fair Fight
Automation	Improved Outputs
Consolidation	Better Prepared Warfighters

The highest recurring benefits were considered as qualitative measures for evaluation.

2.4 EVALUATION TECHNIQUES

In consideration of the conceptual phase for MSG-136, the concept development timeline indicated in the Operational Concept Document, the Evaluation Team considered the most appropriate evaluation techniques in accordance with the table set out by Bass, Clements, and Kazman in Figure 2-1, below.

	Technique	Generality	Detail Level	Phase	Target
Questioning Techniques	Questionnaire	General	Coarse	Early	Artifact, process
	Checklist	Domain-specific	Varied	Middle	Artifact, process
	Scenarios	System-specific	Medium	Middle	Artifact
Measuring Techniques	Prototype, Simulation, Experiment	Domain-specific	Varied	Early	Artifact
	Metrics	General or Domain-specific	Fine	Middle	Artifact

Figure 2-1: Overview of Evaluation Techniques. Source: Ref. [1]

Based on the current state of MSaaS being in the 'Early' phase, the Questionnaire was selected as the primary research technique for collecting feedback on the MSaaS concept from a broad M&S community of interest, consisting of representation from government, military and industry from various countries.

Technical Volume 4 identifies the experimentation plan and schedule of events which provide opportunity for collecting feedback from the event audiences, and participating technical staff. The agreed approach for evaluation included consideration and recommendations for establishing metrics as MSaaS prototypes increase in rigor and Technical Readiness Level. The current prototypes planned in the Experimentation Plan were considered too limited in scale and functionality to perform realistic system performance measurement that might be used to validate the Technical Reference Architecture.

2.4.1 Questioning Techniques

2.4.1.1 Questionnaire

Questionnaire-based techniques are in the form of open questions applicable to all kinds of architectures, operational and governance processes, and the software architecture product. Questionnaires provide a means of gathering sample data from a broad set of stakeholders, represented by or gathered by members of MSG-136. Members of MSG-136 represent a set of *Experts*, from the military simulation and training community of interest, across at least twelve different countries. These experts have access to larger populations within their own country communities of interest.

2.4.1.2 Checklist

Checklist-based techniques are a set of specific questions for a given application domain. In the case of MSaaS, the questions will relate to alignment with work undertaken within two specific communities of interest; the Simulation Interoperability Standards Organization, and the NATO Modelling and Simulation Group. The checklists will be based upon standards and best practices within these communities, such as DSEEP.

2.4.1.3 Scenarios

Scenario based techniques such as the Software Architecture Analysis Method (SAAM) used as the basis for ATAM describes specific interactions between a stakeholder and the system. In each scenario, the stakeholder will be exposed to a conceptual or experimental interface with which they might interact. For the purposes of the MSaaS Architecture Evaluation, each scenario will be selected specifically to address an Architecturally Significant Requirement for a given stakeholder. Based on this user experience, the stakeholder will then answer questions directly related to the Architecturally Significant Requirement.

2.4.2 Measuring Techniques

2.4.2.1 Simulations, Prototypes, and Experiments

The MSaaS Technical Team has developed a set of prototype implementation procedures, services and interfaces, in order to assist the validation of the Reference Architecture and Operational Concepts. The advantage of using these prototypes in experiments is that the prototype behavior relates to the actual system (instantiation of the Reference Architecture). The assumptions are clearer than those for metrics and can be derived directly from scenarios. The problem with utilizing prototypes and experiments is the cost of development and staging, and the subsequent restriction of functionality. For the purposes of the evaluation, specific scenarios have been defined within an experiment to focus on Architecturally Significant Requirements.

2.4.2.2 Metrics

Quantitative interpretations about observable measurements on the architecture provide unambiguous and specific values. The drawback is that assumptions must be made about their use, which may return values that are too specific. At this early phase of Reference Architecture definition, there is limited opportunity to instrument sample instances of an MSaaS system. There are limited resources available to test infrastructure considerations across the varied cloud deployment models, and very few simulations accessible from any cloud readily available to test. The isolated instrumentation of prototype implementations is of limited technical value, without proper allocation of the resources needed to fulfil a realistic level of complexity. The intent of MSaaS is to ultimately provide on-demand access to a large multi-national training and simulation community. The magnitude of this end state is currently beyond physical measurement.

2.5 EVALUATION PRECONDITIONS

Preconditions are the set of necessary assets and conditions that must be in place before a successful evaluation can proceed. Preconditions include an understanding of the evaluation context, involvement of the right people, organizational expectations and support, evaluation preparation, and an appropriate representation of the architecture being examined.

2.5.1 Stakeholders

Table 2-3 shows the members of the M&S community of interest that were surveyed in this evaluation.

Table 2-3: Survey Participants.

Country	Agencies/Organizations	#
United States of America	Air Force, Army, Navy, USMC, Joint Staff, ARL, Industry	25
United Kingdom	DSTL, Industry	3
Australia	Joint Staff, Industry	2
Canada	Air Force, Army	4
Germany	Army	1
Italy	Army	1
Greece	Army	1
Denmark	Industry	1

2.5.2 Data Preparation

The set of documentation used and analyzed in the evaluation includes the MSG-136 Technical Volumes, Operational Concept Document, Reference Architecture, prototype simulation software descriptions and development procedures.

The key data items to undergo analysis are provided below:

a) Operational Concept Document:

The Operational Concept Document (OCD) describes the intended use, key capabilities and desired effects of the Allied Framework for MSaaS from a user's perspective.

b) Governance Policies:

The Governance Policies identify MSaaS stakeholders, relationships and provide guidance for implementing and maintaining the Allied Framework for MSaaS.

c) Technical Reference Architecture and associated volumes:

The Technical Reference Architecture (Vol. 1) describes the architectural building blocks and patterns for realizing MSaaS capabilities. Volumes 2 – 4 define service discovery and metadata, describe a reference engineering process and document the experimentation and validation efforts.

2.6 EVALUATION ACTIVITIES

2.6.1 Recording and Prioritizing

During the evaluation, the evaluation team is attempting to highlight critical issues that are raised in support of or (more importantly) against the MSaaS concepts and architecture. Each issue raised during the review is documented in an MSaaS Capability Matrix (Annex A).

2.6.2 Evaluating Qualities

There are many qualities that can be the subject of an evaluation. As one of the preconditions of the evaluation, the primary qualities to examine have been agreed upon. The most common ones have been defined as MSaaS Measures of Effectiveness and are identified in Table 2-4.

Table 2-4: MSaaS Measures of Effectiveness.

Key MOEs	Factors and Considerations
Affordability	Time, software license cost, shared services / hosting subscription fees, distributed support, fee for use (only pay for what you need)
Flexibility	Agility, rapid provisioning of resources, rapid configuration management, migration of legacy systems, business dynamics, service discovery
Coherence	Consistency, repeatability, understandability
Accessibility	Global access without need for sim support staff on location, access to a common experiment / exercise data repository, pre-training on demand
Reusability	Hardware reuse (provider POV)
Availability	Uptime (reduced MTBF), timely access to service through scheduled management – on demand self-service, always ready

Key MOEs	Factors and Considerations
Scalability	Simultaneous simulations, reduced license costs, capacity/provisioning, platoon to brigade to platoon, distributed mission operations
Modularity	Openness, switchable functionality in real time
Composability	Mode (do what), scenario (data needs), tuning (export configurations) patterns
Usability	Time to configure, ease of discovery and integration, warfighter interfaces, ease of implementation by application / sim engineers
Elasticity	The ability to increase or decrease computational resources according to the users' needs, statically or dynamically
Supportability	Online help and failover/monitoring/documentation
Suitability	Ability to sandbox several sim environments to select the most suitable

2.6.3 Reviewing Issues

All of the issues that are raised during the review, as well as their ongoing ranking, should be discussed in feedback made available to the working group. In addition, there should be a checklist for the following considerations:

- The architecture is forced to match the technical capabilities of the MSG-136 working group.
- Top-level architecture components number more than 25.
- One requirement or quality drives the rest of the architecture design.
- The architecture depends upon alternatives in the operating system or middleware.
- Proprietary components are being used when open standard components would do.
- There is too much complexity (low cohesion, high coupling).
- The design is exception-driven; the emphasis is on the extensibility and not core commonalities.

2.6.4 Reporting Ranked Issues

The final review activity is to create and present a report in which all of the issues, along with supporting data surfaced during the review, are described. The report should be circulated in draft form to all of the review participants to catch and correct any misconceptions and biases and to correlate elements before the report is finalized.

Chapter 3 – EVALUATION DESIGN

3.1 EVALUATION EVENT PLANNING

The experiments to be performed as part of the evaluation will consist of a set of trials that are controlled and designed to discover new information about the MSaaS concept. The discovery experiment is not intended to test or evaluate an existing MSaaS system, but to generate a hypothesis and to test new concepts, ideas and technologies with potential to further development. The use of MSG-136 prototype simulation services will provide a means to evaluate the MSaaS operational concepts and reference architecture at this early stage of development. In order for new concepts and capability needs to be discovered, the experiment will require some flexibility, real time interpretation, collection adjustment, and analysis.

The experiment will consist of a set of trials, each aimed at specific use cases that expose key MSaaS capabilities and explore architecturally significant requirements. The experiments set out in Volume 4 (Experimentation Report) were demonstrated at a series of public events over the period 2016 – 2017. These demonstrations were accompanied with explanatory presentations and provided a forum to engage independent opinion and obtain feedback from industry, military and government.

These events included:

- 2016 NATO CWIX, Bydgoszcz, POL.
- 2016 NATO CAX Forum, Munich, DEU.
- 2016 I/ITSEC Conference, Orlando, USA.
- 2017 NATO CWIX, Bydgoszcz, POL.
- 2017 TIDESPRINT, Virginia Beach, USA.
- 2017 ITEC Conference, Rotterdam, NLD.
- 2017 NATO CAX Forum, Florence, ITA.

As part of the development effort performed by industry and government in support of the experiments and demonstrations, additional technical feedback was also collected from the participating engineers.

Chapter 4 – EVALUATION RESULTS

4.1 EVALUATION ACTIVITIES CONDUCTED

4.1.1 CWIX 2016

The Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX) is a Bi-SC exercise that is North Atlantic Council (NAC) endorsed, Military Committee (MC) directed and C3 Board (C3B) guided. The 2016 CWIX Focus Area Final Report on Modelling and Simulation identifies the following objectives which aim to seek better use of technology within the Connected Forces Initiative (CFI):

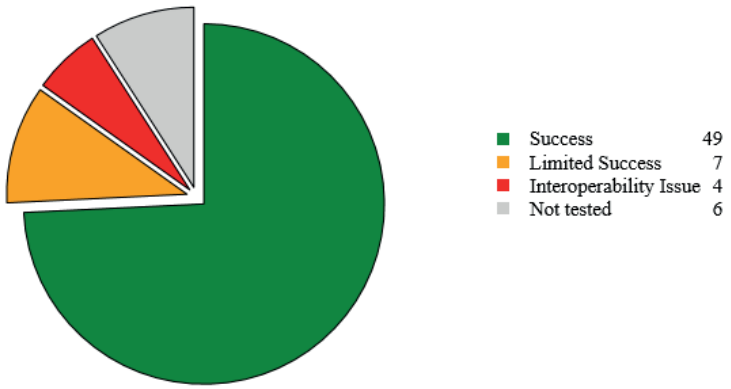
- **Objective #1** – Federate different types of simulation systems and record test results for contributions to NATO STO MSG-134. This was the baseline for the M&S Focus Area: the goal was to create federations among different simulation systems in order to verify their interoperability as well as their capability to consume scenario data from the GEOMETOC Focus Area, through the investigation of the current alternatives and technologies for simulation and the identification of the interoperability weaknesses.
- **Objective #2** – Test the interoperability features with all the other participants' systems joining the Focus Area within the M&S as a Service implementation, in coordination with MSG-136. This was a first step ahead from the baseline. The goal was to identify possible interoperability issues for Simulation Suite Services tested as consumer of the Cloud Computing Architecture provided by JFTC – Infrastructure as a Service (IaaS) and determine if a capability that is streamed from the Cloud to a platform can be operated as a user without a license or other governing sources.
- **Objective #3** – Test the interoperability with other C2 systems (C2SIM interoperability) during distributed exercises in order to support the NRF Testing and Certification Process, in coordination with NATO JWC. This was a further step ahead from the baseline: the goal was to identify possible interoperability issues between Simulation Systems and C2 Systems, involved within Land/Air/Maritime/Logistics/Operational Command Focus Areas and IETV area, during initialization and exchange of information during an Exercise.

The 2016 CWIX exercise M&S tests involved participation from six nations and the NATO M&S COE, including Canada, Germany, Norway, Poland, Turkey, and the United States. The M&S Focus Area managed to realize a complex Federation among the participating simulation systems, a federation composed of different subnets based on both Distributed Interactive Simulation (DIS) v6 standard (IEEE 1278a-1998) and High Level Architecture (IEEE 1516-2010 configured using Pitch and MAK Run-Time Infrastructure (RTI) products). Compared with CWIX 2015, the overall effort to set up the federation was significantly reduced. This was achieved despite the increased number of involved capabilities and as a result of previous lessons learnt that identified solutions to solve known interoperability issues. Figure 4-1 presents CWIX 2016 M&S Test Case Results.

A number of significant challenges were identified in the CWIX Focus Area Final Report, as follows:

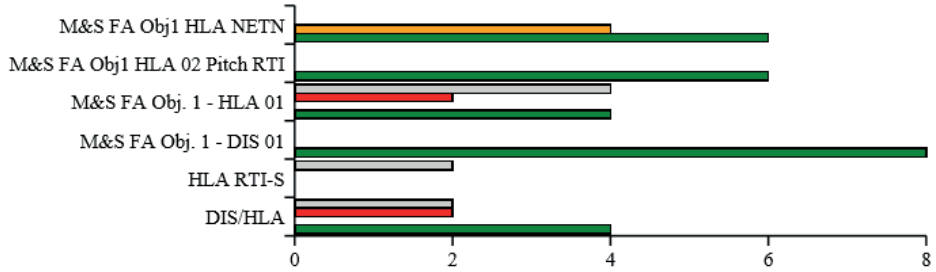
1) The main challenge every year was to configure each system in order to be able to provide and consume the simulated entities to and from other participants. Emphasis should be given to the proper use of exactly the same FOM in a federation as well as the terrain correlation and the nominal holdings of entities (their position, for example).
2) M&S FA participants agreed during FCC to prepare and issue a CWIX 2016 Distributed Simulation Agreement (DSA), which will include all the required information in order a federate to join the federation. Unfortunately, the document was not completed with all relevant and required information, before the execution phase.

Total



By Test Case Templates

This section presents the test results grouped by the Test Case Templates.



Test Case Templates	Success	Limited Success	Interop. Issue	Not tested
DIS/HLA	4		2	2
HLA RTI-S				2
M&S FA Obj. 1 - DIS 01	8			
M&S FA Obj. 1 - HLA 01	4		2	4
M&S FA Obj1 HLA 02 Pitch RTI	6			
M&S FA Obj1 HLA NETN	6	4		
Total	28	4	4	8

Figure 4-1: CWIX 2016 M&S Test Case Results.

3) The US capabilities JMSC_JMECS #203, JMSC_JSPA #203 and MUSE #194 had interoperability issues due to trouble in their primary federation translation tool between DIS and HLA, which does not interface with the RTI by PITCH or MAK producers, so they needed to perform all the tests in DIS through gateways provided by other capabilities (e.g., SGA, MoSIM GTW). Moreover, their system to translate simulation data into mission command data (JMECS) did not support NFFI. Therefore, these tools were not fully integrated with other NATO capabilities.

4) Internal issues limited the utilization of BMD_TDACS #102 capability of EIAMDC in terms of providing Link-16 message traffic associated with BMD fly-outs and shots taken, so some data was pushed into simulators through a gateway.

5) The central challenge for CAN_MSAAS_0.1 #170 capability was the configuration of the virtual machines created in Canada matching the requirements for import and then execution within the JFTC Cloud, so it was important to understand the JFTC VCloud Director security settings for virtual machines and how they interact differently with the different operating systems.

6) The initial planned participation of STO MSG-136 member nations did not take place due to the constraints on the classified network. This had an impact on the M&S FA objective n. 2 achievement.

7) The M&S Focus Area did not interact with the FMN Focus Area, but this was requested for the future in order to provide M&S specifications for future FMN spirals.

8) The testing with the CMRE-REPS #23 capability represented the main interaction with Maritime FA, but this capability had an issue with the version of the PITCH_RTI, due to funds availability, so the Anti-Submarine Warfare scenario was not tested with the M&S FA.

9) Although the ATO-G #146 generated ATOs could be parsed by ICC, there were two issues that require developer attention subsequent to CWIX 2016 conclusion. Testing with FRA-SEI identified a set in the ATO that is required in some conditions but was not being filled. Secondly, the ATO was filling the location name field with the mission name rather than the location name.

10) ICC ATO translation by ATO-T (#210) was challenged by data mapping issues associated with the data sets used by the respective systems. This is a common issue and the ATO-T GUI service supports mapping and resolving data mismatches; even so, data mapping slows ATO translation and therefore subsequent execution.

11) Regarding the OR&A DFTOP #128 capability, one test case with NCI Agency's TOPFAS system has not been tested because an issue related to the linkage between black and red system environments could not be resolved. Another test case with NCI Agency / ATOT MSG-136 has been looked into but had to be withdrawn without a possible outcome because of the incompatibility of the capabilities' systems, on one hand, and because of the quite different specializations of the systems, on the other hand.

The main recommendations derived from the identified challenges are as follows:

1) The M&S FA should start working on the syntax of the Distributed Simulation Agreement (DSA) from a very early stage of CWIX planning. The draft document used for CWIX 2016 should be distributed to possible M&S FA participants during the IPC in order to have a mature draft before MPC and produce an almost complete document during or immediately after FCC (surely before the CWIX 2017 execution).

2) As a consequence of the previous point, it is recommended to configure each system in order to be able to provide and consume the simulated entities to and from other participants. Emphasis should be given to the proper use of exactly the same FOM in a federation as well as the terrain correlation and the nominal holdings of entities (their position, for example).

3) Provide access to NATO STANAGS library on the network. A shared STANAG library could be useful on the Sharepoint Portal in order to implement the correct ATO and ADatP-3 formats.

4) The other FAs (operational users) requirements for M&S FA should be clearly defined during the several planning conferences in order to design a unified simulation federation able to stimulate their systems in the framework of more realistic scenarios. This would need to be finalized during the FCC.

5) The CWIX 2017 Test Case scheduling should follow a logical order that is aligned with overall CWIX execution.

6) Greater emphasis on MSaaS experimentation of NMSG-136 in CWIX 2017, planning separate classified and unclassified cloud access. It could be considered by the Technical subgroup developing the Reference Architecture (RA) as a result of participating in CWIX 2016.

7) Implement a disciplined systems engineering process for preparing for and executing CWIX 2017 and subsequent CWIXs with the two-fold intent of improving the quality of interoperability testing at CWIX and of establishing M&S Specifications for the Federated Mission Network (FMN).

8) Simulation application versions need to be specified prior to execution. This is probably best achieved within the Distributed Simulation Agreements Document.

9) A data interchange diagram or model is recommended for each test case in order to visualize the pathways that the data is to take and the applications involved.

10) It is recommended that simulation application and site IDs be documented in advance and required configuration files be amended in advance of execution. A suitable document for this information is potentially the Distributed Simulation Agreements Document.

11) Constant monitoring of VMs is required on the JFTC Cloud, or some form of application health monitoring would be useful to push notifications to the staff that there is a potential issue with an application running in the Cloud.

12) In order to address several issues encountered when attempting to transfer Virtual Machines (VM) to the JFTC Cloud, it is recommended to:

    a) Discuss VM upload strategies with JFTC to work through the timeout issue;

    b) Investigate the failure of the CentOS and Windows VM;

    c) Ensure proper network configuration of the VM prior to upload; and

    d) Ensure Windows operating system license is available for SYSPREP relicensing.

13) The partners have to ensure that SW distributed for testing has to include user licenses otherwise, as it happened in CWIX 2016 for RTI-S, tests could not be performed.

14) M&S FA participants during FCC should prepare a CWIX 2016 Distributed Simulation Agreement (DSA), which will include all the required information in order a federate to join the federation, because the M&S FA works in accordance with Distributed Simulation Engineering and Execution process DSEEP IEEE 1730.

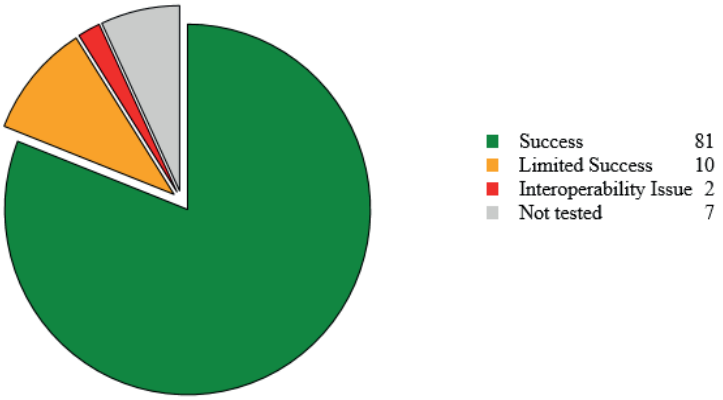
15) Some tools were not fully integrated with other NATO capabilities. The M&S FA partners have to bring this topic to the higher level for resolution.

16) The M&S Focus Area will promote a closer interaction with the FMN Focus Area, in order to provide M&S specifications for future FMN spirals.

Although the initial MSaaS experimental prototypes were not included in CWIX 2016, the key findings and lessons learned from the CWIX 2016 M&S Focus Area Final Report provide special insight for design and execution of future MSaaS experiments, and planned participation in upcoming CWIX events. This information has been incorporated into the Evaluation Report to ensure these considerations are incorporated into continued MSaaS Concept Development and Experimentation.

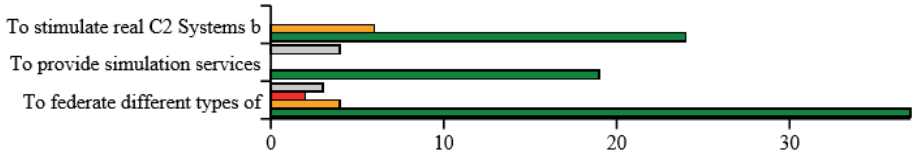
4.1.2 CWIX 2017

During the execution phase of CWIX 2017, the main challenge was to coordinate the different testing activities of the participating capabilities inside the FA and with the other Focus Areas, in support of their own activities and of the Joint Vignette. The execution scheduling of this year was also more challenging because NAC visit was in the second week and the Visitor/VIP days in the third. This took out time that usually was allocated for tests and reporting. Success stories and lessons learned will be a valuable input for facing at the best the next year's challenges. Figure 4-2, below, presents CWIX 2017 M&S Test Case Results.



By Objectives

This section presents the test results grouped by the Objectives.



Objectives	Success	Limited Success	Interop. Issue	Not tested
To federate different types of networked simulation systems building a complex federation facilitated by NATO MSG-134's Integration, Verification and Certification Tool and associated Process.	37	4	2	3
To provide simulation services both inside and outside the FA according to NATO MSG-136's Modelling and Simulation as a Service paradigms and architecture.	19			4
To stimulate real C2 Systems by actively supporting Joint Vignette.	24	6		
Total	80	10	2	7

Figure 4-2: CWIX 2017 M&S Test Case Results.

The key recommendations identified in the Focus Area Final Report are as follows:

1) For the first time this year the M&S Focus Area has adopted a DSEEP process, by referring to a Distributed Simulation Agreement document and introducing the role of Federation Manager. A strong recommendation for next year is to improve this process starting from IPC and requesting contributions from all the participants from the beginning, in order to have capabilities already properly configured for the execution avoiding mismatching and conflicts among the different configurations of the participating systems.
2) To facilitate the enhancement of the IVCT it is strongly recommended to have more capabilities participating in the test phase therefore providing more inputs for the improvement of the tool.
3) With the increasing number of participants and capabilities and with the good level of maturity achieved by the M&S services offered by the M&S Focus Area, it is strongly recommended to increase the interaction with FMN Focus Area for testing these services against FMN Spirals specifications.

4.1.3 MSG-136 Capability/Technology Taxonomy Workshop

The 8th MSG-136 meeting held in Rome, Italy provided an opportunity to conduct a Capability/Technology Taxonomy Workshop internal to the MSG-136 members. The objective of the workshop was to identify and assess key enabling technologies and their current maturity (Technical Readiness Level), in order to develop an initial MSaaS Technology Roadmap. The MSaaS Taxonomy and Investment Scoring process was facilitated by UK Dstl technical attendees to gather and define recognized MSaaS capabilities from the various MSG-136 meeting attendees and score the importance of these capabilities in order to prioritize them within a nominal roadmap (see Figure 4-3).

Figure 4-3: Capability/Technology Scoring.

These capabilities were categorized in accordance with the Operational Concept Document service definitions, and the results of this workshop are provided in the following tables:

- Table 4-1: MSaaS Discovery – Capabilities and Enabling Technologies.
- Table 4-2: MSaaS Composition – Capabilities and Enabling Technologies.
- Table 4-3: MSaaS Execution – Capabilities and Enabling Technologies #1.
- Table 4-4: MSaaS Execution – Capabilities and Enabling Technologies #2.
- Table 4-5: MSaaS Support – Capabilities and Enabling Technologies.

Each capability/enabling technology was identified, described, and an assessment of the current TRL was undertaken by MSG-136 workshop attendees. In addition to providing a definition of what each function/enabling technology is, a scoring has been carried out based on the required investment by the defence community in that function/enabling technology in order to achieve the recommended maturity level (see scoring criteria below). This provides a simple view to understand how important each element is and identify where the defence community should focus their research and capability development efforts, and which technologies that can be left to mature outside of the defence community.

Table 4-1: MSaaS Discovery – Capabilities and Enabling Technologies.

Ref	Capability / Enabling Technology	Current Maturity	Definition	Score
M1	Technical Registry	TRL4	A technical registry for components/assets/scenarios/training packages, which supports categorisation/searchable metadata for both training platform and simulation content harvesting from multiple registries. Searchable to provide a prioritised list of assets that match user supplied keywords and capability requirements. The registry shall implement access restrictions that allow authorised users to gain access to information that they have been granted permission to view.	3
M2	Repository System	TRL4	A mechanism for storing simulation assets from NATO, National, Industry or Academic organisations, which support categorisation/searchable metadata.	3
M3	Linked Registry and Repositories	TRL1	The capability to link the Technical Registry and Repository Systems together to support discovery service. Includes the linking of linking to registries and repositories of allied nations.	3
M4	Automated Intelligent Discovery Service	TRL1	A service which, when provided with a set of user requirements for a simulation, performs a search of the technical registry and connected registries and provides a ranked list of suitable combinations of assets that will best meet the users requirements and identify any capability gaps that exist.	3
M5	Meta Data Ontology	TRL6	The authoritative definition of the names and types of properties of simulation assets that are used as meta data to within registries and repositories.	3
M6	Automated Meta Data Extraction	TRL1	A system which extracts meta data for the technical registry from asset requirements, design, interface definitions, verification and validation data, Object Models, etc., presented as (machine and human readable) structured data and even unstructured data.	2
M7	Composition Evaluation	TRL1	The ability to evaluate a proposed composition's ability to meet the initial system objectives and outcomes.	3
M8	Active Discovery System	TRL3	A system that regularly search repositories for new and updated assets and when found extracts the meta data and adds it to the registry.	3

Table 4-2: MSaaS Composition – Capabilities and Enabling Technologies.

Ref	Capability / Enabling Technology	Current Maturity	Definition	
M9	MSaaS Composition Aide	TRL2	A system which allows the user to produce composition definitions by importing component definitions from the registry and allocate them to physical or logical devices and creating logical connections between the components.	3
M10	Automated MSaaS Composition Service	TRL0	A service that, given a set of components, definitions and constraints, will automatically generate executable composition definitions that allocates the components to physical and logical devices and creates logical connections between the components.	2
M11	Cloud Deployment	TRL6	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (NIST 2011)	5
M12	Deployment service	TRL4	A service that, given a composition definition, will to install and configure the selected components where they are required either on Virtual Machines or equivalent container.	3
M13	Negotiable Interfaces for simulation	TRL3	The ability for a component to automatically negotiate the transport mechanism to receive data from an agile service (e.g. by using Self Describing Data).	3
M14	Automated Test Agent	TRL3	The ability to configure, instantiate and test services built from individual applications (a.k.a. federates).	3
M15	Automated Validation Agent	TRL1	The capability of the repository to validate that the resulting system meets the its objectives.	2
M27	Composition Optimisation	TRL1	Mechanism that analyses a composition and optimises the implementation based on user performance requirements. This will ensure services that require minimum latency are run locally to where the output from the service is required.	3

Table 4-3: MSaaS Execution – Capabilities and Enabling Technologies #1.

Ref	Capability / Enabling Technology	Current Maturity	Definition	
M16	Architectural Models	TRL4	Starting with an MSaaS Reference Architecture which defines a framework for the concepts and relationship between components in the MSaaS environment one or more concrete architectures can be defined that specify the standards and technologies that are to be used.	3
M17	MSaaS Design Patterns	TRL3	A set of formal definitions of a generally reusable solution to a commonly occurring problem within MSaaS. The pattern defines the relationship and interactions between assets, components and the MSaaS architecture that form a template for solving the problem. Patterns can be used to define how components should interact at all phases of the MSaaS lifecycle from discovery, orchestration through to deployment and run-time execution.	3
M18	Execution Management Service	TRL3	A service that allows the user to deploy, start-up and set initial conditions in each simulation system and joined to a single exercise in a ready for exercise start state. For real-life systems this could include the injection of track and intelligence data to provide a suitable history to provide a suitable common operating picture. Whilst the system is executing monitors the health of all components in the system and, upon discovering a problem, automatically reconfigures the system, restarting or initiating services where required, and, if necessary pausing the execution until the system is ready to resume.	3
M19 (T3.1)	Cross-Domain Security	TRL4	The ability to connect MSaaS components working at different security and access levels in a manner that prevents secure data leaking across into other domains. (Also known as Multi-Level Security)	3

- Note that a reference in brackets means that the item is linked to the specified enabling technology, e.g. M19 is linked to enabling technology T3.1

Table 4-4: MSaaS Execution – Capabilities and Enabling Technologies #2.

Ref	Capability / Enabling Technology	Current Maturity	Definition	
M20	Rapid Accreditation aide	TRL2	A system that, when provided with a set of components with associated accreditation data and a composition definition, produces elements of the Risk Management and Accreditation Document Set (RMADS) that can be reviewed and approved by Information Assurance personnel. This provides for a flexible and rapid accreditation response to requests to set-up a combination of components to support a simulation need whilst controlling access to classified and export controlled information and protecting against attack.	3
M21	Encrypted Run-Time Containers	TRL1	The ability to run components on MSaaS container where not only is the container encrypted when stored on disk but the in memory image is encrypted with all data flowing over the container boundary, including networking and storage data, also being encrypted. Decryption happened on the fly within the MSaaS container.	4
M22	Load Balancing/Scalability	TRL3	The ability to improve the distribution of workloads across multiple computing resources by optimising resource use, maximizing throughput, minimizing response time, and avoiding overload of any single resource. Using multiple components with load balancing instead of a single component would increase reliability and availability through redundancy.	3
M28	Mediation Services	TRL6	Mediation services provides the translation required when different interoperability protocols are used.	3

Table 4-5: MSaaS Support – Capabilities and Enabling Technologies.

Ref	Capability / Enabling Technology	Current Maturity	Definition	
M23	Translation/Conversion Service	TRL4	A service which allows contents of the technical registry to be translated or converted from their original format into one which has been requested by a consumer of the MSaaS system.	3
M24	Costing/Advisory Service	TRL2	A service which advises as to the run-time cost of the proposed exercise, either resource cost or financial cost.	3
M25 (T1)	Business Models	TRL2	Flexible and agile business models that support the procurement and support of MSaaS capabilities, components and services (e.g. pay-by-the-hour procurement of a service from a Cloud provider).	4
M26 (T2.1)	License Management Solutions	TRL7	The ability of commercial organisations to manage the deployment and use of their tools, applications and services in a user's environment to protect their intellectual property rights and receive the appropriate financial recompense especially when the user's environment includes virtualisation and MSaaS technologies.	4

4.1.3.1 Taxonomy Workshop Output Summary

All discovery services identified need investment from defence communities, with only "Automated Meta Data extraction" needing significant investment. All but one of the composition services identified need investment. Cloud deployment technology maturity will be driven by the commercial sector. Automated

composition services and automated validation agents will require significant investment to mature. All execution services need investment to mature. If an encrypted runtime container approach is required to ensure delivery of secure services, then collaboration will be required across the community, as this approach was assessed as TRL 1. MSaaS supporting services also all need investment, in particularly in a collaborative manner by the community to develop business models and license management approaches.

4.1.4 CAX Forum 2017

A scheduled presentation and a demonstration event were held during the 2017 CAX Forum at Florence Italy. The CAX Forum was attended by over 250 Technology, Government and Military representatives from 29 nations. The presentation and demonstration of both constructive and virtual simulations provided a tangible working example of simulation services provided from the public Internet (Amazon Web Services).

Following the demonstration, the entire CAX Forum was opened to questions, which provided significant observations, interests and concerns from the broad user community. The following 21 questions were captured from the audience:

1) How will trust be established in the use of MSaaS?
2) Who and what support will be provided for MSaaS?
3) When do we aim to drop legacy systems?
4) What does the tech roadmap look like for MSaaS?
5) Who supports the development of the OPFOR across allied networks?
6) Will thin and zero client based delivery methods be incorporated in the solution architecture?
7) Will MSaaS incorporate VR based virtual simulations in the future?
8) How will MSaaS tie simulation exercises to training objectives?
9) Will MSaaS connect with Training Information Management systems?
10) What are the actions ahead to ensure goal achievement such as pay by the hour?
11) How can MSaaS prove enhanced operational readiness? When?
12) Where are the servers hosting MSaaS, and which networks will be used?
13) How should MSaaS be implemented?
14) What is the proposed business model and hosting approach?
15) How is MSaaS doing a better job? How can it be measured?
16) Which protocols are supported (DIS, HLA)?
17) What are the limitations of MSaaS?
18) Who/which Organization will own, operate, maintain, funding, (NCIA)?
19) How will platforms (tasks) and threats (relevance) be managed cohesively?
20) How will MSaaS handle the challenge of sharing data with industry?
21) What framework should be used for assessing cost and technology for acquiring M&S capabilities and services?

These questions provided some broader and somewhat unexpected perspectives on MSaaS which have been included in the Questionnaire results by the Evaluation Team.

In preparation for the CAX Forum MSaaS demonstration event, industry participants within MSG-136 were interviewed to collect data on the prototype implementation in accordance with the Technical Reference Architecture, tools, techniques and technologies provided in the MSG-136 GitHub repository.

Table 4-6 identifies a summary of the technical observations using the Docker container technology throughout the prototyping activities.

Table 4-6: Technical Observations Using the Docker Container Technology.

Benefits	Limitations	Challenges
Reliability, open source community, extensive documentation, free/affordability, high usability in creating compositions, high flexibility in scripting capabilities and API, less than 40 hours to install-configure-test a complete environment, less than 8 hours to configure and test the addition of an HLA/DIS gateway in the cloud, built in Dynamic Naming Service.	Some difficulty and effort required when developing across different operating systems \ VMs, self-signing certificates would simplify use in restricted network environments, Docker support primarily focused on VirtualBox, difficult to diagnose problems using the Windows based Docker Compose, Hyper-V does not run on Windows Home Edition.	Docker Toolbox version and VirtualBox version configuration management, Certificate management, Network management, Limited diagnostic capabilities, Drive dismount on VM shutdown, AWS latency effecting update rate and event synchronization, IP mapping and MAC addressing for legacy software and hardware (i.e., license dongles).
Reduces complexity and use of centralized OEM site infrastructure, development and test can occur at user location, reduced technical risk for developer and user, reduced turn-around time for user feedback to developer, saves time and money, improved configuration and dependency management with YML files.	No guidance on definition of names-nodes-containers, need for manual network configuration if a dynamic network provisioning service is not available, subtle issues between Docker versions, need to test and then retest compositions when changes occur – including software version updates and security patches.	Lack of consistent and human readable naming conventions, network bandwidth and network design for optimized performance, overlay network connectivity issues, potential test and re-test effort for compose file verification.

4.1.5 Stakeholder Feedback

Additional feedback was gathered over a series of events and interviews based on MSaaS discussions, panel events, presentations, and demonstrations. As time was limited in almost every case, stakeholders were either asked to provide their top three key benefits and limitations based on their understanding of MSaaS, or they provided their most important requirements and concerns of a shared services based approach to M&S capabilities for their agency/organization's program.

The stakeholder feedback is provided in Annex D. Individual contributor names have been removed as a courtesy.

4.2 ANALYSIS OF RESULTS

The stakeholder feedback underwent analysis to identify any and all new or existing qualitative measures, to compare with the internal assessment performed by the MSG-136 working group. This information was merged with the internal assessment to provide a broader market assessment of the key system and capability benefits, and the most important limitations or concerns.

The results were typified and categorized in accordance with the four key MSaaS Measures of Effectiveness (see Table 4-7). Based on analysis of the customer feedback gathered at scheduled events, the following observations were made:

1) The providers of feedback were exposed to presentations and demonstrations on MSaaS over the past 12 months. Their feedback was based on questions and observations made during these sessions or through direct questioning after the events.
2) The feedback identified from the CAX Forum Q&A introduced 21 new questions revolving around Accessibility, Suitability, Affordability, and Usability (in order of importance).
3) MSaaS presentations and demonstrations primarily addressed the comparably less important issues of Affordability and Usability (well communicated benefits), while less information was provided on the more important issues of Accessibility and Suitability. Several of these questions were not directly addressed in the information sessions.
4) The overall importance of Affordability and Suitability represents a general expectation of Value (Fit For Purpose / Training Effect) for Money (Reduced operating costs / time to deploy / support costs).
5) The middle tier of importance which includes Coherence/Cohesion, Scalability, Accessibility, Supportability, and Roadmap coincides with a recognized need for a clear system solution available, accessible and supportable at a known point of time (capability technology roadmap).
6) Four new quality measures were identified as key concerns or potential limitations of MSaaS, including a recognized need for a Roadmap, a Business Model, an understanding of Performance of a potential solution based on the Technical Reference Architecture, and importance of Trust in M&S services that utilizes verified and validated models and behaviors.
7) The most important concerns expressed by stakeholders were Vulnerability (Cyber Security), and Supportability of MSaaS systems.

Table 4-7: Technical Observations Using the Docker Container Technology.

Key System Benefits	Key Capability Benefits	Key Limitations
Affordability (24)	Suitability / Improved Training Outcomes (30)	Security/Vulnerability (10)
Coherence (20)	Increased Accessibility (26)	Supportability (7)
Scalability (15)	Increased Availability (11)	Roadmap (6)
Reusability (7)	Increased Usability (5)	Governance (4)
Flexibility (7)	On Demand (3)	Trust (4)
Composability (2)	Improved Interoperability (3)	Performance (4)
Modularity (2)	Reduced Manpower (2)	Business Model (3)

Key System Benefits	Key Capability Benefits	Key Limitations
Earlier Runtime	Increased Functionality (2)	
Open Source	Commonality	
Load Balancing	Improved Fair Fight	
Automation	Increased Maintainability	
Consolidation		

The challenges and recommendations from both CWIX events were analyzed for relevance and opportunity to improve planning and execution of events in the future by utilizing MSaaS capabilities. In short, the most relevant challenges were identified as follows:

1) Too much time is spent on configuration of M&S services, not only in technical issues but also related to scenario issues. More automation and diagnostic capability are required.
2) Service interoperability issues are primarily concerning federation issues between separate standards like DIS/HLA Pitch/MaK RTI. The need for a federation manager or service was identified.
3) A tool for displaying the information track through the MSaaS was identified as required.

4.2.1 Analysis of Accessibility

The pressure on facilities and personnel in provision of simulation capabilities is currently high which inhibits the ability to modernize their systems and approaches. MSaaS approaches need to demonstrate how they alleviate some of this pressure through decreasing the preparation time to establish an event (e.g., training environment) and how this enables execution of more events because less time is spent in preparation of the synthetic environment (e.g., more throughput of personnel through a training center).

Future work should seek to show how organizations and nations will have an increased interest to use these events as the barrier to entry will be reduced, particularly the training burden for use of tools. It is also thought that integration of MSaaS into supporting tools (e.g., exercise management tools, after action review tools) will make it more attractive to use as the efficiency will be apparent. The use of cloud and web technologies provides an opportunity to access simulation technology on demand whenever (24 hours a day) and wherever needed (operationally, in the live training area, multiple training facilities, at home). This will also need to be demonstrated on defence/government-owned IT infrastructure. This offers the opportunity to scale access to as many users that want to use and access the technology.

4.2.2 Analysis of Suitability

As with any new defence system, MSaaS needs to prove that it provides increased operational effectiveness (e.g., increased readiness, increased human performance, increased understanding). Being able to provide a golden thread that links simulation discovery, composition and outputs back to user objectives (e.g., training objectives, MOEs) will be key to evidencing the role of MSaaS in making this golden thread more transparent.

There is a big drive from the simulation user community to understand how simulation capabilities can be developed to meet current and future operating environments (areas of interest include whole world terrain, human terrain, operational scenarios, hybrid/information warfare, megacities, non-lethal/non-kinetic effects, ORBATS, equipment, platforms, communications systems, UAVs, etc.) and use should not be limited by the simulation technology (e.g., scaling to millions of entities may be required to meet a particular requirement should be possible if required). So MSaaS needs to demonstrate how the modular aspect of the framework

and elastic nature of the cloud can enable simulation systems to stay current and meet complex operational environments in order to gain traction with the user community. The approach also needs to be integrated with existing/future host infrastructure and ways of working so as not to have a negative impact on other areas (e.g., integration with networks, command and control environments, training information management systems, operational analysis toolsets, After Action Review tools, Live and Virtual systems as well as constructive).

Ultimately MSaaS development needs to provide hard evidence (that will stand up to scientific rigor) of its operational benefit so that the business cases can be made to decision makers who can clearly see the return on investment. Given the complexity of implementation an incremental approach will need to evidence incremental improvements in benefit.

4.2.3 Analysis of Affordability

MSaaS provides an opportunity to employ new business models (i.e., “pay per use” or “Gainshare” models) for acquiring simulation capability. The community wants to avoid stove piped approaches and reliance on a few providers of system solutions. The community has as a goal that the system solution should become more flexible and adaptable for introduction of emerging capability requirements. The MSaaS concept is built up on the principle that the community is sharing sources within the community and thus providing cost efficiencies. An incremental approach should be taken to avoid a big bang approach to delivery; however certain infrastructures such as cloud infrastructure will need to be available up front.

Chapter 5 – RECOMMENDATIONS

Based on analysis of the results and summary of the feedback, the following recommendations are provided:

1) Investigate and recommend a robust business model and governance body for supporting Accessibility to MSaaS based M&S services.

2) Provide and maintain a notional technology roadmap that indicates key technical insertions and capability milestones to guide the user and acquisition communities in planning migration to interoperable MSaaS services.

3) Review the definition of Measures of Performance, to determine key performance measures to be included in MSaaS Service Level Agreements and establish an MSaaS Verification and Validation framework.

4) Continue to collect feedback at upcoming scheduled events, in order to capture data from Technical, Government and Operations representation from all NATO countries.

5) Schedule a formal feedback forum when all MSaaS documentation is made available to the public.

6) Adopt and refine the Measures of Performance identified in Annex B to establish minimum performance criteria for incorporation into MSaaS based system performance specifications, Service Level Agreements and contractual KPIs, which level set industry, government and military expectations.

7) Define standards for simulation data unification, verification and validation of models and behaviours in order to establish trust in the proposed simulation services.

8) Identify related Cyber Security frameworks and roadmaps that will impact the selection of key MSaaS technologies and facilitate network interoperability at future milestones. Identify the importance and dependencies of obtaining security accreditation of key services and technologies.

9) Perform further comparative evaluation of alternate container technologies (Microsoft, Kubernetes, Weaver, etc.) including considerations in cost, licensing models, and relative performance.

10) Continue to evolve the MSaaS Capability Technology Roadmap, leveraging the ranked functions and services identified in the Taxonomy Workshop. Align these capabilities in accordance with key calendar milestones (IOC, FOC, and annual CWIX sprints) in order to provide the M&S community of interest a cohesive view of when specific services will become available and accessible.

11) Future experimentation and evaluation work should demonstrate and assess the ability of MSaaS to evidence provision of the following areas:

    a) Increased Operational Effectiveness (e.g., increased readiness);

    b) A golden thread that links simulation discovery, composition and outputs back to user objectives (e.g., training objectives, MOEs);

    c) An ability to stay current and represent complex current and future operational environments, including the ability to customize the system solution to suit emerging and urgent operational needs;

    d) How MSaaS can be integrated with existing/future host infrastructure (e.g., integration with networks, command and control environments); and

e) A clear business model and how service fees and licensing costs should be managed. This is an important topic that directly relates to the Accessibility and feasibility of launching MSaaS services in the future. The credibility of reduced costs depends entirely on a successful and easily executable, coherent business model that provides best value for industry, government and the military.

12) Continue to monitor challenges and recommendations from the ongoing CWIX events, and address the recognized need for the following MSaaS capabilities:

a) Federation management service;

b) Increased automation in composition and scenario planning; and

c) Improved diagnostic capabilities and information reporting services.

Chapter 6 – REFERENCES

[1] Bass, L., Clements, P., Kazman, R., Software Architecture in Practice. Addison-Wesley Professional, 1998.

[2] The Open Group, Service-Oriented Architecture – What Is SOA? [Online]. Available: http://www.opengroup.org/soa/source-book/soa/p1.htm#soa_definition. Accessed February 2017.

[3] The Open Group, SOA Reference Architecture, [Online]. Available: http://www.opengroup.org/soa/source-book/soa_refarch/. Accessed February 2017.

[4] The Open Group, Service-Oriented Cloud Computing Infrastructure (SOCCI) Framework, December 2001. [Online]. Available: http://www.opengroup.org/soa/source-book/socci/index.htm. [Accessed February 2017].

[5] The Open Group, SOA Governance Framework, August 2009. [Online]. Available: http://www.opengroup.org/soa/source-book/gov/index.htm. Accessed February 2017.

[6] Tolk, A., and Muguira, J., The Levels of Conceptual Interoperability Model, in the Proceedings of the 2003 Fall Simulation Interoperability Workshop, Orlando, 2003.

[7] The Open Group, SOA Governance Framework, 2012.

[8] NATO STO: Modelling and Simulation as a Service, Volume 1: MSaaS Technical Reference Architecture. STO Technical Report STO-TR-MSG-136-Part-IV. To be published.

[9] Grom, A., Rheinsmith, R., Blount, E., and Janele, J., Joint Staff J7 Joint Training Tools for Campaign Planning, in the Proceedings of MODSIM World 2017, Virginia Beach, VA, 2017.

[10] Simulation Interoperability Standards Organization, Base Object Model (BOM) Template Specification, 2006.

[11] IEEE Computer Society: IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) – Framework and Rules, 2010.

[12] IEEE Standards Association: IEEE Recommended Practice for Distributed Simulation Engineering and Execution Process Multi-Architecture Overlay (DMAO), 2013.

[13] IEEE Standards Association. 1730-2010: Recommended Practice for Distributed Simulation Engineering and Execution Process (DSEEP), 2010.

[14] NATO C3 Board: C3 Taxonomy Version 2.0, 2015.

[15] SISO-STD-012-2013: Standard for Federation Engineering Agreements Template (FEAT), SISO, 2013.

[16] NATO STO: Operational Concept Document (OCD) for the Allied Framework for M&S as a Service, STO Technical Report STO-TR-MSG-136-Part-III. To be published.

[17] NATO STO: AMSP-02 Allied Framework for Modelling & Simulation (MSaaS) Governance Policies. Edition (A), Version 1. To be published.

[18] NATO STO: Modelling and Simulation as a Service, Volume 2: Discovery Service and Metadata. STO Technical Report STO-TR-MSG-136-Part-V. To be published.

Annex A – CAPABILITY MATRIX

The Capability Matrix can be found in "**Sheet 2**" of the Excel file ("**TR-MSG-136-Part-II-EVAL-Verification-Matrix-v3_20180423.xlsx**") provided with this report.

Annex B – MSAAS MEASURES

The MSaaS Measures can be found in "**Sheet 3**" of the Excel file ("**TR-MSG-136-Part-II-EVAL-Verification-Matrix-v3_20180423.xlsxB**") provided with this report.

Annex C – QUESTIONNAIRE RESULTS

The Questionnaire Results can be found in "**Sheet 4**" of the Excel file ("**TR-MSG-136-Part-II-EVAL-Verification-Matrix-v3_20180423.xlsx**") provided with this report.

Annex D – STAKEHOLDER FEEDBACK

D.1 OPERATIONAL STAKEHOLDER

D.1.1 OPS 1

OPS – US Navy – Vice Admiral – MSaaS will need to support Ready Relevant Learning delivery methods in accordance with SAILOR 2025.

D.1.2 OPS 2

OPS – Greece Army – Brigadier General – MSaaS will need to incorporate C2SIM for tactical training and extend to a C2+LVC training capability.

D.1.3 OPS 3

OPS – US Army – Brigadier General – Current training systems have mutual depiction of live players in the synthetic environment. MSaaS will need to also support mutual depiction of virtual players in the live environment, (i.e., via Augmented Reality).

D.1.4 OPS 4

OPS – Italy Army – Colonel, CD&E Branch Chief – MSaaS will need to provide NATO's Archaria mega city model as a service. There is a need for a common UML/NAF repository, and MSaaS service definitions covering CD&E.

D.1.5 OPS 5

OPS – AUS ADSTC J7 Chief Scientist – Focus on operations. Adopt a holistic approach rather than stove-piping. Address the cultural aspects of cost and ownership. Consider interconnection of Joint Forces Battle Labs. Include C2/C4I for Joint Forces Experimentation.

D.1.6 OPS 6

OPS – USA Joint Training – Environment Architecture Director – Benefits of MSaaS are that it addresses cost issues of monolithic simulations and scalability. Need more repetition of events between major events for staff, rapidly dynamic, multi-domain, multi-national.

D.1.7 OPS 7

OPS – Joint Forces M&S Branch Head – must be available faster, address command staff training, include hybrid warfare and cyber warfare, money and security challenges.

Migration to centralized IT infrastructure has a two year plan ahead, significant fiscal constraints, monolithic in totality, significant license expenses, no time to modernize it more quickly, can't keep up with multi-national training needs.

D.1.8 OPS 8

OPS – USMC – Current training gap for escalation and de-escalation, no task attribute analysis or linkage to competency framework, need clear dashboard of training readiness reporting, need to incorporate more human terrain, effects and non-lethal/non-kinetic models.

D.1.9 OPS 9

OPS – Canadian Armed Forces DND – need an enterprise approach to managing simulation infrastructure, both real time and not real time services (EXCON, Terrain, AAR, WHITECELL, ORBAT) for virtual and live training exercises, license costs are an increasing concern.

D.1.10 OPS 10

OPS – USMC – MC STE LVC requires:

1) Enumeration services;
2) Filters (constructive to virtual/virtual to constructive, geo-filtering, entity based);
3) Gateways (stable, quick remote restart);
4) Analogs are an issue, need standards for integrating legacy weapon system controls (IP pass through to h/w challenges); and
5) Certified network architecture standard that supports multi-domain / multi-security / coast to coast latency / data replication services other than DIS / operable over contested bandwidth environments at Point Of Need.

D.1.11 OPS 11

OPS – US Army Aviation – key concerns are system stability, complexity of interconnections and ability to diagnose/treat problems, certificates of net worthiness, entity count limitations in simulation components or network, h/w in the loop and latency tolerances, need to enable IAMD and Cyber/EW exercises rapidly, what does the tech roadmap look like for MSaaS?, who supports the development of the OPFOR across allied networks? (ORBATs, equipment, platforms, comms, jammers, drones, effects).

D.1.12 OPS 12

OPS – US Army CAC-T – must support platoon to battalion level exercises where ever they are, integrate existing training capabilities, include National Guard and OCONUS, National Training Center must define performance requirements for collective exercises, build exercises faster.

Lower cost, quicker pace, more repetitions, must include voice communications (and C2 where possible), affordability, availability, scalability, One World Terrain, cloud stream to PON, 2 million entities, thousands of simultaneous users, 120 Hz VR to avoid motion sickness, virtual role players, simple exercise design tools, classified and unclassified network connectivity, must be simple to use, easy to integrate with allies.

Need a Training Management Tool that includes planning, execution, and assessment functionality/services.

D.1.13 OPS 13

OPS – Dep Dir NATO M&S COE – Benefits:

1) Affordability – acquisition versus service model;
2) Availability – persistent and interoperable for US, Canada, Korea, Australia; and
3) Scalability – scale upward.

Barriers/Limitations:

1) Ownership – own, operate, maintain, funding, NCIA?
2) Vulnerability – ownership, governance, risk, information assurance.

COE demonstration:

- Did not utilise container technology or MSaaS TRA.
- Uses VMWare and Remote Desktop (Virtual Desktop Infrastructure).
- Unity3D virtual front end.

Challenges – Bandwidth limitations, HTC VIVE sensor performance with lighting.

Benefits – Graduate level developers, no licensing issues, open source engine – (all Unity3D value statements, not to do with VMWare).

D.1.14 OPS 14

OPS – USAF Chief Simulators Division – Need a roadmap for a common open and modular simulation architecture and operational training infrastructure which integrates cyber tech insertions, minimizes lifecycle costs, incorporates VMs, containerization, libraries, and general purposes processing, leveraging existing WANs.

Need examples of how to provide Security Operations Centers across partner networks, including remote scanning and Public Key Infrastructure.

D.1.15 OPS 15

OPS – US Army Dep Dir Army Modeling and Simulation Office – Need to develop a roadmap for migration to services, need to stop paying the same vendor twice for adjacent programs and capabilities, Need to adopt an enterprise view (common data, terrain, tools, practices), build once – reuse often, need a knowledge management assessment to find out what exists.

Need to define API based browser plug-ins which utilise layers and leverage data services (like GIS industry tool adoption).

D.1.16 OPS 16

OPS – USAF Dir Training and Readiness – How will platforms (tasks) and threats (relevance) be managed cohesively? How should USAF improve operational training infrastructure in order to create venues (services) which increase repetitions and sets, How will MSaaS handle the challenge of sharing data with industry?, need for rapid prototyping and integration for end user evaluation.

D.1.17 OPS 17

OPS – Director Airman Systems Directorate AFRL – Key objectives:

1) Maximise Airman Availability;
2) Optimise Resource Efficiency; and
3) Enhance Human Performance, need a knowledge management system to provide performance based management capabilities for LVC events.

Need:

1) Scenario Development, Delivery, Management;
2) Performance Management and tracking of Live and Virtual entities; and
3) Integrated live and virtual performance based debrief services.

D.1.18 OPS 18

OPS – TRADOC Capability Manager for Virtual and Gaming – The MSaaS cloud concept needs to extend to the soldier Point of Need – not only at training centers, needs to provide virtual gaming capability for both training and mission rehearsal, utilize a common One World Terrain.

D.1.19 OPS 19

OPS – USMC Dir M&S Management Office – What framework should be used for assessing cost and technology for acquiring M&S capabilities and services?

Key concerns:

1) Enable LVC – training, metrics;
2) Wargaming – capabilities and concepts; and
3) Cyber security – network based, stimulate real world systems.

D.1.20 OPS 20

OPS – Dir Data Science, Models, Simulations TRADOC G2 – Need a common exercise design tool (browser based and open source), need a unified M&S data approach, need:

1) Common red and blue force structures – common naming conventions with mission command; and
2) One World Terrain
3) Common Probability of Kill parametrics – common damage models, fair fight.

Need a unified data approach through SISO standards.

D.1.21 OPS 21

OPS – Dep Dir Medical Simulation and Information Sciences Research Program – Need standardized training tools for reuse across all levels of training – Joint, Combined, National Partners exercise support, on public and defence networks, need standardized approach to inputs, methods and outputs, need a deployable training capability – transportable / mobile networked to distributed exercises.

Need to do a DSA assessment on training networks to utilize public infrastructure, need to incorporate Augmented Reality at Point of Need – bandwidth considerations / common content.

D.1.22 OPS 22

OPS – USAF National Guard LVC Enterprise Lead, Distributed Training Operations Center – Key objective is ability to perform daily LVC simulation exercises for Multi-Domain Battle Readiness.

Key challenges are:

1) Cybersecurity accreditation of operational training infrastructure; and
2) Interoperability at Joint and Partner Nation levels.

D.1.23 OPS 23

OPS – CAF M&S Coordination Office, Canadian Forces Warfare Centre.

What would the top 3 benefits of MSaaS be?

1) Force multiplier – significantly increases the ability to be more effective, efficient and handle more (the ability to handle more is directly related to scalability).
2) On Demand Service – the ability to utilize services/applications when and where needed is a huge benefit. As an unintended benefit, On Demand should help address interoperability issues.
3) Return on Investment/Value – This is what will help sell it to commanders and facilitate its institutionalization.

What do you think are the three main limitations or barriers to adoption in your country or service and why? (Security, business model, procurement etc.):

1) Security/Policy – Current IT and security rules/regulations/policies do not consider the integration new technologies and innovations. While basic and sound fundamentals are extremely important, these rules/regulations/policies need to be flexible enough to incorporate future developments in a timely manner.
2) Expertise to implement and upgrade – Currently there are only a limited number of subject matter experts who are able to incorporate these concepts – high demand, low availability.
3) Simulation Application Architecture – A lot of the current legacy/bespoke applications simply won't be able to migrate to a cloud based infrastructure and it will very much be future applications in most cases that will be populated onto the "cloud".

D.2 GOVERNMENT STAKEHOLDER

D.2.1 GOV 1

GOV – USA Joint Staff J7 – Benefits: Discoverability, Scalability. Other: Do no harm to the JLVC federation. Core and common services first. Use an incremental approach consistent with DoD initiatives.

D.2.2 GOV 2

GOV – USA Office of the Secretary of Defense – Director, Training Readiness and Strategy – MSaaS will need to support an infinite game concept whereby a persistent virtual training environment will allow users to join, collaborate and exit the environment on demand.

D.2.3 GOV 3

GOV – USA TCM ITE Chief Constructive Engineer – increase readiness, common operating environment, squad to echelon 4, LVC-IA enhancement, MC+SIM COE, scalability, flexibility, affordability, sustainment cost, accessibility.

D.2.4 GOV 4

GOV – USA TCM ITE Chief Virtual Engineer – focus on Point of Need, semi immersive, latency, GFT as a service, improve usability, terrain as a service, AAR services, scenario generation as a service, SAF/Models/Behaviors as a Service.

Key challenges are governance and funding are currently by product stovepipes, requirements are stovepiped capability based, need service oriented approach rather than product oriented.

Incremental prototyping, business case analysis.

D.2.5 GOV 5

GOV – Dir Advanced Distributed Learning, Dep Asst Sec Defense Force Education and Training – need a Total Learning Architecture – collection of specifications and technology roadmaps describing common microservices that publish training data across the enterprise, common naming conventions and competency framework.

D.3 TECHNICAL STAKEHOLDER

D.3.1 TECH 1

TECH – USA Lockheed Martin Corporation – Software Engineer.

Benefits:

- Docker:
  - Only need to get something right once and it's done;
  - Reliable;
  - Open source community;
  - Extensive documentation available;
  - Free/affordable;
  - Docker Compose is easy to use/create compositions;
  - Docker Compose files are flexible – can nest scripting or call externals; and
  - Mature API.
- VirtualBox:
  - Docker Machine supports VirtualBox; and
  - Docker support is mostly based on using VirtualBox.

Limitations/Challenges/Concerns:

- Docker:
  - Would be easier on one single OS;
  - Working across several VM OSs is time consuming for development;
  - More OS specific nuances during development;
  - Need to install a self-signed certificate for Harbor Docker images – difficult with LM network restrictions;
  - Need a certificate management strategy across different enterprises;
  - Docker support is mostly based on using VirtualBox; and
  - Any problems with Docker Compose (in Windows) are difficult to resolve.
- VirtualBox:
  - HyperV does not run on Windows 10 Home Edition; and
  - Versions of Docker Toolbox and VirtualBox need to be paired – drives unmount when VMs are shut down.

Other Key Points / Needs / Recommendations:

- Need to compare Docker and Weaver to Kubernetes and other container technology providers;
- Time to setup:
  - About 40 hours to install, configure, and run test complete environment;
  - Less than 8 hours to configure and test HLA/DIS gateway to integrate DIS simulations; and
  - FOMs were already supplied for run time.
- AWS Configuration:
  - Cannot use localhost in AWS, must use IP address in compose file;
  - Have to reset IP security settings when launching new AWS instance (new IP address assigned);
  - Issues with real time event synchronization, update rate, and propagation delay.

D.3.2 TECH 2

TECH – US Army ARL – DIS, HLA and TENA are well established old interoperability techniques; if cloud computing poses a new solution What trust? What support? Business models are slower than technology, when do we aim to drop legacy systems?

D.3.3 TECH 3

GOV/TECH – MITRE – Key considerations are:

1) Technical domain;
2) Governance;
3) Business model;
4) Security; and
5) Trust.

Need conceptual composability, VMs don't make it composable, conceptual model is needed, need to address fair fight challenge, need to consider transition of legacy systems in the interim.

Need a certified conceptual model – high cohesion, low coupling.

Key benefits are reduced TCO, speed of training delivery, translations from MS Office products.

Need prioritization of urgent needs; need a National Information Exchange Model; how do we ensure we do not lose embedded knowledge within legacy simulations and models? need an overall requirements consolidation and perform a relevance refresh; also strategic training needs not well supported by M&S (currently limited to table top methods).

D.3.4 TECH 4

TECH – IFAD Software Lead – Easy to get lost in definition of names, nodes, and dockers (DSEEP or MSG-136 should consider this).

Benefits:

1) Reduces complexity and use of centralized OEM site infrastructure – development can occur at user location;

2) Saves development time and money (technical and user risk);
3) Improves user feedback by remote access – fast turnaround; and
4) Configuration management is easier (however see limitations on same topic below) – YML file makes it easy as it shows dependencies.

Barriers/Limitations:

1) Network configuration control is challenging, need to manage networks (normally fixed infrastructure) – IFAD runs its own DNS server in the cloud to simplify IP mapping.

Technical Issues:

1) Network bandwidth issues;
2) Overlay network connectivity issues (may be solved with more Docker experience – need to pull down and run up nodes); and
3) Short ramp up time to learn Docker changes – but there are issues between old and new versions / configuration management issues. There is a need to test and retest compositions when regular updates occur, and all combinations. Security patches may also present regular retest overload.

D.3.5 TECH 5

TECH – Analyst Programmer, Air Synthetic Environment, Canadian Forces Aerospace Warfare Center.

On the assumption that MSaaS is essentially a single-provider that will configure the environment and push out the graphics needed to a remote location…

Advantages:

1) Reduced infrastructure and maintenance costs.
2) Flexibility (assuming whomever is the service provider, does this sort of thing regularly enough).
3) Single point of knowledge – meaning that standards can be adhered to easier than a distributed approach.

Disadvantages:

1) We are tethered to whatever equipment the provider wishes to use, meaning we cannot take advantage of low-cost options when they appear, nor are we authorized to fix something when it breaks, because it doesn't belong to us (Oculus Rift/HTC Vive/etc.).
2) Third-party providers are often slow to respond to changes, so the sales pitch of adaptive flexibility doesn't hold water with me. I've yet to see a third-party capable of leveraging the resources needed toward solving a problem quicker than on-site support.
3) Silos and protectionism abound in the DND. We have very strict security policies to observe, and few understand the complexity before promising the world in contracted services. (Shared Services Canada* comes to mind – where level II support is measured in weeks, not hours or days.) Yes, DND may very well be shooting itself in the foot with such things, but to circumvent in the name of convenience wouldn't be an acceptable workaround IMHO.
4) Further, MSaaS could very well eliminate my own current role as a simulation support technician – though this last one is rather personally motivated. :0)

- http://www.canberratimes.com.au/national/public-service/government-abandons-210-million-shared-services-white-elephant-20170524-gwc0u6.html.

- http://www.watoday.com.au/wa-news/1bn-to-fix-shared-services-disaster-as-barnett-drops-axe-on-troubleplagued-department-20110707-1h3s6.html.

Both of the above are examples of "IT as a Service", which are being echoed in the Canadian Government right now. http://www.cbc.ca/news/politics/mandate-letters-new-released-shuffle-1.4328966.

Admittedly, they did not fully understand the scope of the issue before trying to encapsulate it in the "as-a-service" framework, but to me, it seems a risky endeavour given the sheer amount of SIM exercises and local work we have to do to make it function to avoid "negative training".

I may have misinterpreted the intent of MSaaS, but I see plenty of similarities to be sceptical of the hype.

D.3.6 TECH 6

OPS/GOV/TECH – NATO CAX FORUM Feedback – MSaaS Demonstration:

- Will thin and zero client based delivery methods be incorporated in the solution architecture?
- Will MSaaS incorporate VR based virtual simulations in the future?
- How will MSaaS tie simulation exercises to training objectives?
- Will MSaaS connect with Training Information Management systems?
- Recognized need to improve the usability of composition and orchestration.
- What are the actions ahead to ensure goal achievement such as pay by the hour?
- How can MSaaS prove enhanced operational readiness? When?
- Where are the servers hosting MSaaS, and which networks will be used?
- How should MSaaS be implemented?
- What is the proposed business model and hosting approach?
- How is MSaaS doing a better job? How can it be measured?
- Which protocols are supported (DIS, HLA)?
- What are the limitations of MSaaS?

Annex E – FEEDBACK ON INTEGRATION OF VIRTUAL SIMULATION AND CONTAINER ENVIRONMENTS

E.1 INTRODUCTION

As part of a recent integration effort, Calytrix has been testing approaches for integrating the high-fidelity synthetic training environment, Titan Vanguard, into the Modelling and Simulation as a Service (MSaaS) testbed framework built up by the NATO working group MSG-136.

This report summarizes those activities and the challenges faced throughout this activity, and highlights some recommended areas for future research and investigation when considering the integration of graphically intensive applications into container-based environments.

E.1.1 Modelling and Simulation as a Service

The MSaaS working group seeks to explore ways in which advancements and trends in service-oriented and cloud-based architectures can be applied to modelling and simulation in order to meet critical NATO needs.

Driven by the broad goals of enabling rapid composition of credible simulation environments, the working group has built a testbed that leverages container-based technologies to allow resources to be automatically provisioned and configured, supporting the dynamic scaling out of resources to enable flexibility in meeting infrastructure demands even once an activity is under way.

The working group exemplar testbed is built around a container-based technology known as Docker. Before continuing, it is important to understand the difference between approaches built around "Container" technology and those that leverage Virtual Machines (VM).

E.1.1.1 Containers *vs.* Virtual Machines

The key difference between containers and virtual machines can best be described by the level of abstraction they focus on. A VM seeks to abstract an entire computer as a whole, from application all the way through to the operating system itself. For most purposes, VMs can be considered virtual instances of a full computer.

In contrast, Container environments seek to abstract a single application or process. Like VMs, they provide an isolated environment to the application, but they do not virtualize the full computer. Rather, technology is built into the operating system to allow a "containerized" application the illusion that it is running in a standalone fashion. Container environments have isolation for process trees, file systems and network stacks so that the process can act as if it were the only one running on the hardware when in reality it is sharing a server with many other containerized applications.

E.1.1.2 Why Use Containers?

There are many reasons to use containers, but the two most often cited are **performance** and **configuration management**.

Because the entire operating system is not being virtualized there is a much lower overhead on system resources. For the most part the applications themselves are running natively on the server rather than through a virtualization layer, allowing them to execute at much closer to native speeds.

Secondly, in the process of preparing an application to run in a container environment one must specify all its dependencies and operating configuration environment. This includes elements such as network ports

required and how they should be exposed. It also includes any other services that an environment depends on, many of which may be provisioned through containers of their own.

As container configuration is specified at a level of the application's functionality, the container configuration effectively describes the full operating needs of the application. This allows fully repeatable and reproducible environments to be set up in an automated manner according to this specification rather than relying on an administration to put all the necessary pieces in place by hand.

This in turn has a number of positive flow-on effects. The application environment is the same in testing as it is in production, allowing better testing and validation, but also simpler development and problem debugging. Further, new instances of an application can be quickly and easily spun up to meet expanding operational needs. If more seats of a Common-Operating Picture (COP) application are required due to the availability of extra participants in an exercise, new instances of the image can be automatically provisioned.

In contrast, Virtual Machines provide only a way to abstract the actual computer and do not address this specification of the applications that sit on top of them. They essentially do the job of moving the computing resources into a central location but do not necessarily address the configuration management of what is running on those computers. Today, the integration burden associated with delivering simulation environments is the source of considerable variability, cost and risk.

E.1.1.3 The MSaaS Infrastructure

As mentioned above, the current MSaaS testbed is built around the Docker container environment. It includes a number of services and simulations that have been integrated in a manner that allows participants to rapidly compose simulation activities that use these pre-configured environments.

During an exercise, parts of the simulation can be instantly scaled up or down as required. For example, in a recent demonstration the working group showed how through the click of a button in a control interface, new instances of a maritime simulation could be instantly added to a running exercise [1]. This simple concept quite powerfully shows the potential of such environments.

E.1.1.4 Summary

Now that we have some background and context to understand both MSaaS and container-based environments we will next look at the goals and challenges associated with the work of integrating Titan Vanguard.

E.2 INTEGRATING VIRTUAL AND SYNTHETIC ENVIRONMENTS

Since mid-2017 Calytrix has been engaging with the working group with the goal of integrating its high-fidelity virtual training environment, Titan Vanguard, into the testbed. This work has focused on three points:

1) Effectively containerize Vanguard and its critical integration configuration;
2) Enable Vanguard on cloud-infrastructure such as Amazon Web Services; and
3) Integrate Vanguard into an MSaaS exercise environment, enabling bi-directional communication on the simulation network.

The integration of Vanguard begins to address a number of important questions that impact how readily MSaaS-like environments could be rolled out to support particular types of simulation activities.

While ultimately successful in allowing all three of these goals to be met, the process and final solution do highlight some problems that will be experienced whenever one attempts to tie together intensive graphical applications or Windows-based simulations into a similar infrastructure.

E.2.1 What is Different About Vanguard?

Before looking at the developed solution we should first understand what is different about the Vanguard environment that makes its deployment into MSaaS novel.

E.2.1.1 Graphically Intensive and Accelerated

First and foremost, Vanguard is a graphically intensive application that makes heavy use of a computer's Graphical Processing Unit (GPU). In Vanguard, the GPU is used both for the rendering of the virtual world and for various computation tasks.

While GPUs are found in any modern gaming PC, they are not as common in cloud-based infrastructure. The availability of GPU accelerators in cloud-based infrastructure does exist, however many applications are focused on the needs of machine learning and other computational problems rather than those of interactive graphical applications.

E.2.1.2 Human-in-the-Loop

Secondly, Vanguard is inherently built to power human-in-the-loop simulations. These environments put a trainee into a virtual environment and requires their input to control their view and actions. One critical side-effect of this is that users require **low-latency** access to the environment in order use it effectively. Unlike simulation models which run without human intervention or non-3D user interfaces where latency can be more readily tolerated, simulations such as Vanguard which can operate in a first-person capacity needs to support what is often referred to as "twitch response" actions that are not possible in the presence of lag.

When deployed into a typical battle simulation centre, the trainee has direct access to physical hardware that the simulation is executing on. When deployed into an MSaaS environment this hardware may be housed some distance away, and will likely be multi-tenanted and virtualized. A simple, effective way to get the user to the virtual desktop is essential.

E.2.1.3 Windows-Based Applications

Finally, like most 3D synthetic environments, Vanguard is a Microsoft Windows-based application. To date, Docker-based container environments are built around the Linux operating system.

Somewhat ironically, the accepted method to get Docker running on Windows is to run it inside a Linux Virtual Machine that sits on-top of windows. Although this does allow Docker environment to run on Windows computers and servers, the containers themselves are still running on Linux, and as such, do not support native integration of Windows applications. To effectively integrate Vanguard into the existing MSaaS infrastructure some solution to this problem is required.

Taken together, these problems represent a number of significant hurdles that needed to be overcome. The next section will discuss the ultimate solution that was devised to address these issues and the manner in which Vanguard has been integrated into the MSaaS testbed.

E.3 INTEGRATING TITAN VANGUARD

The integration activity completed by Calytrix has focused on the three major issues identified in the previous section:

- GPU-intensive applications running on cloud infrastructure;
- Low-latency access to the simulation environment; and
- Integration of Windows-based applications into MSaaS testbed.

To get started, let's first outline what our end-state looks like.

E.3.1 Experiment Goals and End-State Description

The final demonstration of this capability builds on the existing MSaaS testbed demonstration that was shown at the 2017 NATO CAX Forum [1]. The goals for this experiment were to have:

- An instance of Titan Vanguard running on Amazon-hosted infrastructure;
- Remote, native-speed access as a "player" in this environment;
- Integration of simulation data between Vanguard and the MSaaS simulations; and
- Lifecycle (setup/teardown) of a Vanguard instance fully integrated into the existing MSaaS testbed.

When an exercise is kicked off and the containers are spun up as per the exercise description, instances of Vanguard should be auto-provisioned like any other Docker-based application.

Users should be presented with a way to access these instances as they come online, and then from within the application they should be able to see all the simulated data, as should the other simulations be able to see Titan-generated data.

To show this, a small scenario was created that will fly a Vanguard-based Predator UAV aircraft over the exercise objective area providing a sensor view of the platforms injected by other simulations. This entity is visible in the other simulation applications that form the existing MSaaS testbed and the platforms injected by those applications are visible inside Vanguard.

E.3.2 Architecture

The overall system architecture can be seen in Figure E-1, below. We will spend the rest of this section discussing its key elements and how they address the experiment goals listed above.

Here you can see three main parts to this system. The newly introduced parts to this setup are shown in orange, while the existing elements are in black.

On the left we have the container based services that form the existing MSaaS testbed. These have been extended to allow new data pathways.

To the right there is a separate box for the Vanguard instances running on the same cloud-infrastructure provider, but using a different technology base. This infrastructure has a point-to-point link into the container-based environment to bring the simulation data stream in and out.

Finally, in the top-right we have the end-user who has access to the instance of the virtual environment that is running. Let's step through each of these and discuss them in some more detail.

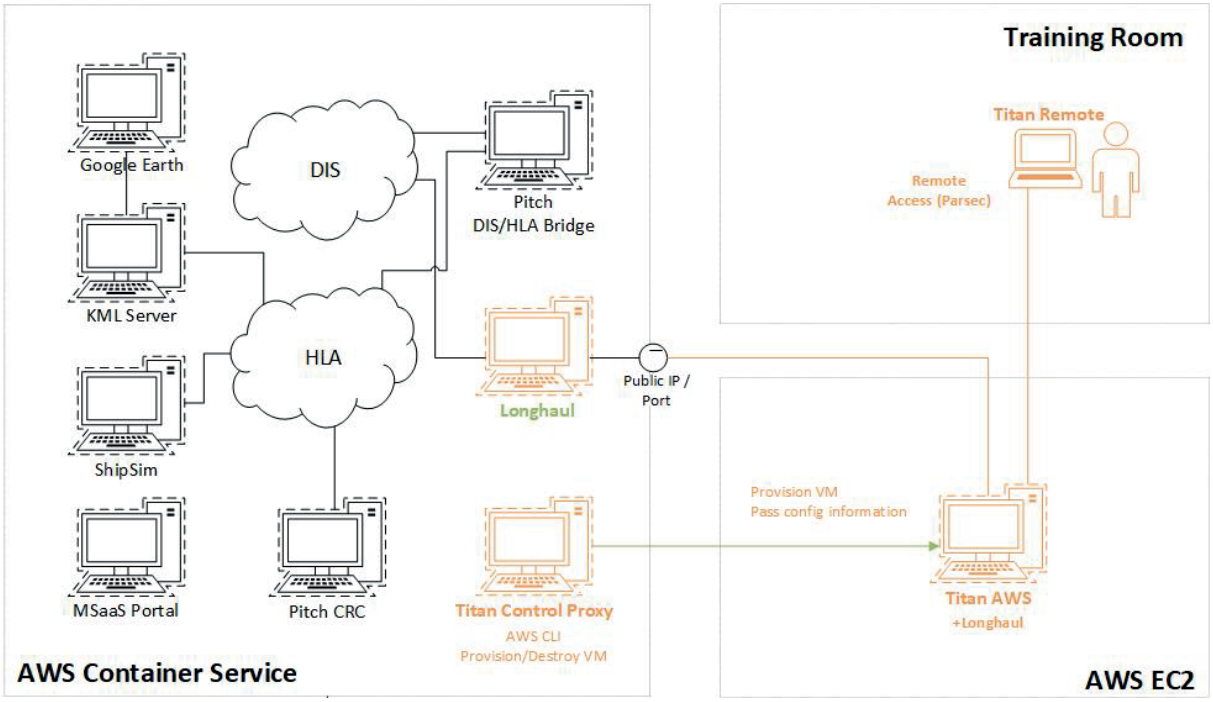


Figure E-1: Experimental Architecture.

E.3.2.1 Vanguard in the Cloud

The first step in this activity was to enable Titan to run on one of the existing cloud providers. We cannot directly integrate Vanguard into the existing Docker infrastructure because of its requirement for Windows and for GPU acceleration. As such, we need an alternative, and in this case only virtual machines are able to provide the necessary capabilities.

The MSaaS testbed has been active on AWS and so this was chosen as the target deployment platform for Vanguard as well. For this reason, we have deployed Vanguard to the Amazon Web Services (AWS) Elastic Compute Cloud (EC2) as a virtual machine.

The VMs are powered by the AWS graphics-accelerated line, with our test instances based on the **g2.2xlarge** instance type. Table E-1 shows the AWS VM Specifications.

Table E-1: AWS VM Specifications.

	vCPU	RAM	GPU	Network	Storage
g2.2xlarge	8	15 GB	1 (4 GB VRAM)	1 Gbps	1 x 60 GB SSD + EBS

This configuration is the smallest available on AWS that includes GPU acceleration and provides adequate system resources to run Titan. In general tests we found we were able to sustain performance exceeding 60 fps in most common scenarios.

With Vanguard now running successfully in the cloud we needed the trainee to be able to access it.

E.3.2.2 Remote Access to Virtual Applications in the Cloud

Virtual training environments are not like standard applications or web-based tools. They present an immersive 3D graphical environment to the trainee that demands low-latency links between the user and the application to ensure movements are smooth and faithfully represent the user intent.

Regular remote desktop technologies such as Microsoft Remote Desktop or VNC are designed for standard application use and present either too much lag to be usable, or simply will not work with OpenGL-based applications. To ensure that the experimentation environment represented a credible deployment profile, a better access solution was required.

To support this, Calytrix worked with a company called Parsec [2]. Parsec is remote streaming software designed specifically to address the demanding requirements of remote gaming. Aggressively optimized to support video stream transmission and low latency input, Parsec can deliver 60 FPS+ full HD streams while remaining responsive.

Software is installed on the client-computer (in this case, our AWS instances) and clients end-point software to access the remote environment and stream input and video back and forth. The client-side software can be deployed by a number of devices, including Windows, Linux, Apple Mac and Android devices, and even a Raspberry Pi.

The user is presented with a login screen (Figure E-2) against which they can see the resources which are available as they come online. They click “Connect” and they are taken directly to the application.

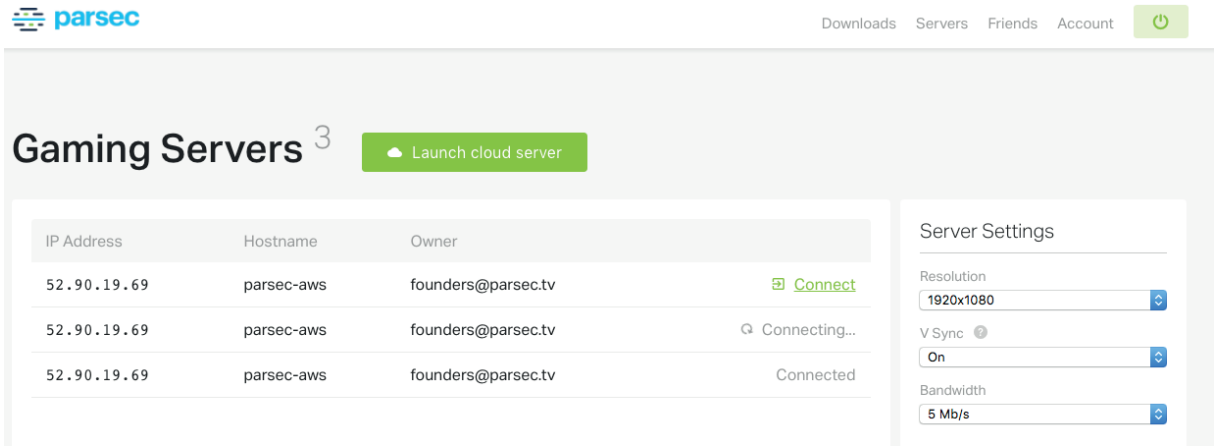


Figure E-2: Parsec Login Screen.

This access mode naturally fits into the MSaaS deployment model where infrastructure is deployed at a button click and becomes available soon after. When a Vanguard VM has completed start-up and is accessible, it appears in the list and is available for user access.

E.3.2.3 Bridging Simulation Data

Now we have remotely deployed Vanguard resources that can be spun up on demand available, and we have a way for the end-user to access them. The next step is to establish simulation data connectivity between these Vanguard VMs and the MSaaS container testbed.

When deployed, MSaaS container applications have connectivity between one another via a private virtual network. Container applications believe they are running on a private network and without explicit

configuration there is no way for external applications to gain access. In the architecture diagram we can note that there are both DIS and HLA applications running inside the MSaaS containers. We need to create a bridge between external Vanguard VMs and this network.

For this experiment we are making use of Vanguard native DIS bridge. However, DIS traffic is natively multicast or broadcast and cannot be natively routed through cloud infrastructure like AWS. To address this, we need a bridging application.

Disco is an open-source DIS library that includes a tool called the DIStributor [3]. It will allow DIS traffic to be routed via point-to-point connections across the Internet. It is also able to run on Linux, meaning it can easily be deployed as a container making it ideal for this purpose.

To support this experiment, we have generated a containerized version of Disco and added it to the MSaaS federation. When the experiment is started a copy of Disco is also activated. It listens on the local container network for all DIS traffic and sends it to any clients connected outside the container. It also forwards incoming information from external applications into the container DIS network.

With this bridge in place, the remote instances of Vanguard are able to bi-directionally exchange simulation traffic with the native container simulations despite the isolation boundary between their networks.

E.3.2.4 Lifecycle Management

With these elements established we now have a high-performance synthetic environment running on cloud-based infrastructure, remotely accessible to an end-user at their point of need and integrated into the MSaaS tested simulation stream.

The final piece required is to link the lifecycle of the Vanguard virtual machines to that of the container-based environment so that exercises may be started and stopped as a single unit.

To achieve this, we created a Vanguard “Proxy” container. Using the Amazon EC2 API we have a set of Linux shell scripts that we have turned into a Docker container. These scripts perform critical management actions when the container is started or shut down.

On Exercise Start-up

All MSaaS testbed containers will be started, including the newly integrated Vanguard proxy container which will:

- Provision and start a new Vanguard VM from existing snapshot;
- Use AWS tags to pass configuration information into the VM:
  - Disco end-point to connect to.
  - Parsec account log-in information.
- Start-up Windows Powershell scripts inside the VM will:
  - Auto-launch Vanguard.
  - Read AWS tags and configure Disco to connect to the correct server.
  - Read AWS tags and configure Parsec to log into the correct account.

As the VM boots and comes online it will log into the Parsec account and become available for an end user to connect with.

The use of the AWS tagging mechanism allows key configuration information to pass from the proxy container description into the external VM, effectively allowing customization.

On Exercise Shutdown

When the exercise is stopped, a shutdown command is passed to the containers. The Vanguard proxy will catch this and:

- Shutdown the linked VM.
- Destroy the VM to clean up resources.

Each proxy container is a one-to-one link to the VM that is created, allowing these to be auto-scaled as needed.

By including the proxy container in an exercise Vanguard resources can now be automatically provisioned like any container application.

E.3.3 Demonstration Environment

With the experimental infrastructure complete we have run several tests to ensure that the connectivity between the Docker-based MSaaS testbed, the external Vanguard VM and the Parsec remote access end-point all work as expected. We have also created a video that shows this activity in progress.

The demonstration scenario allows a player to operate the sensor view of an MQ-1 Predator UAV feed that is flying over the objective area inside Vanguard. This platform can see the incoming platforms from the ShipSim. In turn, the simulation data for the platform is being injected into the MSaaS testbed. This data is detected by an application that converts it into KML which it then fed into a container version of Google Earth in which the symbology and location of the UAV can be seen and tracked.

E.3.3.1 Demonstration Simulations and Systems

Table E-2 lists the various systems that are deployed in the experiment and the locations where they each reside.

Table E-2: Demonstration Simulations and Systems.

Application	Location	Provider	Description
MSaaS Portal	Docker	MSG-136	Web-based UI to control exercise creation and shutdown.
ShipSim	Docker	DSTG	Maritime simulator injecting virtual ship platforms into the simulation. Provided by Australian Defence Scenario and Technology Group (DSTG) [4].
KML Server	Docker	TBA	Reads simulation traffic and generates KML feed from it.
GE Viewer	Docker	MSG-136	Google Earth viewer that reads KML feed.
HLA RTI/CRC	Docker	Pitch Technologies	HLA Simulation Connectivity Backbone [5].

Application	Location	Provider	Description
DIS Adapter	Docker	Pitch Technologies	Bridge between DIS and HLA protocols [6].
Disco Bridge	Docker	Open Source	Long-haul DIS connectivity. Open Source.
Titan Control Proxy	Docker	Calytrix Technologies	Custom-build AWS API control scripts in Docker container.
Titan Vanguard	AWS EC2	Calytrix Technologies	Titan Vanguard virtual synthetic training environment [7].
Parsec Client	End User	Parsec.tv	Application on user device to access Vanguard [2].

The items highlighted above represent those components that were built as part of this experiment to extend the existing MSaaS testbed. The next section describes a typical demonstration exercise and includes screenshots that show the pieces in progress.

E.3.4 Demonstration Process

When running the demonstration, the process is largely the same as that done for previous MSaaS demonstrations.

E.3.4.1 Step 1: Start the MSaaS Portal Container

The MSaaS portal container provides a list of exercise configurations. Users can select one of these and start all the components with the click of a button (Figure E-3).

Figure E-3: MSaaS Portal Prior to Exercise Start.

E.3.4.2 Step 2: Start the Exercise

The user selects the exercise they want and starts it. This spins up the various containers listed in Section 3.3, including the Titan Control Proxy which in turn will auto-provision a virtual machine and begin the process of booting it (Figure E-4).

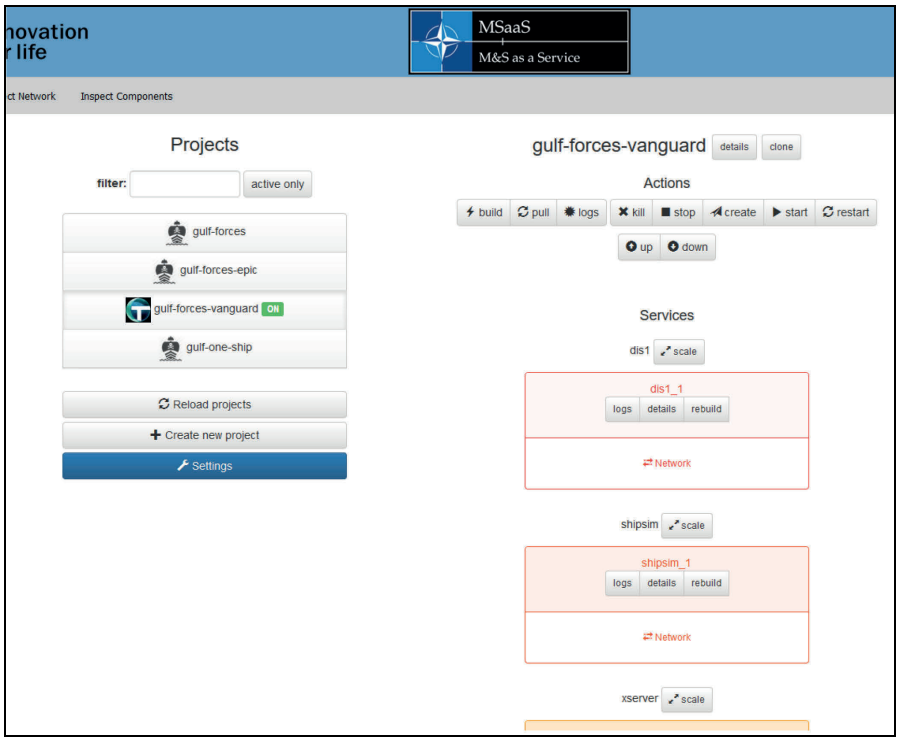


Figure E-4: MSaaS Portal with Active Containers.

E.3.4.3 Step 3: Inspect Exercise Environment

Once the various containers are loaded, we can navigate to the Google Earth viewer. Here we will be able to see the locations of the ships that are being injected by the ShipSim (Figure E-5).

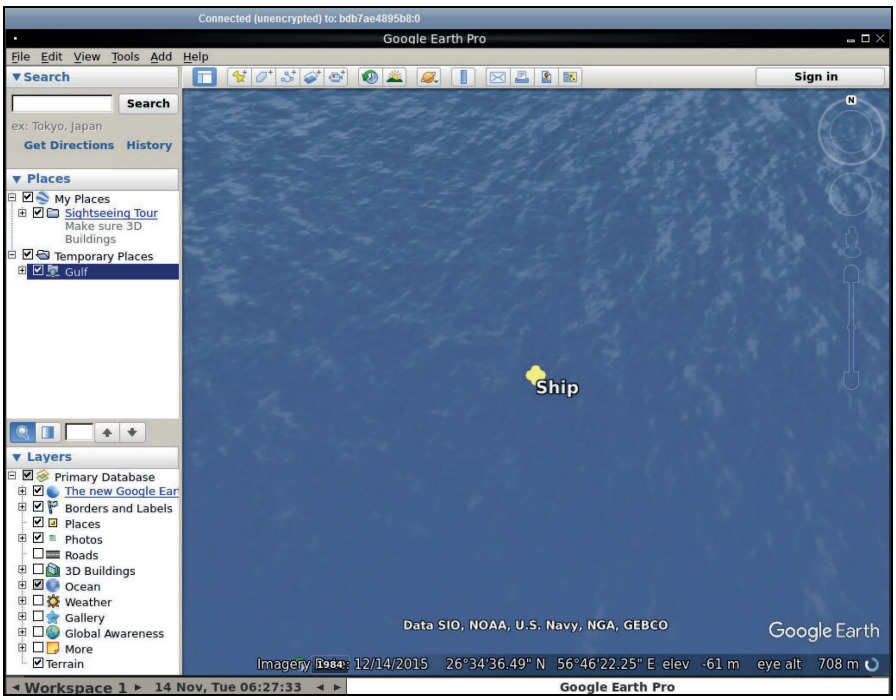


Figure E-5: Google Earth View of Simulation Data from Exercise (GE Running in Container).

For effect we will dynamically provision another ShipSim instance by clicking the "Scale" button and entering "2" as the number of ShipSim containers we want running (Figure E-6).

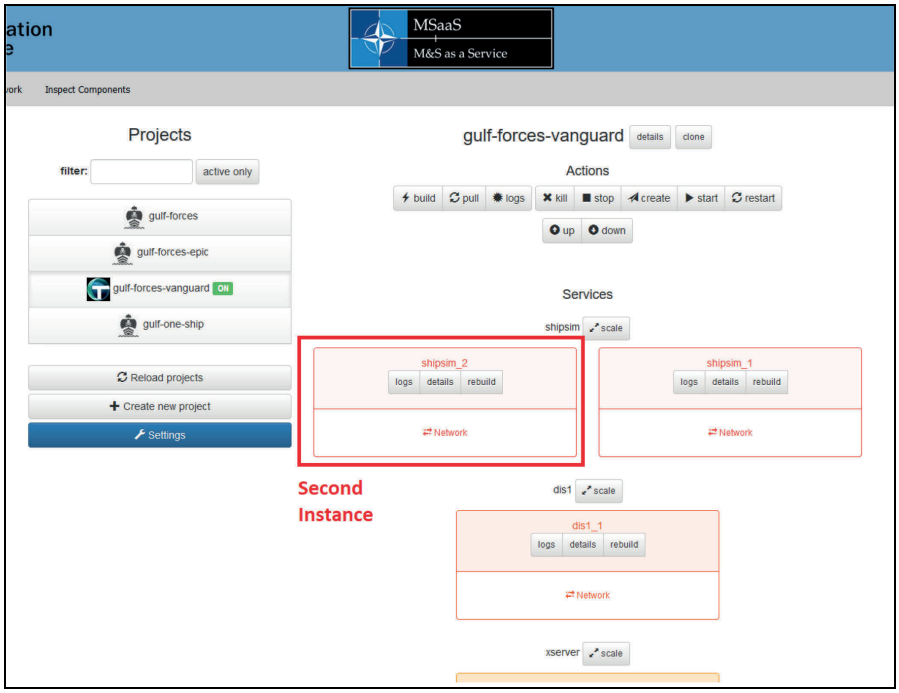


Figure E-6: Dynamically Adding New Containers.

This then gives us a second ship in the simulation (Figure E-7).

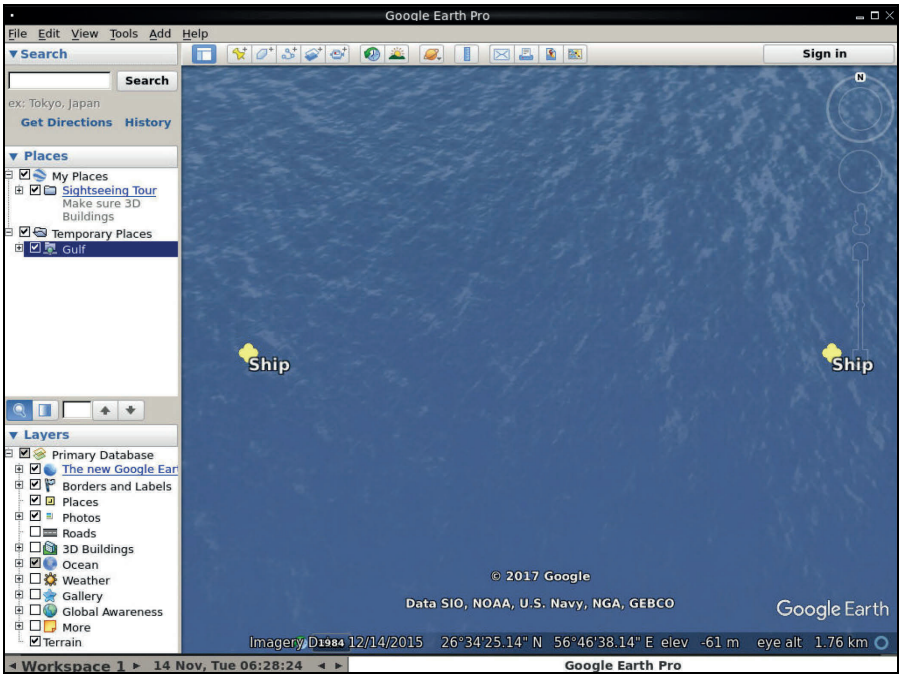


Figure E-7: Second ShipSim Present in Federation.

E.3.4.4 Step 4: Connect to Vanguard Instance

With the MSaaS standard testbed up and running we can open our Parsec client and wait for the Vanguard VM to become available (Figure E-8).

Once it appears in the list we can connect, enter the scenario and take control of the UAV. In the image below we have locked the UAV on the ships being injected from the ShipSim. You can see the first ship in the foreground and the second one in the background (Figure E-9 and Figure E-10).

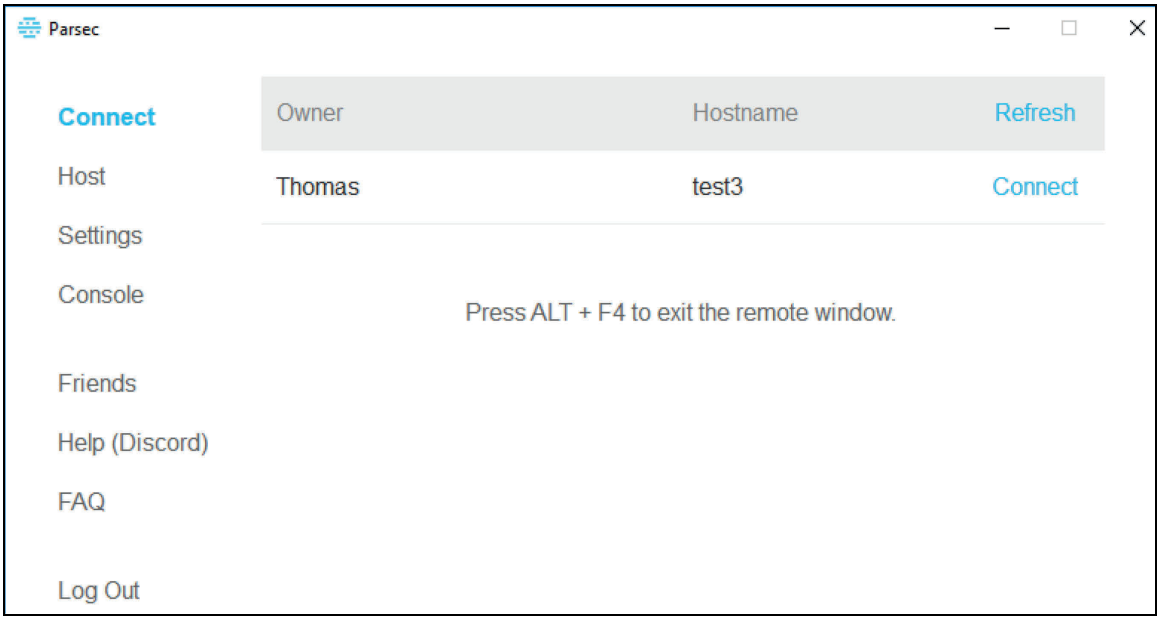


Figure E-8: Parsec Client Window.

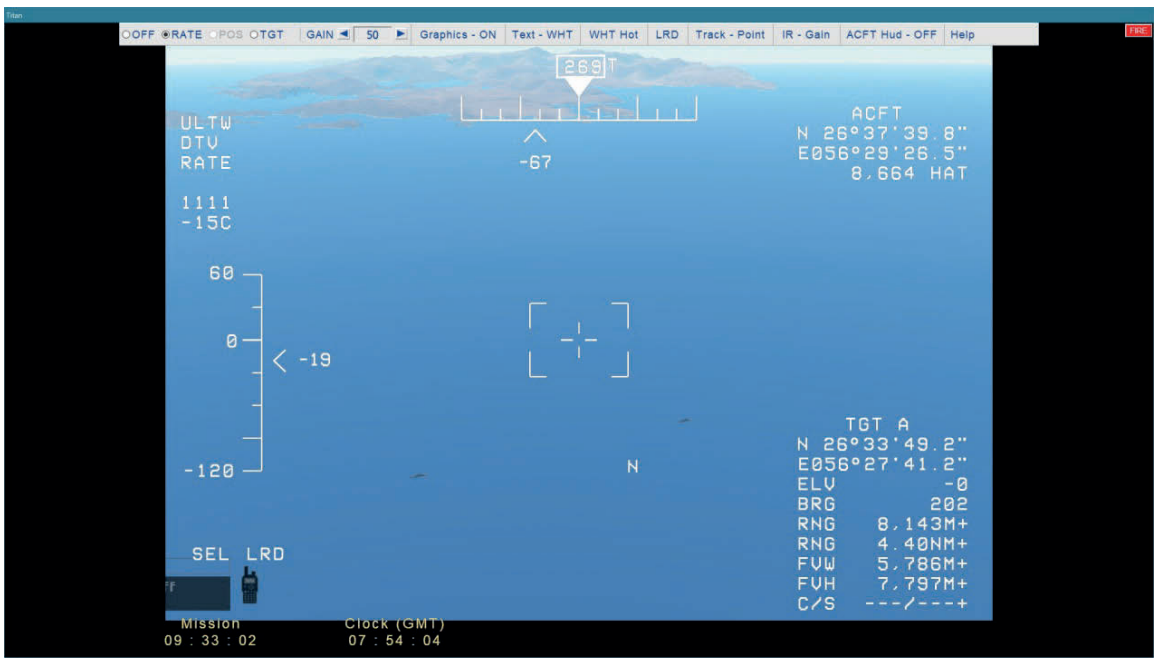


Figure E-9: UAV View of ShipSim Platforms.

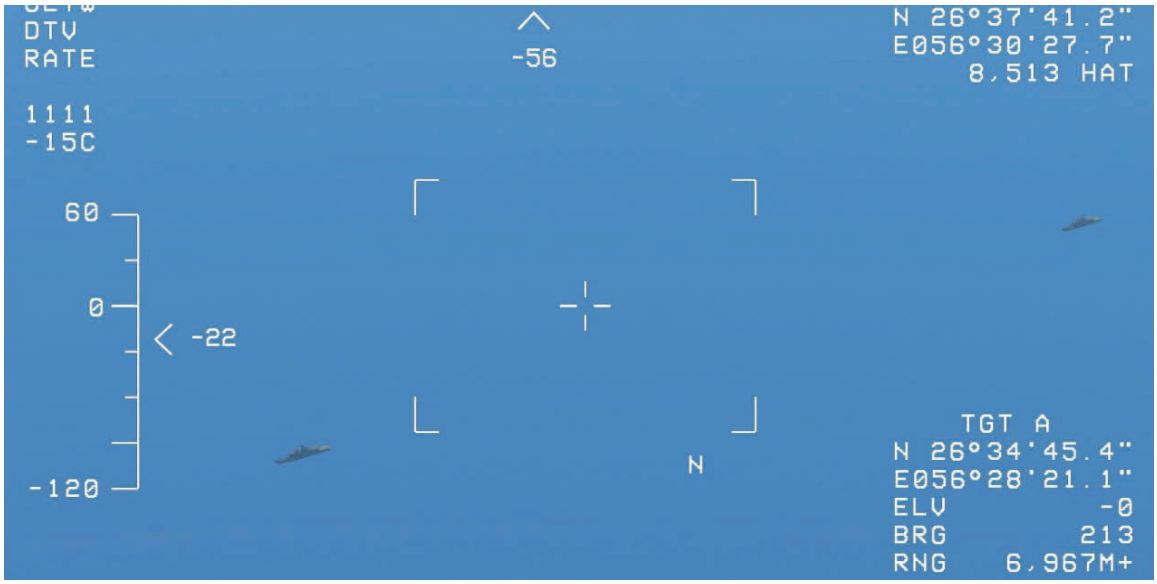


Figure E-10: UAV View of ShipSim Platforms (Detail).

E.3.4.5 Step 5: Exercise Shutdown

Once the activity is completed a user can return to the MSaaS portal and shut the exercise down. This will terminate the containers and free the resources. Each Titan Control Proxy container terminates the associated Vanguard AWS instance and destroys it.

E.4 CONCLUSION

There can be little question that the application of service-based architectures can deliver significant benefits when applied to the Modelling and Simulation spaces. Once the initial work has been done to integrate simulations in the first instance, they can rapidly be pulled into new exercises with relatively little effort or the need for a deep understanding of their complex environmental dependency needs.

Further, the ability to build reproducible environments significantly assists in the pre-exercise verification of integration and is also able to more readily support the need to respond to changes in the volume of required infrastructure needed either shortly before or even during an activity.

Taken together, these advantages lead to better integrated simulation environments, which are able to be delivered faster, with more flexibility and less risk.

E.4.1 Recommendations

The current infrastructure approach works best for analytical simulation workloads. By their nature they are best suited to take advantage of large infrastructure and the scale it affords. They typically lack a significant human-in-the-loop element and are commonly CPU-bound.

Further work is needed to better understand how the MSaaS approach and infrastructure can be uniformly applied across the full spectrum of simulation applications, including those that are often deployed to support training applications or involve immersive virtual environments. The limitations that prevent the native integration of Windows applications or those that require GPU-accelerated graphical workloads represent a large number of simulation systems that are often deployed into environments that could equally benefit from the improved configuration management, environmental repeatability and rapid provisioning that MSaaS can deliver.

In this experiment we have custom designed the glue necessary to bring these two environments together, showing that it can be achieved. However, this approach also depends on a number of environmental specifics, such as the use of AWS GPU VM profiles and the AWS API. Investigation into more standardized, first-class options would help to broaden the applicability of MSaaS and would build on the excellent work that has been done by the working group to date.

E.5 REFERENCES

[1] Modelling and Simulation as a Service Demonstration, NATO CAX Forum 2017, Florence, Italy.

[2] Parsec website, https://parsec.tv. Accessed 23 April, 2018.

[3] Disco Distributor, https://github.com/openlvc/disco. Accessed 23 April, 2018.

[4] Australian Defence Science and Technology Group (DSTG). Virtual Ship. Accessed 23 April, 2018.

[5] Pitch pRTI, provided by Pitch Technologies: http://www.pitchtechnologies.com/products/prti/. Accessed 23 April, 2018.

[6] Pitch DIS Adapter, DIS/HLA bridge, provided by Pitch Technologies: http://www.pitchtechnologies.com/products/disadapter/. Accessed 23 April, 2018.

[7] Titan Vanguard, provided by Titan.IM and Calytrix Technologies: http://www.calytrix.com/products/titan/. Accessed 23 April, 2018.

E.6 CONTACT INFORMATION

For additional information, please contact:

Name: Dr. Tim Pokorny
Email: tim.pokorny@calytrix.com
Phone: +61 4 3965 9193

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TR-MSG-136-Part-II AC/323(MSG-136)TP/829	ISBN 978-92-837-2155-0	PUBLIC RELEASE

5. Originator

Science and Technology Organization
North Atlantic Treaty Organization
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

6. Title

MSaaS Concept and Reference Architecture Evaluation Report

7. Presented at/Sponsored by

Evaluation Report of NATO MSG-136.

8. Author(s)/Editor(s)	9. Date
Multiple	May 2019
10. Author's/Editor's Address	**11. Pages**
Multiple	82

12. Distribution Statement

There are no restrictions on the distribution of this document. Information about the availability of this and other STO unclassified publications is given on the back cover.

13. Keywords/Descriptors

Cloud computing
Composability
Distributed simulation
Interoperability
Live, Virtual, Constructive (LVC) Modelling
Modelling and Simulation (M&S)
Modelling and Simulation as a Service (MSaaS)
M&S Services
NATO C3 Classification Taxonomy
Reference architecture
Service-Oriented Architecture (SOA)
Simulation
Simulation Architecture
Simulation Environments
Simulation Interoperability

14. Abstract

M&S as a Service (MSaaS) is a concept that combines service orientation and the provision of M&S applications via the as-a-service model of cloud computing to enable more composable simulation environments that can be deployed and executed on-demand. NATO MSG-136 investigated the concept of MSaaS and provided technical and organizational foundations to establish the Allied Framework for M&S as a Service within NATO and partner nations. The Allied Framework for M&S as a Service is the common approach of NATO and nations towards implementing MSaaS and is defined by the Operational Concept Document, Technical Reference Architecture, and MSaaS Governance Policies.

This document contains the Evaluation Report that provides an assessment of independent review on MSaaS. It provides an overview of all results and makes recommendations for consideration in future increments of the Allied Framework for MSaaS.

NORTH ATLANTIC TREATY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DIFFUSION DES PUBLICATIONS
STO NON CLASSIFIEES

Les publications de l'AGARD, de la RTO et de la STO peuvent parfois être obtenues auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la STO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus soit à titre personnel, soit au nom de votre organisation, sur la liste d'envoi.

Les publications de la STO, de la RTO et de l'AGARD sont également en vente auprès des agences de vente indiquées ci-dessous.

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivi du numéro de série. Des informations analogues, telles que le titre est la date de publication sont souhaitables.

Si vous souhaitez recevoir une notification électronique de la disponibilité des rapports de la STO au fur et à mesure de leur publication, vous pouvez consulter notre site Web (http://www.sto.nato.int/) et vous abonner à ce service.

CENTRES DE DIFFUSION NATIONAUX

ALLEMAGNE
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7, D-53229 Bonn

BELGIQUE
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research
for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30, 1000 Bruxelles

BULGARIE
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DGSIST 2
Recherche et développement pour la défense Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

DANEMARK
Danish Acquisition and Logistics Organization
(DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESPAGNE
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

ESTONIE
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

ETATS-UNIS
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72
92322 Châtillon Cedex

GRECE (Correspondant)
Defence Industry & Research General
Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HONGRIE
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALIE
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

LUXEMBOURG
Voir Belgique

NORVEGE
Norwegian Defence Research
Establishment
Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

PAYS-BAS
Royal Netherlands Military
Academy Library
P.O. Box 90.002
4800 PA Breda

POLOGNE
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

REPUBLIQUE TCHEQUE
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

ROUMANIE
Romanian National Distribution
Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

ROYAUME-UNI
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down
Salisbury SP4 0JQ

SLOVAQUIE
Akadémia ozbrojených síl gen.
M.R. Štefánika, Distribučné a
informačné stredisko STO
Demänová 393
031 06 Liptovský Mikuláš 6

SLOVENIE
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

TURQUIE
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi
Başkanlığı
06650 Bakanliklar – Ankara

AGENCES DE VENTE

The British Library Document
Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
ROYAUME-UNI

Canada Institute for Scientific and
Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications STO, RTO et AGARD figurent dans le « NTIS Publications Database » (http://www.ntis.gov).

NORTH ATLANTIC TREATY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DISTRIBUTION OF UNCLASSIFIED STO PUBLICATIONS

AGARD, RTO & STO publications are sometimes available from the National Distribution Centres listed below. If you wish to receive all STO reports, or just those relating to one or more specific STO Panels, they may be willing to include you (or your Organisation) in their distribution.

STO, RTO and AGARD reports may also be purchased from the Sales Agencies listed below.

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number. Collateral information such as title and publication date is desirable.

If you wish to receive electronic notification of STO reports as they are published, please visit our website (http://www.sto.nato.int/) from where you can register for this service.

NATIONAL DISTRIBUTION CENTRES

BELGIUM
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30
1000 Brussels

BULGARIA
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DSTKIM 2
Defence Research and Development Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

CZECH REPUBLIC
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

DENMARK
Danish Acquisition and Logistics Organization (DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESTONIA
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc – BP 72
92322 Châtillon Cedex

GERMANY
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7
D-53229 Bonn

GREECE (Point of Contact)
Defence Industry & Research General Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HUNGARY
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALY
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

LUXEMBOURG
See Belgium

NETHERLANDS
Royal Netherlands Military Academy Library
P.O. Box 90.002
4800 PA Breda

NORWAY
Norwegian Defence Research Establishment, Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

POLAND
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

ROMANIA
Romanian National Distribution Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

SLOVAKIA
Akadémia ozbrojených síl gen M.R. Štefánika, Distribučné a informačné stredisko STO
Demänová 393
031 06 Liptovský Mikuláš 6

SLOVENIA
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

SPAIN
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

TURKEY
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanliklar – Ankara

UNITED KINGDOM
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down, Salisbury SP4 0JQ

UNITED STATES
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

SALES AGENCIES

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
UNITED KINGDOM

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of STO, RTO and AGARD publications are given in "NTIS Publications Database" (http://www.ntis.gov).

ISBN 978-92-837-2155-0