NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(MSG-164)TP/1183

www.sto.nato.int

STO TECHNICAL REPORT **TR-MSG-164-Vol-I**

Modelling and Simulation as a Service (Phase 2)

(Modélisation et simulation en tant que service (phase 2))

Final report.

Published April 2024

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(MSG-164)TP/1183

www.sto.nato.int

STO TECHNICAL REPORT **TR-MSG-164-Vol-I**

Modelling and Simulation as a Service (Phase 2)

(Modélisation et simulation en tant que service (phase 2))

Final report.

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 April 2024

ISBN 978-92-837-2495-7

Table of Contents

List of Figures

List of Tables

List of Acronyms

ABB	Architecture Building Block
ACT	Allied Command Transformation
AMSP	Allied Modeling and Simulation Publication
AP	Architecture Pattern
API	Application Programming Interface
BM	Business Model
C2	Command and Control
C2IS	C2 Information System
C3	Consultation, Command, and Control
CA2X2	Computer Aided Analysis, Exercise, Experimentation
CAX	Computer Assisted Exercise
CJSE	Combined Joint Staff Exercise
COI	Community of Interest
CONEMP	Concept of Employment
COP	Common Operating Picture
COTS	Commercial Off The Shelf
CWIX	Coalition Warrior Interoperability Exercise
DIS	Distributed Interactive Simulation
DNK	Denmark
DSEEP	Distributed Simulation Engineering and Execution Process
EVAL	Evaluation Task Group
EVAL/EXP	Evaluation and Experimentation Task Groups
EXP	Experimentation Task Group
FMN	Federated Mission Networking
FOC	Final Operational Capability
FOM	Federation Object Model
GOV/OPS	Government and Operations Task Group
HLA	High Level Architecture
HTTPS	Hypertext Transfer Protocol Secure
I/ITSEC	Interservice/Industry Training, Simulation and Education Conference
iGeosit	Interim Geo-Spatial Intelligence Tool
IM	Information Model
IOC	Initial Operational Capability
KPI	Key Performance Indicator
M&S COE	Modelling and Simulation Center Of Excellence
M&S	Modelling and Simulation
MOE	Measure Of Effectiveness
MOP	Measure Of Performance
MSaaS	Modelling and Simulation as a Service

MSG	Modelling and Simulation Group
MTBF	Mean Time Between Failure
NAF	NATO Architecture Framework
NATO	North Atlantic Treaty Organization
NCIA	NATO Communications and Information Agency
NLD	Netherlands
NMSG	NATO Modelling and Simulation Group
OCD	Operational Concept Document
pRTI	Pitch Real Time Infrastructure
QoS	Quality of Service
RA	Reference Architecture
REST	Representational State Transfer
S&T	Science and Technology
SA	Situational Awareness
SDT	Service Description Template
SISO	Simulation Interoperability Standards Organization
SLA	Service Level Agreement
SMC	Service Management and Control
SME	Subject Matter Expert
STANAG	Standardization Agreement
STANREC	Standardization Recommendation
SWE	Sweden
T&E	Test and Evaluation
TAP	Technical Activity Proposal
TEK	Technical Task Group
TENA	Test and Training Enabling Architecture
TNO	Netherlands Organization for Applied Scientific Research
TRA	Technical Reference Architecture
TRL	Technology Readiness Level
UC	Use Case
US	United States
VPN	Virtual Private Network
WebLVC	Web Live Virtual Constructive

MSG-164 Membership List

CO-CHAIRS

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

Mr. Tom VAN DEN BERG
TNO
NETHERLANDS
Email: tom.vandenberg@tno.nl

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

Mr. Christopher MCGROARTY
US Army CCDC – DEVCOM SC
UNITED STATES
Email: christopher.j.mcgroarty.civ@army.mil

MEMBERS[1]

Mr. Boon-Hwa ANG
Defence Science and Technology Agency (DSTA)
SINGAPORE
Email: aboonhwa@dsta.gov.sg

Dr. Michael BERTSCHIK
Bundeswehr
GERMANY
Email: michaelbertschik@bundeswehr.org

LTC (OF4) Dr. Marco BIAGINI
ITA MoD
ITALY
Email: r5cscgc@sgd.difesa.it

Ms. Martina BINI
Leonardo S.p.A.
ITALY
Email: martina.bini@leonardocompany.com

Dr. Paolo BOCCIARELLI
University of Rome Tor Vergata
ITALY
Email: paolo.bocciarelli@uniroma2.it

Mr. Michiel BON
Dutch MoD
NETHERLANDS
Email: Netherlandsmf.bon@mindef.nl

Mr. Maxwell BRITTON
Department of Defence
AUSTRALIA
Email: alexburne@skymesh.com.au

Mr. Ahmet-Birol CAVDAR
HAVELSAN A.S.
TÜRKIYE
Email: abcavdar@havelsan.com.tr

Dr. Anthony CRAMP
Defence Science and Technology Group of the
Australian Department of Defence
AUSTRALIA
Email: anthony.cramp@defence.gov.au

Prof. Andrea D'AMBROGIO
University of Roma TorVergata
ITALY
Email: dambro@uniroma2.it

Mr. Marius DICKEBOHM
German Armed Forces
GERMANY
Email: Marius1Dickebohm@bundeswehr.org

Dr. Salvatore D'ONOFRIO
Leonardo S.p.A
ITALY
Email: salvatore.donofrio@leonardocompany.com

[1] MSG-164 attracted a large number of members. While some of them formed the core group and participated over the whole lifecycle of MSG-164, many subject matter experts and representatives of various communities of interest participated in specific meetings only. The membership list includes all members who participated in at least one meeting or contributed significantly to MSG-164 deliverables.

Mr. Efthimios DOUKLIAS
Joint Staff J6, Joint All-Domain Command and Control (JADC2)
UNITED STATES
Email: efthimios.d.douklias.civ@mail.mil

Ms. Katherine ESCOBAR
Joint Staff J6
UNITED STATES
Email: katherine.b.escobar.civ@mail.mil

Dr. Christian FAILLACE
Leonardo S.p.A
ITALY
Email: christian.faillace@leonardocompany.com

Mr. John FERRELL
Lockheed Martin
UNITED STATES
Email: john.ferrell@lmco.com

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

Mr. Brad FRIEDMAN
Army Futures Command
UNITED STATES
Email: brad.d.friedman.civ@army.mil

Mr. Scott GALLANT
Effective Applications Corporation
UNITED STATES
Email: scott@EffectiveApplications.com

Mr. Sabas GONZALEZ GODOY
NATO ACT
ACT – ALLIED COMMAND TRANSFORMATION
Email: Sabas.Gonzalez@act.nato.int

Mr. Yannick GUILLEMER
French Ministry of Armed Forces
FRANCE
Email: yannick.guillemer@intradef.gouv.fr

Mr. Douglas HENRY
Dstl
UNITED KINGDOM
Email: djhenry@dstl.gov.uk

Dr. Andre HOOGSTRATE
Ministry of Defense
NETHERLANDS
Email: aj.hoogstrate@mindef.nl

Mr. Tom HOUWELING
Defence Material Organisation (DMO)
NETHERLANDS
Email: tlj.houweling@mindef.nl

Mr. Willem HUISKAMP
TNO Defence Research
NETHERLANDS
Email: wim.huiskamp@tno.nl

Mr. John HUTT
US Air Force Agency for Modeling & Simulation (AFAMS)
UNITED STATES
Email: john.hutt@us.af.mil

Mr. Lars JANSSON
Swedish Defence Material Administration (FMV)
SWEDEN
Email: lars.jansson@fmv.se

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

Mr. James KEARSE
NSC Ltd
UNITED KINGDOM
Email: james.kearse@nsc.co.uk

Mr. Rob KEWLEY
simlytics.cloud LLC
UNITED STATES
Email: rob@simlytics.cloud

Mr. Gerardus KONIJN
Ministry of Defence
NETHERLANDS
Email: GA.Konijn@Mindef.nl

Mr. Niels KRARUP-HANSEN
MoD DALO
DENMARK
Email: niels@krarup-hansen.dk

Mr. Patrice LE LEYDOUR
Thales
NIAG-NATO INDUSTRIAL ADVISORY GROUP
Email: patrice.leleydour@thalesgroup.com

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

Mr. Björn LÖFSTRAND
Pitch Technologies AB
SWEDEN
Email: bjorn.lofstrand@pitchtechnologies.com

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

Dr. Giovanni MAGLIONE
NATO STO CENTRE FOR MARITIME RESEARCH AND EXPERIMENTATION
CMRE
Email: Giovanni.Maglione@cmre.nato.int

Mr. Benjamin MAGUIRE
Defence Science and Technology Group of the Australian Department of Defence
AUSTRALIA
Email: ben.maguire@defence.gov.au

Mr. Hans MULDER
Antwerp Management School
NETHERLANDS
Email: Hans.Mulder@ams.ac.be

Mr. Agatino MURSIA
Leonardo S.p.A
ITALY
Email: agatino.mursia@leonardo.com

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

Mr. Dirk OUDE EGBRINK
Royal Netherlands Aerospace Center NLR
NETHERLANDS
Email: dirk.oude.egbrink@nlr.nl

Mr. Bharatkumar PATEL
Dstl
UNITED KINGDOM
Email: bmpatel@dstl.gov.uk

Mr. Dominique PALABOST
CASPOA – NATO Air Operations Centre of Excellence
COE – Air Operations (CASPOA)
Email: dominique.palabost@intradef.gouv.fr

Mr. Robbie PHILLIPS
Lockheed Martin
UNITED STATES
Email: robbie.phillips@lmco.com

Mr. Marco PICOLLO
Leonardo S.p.A
ITALY
Email: marco.picollo@leonardocompany.com

Mr. Johnny POWERS
Lockheed Martin
UNITED STATES
Email: johnny.j.powers@lmco.com

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

Dr. Manfred ROZA
NLR – National Aerospace Laboratory
NETHERLANDS
Email: Manfred.Roza@nlr.nl

Mr. José RUIZ
DGA
FRANCE
Email: jose.ruiz@intradef.gouv.fr

Mr. Angel SAN JOSE MARTIN
ACT
ACT – ALLIED COMMAND TRANSFORMATION
Email: Angel.SanJoseMartin@act.nato.int

LTC (ret) Wolfhard SCHMIDT
ST Engineering Antycip SAS
UNITED KINGDOM
Email: Wolfhard.schmidt@steantycip.com

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

Mr. Chris STRUSELIS
ST Engineering Antycip
UNITED KINGDOM
Email: chris.struselis@steantycip.com

MAJ Rafal SUPLATOWICZ
NATO JFTC
JFTC – JOINT FORCES TRAINING CENTRE
Email: rafal.suplatowicz@jftc.nato.int

Mr. Chong-Lai TEO
Defence Science & Technology Agency
SINGAPORE
Email: tchongla@dsta.gov.sg

LTC Davide-Marco TRIMANI
Modelling and Simulation Centre of Excellence
COE – MODELLING AND SIMULATION (MS)
Email: mscoe.cde08@smd.difesa.it

Capt Pascal TRUCHON
Canadian Armed Forces
CANADA
Email: Pascal.Truchon@gmail.com

Mr. Andrew WARHURST
Department of Defence
AUSTRALIA
Email: Andrew.Warhurst2@dst.defence.gov.au

Modelling and Simulation as a Service (Phase 2)

(STO-TR-MSG-164-Vol-I)

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 holistic 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-164 ("Modelling and Simulation as a Service – Phase 2") developed 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:

- Allied Framework for M&S as a Service (MSaaS), Operational Concept Document (STO-TR-MSG-136-Part-III);
- Modelling and Simulation as a Service (MSaaS) Technical Reference Architecture (STO-TR-MSG-164-Vol-II);
- Business Model for the Allied Framework for M&S as a Service (MSaaS) (STO-TR-MSG-164-Vol-III);
- Allied Framework for M&S as a Service (MSaaS), Concept of Employment (AMSP-02).

MSG-164 evaluated key MSaaS concepts like Service Discovery and Service Management & Control in various experiments. The experimentation results and operational applications demonstrate that MSaaS is capable of realizing the vision that M&S products, data and processes are conveniently accessible to a large number of users whenever and wherever needed. MSG-164 has defined the cornerstones for implementing an open, interoperable MSaaS Ecosystem in NATO, where each participant is free to develop its own implementation while the common framework enables federated, potentially multi-national, MSaaS environments to satisfy the operational needs.

As many nations and NATO organizations are currently implementing MSaaS, MSG-164 strongly recommends that key documents, specifically the Concept of Employment and the Technical Reference Architecture, are formally published as NATO standards. To advance and to promote the operational

readiness of MSaaS, and to conduct required Science & Technology efforts to close current gaps, MSG-164 developed a Technical Activity Proposal (TAP) to address the next phase (MSG-195). It proposes an incremental development and implementation strategy for the Allied Framework for M&S as a Service that facilitates a smooth transition and offers a route that will incrementally build an Allied Framework for M&S as a Service.

Modélisation et simulation en tant que service (phase 2)

(STO-TR-MSG-164-Vol-I)

Synthèse

L'OTAN et les pays utilisent les environnements de simulation à différentes fins, telles que la formation, le développement des capacités, la répétition des missions 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. Les produits de M&S sont des ressources extrêmement précieuses ; il est essentiel que les produits, données et procédés de M&S soient commodément accessibles à un grand nombre d'utilisateurs aussi fréquemment que possible. Toutefois, l'interopérabilité entre 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 concept holistique 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 de la 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-164 de l'OTAN (« Modélisation et simulation en tant que service – Phase 2 ») a développé 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 suivants :

- Cadre allié de M&S en tant que service (MSaaS), document de définition opérationnelle (OCD) (STO-TR-MSG-136-Part-III) ;
- Architecture de référence technique de la modélisation et simulation en tant que service (MSaaS) (STO-TR-MSG-164-Vol-II) ;
- Modèle économique du cadre allié de M&S en tant que service (MSaaS) ; (STO-TR-MSG-164-Vol-III) ;
- Cadre allié de M&S en tant que service (MSaaS), concept d'emploi. (AMSP-02).

Le MSG-164 a évalué des concepts clés de MSaaS tels que la communication des services et la gestion et le contrôle des services dans le cadre de diverses expériences. Les résultats d'expérimentation et les applications opérationnelles démontrent que la MSaaS est capable de rendre les produits, données et processus de M&S commodément accessibles à un grand nombre d'utilisateurs, quels que soient l'endroit et le moment où le besoin s'en fait sentir. Le MSG-164 a établi les fondements de mise en œuvre d'un écosystème de MSaaS ouvert et interopérable au sein de l'OTAN, dans lequel chaque participant est libre de développer sa propre mise en œuvre, tandis que le cadre commun permet aux environnements de MSaaS fédérés, potentiellement multinationaux, de répondre aux besoins opérationnels.

Étant donné que de nombreux pays et organisations de l'OTAN mettent actuellement en œuvre la MSaaS, le MSG-164 recommande vivement que les documents essentiels, en particulier le concept d'emploi

et l'architecture technique de référence, soient officiellement publiés en tant que normes de l'OTAN. Afin de servir et promouvoir la préparation opérationnelle de la MSaaS et de mener les travaux requis en science et technologie pour combler les lacunes actuelles, le MSG-164 a élaboré une proposition d'activité technique (TAP) abordant la phase suivante (MSG-195). Il propose une stratégie progressive de développement et de mise en œuvre du cadre allié de M&S en tant que service qui facilite une transition en douceur et offre un parcours qui construira graduellement un cadre allié de M&S en tant que service.

MODELLING AND SIMULATION AS A SERVICE (PHASE 2)

1.0 INTRODUCTION

1.1 Background

Modelling and Simulation (M&S) is a critical capability for NATO that is used for various purposes, such as training, mission rehearsal, or decision support in acquisition processes. Efficiency in simulation use and flexible utilization of valuable simulation resources is a critical factor to sustain the asymmetrical advantage that simulation provides to NATO and its partners. It is essential that M&S products, data, and processes are conveniently accessible to a large number of users whenever and wherever required.

Yet, setting up simulation environments today still requires enormous effort with regards to time, personnel, and budget. Achieving interoperability between simulation systems and ensuring credibility of results are two key challenges that users currently face.

Recent developments in cloud computing technology and service-oriented architectures offer opportunities to address these NATO critical needs. Specifically, M&S as a Service (MSaaS) combines service orientation and the "as a service" delivery 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.

1.2 Objectives

Building upon the *Allied Framework for M&S as a Service* (as defined by MSG-136), MSG-164 addressed three main objectives:

1) To advance and promote the operational readiness of M&S as a Service;
2) To align national efforts and share national experiences in establishing MSaaS capabilities;
3) To investigate critical research and development topics to further enhance MSaaS benefits.

This activity continued MSaaS experimentation and evaluation efforts to validate initial concepts and generate evidence for the benefits of MSaaS.

Specific recommendations were identified in the MSG-136 Final Report, based on observations and formal feedback. Appendix 1 identifies the scope of these recommendations addressed by MSG-164.

1.3 MSaaS Vision and MSG-164 General Approach

The MSaaS Vision Statement is defined as: [1].

> *M&S products, data and processes are conveniently accessible and available on-demand to all users in order to enhance operational effectiveness.*

The combination of service-based approaches (i.e., M&S services) with ideas taken from cloud computing is known as "Modelling and Simulation as a Service" (MSaaS). This document uses the following definition:

> *M&S as a Service (MSaaS) is an enterprise-level approach for discovery, composition, execution and management of M&S services.*

Enterprise level refers to the fact that MSaaS satisfies the needs of a broader community rather than individual service consumers. This definition stresses the fact that MSaaS is not only a technical solution, but also includes organizational aspects on the enterprise level (e.g., overarching management, governance, funding and oversight).

The Allied Framework for MSaaS is a reference architecture providing a common approach in the NATO coalition towards a **federated MSaaS Ecosystem**, consisting of national and NATO MSaaS implementations, and underpinned by a common technical reference architecture, common processes and a common business model. Figure 1 shows the high-level overview of the Allied Framework for MSaaS depicting a variety of suppliers and providers offering services that may be used by a large number of users.

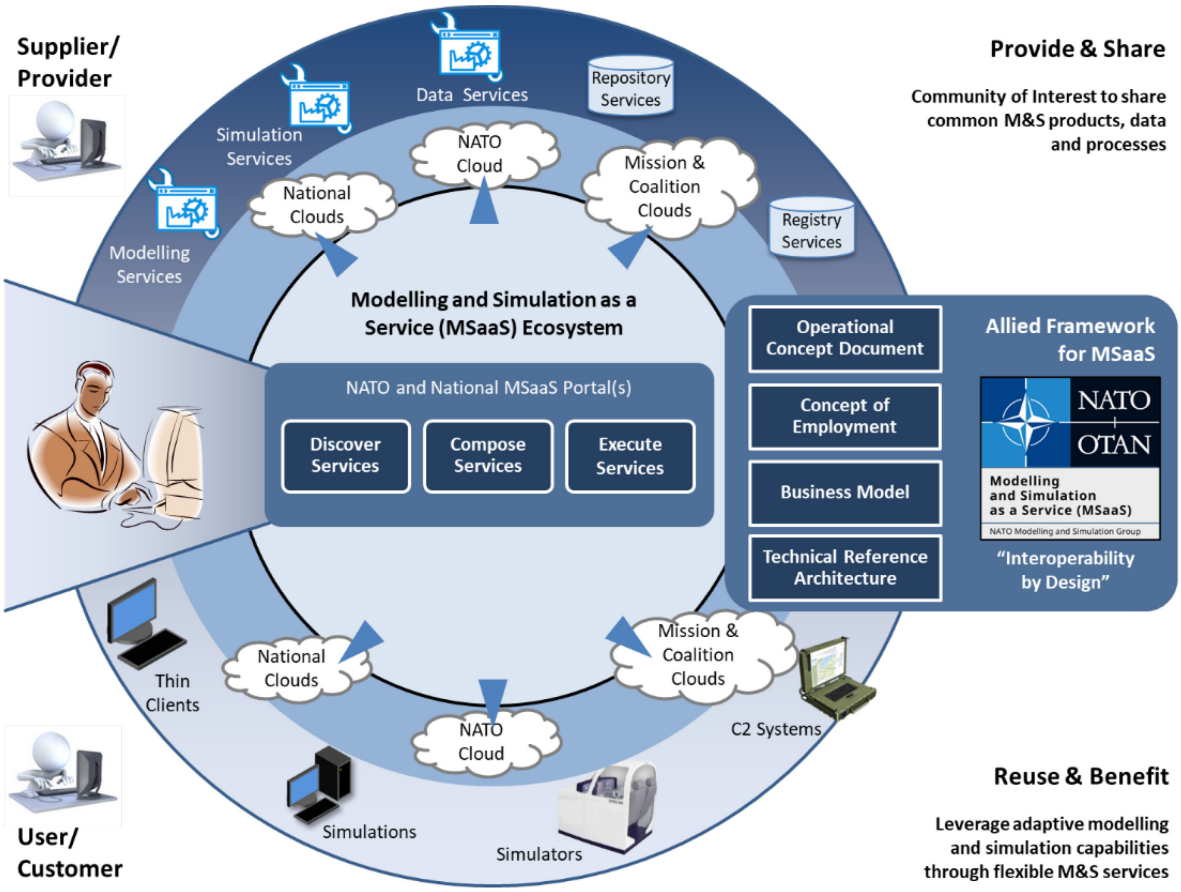

Figure 1: Allied Framework for MSaaS.

To allow easy sharing and to enable broad adoption, key aspects of the Allied Framework for MSaaS are provided as separate documents. In total, the Allied Framework for MSaaS is defined by the following documents (see also Figure 1):

1) **Operational Concept Document (OCD):** The OCD describes the general vision and concepts of MSaaS, the intended use, key capabilities and desired effects of the Allied Framework for MSaaS from a user's perspective [2].
2) **Concept of Employment (CONEMP):** The CONEMP identifies MSaaS stakeholders, their relationships and provides guidance for implementing and maintaining the Allied Framework for MSaaS as a persistent capability [3].

3) **Business Model (BM):** The BM describes how MSaaS will manage and enable the intended use, key capabilities and desired effects of the Allied Framework for MSaaS from a stakeholder's perspective in the multi-government business space [4].

4) **Technical Reference Architecture (TRA):** The TRA describes the architectural building blocks and patterns for realizing MSaaS capabilities [5].

The MSaaS CONEMP and the MSaaS TRA will be published as Allied Modelling and Simulation Publications (AMSPs) and will be covered by a NATO Standardization Recommendation (STANREC).

1.4 Team Structure

To address the technical and organizational topics as well as the associated experimentation and evaluation efforts, MSG-164 established four dedicated subgroups as illustrated in Figure 2.

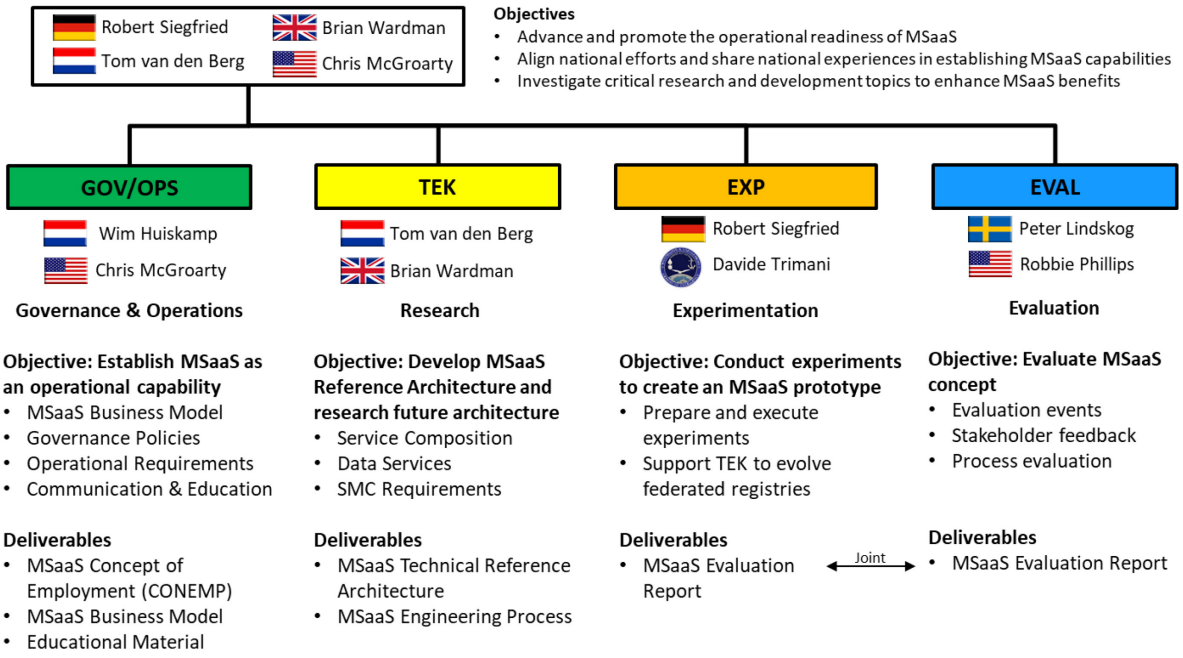

Figure 2: MSG-164 Internal Organization.

The MSG-164 GOV/OPS subgroup was responsible for all topics related to MSaaS governance and operations. Key deliverables of the GOV/OPS subgroup are the MSaaS Concept of Employment (CONEMP) and the MSaaS Business Model. Additionally, the GOV/OPS subgroup maintained the MSG-164 Communications Plan and provided educational material for various outreach activities. In this role, the GOV/OPS subgroup acted as the liaison to MSG-168 (MSaaS Lecture Series).

The MSG-164 TEK subgroup was responsible for architectural and technical aspects of MSaaS. Based on the operational requirements the TEK subgroup evolved the technical reference architecture and engineering process for MSaaS, investigated service discovery, and conducted several experiments to test and validate solutions for architecture building blocks defined in the reference architecture. The TEK subgroup was actively reaching out to the wider community of interest to learn about related technologies and approaches, as well as to educate the community about their ongoing technical efforts.

The MSG-164 EXP/EVAL subgroup was responsible for continuous evaluation and concept verification. Initially started as two separate teams, the overlap in activities and participants led to a de facto merger into a combined EXP/EVAL subgroup. Jointly with the TEK subgroup, the EXP/EVAL group prepared various technical experiments and demonstrations to validate key aspects of the MSaaS TRA and collect evidence on the usefulness and benefits of MSaaS. The EXP/EVAL subgroup also acted as internal quality assurance group (are we doing the right things?) and collected external feedback from various communities of interests and stakeholders to ensure the appropriateness of the work of MSG-164.

2.0 MSaaS FROM A BUSINESS PERSPECTIVE

2.1 Overview

Defence currently cannot respond effectively to the growing need for Modelling and Simulation (M&S) or synthetic environments. The full value of M&S is only realized when they are rapidly accessed and used across domains, across government and with allies, to meet the demands of a fast-changing defence operating environment and the complexity of full spectrum of adversarial and defensive effects. In an increasingly complex, competitive and connected world, the defence and security Forces will need to be highly prepared and ready, and to rapidly make the right decision during operations.

To realize that full value, an Allied Framework for M&S as a Service or MSaaS Ecosystem, based on similar commercial ecosystems, is proposed to supply a sustainable on-line on-demand service at the point of need. It was recognized in this phase that the business aspects of the underpinning demand-supply marketplace needed to be addressed. This was done through developing a Business Model to change towards the Ecosystem, which also required an update of the Concept of Employment (CONEMP).

Below are summaries of the MSaaS Business Model, which defines the relationships between the various stakeholders and lays out the concepts for establishing a sustainable and vital MSaaS Ecosystem. This is followed by a summary of the MSaaS CONEMP.

2.2 Business Model

The MSaaS Business Model is an integral part of the MSaaS Concept of Employment and is essential to sustain an M&S ecosystem. The Business Model describes how MSaaS will manage and enable the intended use, key capabilities and desired effects of the Allied Framework for M&S as a Service from a user's perspective. The Business Model was developed in the current phase of MSaaS approach under the MSG-164 Task Group, and the detailed version is available in Ref. [4].

2.2.1 MSaaS Ecosystem

The MSaaS Ecosystem is essentially the defence and dual civilian-military marketplace characterized by customers demanding M&S services to their user applications (e.g., training, decision support, mission planning, capability development) balanced by suppliers or providers meeting that demand. The ecosystem may provide infrastructure, platform and software as services to support the applications.

2.2.2 Business Model Canvas

The purpose of the Business Model (BM) for the Allied Framework for M&S as a Service (MSaaS) is to inform relevant stakeholders how the MSaaS will operate in the multi-government business space for the sharing of M&S technologies. The Business Model Canvas is a strategic management template for developing new or documenting existing business models. It is a visual chart with elements that describe the organization's value proposition, infrastructure, customers, and finances. It assists organizations in aligning their activities by illustrating potential trade-offs. Figure 3 shows the visual chart. It shows typical defence and security perspectives that are being currently considered for the MSaaS BM.

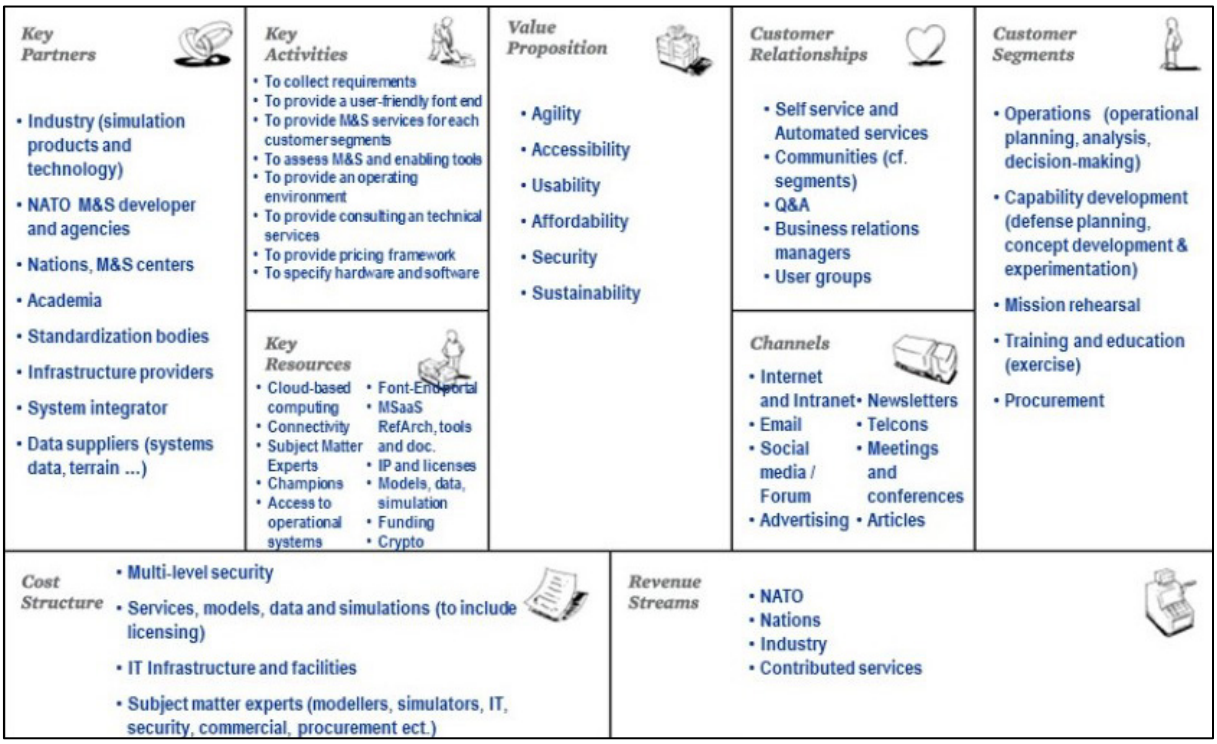

Figure 3: MSaaS Business Model Canvas.

2.2.3 Business Model Stakeholder Relationships

The MSaaS concept requires negotiation and interactions between Customers, Suppliers, Service Providers and Users. Figure 4 shows the interactions between the stakeholders.

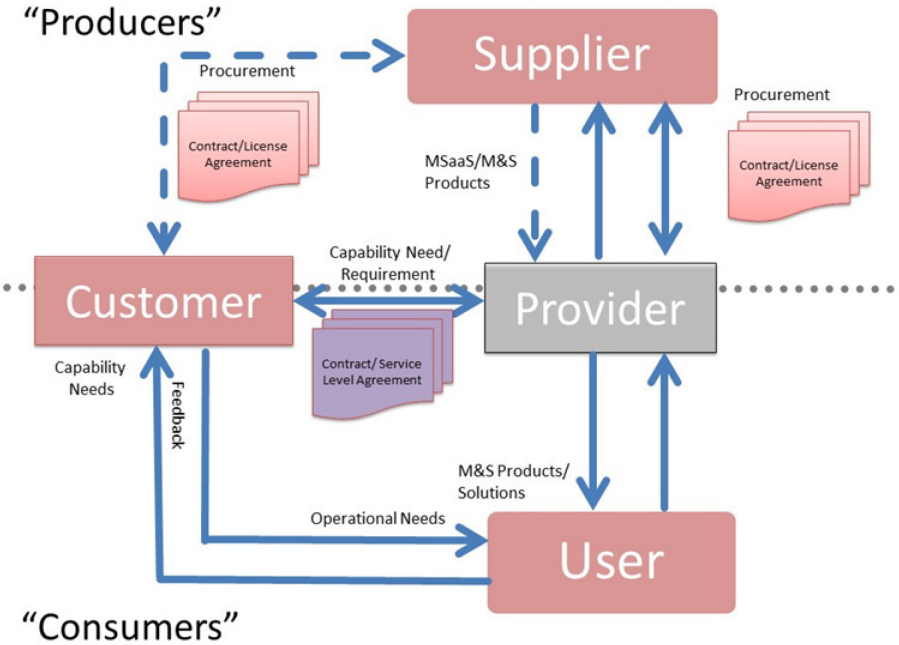

Figure 4: Stakeholders and Interactions.

The Customer will define the operational needs. The User will assist the Customer by capturing the capability needs and breaking these down in technical requirements.

The Customer negotiates and secures MSaaS capabilities from a Provider typically via a Service Level Agreement (SLA), or via an on-line contract or license agreement. The Customer also captures User feedback on performance and functionality as part of verifying and validating M&S products and services.

Service Providers will engage with Suppliers to acquire and integrate M&S products in accordance with SLAs agreed with Customers. The resultant products and services will then be made available for composing services to Users who have been verified for access. Providers will engage with Users and Customers to capture any feedback on the deployment, integration and execution of M&S products and services, and where relevant provide information back to Suppliers.

The User defines the capability needs to the Customer and will consume M&S products and services in accordance with the SLA between the Customer and the Service Provider. The User shall also inform the Customer on performance and functionality so that the Customer and Provider together can verify and validate M&S products and services.

The Supplier will respond to requests from service Providers and Customers for the provision of M&S products and services. Any subsequent delivery of M&S products and services will require a contract or license agreement between the Supplier and Service Provider/Customer. The Supplier will capture feedback from the Service Provider on delivered M&S products and services.

2.2.4 Procurement Considerations

The MSaaS approach will need acceptance of a new way for defence to meet users M&S requirements. It moves away from traditional development cycles and contracting procedures but will still maintain the need for value for money. An M&S Ecosystem driven by MSaaS, modelled around commercial app-based ecosystems, would provide greater choices of models and simulations, foster competition as well as collaboration amongst the ecosystem stakeholders, and tools to discover, compose, and execute efficiently and securely the required model, simulation or synthetic environment.

2.2.5 Acquisition of Services

The acquisition of M&S services will need to address different types of licensing and payment methods. This would include modern ecosystem mechanisms that provide on-line on-demand methods of delivery and payment such as:

- App store, including micro-payments: The As-you-go consumption-based payments will make the funding of the NATO MSaaS somewhat different than the traditional government contract.
- Pay per use: the transfer of funds from the end consumers within the MSaaS community to the NATO managing body will need to be well defined, since a micro-payment for “service” usage will be more appropriate to meet the demands of more frequent and flexible transactions take place between the provider, supplier, and consumer in relation to provisioning and accepting “services”.
- Open source, possibly with contributions in kind (e.g., additional functionality added by users).
- Subscription: to meet the warfighters’ needs for services on demand, a phased approach is recommended to fund the establishment through a subscription model.
- On-line contracting.

There will need to be support services that track and manage licensing as well as legal services to ensure compliance with operating in such a manner, e.g., Data Protection Laws. Many of these services are not new in the everyday commercial world. Initially, suppliers or providers may need to port legacy defence M&S capability into MSaaS if such models do not exist in the ecosystem. The delivery options for the required M&S services will also need to accommodate local restrictions (e.g., security of physical assets), distributed (e.g., to address team, joint or coalition requirement), or a mix of the two (hybrid).

2.2.6 Typical Governance Approach

The MSaaS Provider needs to manage and maintain a core set of services in order to meet SLAs. This will include the use of registry and discovery services to maintain visibility and availability of M&S products, either already owned by defence organizations or available from Suppliers through a license agreement, purchase order, another kind of a legal contract or agreement. The governance approach will need to include:

- Lifecycle management of services and apps.
- Configuration and change management.
- Risk and incident Management.
- Compliance and governance.
- Data management.
- Business continuity and disaster recovery plans.

2.2.7 Security

Access, commercial and defence security will be essential to the success of taking an MSaaS Ecosystem approach. This will include but not limited to:

- User management.
- Single sign-on and authentication.
- Accreditation, licensing and IP protection.
- Data and cyber security management.

The use of enablers such as cloud computing, smart communications (e.g., 5G), autonomy, etc. is not unique to MSaaS, as many other defence capabilities are looking to leverage these commercial-sector technologies.

2.2.8 Improvements and Benefits

Implementing an MSaaS Ecosystem will result in various benefits and improvements for the different stakeholders. The MSaaS Business Model is designed to:

- Increase operational effectiveness by streamlining processes, greater access of M&S services from remote locations, and increased efficiency and productivity for defence applications, and improved quality.
- Increase efficiency by reduced manpower requirements, reduced reliance on SMEs and available expertise: Increased reuse opportunities, reduced duplication of effort, reduced cost of ownership, single point of access to M&S services, provisioning of M&S resources during runtime, leverage benefits of cloud computing.

2.2.9 Implementation Risks

Stakeholders that will implement the proposed concept into their organizations will also face risks and some major challenges. The following general (i.e., not defence-specific) risks associated with service-based M&S approaches have been identified as:

- Managing security, privacy, accountability, risk and trust become more complex.
- Advanced aspects of composability of M&S services are still maturing.
- Dependency on network connections makes M&S applications vulnerable to network effects.
- Adapting legacy M&S applications with a service interface or for hosting in the cloud may be complex and/or costly.
- Updated composed simulation for another use may reduce validation of original use case.

In addition to these general risks, there are also several (perceived) defence-specific risks:

- Dependency on remote infrastructure and services increases vulnerability in front-line/combat situations which may reduce benefits as local fallback options or backup systems must still be maintained.
- Validation of specific services may be more difficult when they are more remote and internal operation is shielded to a large degree.
- Unwillingness of nations/companies to share resources.
- Unwillingness of defence companies to move to ecosystem procurement models.
- Vendor (e.g., cloud provider) lock-in.

2.3 Concept of Employment

The Concept of Employment for the Allied Framework for MSaaS is defined in an Allied Modelling and Simulation Publication (AMSP-02) [3]. The Concept of Employment (CONEMP) is a guideline for NATO and (multi)-national MSaaS implementations that establishes the concept of employment, identifying MSaaS stakeholders and their relationships, describing or referencing operating procedures and business model, and provides guidance and technical references for implementing and maintaining the Allied Framework for MSaaS as a persistent capability.

The operating procedures and technical references in the publication are recommended by the NMSG to promote M&S service sharing and interoperability between MSaaS implementations. These operating procedures and technical references are not formally mandated by NATO, unless supported by a specific NATO Standardization Agreement (STANAG). The AMSP-02 will be covered by a Standardization Recommendation (STANREC).

The operating procedures and technical references specified in the publication should be applied to all current and prospective MSaaS-enabled implementation programs and efforts in NATO and Nations.

2.3.1 Implementation

The Allied Framework for MSaaS defines the blueprint for stakeholders to implement MSaaS. The specific solution architecture of MSaaS may be different for each implementation:

- “An MSaaS Implementation is the specific realization of M&S as a Service by a certain stakeholder. An MSaaS Implementation includes both technical and organizational aspects.”
- “An MSaaS Solution Architecture is the architecture of a specific MSaaS implementation and is derived from the Operational Concept Document and the Technical Reference Architecture.”

MSaaS documents, data and tools should be managed through an MSaaS Portal as outlined in the MSaaS Operational Concept Document and with the capabilities described in the MSaaS Technical Reference Architecture [5]. This will include dissemination of documents, services, datasets (e.g., databases, imagery) and tools (e.g., federate compliance testing tools), dealing with feedback, implementation issues, etc. that are addressed in updates and maintenance activities.

2.3.2 Stakeholders

The stakeholders in MSaaS are defined by their roles as described by the MSaaS Operational Concept Description (OCD) [2] and based on their MSaaS business and operational needs and interactions (see Figure 4 in Section 2.2.3). At the top level, the stakeholders can be classified as Service Producers and Service Consumers. These two categories can be further divided into respectively, Suppliers / Providers and Customers / Users.

2.3.3 Polices

The general policies for MSaaS implementation compliance are defined in AMSP-02. Each policy has a unique identifier to avoid any ambiguity. The general polices are:

- **[GEN-01]** An MSaaS implementation SHALL conform to the principles and policies as identified and established in the NATO M&S Master Plan.
- **[GEN-02]** An MSaaS implementation SHALL be aligned with the NATO M&S Standards Profile AMSP-01. The AMSP-01 includes recommended M&S standards and STANAGs/STANRECs.
- **[GEN-03]** An MSaaS implementation SHALL conform to the practices, architectural principles, and operating procedures as identified and established by this document.
- **[GEN-04]** An MSaaS solution architecture SHALL comply with the MSaaS Technical Reference Architecture. This includes access to the services through a Portal (or a federation of Portals) and support for a federated MSaaS Ecosystem with other solution architectures.
- **[GEN-056]** Any M&S service from a NATO MSaaS implementation that is provided or consumed by a NATO body, Nation or Organization SHOULD comply with the policies defined in this document as formalized by its related STANREC.
- **[GEN-067]** The federated MSaaS Ecosystem SHALL have a NATO MSaaS Portal provided by a NATO assigned organization.

These policies are further elaborated in the publication in terms of:

- **Organizational policies** – governing service identification, service level agreement, service description and business model.
- **Technical policies** – governing the architecture, infrastructure, platform, software and tools.
- **Security polices** – governing the safeguard of all MSaaS stakeholders (Suppliers, Providers, Customers, and Users) by employing a secure environment, for their services, data, account information and Personally Identifiable Information (PII).

3.0 MSaaS FROM A TECHNICAL PERSPECTIVE

The objective of the MSaaS Technical Reference Architecture (TRA) [5] is to provide a source of reference and direction regarding the implementation of an MSaaS Capability. More specifically:

- Provide principles that serve as general rules and guidelines in applying the Technical Reference Architecture;

- Provide requirements and standards in the form of building blocks and patterns for realizing an MSaaS Capability;
- Provide a structure that can be used to identify areas where further technology and requirements development should take place, and that can be expanded over time with new or refined building blocks and patterns.

The TRA is described in a separate document addressing the following topics, organized in three parts:

Part 1: Principles and Concepts:

- **Architecture Principles**. Principles govern the process of developing the TRA, and affect the development, maintenance, and implementation of the TRA.
- **MSaaS Architecture Framework**. Introduces the architecture concepts that are used throughout the description of the TRA. This concerns types of architecture, architecture building blocks, architecture patterns, and solution building blocks.
- **MSaaS Capability**. Introduces the term MSaaS Capability and describes the vision of MSaaS within NATO context to establish an MSaaS Ecosystem, supported by federated MSaaS Capabilities from different nations.

Part 2: Operational Capabilities:

- **Use Cases**. Use cases describe how each organization interacts with the MSaaS Capability. The use cases provide a context for the technical building blocks for the TRA.
- **MSaaS Engineering Process**. This process is a reference process for the engineering and execution of services and compositions, applicable to both the Supplier and Provider. The process complements the use cases with the technical activities that each of these organizations should consider when supplying M&S Services to and providing M&S Services from an MSaaS Implementation.

Part 3: Technical Capabilities:

- **User-Facing Capabilities.** The MSaaS User-Facing Capabilities are formed by the M&S Portal Applications and the M&S User Applications. These are front-end capabilities within an MSaaS Capability that users interact with, hence are called “User-Facing”.
- **Back-End Capabilities**. Back-end capabilities within an MSaaS Capability encompass several building blocks to serve the front-end User-Facing Capabilities. The back-end capabilities are divided into M&S Enabling Services and Simulation Services, where the former enable the latter to function within an MSaaS Capability. Examples of enabling services are M&S Repository Services and Simulation Control Services.
- **Communications and Information Systems (CIS) Security**. CIS Security is a cross-cutting concern that affects all layers of the architecture, both operational and technical. The focus in the TRA is on MSaaS specific security issues.
- **Service Management and Control (SMC)**. SMC is a collection of capabilities to coherently manage components within an MSaaS Capability and across federated MSaaS Capabilities. This is a cross-cutting concern that affects both operational and technical capabilities.
- **Federating MSaaS Capabilities**. MSaaS Capabilities can be federated with the aim to share M&S Resource Metadata, share M&S Resources, and seamlessly use Simulation Services across the federation.

The TRA is aligned with the NATO C3 Taxonomy (summarized in Figure 5) which also outlines the structure of the TRA document itself.

The high-level relationships between the clusters of building blocks of an MSaaS Capability as illustrated in Figure 5:

- M&S Portal Applications, Communications and Information Systems Security, and Service Management and Control *support* the MSaaS Engineering Process;
- Communications and Information Systems Security, and Service Management and Control *manage and control*, and *enforce security* on the M&S User Applications and Simulation Services deployed within an MSaaS Capability;
- Simulation Services serve the M&S User Applications;
- M&S Enabling Services serve the M&S Portal Applications; and
- Core Services *provide technical functionality* for the Services and Applications to execute.

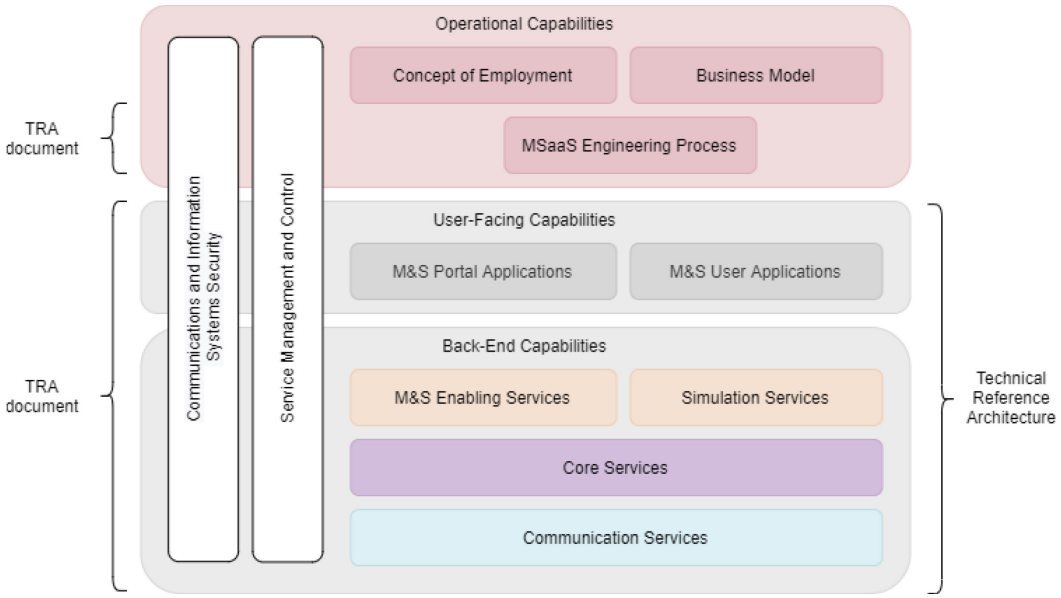

Figure 5: MSaaS Capability: Architecture Building Blocks Clustering.

4.0 MSaaS EXPERIMENTATION AND EVALUATION

4.1 Overview

This section provides the results of the evaluation activities performed by MSG-164. This includes lessons identified, analysis, and considerations based on evaluation of the work products and experiments. The objective is to provide clear recommendations to NATO, Allied Nations, ACT, industry, and any follow-on working groups.

The MSaaS Concept of Employment (CONEMP) states that "M&S as a Service (MSaaS) is an enterprise-level approach for discovery, composition, execution and management of M&S services" [3]. Furthermore, the MSaaS Operational Concept Document (OCD) defines effect goals for MSaaS [2] which were used to structure the test campaign and to relate test results to MSaaS goals. MSG-164 conducted an experimentation campaign designed to:

- Support the evaluation of readiness of the MSaaS concept.
- Test the maturity of Modelling and Simulation as a Service (MSaaS) technologies and processes.
- Collect information about their maturity and suitability.

In addition, the experiment provided experience, insights, and feedback related to ongoing MSG-164 research and development of technical and operational MSaaS standards and concepts of employment.

4.2 Experimentation

Each experiment activity focused on specific aspects of MSaaS. The overall experiment focus was on the delivery of distributed modelling and simulation capabilities provided as a service from a NATO MSaaS Provider and MSaaS Ecosystem to a national consumer of these services. It is important to note that the experiment was not intended to test or evaluate existing implementations of MSaaS services. Instead, the main focus was to test MSaaS concepts, ideas, and approaches.

The experimentation approach was based on the Distributed Simulation Engineering and Execution Process (DSEEP) and specifically on steps in the DSEEP related to MSaaS Core Services to support Discovery, Composition, Execution and Management, see Figure 6. In each step of the DSEEP process, information was generated based on NATO Architectural Framework (NAF) views to capture input required to perform Discovery, Composition and Execution experimentation activities.

As a driver for the experiment, operational requirements were used, based on the Swedish CAX platform and its needs to support the exercise Viking 22. In this use case, the NATO M&S COE acts as the Service Provider and the Swedish Armed Forces as the consumer of NATO MSaaS services. The implementations of these NATO MSaaS services are, in turn, based on software and services available from a NATO-wide MSaaS Ecosystem where different suppliers contribute individual MSaaS Capabilities. A number of development, test and demonstration events also acted as drivers for developing an MSaaS prototype system based on the identified needs, see Figure 7.

It is important to note that the Swedish CAX platform to support the Viking 22 exercise will not be dependent on the existence of NATO provided MSaaS services and an MSaaS prototype (Figure 8).

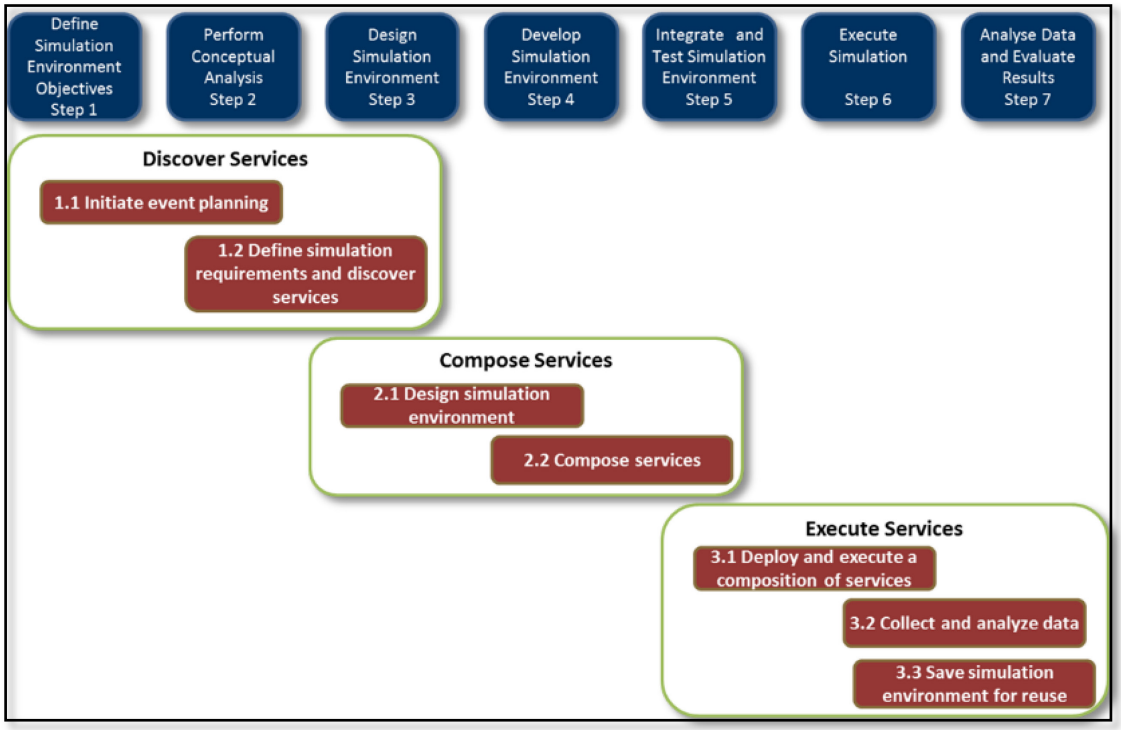

Figure 6: Distributed Simulation Engineering and Execution Process and MSaaS Core Services.

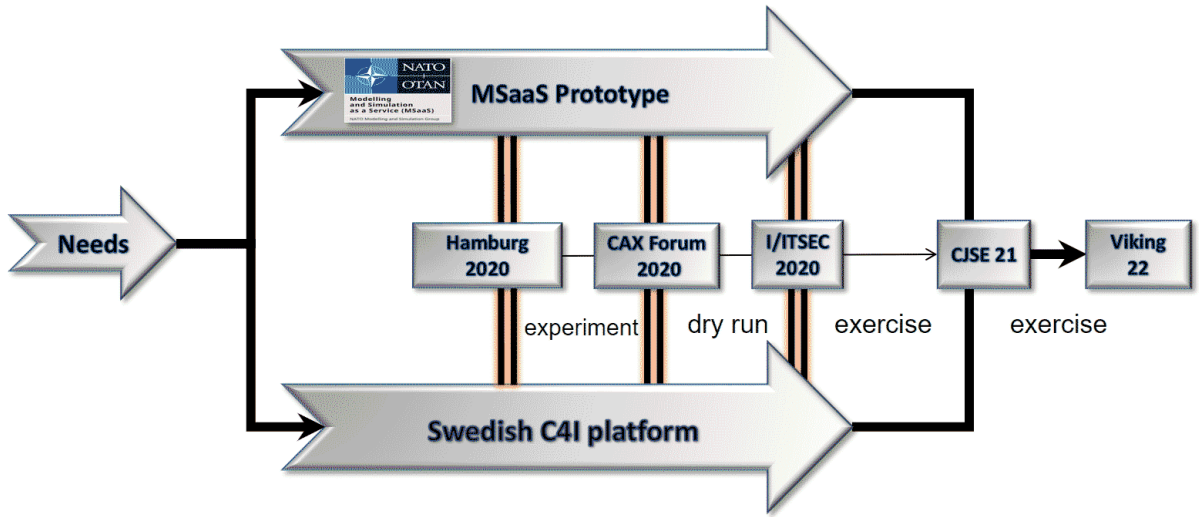

Figure 7: NATO MSaaS Used to Augment the Swedish CAX Platform with NATO Services to Support Real Exercise.

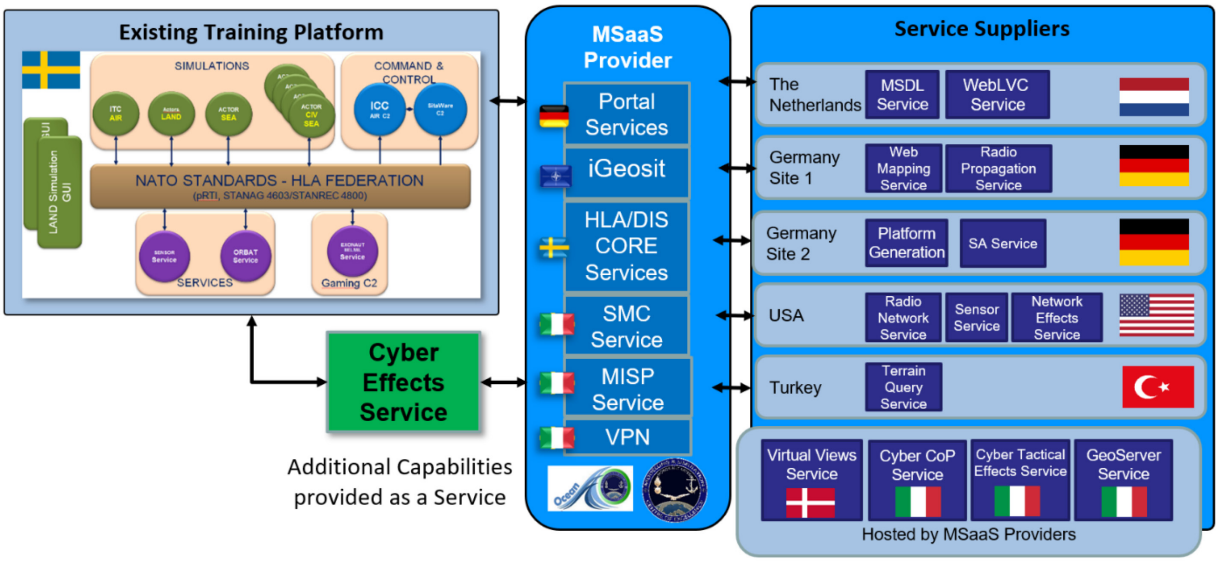

Figure 8: Test Environment for MSG-164 during 2019 – 2020.

The following seven experimentation related activities were conducted, evaluated and have been summarized in this report:

1) Needs Analysis and Conceptual Modelling (Q1 2019).
2) Discovery Experiment Event (Stockholm 3 – 4 June 2019).
3) System Design and Composition (Q2 – Q3 2019).
4) Integration and Deployment (Q4 2019 – Q2 2020).
5) Execution (CA2X2 Forum Demo, September 2020).
6) SLA Table-Top Event (17 – 18 February 2020).
7) US Army M&S Gap Forum Demo (Jan 2021).

4.3 Lessons Identified

The main purpose of MSG-164 experimentation activities was to identify lessons related to the MSaaS goals. Based on these lessons, recommendations for additional MSaaS research and standards development can be made.

As the MSaaS concept and supporting services for discovery, composition and execution are still under development, the readiness level and maturity of tools that implement MSaaS Core Services are limited. Some lessons identified have already been taken into consideration in the MSG-164 TEK and OPS/GOV subgroup work.

4.3.1 General Lessons Identified

Any evaluation of MSaaS effect goals, based on the experimentation results, must carefully consider current state and conditions of the MSaaS implementation in order not to draw wrong conclusions.

- Different understanding of the process, roles and operational concept of using MSaaS in all steps from user needs, via service discovery and composition, to the execution of a simulation.
- Need for a clear definition of what it means if a service is considered MSaaS compliant.
- Need for a common understanding and use of MSaaS terminology, concepts, roles, relationships, etc.
- Need to include cyber security aspects, to a greater extent, in experimentation and reuse Federated Mission Networking (FMN) agreed profiles for security and Service Management and Control (SMC). The success of MSaaS depends on nations being able to accredit simulation and training systems for using NATO MSaaS services.
- Need to focus more on MSaaS Core Services (such as repository and composition services, and service management and control services; see [5] for more). MSG-164 to put more emphasis on testing specific service implementations rather than MSaaS Core Services, due to current availability and maturity reasons. Figure 9 identifies these two separate focus areas, of which MSG-164 concentrated predominantly on MSaaS M&S Services and less on MSaaS Core Services.

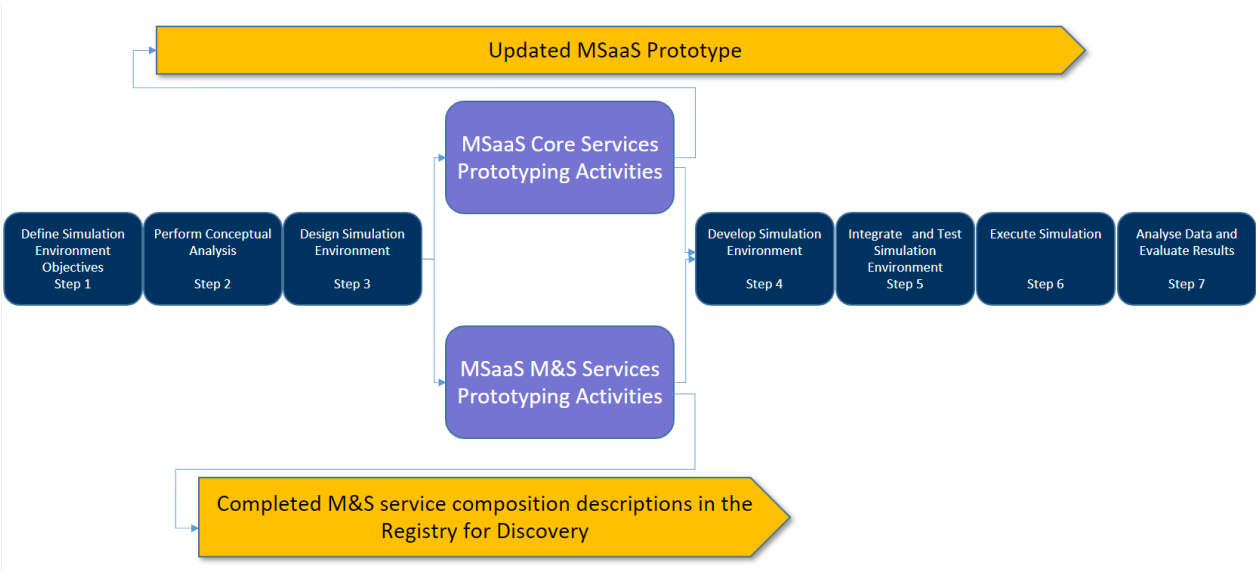

Figure 9: MSaaS Core Services and Prototype Focus vs. Focus on Specific M&S Services Implementations.

4.3.2 Discovery Lessons Identified

The discovery experiment was primarily designed to collect evidence and feedback on the maturity of the Service Description Template (SDT) and its use for describing services. Service descriptions were available from a prototype MSaaS Discovery Service Portal. As input to the service discovery experiment, a set of NAF views developed by the Swedish Armed Forces were used. The content of the registry during the discovery experiment was not from a service provider perspective. The content was limited to software descriptions provided by software suppliers.

- The use of NAF and DSEEP when developing conceptual model and functional requirements provided a structured approach for capturing relevant information elements as the basis for discovery. It was recognized that some additional structure or guidance from an MSaaS discovery/composition perspective would be useful, such as a NAF specific MSaaS profile.
- Need for a classification of services and applications based on a standard ontology and taxonomy, e.g., based on the NATO C3 Taxonomy. Tagging services using a standard classification will allow the user to identify and compare services and compositions that previously and/or potentially fit together and with the user's identified needs and requirements.
- Need for independent third-party assessment of the compliance of a service implementation. This may include an assessment of the self-certification of compliance with respect to MSaaS interfaces and other measures of performance with focus on usability.
- Need the MSaaS Capability to support the verification of service description data is in accordance with the Service Description Template, and that any required supporting documents such as certificates of conformance or configuration information are also present.
- Need for a standard for interoperability between distributed service discovery repositories.
- Need a common definition of a service, and if the service description is describing services or software, and likewise whether the service registry is a registry of services or a repository of software.
- Need to investigate if existing NATO service registries can be used, such as the NCIA Community of Interest (COI) Cooperation portal.

4.3.3 Composition Lessons Identified

Distributed service-oriented M&S environments are developed to represent real-world systems and the natural environment. Composed services are required to interoperate in order to achieve a validated model of the simulated world. When selecting and composing services, it is essential that the simulation environment design meets the simulation requirements.

During the experimentation activities a federation design was developed using NAF views and diagrams to identify individual services, composed services and their interfaces.

- No specific MSaaS tools were used, and a traditional federation agreement was developed manually to support the MSaaS prototype demonstrated at CA2X2 Forum.
- For the purposes of the experiment, the validity and usability of composed services could not be assessed as there were no simulation requirements or composition tools available. This is because the service composition approach used is mainly concerned with the matchmaking of interfaces and functionalities. Selecting and composing services requires a careful design to ensure valid composition that can be used and trusted in a simulation.
    - Manually selecting services is a time-consuming activity and requires professional domain knowledge. Selecting and composing services is currently still a challenge given the lack of MSaaS tools available to support these activities. The complexity of this activity will also grow exponentially as the number of services increases.

    - Quality of Service (QoS) of the composed service depends on the design and QoS of each participating service. Determining QoS of a composed service is a complex task and currently not addressed specifically.

- In MSG-164, the service focus has been on business-to-business data exchange where traditional Web Service composition has undoubtedly become the most promising way to integrate applications. However, in simulation when services are used to collectively represent the real-world (a model of the business), additional mechanisms to ensure the validity of the simulation are required. Using a mix of technologies and standards (e.g., HLA/DIS, HTTPS, web sockets) increases the complexity of composing a valid simulation service.
- Service configuration and parameterization available to the end user is important. Some MSG-164 experiment services provided some level of configuration through the use of Kubernetes (Rancher), but most services required SMEs and support from suppliers and service providers. A self-service capability to configure and test services is important.
- It was not possible to evaluate any effects of using MSaaS compared with the traditional integration approach. This was mainly due to the fact that the tools and environments used were either under new development and/or were not "MSaaS compliant" or ready yet. Effort was spent on implementing agreements and standards in new services, and no accurate measures could be collected for evaluation of on-demand, rapid integration of existing services, and access to these services.
- Selection of individual services and composition did not use an MSaaS Portal. There is currently a lack of information on the discovery portal related to service composition, and no compositions used in the experiments have been adequately described for assessment.
    - The NATO MSaaS Portal prototype contained no information of service compositions from NATO Service Provider, only information from Service Suppliers.
    - No assessment was made based on the different types of MSaaS Portal users.
- No SLA information was provided to support selection of service during design. This caused the roles and responsibilities between the stakeholders to be less clearly defined and expectations of service provisioning were not fully agreed.
- The compositions developed for the CA2X2 Forum demonstration are not described as a composition in the MSaaS Portal and it is not obvious how to reuse the composition on demand without performing the same integration work again.
- Lack of MSaaS core service with respect to SMC. Standards and governance processes were not established for managing credentials to access services in providers hosting environments such as Kubernetes or Rancher to start/stop/control services.
- The Business Model addresses key challenges of acquisition of services, for use with operational systems and exercises. Existing processes for acquisition, accreditation and authorization of changes to existing systems were not adapted to the concept of MSaaS, or currently need to be adapted by individual nations.
- Collaboration tools to support integration were not available on the MSaaS environment using VPN. e.g., teleconferencing systems, sandbox environment for testing, issue tracking, etc.
- The cost of local implementations for service composition and execution was not estimated. Organizations across NATO are going to have different management practices for implementing MSaaS. In turn, there may be costs to develop new user interfaces, invest in infrastructure and maintenance, and to provide local administration of MSaaS.

Test plans for individual services were developed and each service was tested before integration. There was a lack of a uniform test framework to (automatically) test the composition. Tests at this level were mainly manual. The major causes of difficulty may be heterogeneity and complexity of solution, a large set of testing combinations due to integration of autonomous services, etc.

4.3.4 Execution Lessons Identified

The M&S COE acted as the Service Provider and multiple national suppliers provided services from their local Kubernetes based MSaaS implementation through the M&S COE network infrastructure. The MSaaS Technical Reference Architecture provided guidance to the M&S COE and national suppliers.

Each national supplier implemented its own SMC and there was no federated SMC tested as part of the M&S COE MSaaS environment. The monitoring and control of each service was performed using a combination of Rancher/K8s tools.

- During execution, the management of security is very important. Accreditation of the consumer environment using services relies on that SLA being upheld with respect to security aspects. This implies that functions for monitoring compliance with security requirements are implemented. MSG-164 experiments used a VPN provided by M&S COE with security requirements that only allowed a tight control of access to Provider environments. During experiment integration and execution, extensive monitoring was not conducted, and security agreements were not established by the relevant stakeholders.
- Services used in the experimentation were a mix of stateful, stateless, federated and peer-to-peer. Initialization of the new/updated scenario required manual configuration, as automation was not a specific priority of the experiment design. The scenario was designed for a very specific vignette and area of operation. The impact of changing the scenario parameters on the different types of services was not investigated.
- While these experiments did not include automated capturing of state (for later initialization and re-initialization of a re-connecting service), fault-tolerance of individual and composed services, and any impact on the continuity of the entire exercise, is still important to address in future experiments.
- During experimentation each hosting environment provided its own SMC capability and there was no SMC for the composed services provided by NATO. Standards for SMC were missing; however, Kubernetes SMC may be considered a de facto standard. A monitoring and control prototype was developed but it had no interaction with OCEAN SMC at the M&S COE.
- SMC functions in the experiment were limited to the start and stop of services. Monitoring of readiness was only from an execution perspective and not from an M&S perspective. Monitoring service readiness and liveness using Kubernetes was tested to some extent but should be included in future experiment design.
- In the experiment, the start sequence of services and the consumer environment was important. A flexible system should not have these dependencies or clearly define any requirements related to the start sequence. All separate systems and services should continue to work even if one or several systems and services are restarted.
- During execution there was a limited use of Kubernetes tools for retrieving execution logs and for alerting information to be used for debugging, security logging or playback. Performance logging of networks and logging of simulation scenario data was not performed. We were not able to understand what systems and services were directly or indirectly affected and what actions to take in case a service or a service interface fails.
- Users and their Roles were not defined or selected for the experiment. During execution we did not demonstrate the respective duties of every role. The current prototypes and respective service descriptions did not have clearly defined users or roles.

- 'Service' Management and Control as opposed to 'Simulation' Management and Control should be more clearly delineated.
- With the Virtual View Service, it was demonstrated that it was possible for a Supplier to develop a simulation service that could be shared to a foreign Provider. This service was nationally developed by DNK but executed from the M&S COE MSaaS environment. But it also demonstrated that even the Supplier expected that the service was adequately documented; manual interaction with the Provider was still needed. The process of how a service is transferred from a Supplier to a Provider and brought into operation and how the Supplier best can support the Provider was not further reviewed.

4.3.5 Management Lessons Identified

- No business model experiment was conducted. All services and infrastructure were provided free for use in MSG-164. No functions for measuring usage or managing licenses and payments were tested.
- It is not feasible to require all MSaaS service implementations to be made available in a repository and accessible through the MSaaS Portal(s). Metadata in a service registry is possible but providing executable service implementations to a repository may not be possible from a commercial and security perspective. (See AMSP-02 requirements which differs from RA UC-2-2 Supply the M&S Resource).
- There was no experiment where multiple services of the same type were compared and evaluated against each other. There was no feedback provided in the service registry with regards to the use of the selected services.

4.4 The Analysis, Lessons Learned

Specific recommendations were identified in the MSG-136 Final Report, based on observations and formal feedback. Appendix 1 identifies the scope of these recommendations addressed by MSG-164. Lessons learned are derived from an analysis of the lessons identified using a set of Measures of Effectiveness (MOE) to identify remaining gaps to fulfill the MSaaS effect goals. Observations made during the analysis have been categorized according to these measures. Where possible, questions have been identified to address capability gaps or lack of methods/techniques that accurately measure a quality of an MSaaS Capability.

The four main MSaaS goals achieving the MSaaS vision are:

1) To provide a framework that enables credible and effective M&S services: MSaaS aims to provide a common, consistent, seamless and fit for purpose M&S capability to the user that is reusable and scalable in a distributed environment.
2) To make M&S services available on-demand to a large number of users: MSaaS aims to offer the users the ability to get timely access to services through scheduling and computing management. Users can dynamically provision computing capabilities, such as server time and network storage, as needed, automatically without requiring human interaction. Quick deployment of the customer solution is possible since the used services are already installed, configured and on-line.
3) To make M&S Services available in an efficient and cost-effective way: MSaaS aims to achieve convenient short set-up time and low maintenance costs for the community of users. MSaaS offers the service consumers the ability to increase efficiency by automating efforts.
4) To provide the required level of agility to enable convenient and rapid integration of capabilities: MSaaS offers the users the ability to evolve systems by rapid provisioning of resources, re-configuration, configuration management, deployment and migration of legacy systems. It is also tied to business dynamics of M&S that allow for the discovery and use of new services beyond the users' current configuration.

Key MOEs were derived during MSG-136 for evaluating the MSaaS goals defined in the OCD [2]. Table 1 provides key factors and considerations of each MOE. For more information on the derivation and priority ranking of these MOEs, please see the MSG-136 Evaluation Report [6].

Table 1: Key MSaaS MOEs.

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	Secure global access without a need for simulation support staff on location, access to a common experiment/exercise data repository, pre-training on demand.
Reusability	Hardware reuse (Provider Point of View).
Availability	Uptime (reduced MTBF), timely access to service through scheduled management – on-demand self-service, always ready.
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 configuration) 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	On-line help and failover/monitoring/documentation.
Suitability	Ability to sandbox several sim environments to select the most suitable.
Maturity	Assessment of the Technical Readiness Level of a specific technology that is part of an MSaaS Capability, or the overall maturity of the MSaaS Capability.
Security	Assessment of the security and integrity of an MSaaS Capability across the respective layers (logical, network, data, etc.) of the M&S Services.

4.4.1 MSaaS Goal 1: To Provide a Framework that Enables Credible and Effective M&S Services

MSaaS aims to provide a fit for purpose M&S capability that enables users to discover, compose and execute M&S services in a distributed environment. The framework will also enable sharing and pooling of modular services across NATO and Partner Nations.

In order to develop credible and effective M&S Services we need to define and measure maturity of the underlying capabilities. The following observations were made with respect to the maturity of the MSaaS Capabilities utilized in the experiment series, in accordance with the levels at which MSaaS Capabilities can be federated (see TRA):

- **Federated Simulation:** Achieved during the CA2X2 Forum experiment demonstration event.
- **Federated Registries:** Achieved some access to different registries but not entirely.
- **Federated Repositories:** The CA2X2 Forum experiment demonstration only pulled service data from other MSaaS Solutions into OCEAN as a manual process, however automation of service retrieval from remote repositories was demonstrated using Kubernetes. The CA2X2 Forum experiment demonstration used standard containers but with limited automation.
- **Federated Deployment and Execution:** The CA2X2 Forum experiment demonstration did not include sharing of composition and deployment descriptions, for instance Kubernetes Helm Charts with the ability to (seamlessly) pull and deploy resources from repositories. Only the sharing of design-time information regarding services and compositions was achieved.
- **Federated Service Management and Control:** Not demonstrated in the CA2X2 Forum experiment due to national security constraints.

4.4.2 MSaaS Goal 2: To make M&S Services Available On-Demand to a Large Number of Users

MSaaS aims to offer the users the ability to get timely access to services through scheduling and computing management. Users can dynamically provision computing capabilities, such as server time and network storage, as needed, automatically without requiring human interaction. Quick deployment of the customer solution is possible since the used services are already installed, configured and on-line.

While the MSG-164 experimentation efforts did focus on validating the on-demand aspects, the experimentation efforts looking at large numbers of users (i.e., 100 – 1000s of users) have not been executed so far. While the scalability was tested as part of the experiments, the large number of users in this Effect Goal relates to the availability of on-demand MSaaS services.

On-demand execution of simulation environments was part of many MSG-164 experimentation efforts and was successfully demonstrated. By using commercially available and mature technologies like Kubernetes and Rancher, scaling up to large numbers of users is expected behavior, but has not been specifically validated yet.

4.4.3 MSaaS Goal 3: To Make M&S Services Available in an Efficient and Cost-Effective Way

MSaaS aims to achieve convenient short set-up time and low maintenance costs for the community of users. MSaaS offers the service consumers the ability to increase efficiency by automating efforts.

Affordability is an MOE that is difficult to measure and often a case of moving cost from one aspect of a solution to another. For example, selecting not to use COTS may lower cost of licenses but increase cost in terms of hours spent in developing and maintaining a solution. Selecting to develop a bespoke interoperability interface may appear to be a low-cost and quick fix solution but may shift costs to other future integration efforts and other interoperating services. Affordability is also a subjective view of where

the costs appear. For instance, the entire cost of procuring and maintaining a set of software and hardware, for use in a project that do not fully utilize the capability the cost of having it available but not used, may seem less affordable than just paying when it is being used. However, in order for this cost to be reduced, the provided software and hardware use must also be shared with others and between projects. This is the case with using cloud-based solutions where the user can choose to pay for specific capacity of a shared pool of computing and storage provided as a service. The provider of the service can charge less for this capacity since the resources can be shared.

4.4.4 MSaaS Goal 4: To Provide the Required Level of Agility to Enable Convenient and Rapid M&S Integration

MSaaS offers the users the ability to evolve systems by rapid provisioning of resources, re-configuration, configuration management, deployment and migration of legacy systems. It is also tied to business dynamics of M&S that allow for the discovery and use of new services beyond the users' current configuration.

Through the MSaaS experimentation, aspects of this MSaaS Goal were demonstrated successfully in terms of the following MOEs:

- Flexibility was demonstrated through the use of COTS technologies such as Rancher and Kubernetes that provided convenient access to simulation resources and enabled rapid orchestration and provisioning of MSaaS services.
- The modularity of systems was demonstrated through the use of open standard interfaces such as documented APIs (including HLA and REST interfaces). Even though the basic principles of REST interfaces are well documented, we have identified a lack of openly available interface standards for individual services providing REST interfaces (e.g., what does the REST interface look like for a Radio Communication Service in terms of supported actions and information flow?). The same analysis holds true for any other protocols that may be used (Protocol Buffers, etc.) to implement MSaaS services.

Using common standards (like REST-based interfaces) may provide additional convenience through the ability to reuse existing development environments and tools (like network sniffers, protocol analyzers, etc.).

4.5 Maturity of MSaaS Capabilities

The MSaaS Capability / Technology Maturity document in Table 2 identifies and assesses key enabling technologies and their current maturity (Technology Readiness Level). These capabilities were categorized in accordance with the Architecture Building Blocks in the Technical Reference Architecture, and the Operational Concept Document service definitions. Each capability/enabling technology was identified, described, and an assessment of the current TRL was undertaken by MSG-136 workshop attendees. This table was subsequently updated by MSG-164 to include the respective ABBs, and a relative assessment of maturity levels as follows:

- **Low:** Laboratory based concept development and research with a TRL between 0 and 4.
- **Medium:** Engineering feasibility and prototyping with a TRL between 4 and 6.
- **High:** Technology transitioning to a program or fielded product with a TRL between 7 and 9.

Table 2: MSaaS Capability / Technology Maturity Updates.

ABB	Functional Area	Capability/ Enabling Technology	TRL Maturity
Supplier Portal Applications, Integrator Portal Applications, M&S Registry Services	Discovery	Technical Registry	High
	Discovery	Repository System	Med->High
	Discovery	Linked Registry and Repositories	Low
	Discovery	Automated Intelligent Discovery Service	Low
	Discovery	Meta Data Ontology	Med
	Discovery	Automated Meta Data Extraction	Low
	Discovery	Composition Evaluation	Low
	Discovery	Active Discovery System	Low
Integrator Portal Applications, M&S Registry Services, M&S Repository Services, M&S Composition Services, SMC Services	Composition	MSaaS Composition Aide	Low
	Composition	Automated MSaaS Composition Service	Low
	Composition	Cloud Deployment	Med->High
	Composition	Deployment Service	Med
	Composition	Negotiable interfaces for simulation	Low
	Composition	Automated Test Agent	Low
	Composition	Automated Validation Agent	Low
	Composition	Composition Optimization	Low
Operator Portal Applications, SMC Services, CIS Security Services, Enabling Services	Execution	Architectural Models	Med
	Execution	MSaaS Design Patterns	Low
	Execution	Execution Management Service	Low
	Execution	Cross-Domain Security	Med-High
	Execution	Rapid Accreditation Aide	Low
	Execution	Encrypted Runtime Containers	Low
	Execution	Load Balancing / Scalability	Low
	Execution	Mediation Services	Med
SMC Services, Other (new) Applications and Services	Support	Translation / Conversion Service	Med
	Support	Costing / Advisory Service	Low
	Support	Business Models	Low
	Support	License Management Solutions	High

5.0 RECOMMENDATIONS AND WAY FORWARD

5.1 Recommendations

5.1.1 General Recommendations

Nations are recommended to:

- Issue guidelines on how to implement the MSaaS Ecosystem and the proposed funding mechanism, including how to use the Business Model and the canvas to gain understanding and determine at the National level the customer and supplier contributions.
- Initiate MSaaS Core Implementation phase plan for MSaaS Ecosystem growth phase (Steady state).

NATO is recommended to:

- Establish a NATO MSaaS Steering Committee to assist in the governance and maintenance of the (federated) MSaaS Ecosystem.
- Take care of coordination with other ongoing NATO and National M&S projects and initiatives, e.g., NexGen M&S Capability, Federated Mission Network (FMN).

NMSG is recommended to:

- Prefer standards over research reports, e.g., publish the MSaaS CONEMP and the MSaaS TRA as Allied Modelling and Simulation Publications (AMSPs) and cover them by a NATO Standardization Recommendation (STANREC).
- Work with ACT (and other relevant stakeholders) to develop an MSaaS requirements specification that may be used as a template for national/NATO acquisition processes.

5.1.2 Technical Recommendations

- One level of classification is to capture that a service is delivering simulation, or that an application is a simulation system. Another level of classification is to capture the specific functionality of a service/system or what information the service or system handles, in case of a simulation system: what it simulates (what part of reality it models). This classification should map to user needs specification, so that it maps to concepts relevant for an end user (for example developed in the specification process parts of DSEEP) therefore, it should be mandatory to tag a service or application in the repository with concepts from the C3 Taxonomy as well as from a more detailed ontology.
  - Recommendation: Evaluate (and potentially promote) the use of the NATO C3 Taxonomy for classifying M&S services, e.g., as part of the governance policies.
- More focus on requirements and challenges to compose valid services that represent a simulation of the real-world is needed. Synchronization of models is essential for meeting distributed simulation validity requirements. The MSaaS approach to composed services must highlight and address these aspects in future work.
  - Need to expand research in the area of Composition -> current TRL of existing technologies is still too low – this (and the security and business model) are considered one of the remaining hard problems of MSaaS to solve.
- In MSG-164, the service focus has been on business-to-business data exchange where traditional Web Service composition has undoubtedly become the most promising way to integrate applications. However, in simulation when services are used to collectively represent the real-world (i.e., a model of the business), additional mechanisms to ensure the validity of the simulation are required. Using a mix

of technologies and standards (e.g., HLA/DIS, HTTPS, web sockets) increases the complexity of composing a valid simulation service.

  - Recommendation: Investigate impact of service composition to existing Verification and Validation (V&V) methodologies and propose adjustments if required.

- Recommend to analyze ongoing SISO activities on Discovery Metadata Standard for M&S Resources
- Investigate and compare information exchange standards for:
  - Service Implementation and Reusable Compositions Descriptions.
  - Service Compositions (blueprints) & Deployment Descriptions.
- Need to identify which metadata and tools will lead to automation.
- Need to consider including Kubernetes Cluster Management as a community recognized (de facto standard approach to SMC implementation within the TRA).

5.1.3 Business / Governance Recommendations

- Evaluate the MSaaS SLA Template developed by MSG-164 through real-life experimentation.
- Cyber security aspects and support to national accreditation of systems were missing as part of service descriptions to support service discovery. There is a strong need to include information related to security and the conditions under which services can be used. One of the important principles is the alignment of services with the of cybersecurity processes. Therefore, it is important to capture security artefacts from the cybersecurity processes so that they can be effectively documented with the supplied service.
- Recommendation: Investigate existing cybersecurity frameworks and document touchpoints with MSaaS and identify how security-related information for M&S services can best be captured.
- Customer access to configuration, and execution management and control of services (SMC) is a key aspect of MSaaS. More focus on establishing SMC to allow self-service configuration and execution control of services provided from different hosting environments is required. This includes governance processes to manage access credentials across federations and/or nations.
- NATO nations will be accountable for managing the risk to their area of responsibility and that responsibility cannot be transferred through Service Level Agreements. Many recommendations point to the potential benefits of clarifying roles and responsibilities, establishing clear performance metrics, and implementing remediation plans for non-compliance and security incidents. An important element of acquiring cloud/infrastructure services and subsequent content is the clarification and level of services a cloud or content provider must deliver. Such governance, architecture, and operational clarity would help NATO nations ensure services are performed effectively, efficiently, and securely.
- Recommend to analyze and consider (if appropriate) NATO ACT requirements analysis for “Next Generation Simulation” when updating the MSaaS OCD.

5.1.4 Experimentation / Evaluation Recommendations

- Need to focus on MSaaS Core Services with required standards and data exchange protocols and improve the related ABB descriptions in the TRA to guide implementations.
- Future MSaaS research should focus on providing and demonstrating examples of solutions that satisfy national and NATO requirements for the security accreditation of services in existing systems.
- An analysis of service fees and billing methods should be conducted to assess preferred implementation approaches addressing payment for services.

- A persistent MSaaS prototype (Sandbox) should be established for conducting continuous experimentation and demonstration of capabilities. Recommend an organization such as the M&S COE establish an MSaaS sandbox and a central MSaaS coordination cell.
- Future experiments should also focus on:
  - Each user perspective;
  - Role management and access control;
  - License management;
  - Maintenance and monitoring services; and
  - MSaaS Capability measures compared with traditional integration methods.

5.2 Way Forward

Many nations and NATO organizations are currently implementing MSaaS using cloud technology. MSG-164 strongly recommends NATO and Nations to advance and to promote the operational readiness of M&S as a Service, and to conduct required Science & Technology efforts to close current gaps. A key consideration for the near future is to develop and publish technical standards, guidance documents and compatibility metrics to ensure interoperability and security by design, and to provide acquisition authorities and program managers authoritative documents for current and upcoming efforts.

MSG-164 proposes an incremental development and implementation strategy for the Allied Framework for M&S as a Service. The incremental approach facilitates a smooth transition of its adoption and describes a route that will incrementally build an Allied Framework for M&S as a Service.

The proposed strategy also provides a method to control the rate of expansion of the new framework permitting iterative development and training of processes and procedures. Finally, it permits those nations that have been early adopters of an Allied Framework for M&S as a Service and have national capabilities to accrue additional benefits from their investments and highlight the benefits as well as the ability to provide lessons learned and advice to those nations considering similar investments.

Figure 10 shows the MSaaS Implementation Strategy. From the progress made so far, it is evident that initial concept development and basic specification efforts have been completed. The next step is to develop and establish an “MSaaS Core Implementation”. Achieving this requires a concerted approach:

1) The NMSG will continue to investigate critical S&T topics and further develop the Allied Framework for MSaaS, including necessary standards, policies, guidance documents, etc.
2) NATO and Nations will build up initial MSaaS implementations for a variety of Communities of Interest. This includes establishing required infrastructure (like cloud computing environments) as well as defining and prototyping M&S services and validating S&T results.
3) Industry partners will be key to providing service implementations and actually implementing the MSaaS paradigm into products and solutions.

MSG-164 developed a Technical Activity Proposal (TAP) to address the next phase (MSG-195). The TAP was approved by the NSMG in spring 2021, and defines three main objectives to mature the Allied Framework for MSaaS and to ensure the above-mentioned concerted approach:

Objective 1: Develop MSaaS interoperability standards (technical, governance, business model).

Objective 2: Investigate critical S&T topics to further enhance MSaaS benefits.

Objective 3: Educate MSaaS stakeholders and start building an open, federated MSaaS Ecosystem.

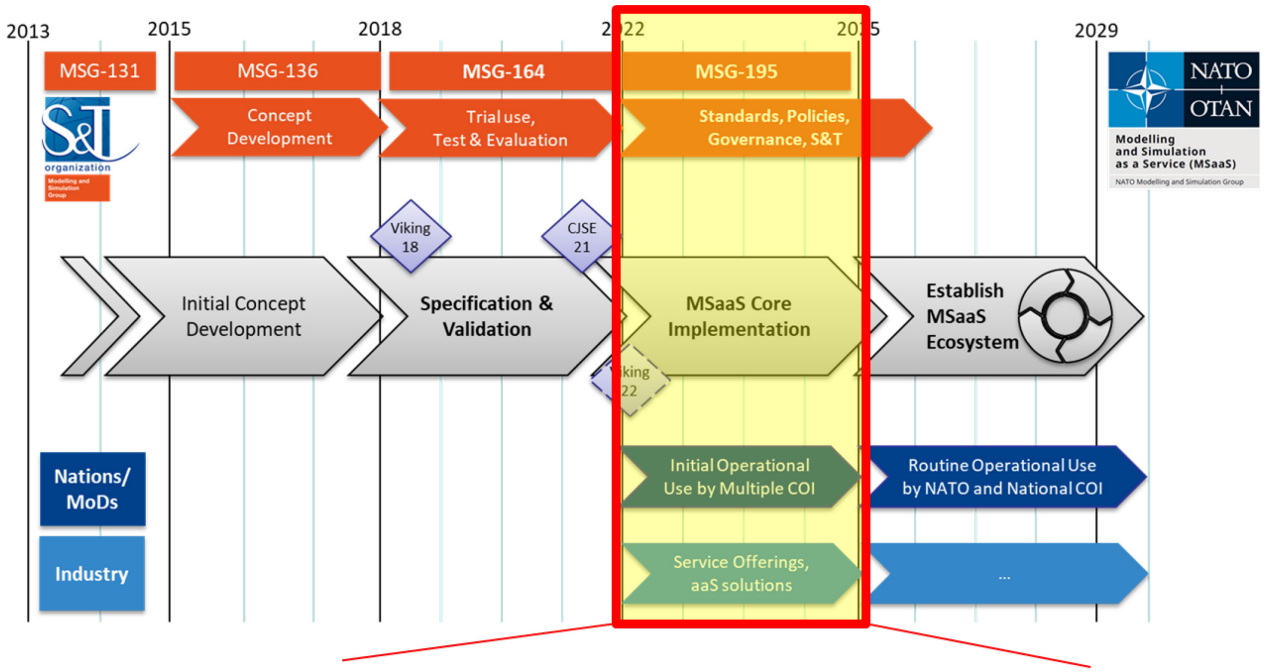

Figure 10: MSaaS Implementation Strategy.

6.0 REFERENCES

[1] NATO STO, "Modelling and Simulation as a Service (MSaaS) – Rapid Deployment of Interoperable and Credible Simulation Environments," 2018. STO-TR-MSG-136-Part-I. NATO Science & Technology Organization, Neuilly-sur Seine, France.

[2] NATO STO, "Operational Concept Document (OCD) for the Allied Framework for M&S as a Service," 2019. STO-TR-MSG-136-Part-III. NATO Science & Technology Organization, Neuilly-sur-Seine, France.

[3] NATO, STANREC 4794 "Allied Framework for Modelling and Simulation as a Service (MSaaS) Concept Of Employment," 2023, AMSP-02 Ed: A Ver. 1, 29-08-2023. https://nso.nato.int/nso/nsdd/main/standards/ap-details/2232/EN

[4] NATO STO, "Business Model for the Allied Framework for M&S as a Service," STO-TR-MSG-164-Vol-III. NATO Science & Technology Organization, Neuilly-sur Seine, France, 2024.

[5] NATO STO, "Modelling and Simulation as a Service (MSaaS) Technical Reference Architecture," STO-TR-MSG-164-Vol-II. NATO Science & Technology Organization, Neuilly-sur Seine, France, 2024.

[6] NATO STO, "MSaaS Concept and Reference Architecture Evaluation Report," 2019. STO-TR-MSG-136-Part-II. NATO Science & Technology Organization, Neuilly-sur Seine, France.

Appendix 1: MAPPING OF MSG-164 EFFORTS AGAINST MSG-136 RECOMMENDATIONS

Specific recommendations were identified in the MSG-136 Final Report, based on observations and formal feedback. Table 1A-1 identifies the scope of these recommendations addressed by MSG-164.

Table 1A-1: Mapping of MSG-136 Recommendations to MSG-164 Efforts.

MSG-136 Recommendations	Scope Addressed Under MSG-164
Investigate and recommend a robust business model and governance body for supporting Accessibility to MSaaS based M&S services.	Cooperation with ACT and NATO Allied Nation labs continues to evolve the accessibility to MSaaS Capabilities through CWIX and CAX events.
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.	MSG-164 recognizes that some Allied Nations have already defined requirements and milestones for MSaaS 'like' capabilities under acquisition programs. In many cases this information is not publicly released in order to accurately maintain a notional technology roadmap. However, MSG-164 has maintained an MSaaS Implementation Strategy and MSaaS Capability / Technology Maturity table identifying evolving MSaaS capabilities.
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.	The development of general Use Cases and MSaaS Requirements has supported the development of a Service Level Agreement template and assisted the validation of the MSaaS TRA during MSG-164.
Continue to collect feedback at upcoming scheduled events, in order to capture data from Technical, Government and Operations representation from all NATO countries.	MSG-164 has continued to collect feedback through presentations, papers, and the experiment series including the 2020 CAX Forum and 2021 US Army M&S Gap Forum.
Schedule a formal feedback forum when all MSaaS documentation is made available to the public.	MSG-164 has extended invitations to the SISO Cloud-Based Simulation group and broader industry and academia to provide feedback on MSG-164 publications and experiments.
Adopt and refine the Measures of Performance 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.	MSaaS Measures of Effectiveness and Measures of Performance have been extended to include test methods and tools where technology is available. Specific performances have not been identified as they are considered Allied Nation or exercise specific. The TRA and MOE/MOPs define MSaaS Capabilities but do not specify minimum performances.

MSG-136 Recommendations	Scope Addressed Under MSG-164
Define standards for simulation data unification, verification and validation of models and behaviors in order to establish trust in the proposed simulation services.	MSG-164 focused on the AMSP as the primary means for defining draft standards for MSaaS. M&S Resources have also been identified through MSaaS Use Case analysis conducted during MSG-164.
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.	A draft cyber security policy for MSaaS was produced and applied to the NATO M&S COE for approving technology insertions into OCEAN, and the federation of external simulations utilizing MSaaS technologies to exchange data with MSaaS technologies in OCEAN as part of the experiment series.
Perform further comparative evaluation of alternate container technologies (Microsoft, Kubernetes, Weave, etc.) including considerations in cost, licensing models, and relative performance.	Rancher and Kubernetes container technologies were included in the evaluation within the experiment series.
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 milestone (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.	Current and emerging MSaaS technologies have been identified and assessed in terms of the MSaaS Capability Maturity level definitions developed under MSG-164. The MSaaS Capability Technology Roadmap has been updated as current to the conclusion of the experiment series. Several more COTS technologies have emerged that enable aspects of MSaaS Capabilities which are already commercially available (TRL 10).
Future experimentation and evaluation work should demonstrate and assess the ability of MSaaS to evidence provision of the following areas: Increased Operational Effectiveness (e.g., increased readiness). A golden thread that links simulation discovery, composition and outputs back to user objectives (e.g., training objectives, MOEs). An ability to stay current and represent complex current and future operational environments, including the ability to customize the system solution to suit emerging/urgent operational needs.	i. MSaaS Capability Maturity has been defined in order to address overall readiness of MSaaS to meet operational effectiveness. ii. Mapping of MOEs and respective test methods have been identified but only Discovery was evaluated under MSG-164. Composition requires further research, experimentation and evaluation as TRL of MSaaS Capabilities continue to increase. iii. Current MSaaS Capabilities are still evolving and are not currently persistent. On-demand simulation services have been adapted to operational needs of national and Allied Nation exercises during the experiment series successfully.

MSG-136 Recommendations	Scope Addressed Under MSG-164
How MSaaS can be integrated with existing/future host infrastructure (e.g., integration with networks, command and control environments). 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 provide best value for industry, government and the military.	iv. National level security accreditation of MSaaS Capabilities, and the integration of C2 systems with simulation capabilities are ongoing activities for the Allied Nations. v. Business models and service fee models were investigated during MSG-164 and culminated in the definition of a Service Level Agreement template. Further research (non-technical in nature) is sought within industry, with many cloud service fee models already in use throughout the broader market. The adoption of Infrastructure as a Service contracts by military acquisition authorities is paving the way for Software as a Service and eventually Simulation as a Service contracting. Current Contractors providing these services rely on a mix of traditional license agreements and service subcontracts.
Continue to monitor challenges and recommendations from the ongoing CWIX events, and address the recognized need for the following MSaaS capabilities: • Federation management service. • Increased automation in composition and scenario planning. • Improved diagnostic capabilities and information reporting services.	The current experiment series recognized some interrelated challenges of security permissions for control of services across federations, and the use of common SMC capabilities. There is still a recognized need for increased automation, and definition of message sets for enabling automation across what is able to be controlled. This is also currently constrained by the relative MSaaS Capability Maturity levels of services across the federation. More diagnostic capabilities to support readiness and monitoring the active state of MSaaS Capabilities across a federation is required.

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TR-MSG-164-Vol-I AC/323(MSG-164)TP/1183	ISBN 978-92-837-2495-7	PUBLIC RELEASE

5. Originator

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

6. Title

Modelling and Simulation as a Service (Phase 2)

7. Presented at/Sponsored by

Final report.

8. Author(s)/Editor(s)	9. Date
Multiple	April 2024
10. Author's/Editor's Address	**11. Pages**
Multiple	52

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

MSaaS; M&S as a Service; Simulation; Training

14. Abstract

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-164 developed the technical and organizational foundations to establish the Allied Framework for M&S as a Service within NATO and partner nations.

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

DANEMARK
Danish Acquisition and Logistics Organization
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

FINLAND
Ministry for Foreign Affairs
Telecommunications Centre (24/7)
P.O Box 176, FI-00023 Government

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

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"

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

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 01 Liptovský Mikuláš 1

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

SUEDE
Regeringskansliet,
Attn: Adam Hidestå
RK IF AR 5
S-103 33 Stockholm

TCHEQUIE
Vojenský technický ústav s.p.
CZ Distribution Information
Mladoboleslavská 944
PO Box 18, 197 06 Praha 9

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

CZECHIA
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

FINLAND
Ministry for Foreign Affairs
Telecommunications Centre (24/7)
P.O Box 176, FI-00023 Government

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 01 Liptovský Mikuláš 1

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

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

SWEDEN
Regeringskansliet, Attn: Adam Hidestål
RK IF AR 5
S-103 33 Stockholm

TÜRKIYE
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 978-92-837-2495-7