NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(MSG-136)TP/826

www.sto.nato.int

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

Modelling and Simulation as a Service (MSaaS) – Rapid Deployment of Interoperable and Credible Simulation Environments

(Modélisation et simulation en tant que service (MSaaS) – Déploiement rapide d'environnements de simulation crédibles et interopérables)

Final Report of NATO MSG-136.

Published October 2018

Distribution and Availability on Back Cover

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(MSG-136)TP/826

www.sto.nato.int

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

Modelling and Simulation as a Service (MSaaS) – Rapid Deployment of Interoperable and Credible Simulation Environments

(Modélisation et simulation en tant que service (MSaaS) – Déploiement rapide d'environnements de simulation crédibles et interopérables)

Final Report of NATO MSG-136.

The NATO Science and Technology Organization

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

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

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

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

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

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

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

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

Published October 2018

ISBN 978-92-837-2154-3

Table of Contents

List of Figures

Figure **Page**

List of Tables

List of Acronyms

ABB	Architecture Building Block
ACT	Allied Command Transformation
AMSP	Allied Modelling and Simulation Publication
AP	Architecture Pattern
AWS	Amazon Web Services
C2	Command and Control
C3	Consultation, Command and Control
CGF	Computer Generated Forces
CSO	Collaboration Support Office
DSEEP	Distributed Simulation Engineering and Execution Process
FOC	Full Operational Capability
IOC	Initial Operational Capability
M&S	Modeling and Simulation
MoE	Measure of Effectiveness
MoP	Measure of Performance
MORS	Military Operational Requirements Subgroup
MS3	M&S Standards Subgroup
MSaaS	M&S as a Service
MSG	Modelling and Simulation Group
NATO	North Atlantic Treaty Organization
NMSG	NATO Modelling and Simulation Group
NMSMP	NATO Modelling and Simulation Master Plan
OCD	Operational Concept Document
RA	Reference Architecture
SES	Synthetic Environment Service
SISO	Simulation Interoperability Standards Organization
SLA	Service Level Agreement
SOA	Service Oriented Architecture
TAP	Technical Activity Proposal

MSG-136 Membership List

CO-CHAIRS

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

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

MEMBERS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Modelling and Simulation as a Service (MSaaS) – Rapid Deployment of Interoperable and Credible Simulation Environments

(STO-TR-MSG-136-Part-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 new concept that includes service orientation and the provision of M&S applications via the as-a-service model of cloud computing to enable more composable simulation environments that can be deployed and executed on-demand. The MSaaS paradigm supports stand-alone use as well as integration of multiple simulated and real systems into a unified cloud-based simulation environment whenever the need arises.

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

- Operational Concept Document;
- Technical Reference Architecture (including service discovery, engineering process and experimentation documentation); and
- Governance Policies.

MSG-136 evaluated the MSaaS concept in various experiments. The experimentation results and initial 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-136 strongly recommends NATO and nations to advance and to promote the operational readiness of M&S as a Service, and to conduct required Science and Technology efforts to close current gaps.

This document contains the Final Report that serves as an umbrella for the individual documents and describes the general approach taken by MSG-136. It provides an overview of all results and makes recommendations for the way forward.

Modélisation et simulation en tant que service (MSaaS) – Déploiement rapide d'environnements de simulation crédibles et interopérables

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

Synthèse

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

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

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

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

Le MSG-136 a évalué le concept de MSaaS au moyen de diverses expériences. Les résultats d'expérimentation et les premières 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-136 recommande vivement à l'OTAN et aux pays membres de faire progresser et d'améliorer l'état de préparation opérationnelle de la M&S en tant que service et de mener les travaux de science et technologie requis pour combler les lacunes actuelles.

Ce document contient le rapport final qui englobe tous les documents individuels et décrit la démarche générale adoptée par le MSG-136. Il donne une vue d'ensemble des résultats et émet des recommandations sur la marche à suivre.

Chapter 1 – INTRODUCTION

1.1 BACKGROUND AND KEY DRIVERS

The NATO Modelling and Simulation Group (NMSG) Specialist Team MSG-131 on request from ACT conducted a one year study into "Modelling and Simulation as a Service (MSaaS): New Concepts and Service-Oriented Architectures" [10]. Based on a survey of existing MSaaS case studies, MSG-131 concluded that service-based approaches can contribute towards more efficient Modelling and Simulation (M&S) and recommended that MSaaS should be investigated in more detail. This resulted in the establishment of MSG Research Task Group 136 ("Modelling and Simulation (M&S) as a Service (MSaaS) – Rapid deployment of interoperable and credible simulation environments"), which began a 3-year program of work in November 2014.

It is anticipated that future military capabilities, including training, mission planning and decision making will be provided through increased use of M&S. However, there are currently two main barriers: the perceived cost and the time taken to compose and develop simulation environments. Furthermore, limited credibility resulting from unknown validity and ad-hoc processes is still a serious problem.

M&S products are highly valuable to NATO and military organizations, and it is essential that M&S products, data and processes are conveniently accessible to a large number of users whenever and wherever needed. Therefore, a new "M&S ecosystem" is required where M&S products can be more readily identified and accessed by a large number of users to meet their specific requirements. This "as a Service" paradigm has to support stand-alone use as well as integration of multiple simulated and real systems into a unified simulation environment whenever the need arises.

Recent technical developments in the area of cloud computing technology and service-oriented architectures may offer opportunities to better utilize M&S capabilities in order to satisfy NATO critical needs. A new concept that includes service orientation and the provision of M&S applications via the as-a-service model of cloud computing may enable composable simulation environments that can be deployed rapidly and on-demand. This new concept is known as M&S as a Service (MSaaS).

NATO MSG-136 investigated the new concept of MSaaS with the aim of providing the technical and organizational foundations for a future permanent service-based *Allied Framework for MSaaS* within NATO and partner nations. MSG-136 started its three-year term of work in November 2014 and finished at the end of 2017. MSaaS is looking to provide a strategic approach to deliver simulation coherent with the NMSMP vision and guiding principles.

1.2 OBJECTIVES

The objectives of MSG-136 are to investigate, propose and evaluate standards, agreements, architectures, implementations, and cost-benefit analysis of Modelling and Simulation (M&S) as a Service (MSaaS) approaches. Specifically, with regards to:

1) Evaluating the use of (M&S domain) services to improve simulation interoperability and credibility.
2) Analyzing the organizational M&S services perspective to establish a sustainable and efficient management of M&S services in NATO.

Specific M&S domain services for detailed investigations are selected by the task group and include (but are not limited to):

- Enabling rapid initialization of simulation systems with correlated synthetic environment data by using a Synthetic Environment Service (SES).

- Reducing development time significantly by scenario management services (including library of typical scenarios that may be used with minimum effort).

1.3 GENERAL APPROACH

The Allied Framework for MSaaS is the common approach of NATO and Nations towards implementing MSaaS and is defined in various documents. Figure 1-1 gives an overview of the documents developed by MSG-136.

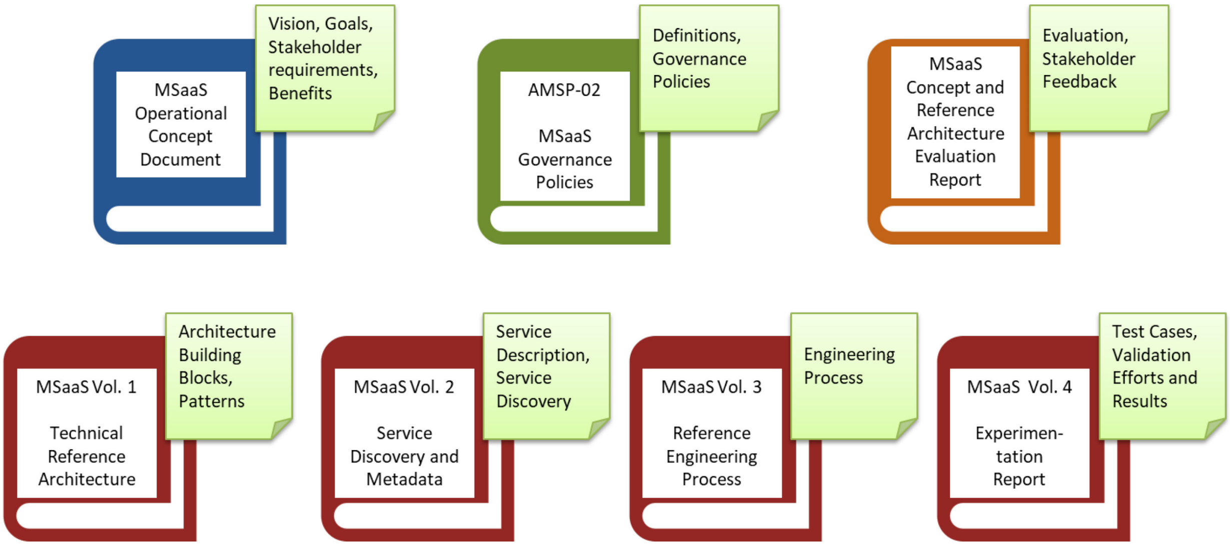

Figure 1-1: MSaaS Document Overview.

The documents are:

- *Operational Concept Document*: The Operational Concept Document (OCD) describes the intended use, key capabilities and desired effects of the Allied Framework for MSaaS from a user's perspective.
- *Governance Policies*: The Governance Policies identify MSaaS stakeholders, relationships and provide guidance for implementing and maintaining the Allied Framework for MSaaS.
- *Technical Reference Architecture and associated volumes*: The Technical Reference Architecture (Vol. 1) describes the architectural building blocks and patterns for realizing MSaaS capabilities. Volumes 2 – 4 define service discovery and metadata, describe a reference engineering process and document the experimentation and validation efforts.
- *MSaaS Evaluation Report*: The MSaaS Evaluation Report contains an external evaluation of all MSG-136 efforts plus stakeholder feedback on MSaaS.

These documents define the blueprint for individual organizations to implement MSaaS. However, specific implementations – i.e. solutions – may be different for each organization.

1.4 TEAM STRUCTURE

To address the technical and organizational topics as well as the associated experimentation and evaluation efforts, MSG-136 established four dedicated subgroups as illustrated in Figure 1-2.

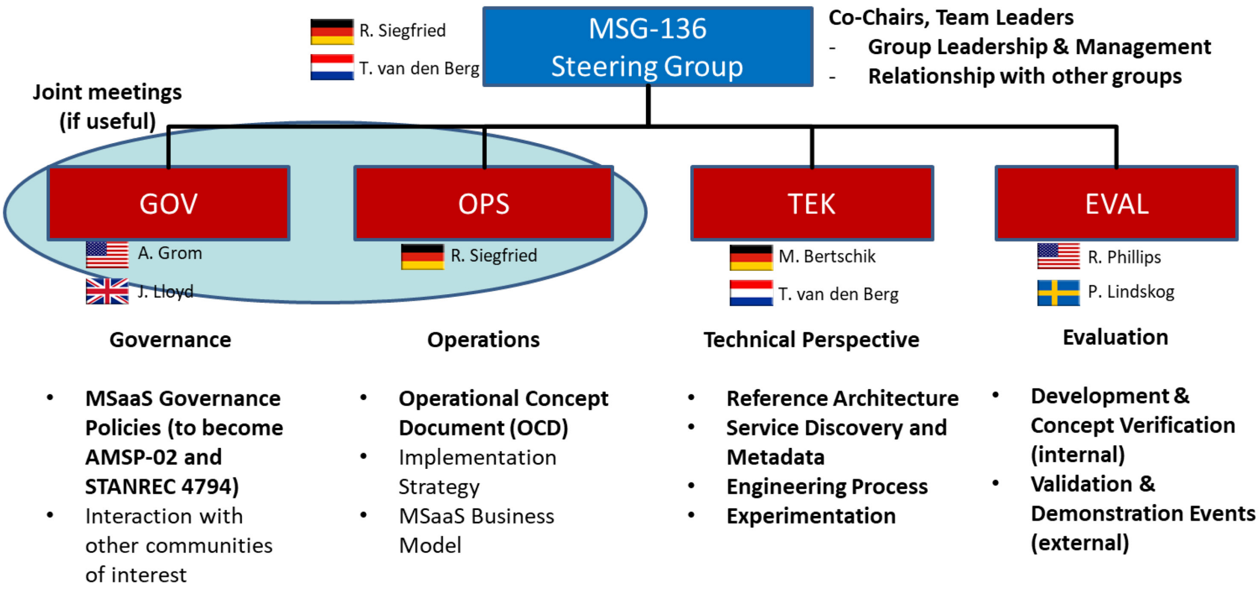

Figure 1-2: MSG-136 Internal Organization with Four Subgroups.

The *MSG-136 OPS* subgroup was responsible for all organizational topics and developed the operational concept that describes the desired characteristics and requirements of MSaaS from a user's perspective including its major structures and capabilities. The primary deliverable of the OPS subgroup is the Operational Concept Document (OCD) (see Section 2.2).

The *MSG-136 TEK* subgroup was responsible for architectural and technical aspects of MSaaS. Based on the operational requirements the TEK subgroup developed a 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 results are covered in four separate volumes (see Section 2.3), where the primary deliverable of the TEK subgroup is the MSaaS Technical Reference Architecture, described in Volume 1.

The *MSG-136 GOV* subgroup was responsible for all governance topics. With regards to the Allied Framework for Modelling and Simulation as a Service the GOV subgroup defined governance policies, processes, and standards for managing the lifecycle of services, service acquisitions, service components and registries, service providers, and service consumers. The primary deliverables of the GOV subgroup are the MSaaS Governance Policies that will be published as AMSP-02 and STANREC 4794 (see Section 2.4).

The *MSG-136 EVAL* subgroup was responsible for continuous evaluation and concept verification. The EVAL subgroup 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-136. The primary deliverable of the EVAL subgroup is the evaluation results (see Chapter 3).

Chapter 2 – ALLIED FRAMEWORK FOR M&S AS A SERVICE

As described in Section 1.3, MSG-136 has developed a set of documents that, in their entirety, define M&S as a Service. The following sections provide an overview of the three core parts: the MSaaS Operational Concept, the MSaaS Technical Reference Architecture, and the MSaaS Governance Policies.

2.1 KEY DEFINITIONS

The key definitions regarding MSaaS that MSG-136 developed are defined in the Allied M&S Publication (AMSP) on the "Allied Framework for Modelling and Simulation (MSaaS) Governance Policies" [2]. Due to their importance, the key definitions are repeated here:

> "An **M&S service** is a specific M&S-related capability delivered by a provider to one or more consumers according to well defined contracts including Service Level Agreements (SLA) and interfaces." [2]
>
> "**M&S as a Service (MSaaS)** is an enterprise-level approach for discovery, composition, execution and management of M&S services." [2]
>
> "An **MSaaS Implementation** is the specific realization of M&S as a Service by a certain organization as defined in the Operational Concept Document. An MSaaS Implementation includes both technical and organizational aspects.") [2]
>
> "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." [2]

2.2 MSAAS OPERATIONAL CONCEPT

The MSaaS Operational Concept describes the vision, goals and objectives from a user's point of view. Its intention is to specify the user requirements, to identify the relevant stakeholders and to evaluate the benefit of implementing M&S as a Service against all dimensions (technical, organizational, etc.).

2.2.1 MSaaS Vision Statement and Goals

The *MSaaS Vision Statement* is defined as:

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

To achieve the MSaaS Vision Statement the following MSaaS goals are defined:

1) To provide a framework that enables credible and effective M&S services by providing a common, consistent, seamless and fit for purpose M&S capability that is reusable and scalable in a distributed environment.
2) To make M&S services available on-demand to a large number of users through scheduling and computing management. Users can dynamically provision computing resources, such as server time and network storage, as needed, without requiring human interaction. Quick deployment of the customer solution is possible since the desired services are already installed, configured and on-line.
3) To make M&S services available in an efficient and cost-effective way, convenient short set-up time and low maintenance costs for the community of users will be available and 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 ability to evolve systems by rapid provisioning of resources, 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.

2.2.2 Operational Concept Document

The purpose of the Operational Concept Document (OCD) for the Allied Framework for MSaaS is to inform relevant stakeholders about how the framework will function in practice. The capabilities and key characteristics of the proposed framework are included in the OCD as well as how stakeholders will interact with the system.

Specifically, the main goals of the OCD are to inform the operational stakeholders how to evolve from their current operational stove-piped systems to the Allied Framework for MSaaS. It also serves as a platform for stakeholders to collaboratively adapt their understanding of the systems operation as new developments, requirements or challenges arise. Therefore, the OCD is written in the common language of all interested parties.

2.2.3 MSaaS from the User Perspective

MSaaS enables users to discover new opportunities for training and working together and enables users to enhance their operational effectiveness, saving costs and effort in the process. By pooling individual user's requirements and bundling individual requests in larger procurement efforts, the position of buying authorities against industrial providers is strengthened.

MSaaS aims to provide the user with discoverable M&S services that are readily available on-demand and deliver a choice of applications in a flexible and adaptive manner. It offers advantages over the existing stove-piped M&S paradigm in which the users are highly dependent on a limited amount of industry partners and subject matter experts.

The MSaaS concept is illustrated in Figure 2-1. MSaaS is an enterprise-level approach for discovery, composition, execution and management of M&S services. MSaaS provides the linking element between M&S services that are provided by a community of stakeholders to be shared and the users that are actually utilizing these capabilities for their individual and organizational needs.

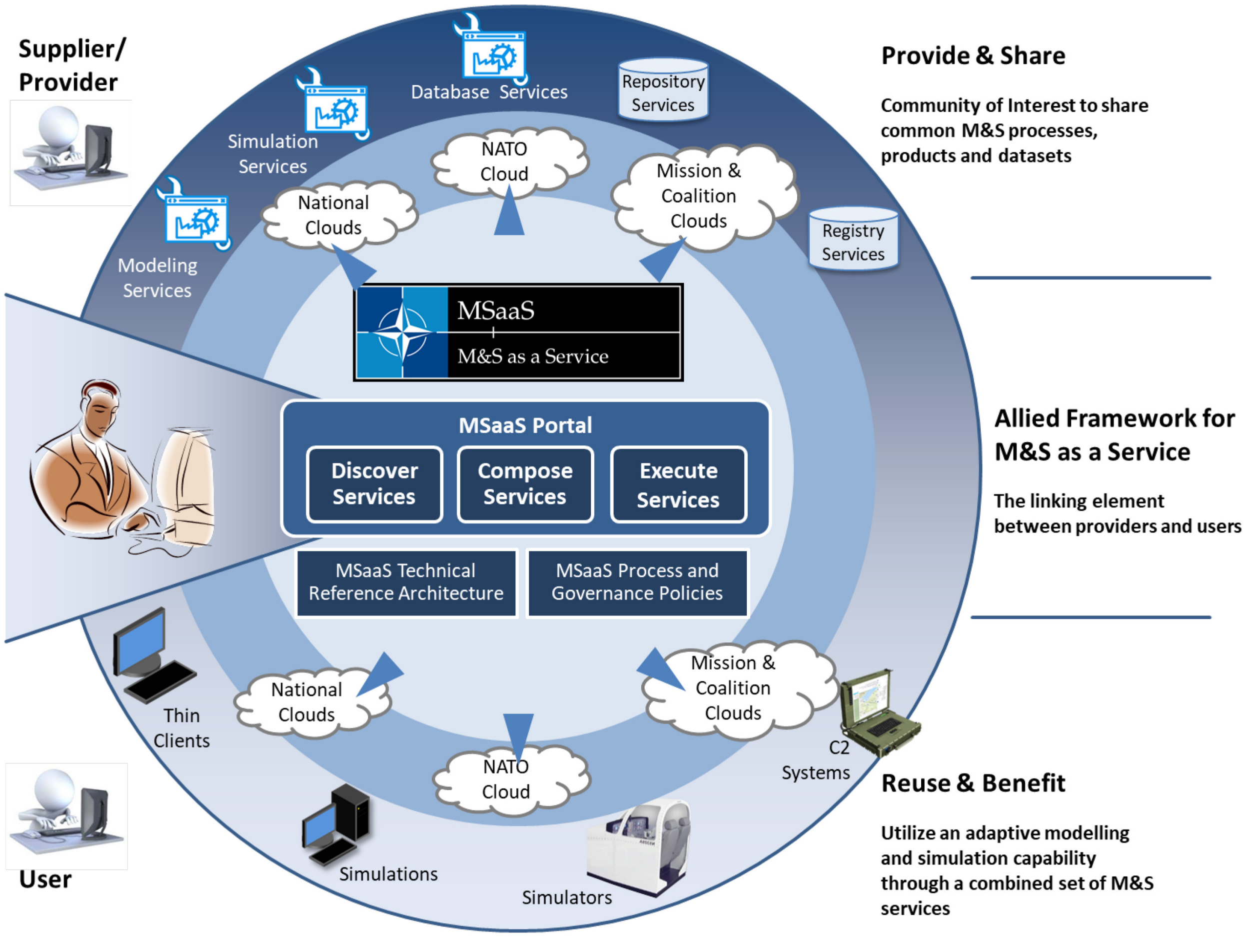

Figure 2-1: Operational Concept of the Allied Framework for M&S as a Service.

The Allied Framework for MSaaS defines user-facing capabilities (front-end) and underlying technical infrastructure (back-end). The front-end is called the MSaaS Portal. The front-end provides access to a large variety of M&S capabilities from which the users are able to select the services that best suit their requirements, and track the experiences and lessons learned of other users. The users can discover, compose and execute M&S services through the front-end, which is the central access point that guides them through the process:

- **Discover:** The Allied Framework for MSaaS provides a mechanism for users to search and discover M&S services and assets (e.g., data, services, models, federations, and scenarios). A registry is used to catalogue available content from NATO, national, industry and academic organizations. This registry provides useful information on available services and assets in a manner that the user is able to assess their suitability to meet a particular requirement (i.e., user rating, requirements, simulation specific information, and verification and validation information). The registry also points to a repository (or owner) where that simulation service or asset is stored and can be obtained, including business model information (i.e., license fees, pay per use costs).
- **Compose:** The framework provides the ability to compose discovered services to perform a given simulation use case. Initially it is envisaged that simulation services will be composed through existing simulation architectures and protocols and can be readily executed on-demand (i.e., with no set up time). In the longer term, distributed simulation technology will evolve, enabling further automation of discovery, composition and execution than is possible today.

- **Execute:** The framework provides the ability to deploy the composed services automatically on a cloud-based or local computing infrastructure. The automated deployment and execution exploits the benefits of cloud computing (e.g., scalability, resilience). Once deployed and executed the M&S services can be accessed on-demand by a range of users (Live, Virtual, Constructive) directly through a simulator (e.g., a flight simulator consuming a weapon effects service), through a C2 system (e.g., embedded route planning functionality that utilizes a route planning service) or may be provided by a thin client or by a dedicated application (e.g., a decision support system utilizing various services like terrain data service, intelligence information service etc.). The execution services support a range of business models and are able to provide data relevant to those models (i.e., capture usage data for a pay-per-use business model).

The Allied Framework for MSaaS is the linking element between service providers and users by providing a coherent and integrated capability with a Technical Reference Architecture, recommendations and specifications for discovery, composition and execution of services, and necessary processes and governance policies.

2.3 MSAAS TECHNICAL REFERENCE ARCHITECTURE

The MSaaS Technical Reference Architecture provides a blueprint for implementing MSaaS. Volume 1 describes the architectural building blocks and patterns for realizing MSaaS capabilities. Volumes 2 to 4 define service discovery and metadata; describe the engineering process for developing simulation environments in an MSaaS context, and document the experimentation and validation efforts.

2.3.1 Volume 1: MSaaS Reference Architecture

2.3.1.1 Principles

The MSaaS Reference Architecture (RA) [6] is defined with a number of principles in mind. These principles are similar to the Open Group SOA Reference Architecture [16] key principles and are the starting point for the architecture work by MSG-136. The seven principles are:

The MSaaS RA:

1) Should be a generic solution that is vendor-neutral.
2) Should be modular, consisting of building blocks that may be separated and recombined.
3) Should be extendable, allowing the addition of more specific capabilities, building blocks, and other attributes.
4) Must be compliant with NATO policies and standards, such as AMSP-01 [1] and STANAG 4603 [17].
5) Must facilitate integration with existing M&S systems.
6) Should be capable of being instantiated to produce:
   a) Intermediary architectures; and
   b) Solution architectures.
7) Should address multiple stakeholder perspectives.

2.3.1.2 Architecture Concepts

The architecture of a system or of a federation of systems describes “the fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution”. Thus, a system architecture provides plans or blueprints for a system.

Architectures can be designed at various levels of abstraction. There is little consensus in general on the various levels of abstraction or on how to name them. The terms used by MSG-136 are illustrated in Figure 2-2. Two notions are central: Architecture Building Block (ABB) and Architecture Pattern (AP). ABBs are the elements that constitute an architecture, and each ABB should have attributes that specify its function. APs are high-level suggestions for ways of combining ABBs.

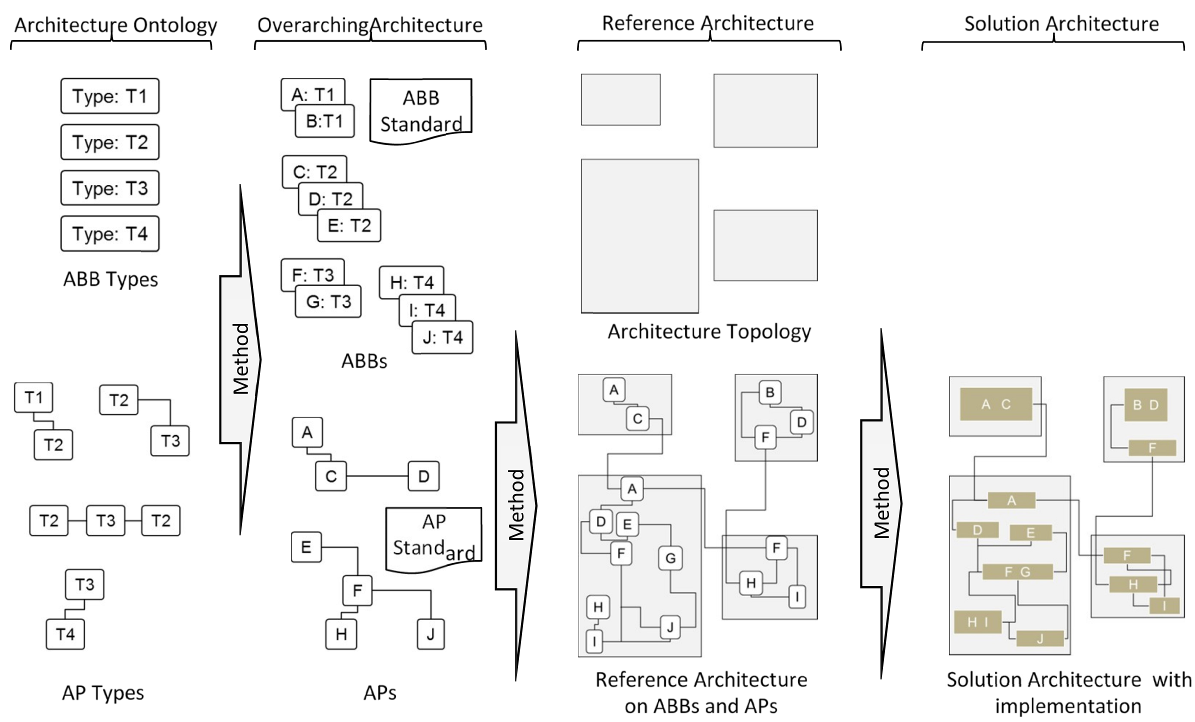

Figure 2-2: MSaaS Architecture Framework.

Figure 2-2 shows several levels of abstraction for architectures. At the highest level, an *architecture ontology* might declare types of ABBs and APs. For example, '(business) process', 'service', 'repository', 'service container'; and AP types, such as 'consumer pattern', 'service invocation pattern', that are pertinent for any SOA. Next, actual ABBs and APs of the various ABB types and AP types can be used for declaring a domain-specific *overarching architecture*. The manner in which ABBs and APs are specified might be standardized. For example an ABB representing a service would be of type 'service' and its specification may follow some standard for service specification.

Then, a *reference architecture* is designed by composing ABBs guided by APs from the overarching architecture. In addition, an architecture topology (or several) should be designed at the reference architecture level to delineate intended systems boundaries and the boundaries in which interoperability standards are enforced. From a reference architecture, individual *solution architectures* (also called target architectures) that specify solution implementations may be derived. There should be methods for refining architectures at one abstraction level to the next. The spectrum of architecture abstraction levels and such methods are what we here refer to as an architecture framework, as shown in Figure 2-2.

The types of architecture are summarized in Figure 2-2. In this figure, an architecture ontology provides types of ABBs and types of APs. Types of ABBs and APs are described in The Open Group SOA Reference Architecture [16]. An overarching architecture consists of specific ABBs and APs of various types, with standards for specifying ABBs and APs. These are defined in the NATO C3 Taxonomy [14]. Various architecture topologies specifying system and interoperability boundaries aid in designing reference architectures using ABBs and APs, in this case the MSaaS RA. From the MSaaS RA, solution architectures with implementation-specific systems or solution implementations (olive) can be derived.

The MSaaS RA [6] describes the MSaaS architecture framework laid out above in more detail.

2.3.1.3 MSaaS Reference Architecture Structure

Table 2-1 provides an overview of the MSaaS RA layers and high-level ABBs per layer. A layer is a cohesive set of ABBs that support a set of related capabilities. The scope of the MSaaS RA is the M&S-particular ABBs. In its present form, some layers of the MSaaS RA are unpopulated, with the understanding that the empty layers may become populated in the future. For these layers, we indicate the assumed NATO C3 Taxonomy categories from which one might find it pertinent to declare M&S-particular ABBs. These ABBs are indicated by “see C3 Taxonomy” in parentheses.

Table 2-1: Layers and Architecture Building Blocks.

Layer	ABB
9. Governance Layer	▪ M&S Repository Services
8. Information Layer	▪ M&S Registry Services
7. Quality of Service Layer	▪ M&S Security Services ▪ M&S Certification Services
6. Integration Layer	▪ M&S Message-Oriented Middleware Services ▪ M&S Mediation Services
5. Consumer Layer	▪ Modelling Applications ▪ Simulation Applications
4. Business Process Layer	▪ Composed Simulation Services ▪ M&S Composition Services ▪ Simulation Control Services ▪ Simulation Scenario Services
3. Services Layer	▪ Modelling Services ▪ Simulation Services
2. Service Components Layer	▪ SOA Platform Services (see C3 Taxonomy)
1. Operational Systems Layer	▪ Infrastructure Services (see C3 Taxonomy) ▪ Communication Services (see C3 Taxonomy)

Layers 6 to 9 are cross-cutting layers as shown in Figure 2-3, e.g., Quality of Service Layer ABBs such as M&S Security Services cross layers 1 to 6. Similarly, Information Layer ABBs cross layers 1 to 7. This is why M&S Security Services are not repeated in Layers 1 to 6.

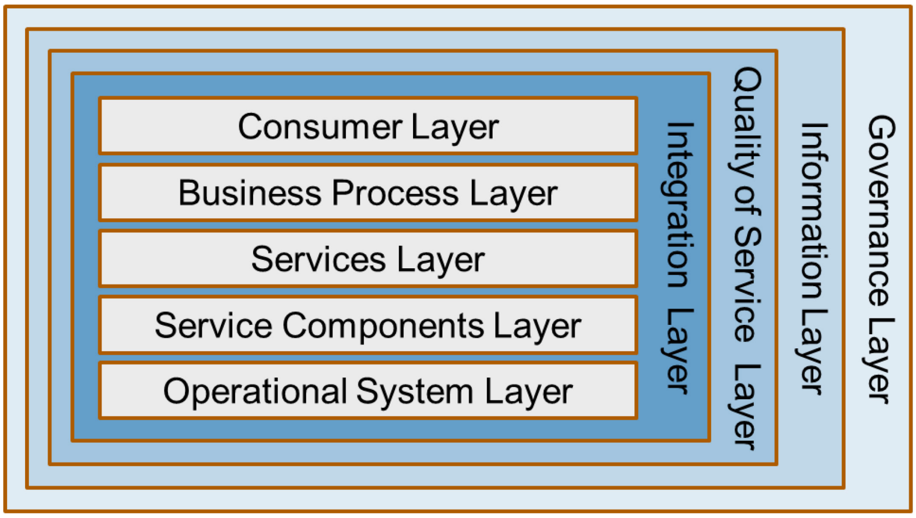

Figure 2-3: MSaaS RA Layers.

The layering structure of the MSaaS RA is inherited from the Open Group SOA Reference Architecture, while the actual (M&S-specific) ABBs and APs for each layer of the MSaaS RA are linked in from the NATO C3 Taxonomy. The NATO C3 Taxonomy is a library for NATO's Consultation, Command and Control (C3) capabilities.

As an example, the Business Process Layer provides the capabilities to compose and execute a simulation, and contains the following ABBs:

- M&S Composition Services: compose a simulation environment from individual services that together meet the objectives of the simulation environment.
- M&S Simulation Control Services: provide input to, control, and collect output from a simulation execution.
- Simulation Scenario Services: manage the simulation of scenarios.

Each of these ABBs has associated requirements and other attributes. As an example, some requirements for the M&S Composition Services are listed in Table 2-2.

Table 2-2: M&S Composition Services Requirements.

Function	Requirements
Manage Lifecycle	1. The M&S Composition Services shall provide the means to define a parameterized simulation composition. 2. The M&S Composition Services shall provide the means to update, delete and retrieve a defined simulation composition.
Execute Composition	3. The M&S Composition Services shall provide the means to start the execution of a simulation composition, and to provide composition parameter values. 4. The M&S Composition Services shall provide the means to orchestrate, restart and stop the execution of a simulation composition.
Programmatic Interfaces	5. The M&S Composition Services shall provide APIs to the Manage Lifecycle and Execute Composition functionality.

The ABBs of the MSaaS RA are organized in a taxonomy, in line with the NATO C3 Taxonomy (see Figure 2-4). Most of the ABBs in Table 2-1 fall under the M&S Enabling Services, providing capabilities to create a simulation environment in which M&S Specific Services are brought together to fulfil the purpose of that simulation environment. M&S Specific Services are mostly Simulation Services and Composed Simulation Services, such as Synthetic Environment Services, Route Planning Services, or Report Generation Services.

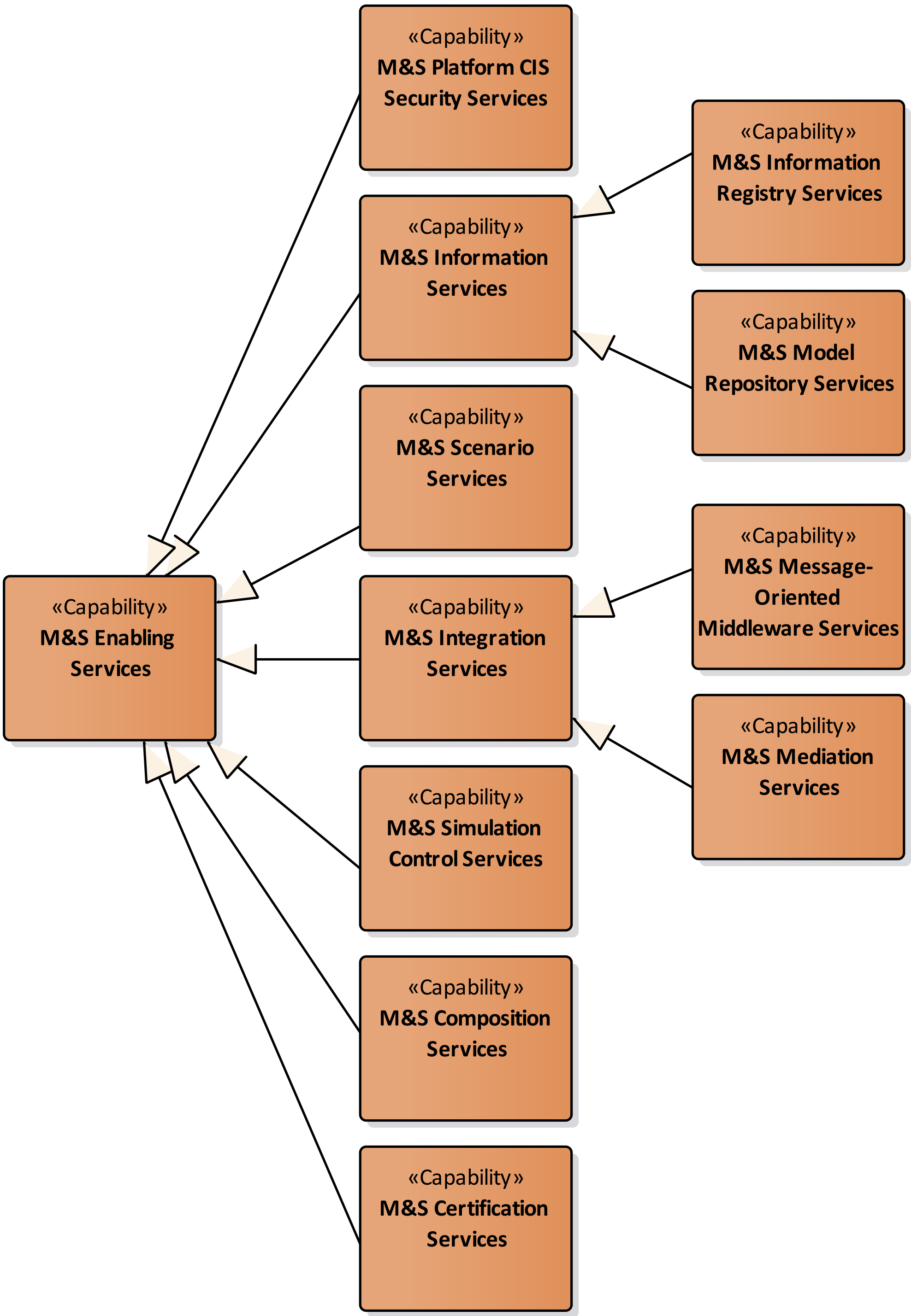

Figure 2-4: Taxonomy of Architecture Building Blocks.

2.3.1.4 Architectural Patterns

The Architectural Patterns (APs) show how ABBs in the MSaaS RA are related to each other and how they can be combined, how they interact, and what information is generally exchanged. The APs serve as reference for solution architectures and design patterns for solution architectures. An initial set of APs is documented, but the idea is that the ABBs as well as the APs in the MSaaS RA are governed as a “living document” and will evolve further as knowledge is gained and as technology evolves.

Figure 2-5 illustrates one example of an AP, in relation to the M&S Composition Services mentioned earlier.

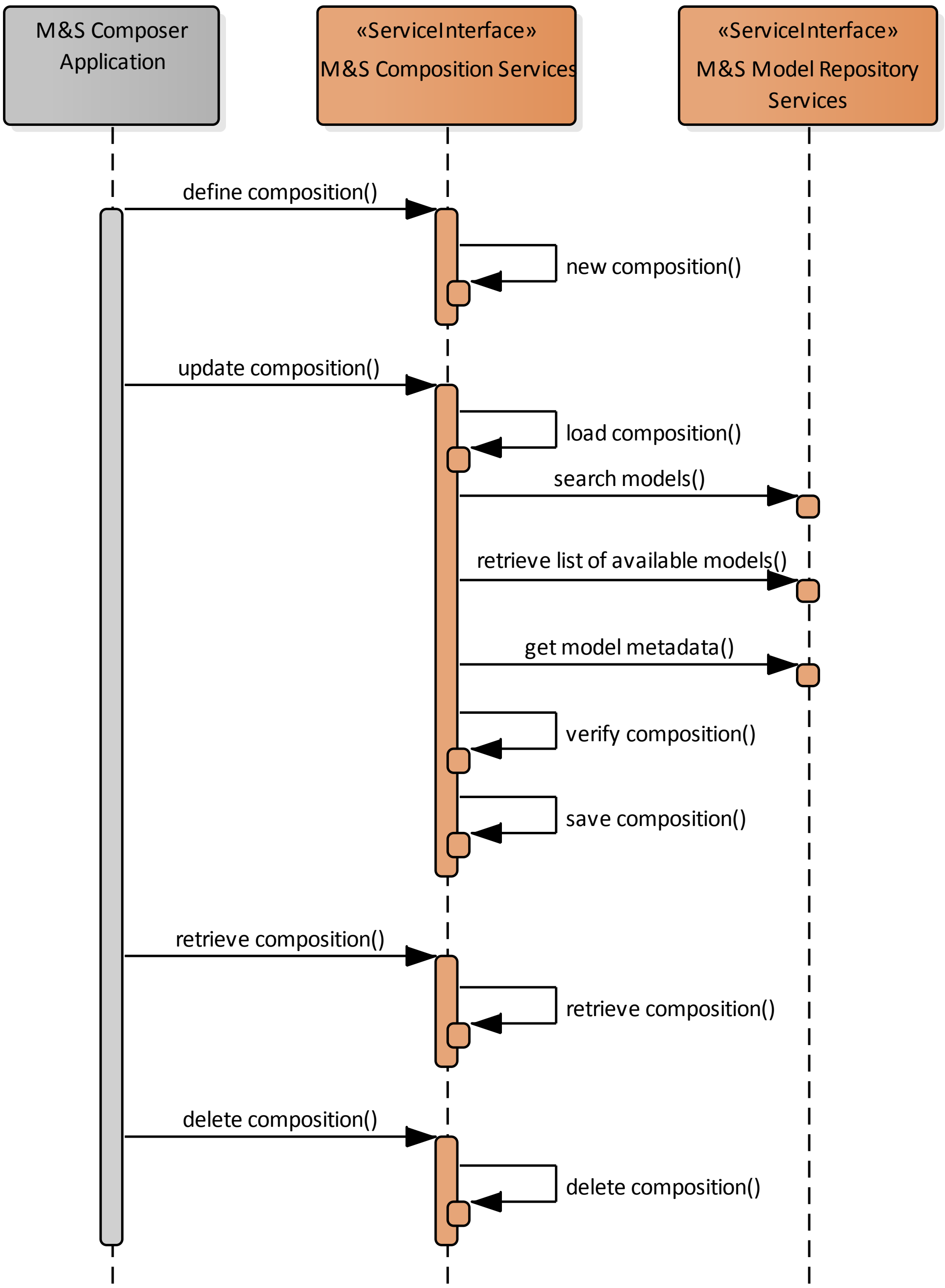

Figure 2-5: Example of an Architecture Pattern.

In this example, a user composes a simulation environment using an M&S Composer Application. This application, in turn, employs the capabilities of M&S Composition Services and the M&S Model Repository Services. This pattern provides support for the definition, update, retrieval, and deletion of compositions. The M&S Composer Application is user-facing while the other architecture building blocks operate "behind the scene". The interactions in the figure also imply requirements on each architecture building block.

2.3.2 Volume 2: MSaaS Discovery Service and Metadata

Volume 2 [7] discusses information and standards related to the description of services and exchange of metadata. More specifically, it:

- Provides an overview of standards related to services discovery and metadata; and
- Presents national initiatives related to the exchange of service metadata, and to create information models that support the (automated) composition, deployment and execution of simulation environments.

This volume relates to several architecture building blocks in the MSaaS RA, such as the M&S Composition Services for automated composition, deployment and execution; and the M&S Model Repository Services for metadata standards.

2.3.3 Volume 3: MSaaS Engineering Processes

Volume 3 [8] discusses the MSaaS Engineering Process (EP). The MSaaS-EP is executed within an existing MSaaS Implementation in order to build a Composed Simulation Service that is compliant with the MSaaS RA described in Ref. [6].

The services used during the MSaaS-EP to construct a Composed Simulation Service are catalogued by the M&S Registry Services. Ref. [7] defines metadata standards that allow service discovery in and MSaaS implementation.

The MSaaS-EP mirrors the IEEE Recommended Practice for Distributed Simulation Engineering and Execution Process (DSEEP) [4]. If the MSaaS-EP is executed in a multi-architecture environment, it will also mirror the DSEEP Multi-Architecture Overlay (DMAO) [3].

2.3.4 Volume 4: MSaaS Experimentation

MSG-136 performed several experiments to test enabling technology for MSaaS. Two strands of experimentation were performed:

1) Experimentation to explore and test enabling technology for architecture building blocks from the reference architecture; and
2) Experimentation to test solutions for certain types of Simulation Services.

Test cases were defined, tests performed, and test results recorded in an experimentation report [9]. A brief overview of the experimentation and test cases follows below.

2.3.4.1 Explore and Test Enabling Technology

Most test cases in this strand of experimentation evolve around container technology as the enabling technology for a number of architecture building blocks. This technology enables M&S Enabling Services and M&S Specific Services to run on a local host as well as in a cloud environment.

The experiment environment that was used for the test cases is illustrated in Figure 2-6. The experiment environment is a collection of private clouds and a common cloud. The common cloud is Amazon Web Service (AWS), sponsored by NATO CSO.

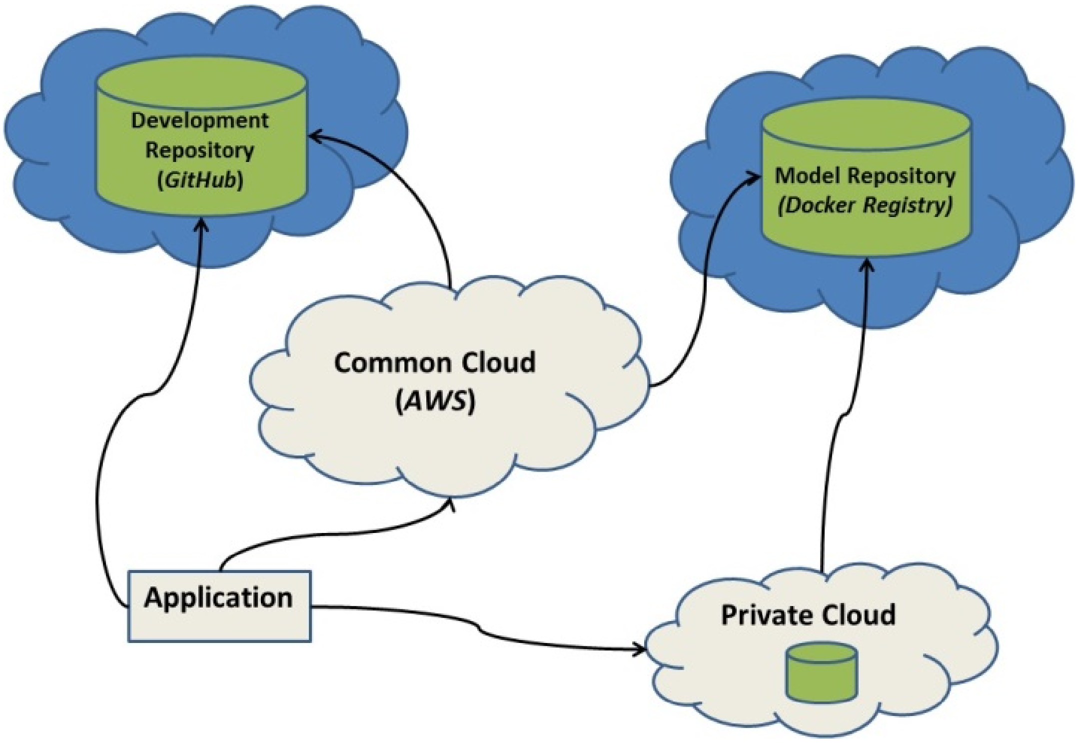

Figure 2-6: Illustration of Experiment Environment.

Common components are:

- A private Docker Registry and a web-based front-end for the exchange of Docker container images (provided by NLD); and
- A private GitHub repository for the description of container images in the Docker Registry, and for the exchange of software, configuration files and other developmental data (provided by USA).

The Docker Registry contains several container images for containerized HLA federates, from which various compositions can be created for the different test cases. Many of these images have been created following the design patterns in Ref. [18].

Test cases include:

- Container networking: explore different container networking models for connecting containerized HLA federate applications.
- Containerization of HLA federates: evaluate approaches in containerizing HLA federate applications (see also Ref. [18]).
- Metadata Repositories and Discovery: Demonstrate interoperation of repositories across nations.
- Simulation Composition: explore automated composition and execution of services.
- Container Orchestration Environments: evaluate two popular container orchestration environments for M&S (see also Ref. [19]).

2.3.4.2 Test Solutions for Simulation Services

Tests cases in this strand of experimentation concern the interoperation of applications with certain types of Simulation Services. Test cases include:

- Computer Generated Forces (CGF) – Synthetic Environment Service: connect a CGF simulator to a Synthetic Environment Service to request environment data in various formats.
- C2 Application – Route Planning Service: connect a C2 Application to a Route Planning Service to request route planning information.

2.4 MSaaS GOVERNANCE POLICIES

2.4.1 Governance and Roles

A challenging aspect of establishing a persistent capability like the Allied Framework for MSaaS is to develop an effective governance model. Governance ensures that all of the independent service-based efforts (i.e., design, development, deployment, or operation of a service) combined will meet customer requirements.

MSG-136 developed policies, processes, and standards for managing the lifecycle of services, service acquisitions, service components and registries, service providers, and consumers. These will be published as Allied Modelling and Simulation Publication AMSP-02 [2] and define the Allied Framework for Modelling and Simulation as a Service (MSaaS) Governance Policies.

The NMSG is the delegated NATO authority for M&S standards and procedures. Nations are encouraged to use the standards nationally or in other multi-national collaborations. After completion of the MSG-136 task group, the NMSG M&S Military Operational Requirements Subgroup (MORS) will become custodian of AMSP-02. MORS is the custodian of best practices with regards to the use of M&S in the training domain and in other domains. The AMSP-02 will be submitted to MORS for future maintenance, updates and dissemination with respect to operational needs of NATO agencies and national stakeholders.

The NMSG M&S Standards Subgroup (MS3) will become custodian of the MSaaS Technical Reference Architecture, and is responsible for the maintenance of the MSaaS technical aspects and standards documents.

2.4.2 General Policies

The general policies for instituting governance mechanisms of MSaaS-based solutions are:

- An MSaaS implementation shall comply with the governance policies as identified and established by the governance document.
- An MSaaS solution architecture shall comply with the MSaaS Technical Reference Architecture (see Section 3, Technical Concept).
- Any M&S service shall conform to the practices and recommendations for Integration, Verification and Compliance Testing as defined by NATO MSG-134 [13].

The ability to effectively manage all stages of the service lifecycle is fundamental to the success of governing M&S services. The Service Lifecycle Management Process contains a set of controlled and well-defined activities performed at each stage for all versions of a given service. Table 2-3 lists the sequential service provider lifecycle stages.

Table 2-3: Service Provider Lifecycle Stages.

Lifecycle Stage	Description
Proposed	The proposed service's needs are identified and assessed as to whether needs can be met through the use of services.
Definition	The service's requirements are gathered and the design is produced based on these requirements.
Development	The service specifications are developed and the service is built.
Verification	The service is inspected and/or tested to confirm it is of sufficient quality, complies with the prescribed set of standards and regulations, and is approved for use.
Production	The service is available for use by its intended consumers.
Deprecated	The service can no longer be used by new consumers.
Retired	The service is removed from the Allied Framework and is no longer used.

All service providers shall define levels for each service (e.g., regarding availability, etc.). Service Providers and users shall agree on a Service Level Agreement (SLA) prior to usage. Service providers are required to indicate the forecasted retirement date of a specific version of a service.

2.4.3 Security Policies

The approach to ensuring security is intrinsically related to the cloud computing service model (SaaS, PaaS, or IaaS) and to the deployment model (Public, Private, Hybrid, or Community) that best fits the Consumer's missions and security requirements. The Consumer must evaluate the particular security requirements in the specific architectural context, and map them to proper security controls and practices in technical, operational, and management classes. Even though the Cloud Security Reference Architecture [15] inherits a rich body of knowledge of general network security and information security, both in theory and in practice, it also addresses the cloud-specific security requirements triggered by characteristics unique to the cloud, such as decreased visibility and control by consumers. Cloud security frameworks including information management within an infrastructure shall support the cloud implementers, providers and consumers [11]. However, MSG-136 recognizes that a more tailored approach may be needed to exploit MSaaS specific capabilities and proposes to develop additional guidelines as part of follow-on work.

2.4.4 Compliancy Policies

Compliancy testing of individual components of a NATO or multi-national simulation environment is the ultimate responsibility of the participating organizations. Currently, NMSG and its support office (MSCO) do not provide compliancy testing services or facilities. Some existing HLA certification tools and services cover only basic testing (i.e., HLA Rules, Interface Specification and Object Model Template (OMT) compliance) and do not provide in-depth functional testing that is needed to support federation integration and validation. The available tools are also outdated. The current NMSG activity MSG-134 is addressing the next generation of compliancy testing and certification needs for HLA [13].

Chapter 3 – MSaaS EVALUATION

Evaluation focusses on whether MSaaS will reduce costs and integration time for creating a new instance of a training environment, compared to what it costs today. What is the main advantage of having an MSaaS-based environment? Evaluation should answer the above questions objectively based on measurements that have been performed and data that has been gathered.

All evaluation results are captured in the MSaaS Concept and Reference Architecture Evaluation Report [5].

3.1 PURPOSE OF EVALUATION

The purpose of the evaluation is to determine if the MSaaS concept offers both feasible and tangible improvement to the establishment of synthetic training environments as a service. The evaluation process will employ qualitative and quantitative methods to determine and measure value. The purpose of the evaluation is also to support the continuation of investigation and development by providing specific evidence based analysis of:

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

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

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

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

3.2 APPROACH

The approach to the evaluation of MSaaS includes the activities presented in the sub-sections below.

3.2.1 Question Preparation

1) Review the MSaaS Operational Concept Document (OCD) and identify the desired effects intended to be achieved when MSaaS is implemented.
2) Elaborate these effects as system and/or capability Measures of Effectiveness (MoE).
3) Prioritize the relative importance of the MoEs and establish an MSaaS hierarchy of needs. Refine the definition of the most significant MoEs that will guide the conceptual development of MSaaS.

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

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

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

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

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

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

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

3.2.2 Gather Feedback

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

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

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

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

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

3.2.3 Perform Analysis

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

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

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

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

3.2.4 Provide Recommendations

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

3.3 STAKEHOLDERS

The M&S community of interest surveyed in this evaluation consisted of members from the following agencies (see Table 3-1).

Table 3-1: Statistics of Survey Participants.

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

3.4 MSAAS MEASURES OF EFFECTIVENESS

There are many qualities that can be the subject of an evaluation. As one of the preconditions of the evaluation, the primary qualities to examine have been agreed upon. The most common ones have been defined as MSaaS Measures of Effectiveness and are identified in Table 3-2.

Table 3-2: MSaaS Measures of Effectiveness.

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

Key MoEs	Factors and Considerations
Supportability	Online help and failover/monitoring/documentation.
Suitability	Ability to sandbox several sim environments to select the most suitable.

3.5 EVALUATION EVENTS

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

The experiment will consist of a set of trials, each aimed at specific use cases that expose key MSaaS capabilities and explore architecturally significant requirements. The experiments set out in Volume 4 (Experimentation Report) [9] were demonstrated at a series of public events over the period 2016 – 2017. These demonstrations were accompanied with explanatory presentations, and provided a forum to engage independent opinion and obtain feedback from industry, military and government. These events included:

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

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

3.6 EVALUATION RESULTS

3.6.1 Stakeholder Feedback

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

3.6.2 Analysis of Results

The stakeholder feedback underwent analysis to identify any and all new or existing qualitative measures, to compare with the internal assessment performed by MSG-136. This information was merged with the internal assessment to provide a broader market assessment of the key system and capability benefits, and the most important limitations or concerns (see Table 3-3).

Table 3-3: MSaaS Key Benefits and Limitations.

Key System Benefits	Key Capability Benefits	Key Limitations
Affordability (24)	Suitability / Improved Training Outcomes (30)	Security/Vulnerability (10)
Coherence (20)	Increased Accessibility (26)	Supportability (7)
Scalability (15)	Increased Availability (11)	Roadmap (6)
Reusability (7)	Increased Usability (5)	Governance (4)
Flexibility (7)	On Demand (3)	Trust (4)
Composability (2)	Improved Interoperability (3)	Performance (4)
Modularity (2)	Reduced Manpower (2)	Business Model (3)
Earlier Runtime	Increased Functionality (2)	
Open Source	Commonality	
Load Balancing	Improved Fair Fight	
Automation	Increased Maintainability	
Consolidation		

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

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

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

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

3.6.2.1 Analysis of Accessibility

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

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

3.6.2.2 Analysis of Suitability

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

There is a big drive from the simulation user community to understand how simulation capabilities can be developed to meet current and future operating environments (areas of interest include whole world terrain, human terrain, operational scenarios, hybrid/information warfare, megacities, non-lethal/non-kinetic effects, ORBATS, equipment, platforms, communications systems, UAVs, etc.) and use should not be limited by the simulation technology (e.g., scaling to millions of entities may be required to meet a particular requirement should be possible if required). So MSaaS needs to demonstrate how the modular aspect of the framework and elastic nature of the cloud can enable simulation systems to stay current and meet complex operational environments in order to gain traction with the user community. The approach also needs to be integrated with existing/future host infrastructure and ways of working so as not to have a negative impact on other areas (e.g., integration with networks, command and control environments, training information management systems, operational analysis toolsets, After Action Review tools, Live and Virtual systems as well as constructive).

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

3.6.2.3 Analysis of Affordability

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

3.7 RECOMMENDATIONS

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

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

b) 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.

c) 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.

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

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

f) 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.

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

h) 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.

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

j) 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.

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

   i) Increased Operational Effectiveness (e.g. increased readiness).

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

   iii) 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.

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

v) 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.

l) Continue to monitor challenges and recommendations from the on-going CWIX events, and address the recognized need for the following MSaaS capabilities:

i) Federation management service.

ii) Increased automation in composition and scenario planning.

iii) Improved diagnostic capabilities and information reporting services.

Chapter 4 – CONCLUSIONS AND RECOMMENDATIONS

This chapter provides conclusions and recommendations for the way forward.

4.1 CONCLUSIONS

MSG-136 investigated the concept of M&S as a Service (MSaaS) with the aim of providing the technical and organizational foundations to establish the *Allied Framework for M&S as a Service* within NATO and partner nations. MSG-136 defined the *Allied Framework for M&S as a Service* as the common approach of NATO and nations towards implementing MSaaS, covering discovery, composition, execution, and management of M&S services. The *Allied Framework for M&S as a Service* is defined by the following documents:

- Operational Concept Document;
- Technical Reference Architecture (including service discovery, engineering process and experimentation documentation); and
- Governance Policies.

Technical implementations of MSaaS have been developed and evaluated in several experiments, demonstrations and initial operational applications.

The experimentation results and initial 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. The conclusion is that MSaaS is a promising innovation towards more accessible and more cost effective M&S capabilities.

MSaaS is a key enabler to achieve the vision and objectives defined in the NATO M&S Master Plan [12], which is to "exploit M&S to its full potential across NATO and the Nations to enhance both operational and cost effectiveness".

4.2 WAY FORWARD

Many nations and NATO organizations are currently implementing MSaaS using cloud technology, based on the MSG-136 research and experimentation efforts and results. MSG-136 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.

MSG-136 proposes an incremental development and implementation strategy for the Allied Framework for M&S as a Service. The incremental approach facilitates a smooth transition in the adoption of an Allied Framework for M&S as a Service 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 the 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 providing lessons learned and advice to those nations considering similar investments.

As illustrated in Figure 4-1, the implementation strategy is broken down into three phases:

- **Phase 1 "Initial Concept Development"**

  The Initial Concept Development (2015 until end of 2017) is executed by NMSG-136 and consists of concept development and initial experimentation. In this phase M&S services are provided by individual members of MSG-136 for trial use.

- **Phase 2 "Specification & Validation"**

  From 2018 – 2021 the initial concepts are extended by NMSG-164 (i.e., specification of issues and challenges not yet addressed) and validated through regular exercise participation and dedicated evaluation events. This phase includes transformation of governance policies into STANAGs or STANRECs, and moving from prototype implementation to operationally usable and mature systems.

  By 2020 Initial Operational Capability (IOC) is established, being defined as an MSaaS solution that is available to an initial set of users. Specifically, IOC will be demonstrated 2020 as part of Trident Jupiter 2020 and 2021 as part of Viking 21.

- **Phase 3 "Implementation"**

  By 2025 Full Operational Capability (FOC) is achieved which includes adaptation of many existing simulation related services to the MSaaS Reference Architecture. This is achieved primarily by adding services to the Allied Framework for M&S as a Service.

  FOC requires that a permanent MSaaS solution (infrastructure, organization, etc.) is established and that it is available to all interested users.

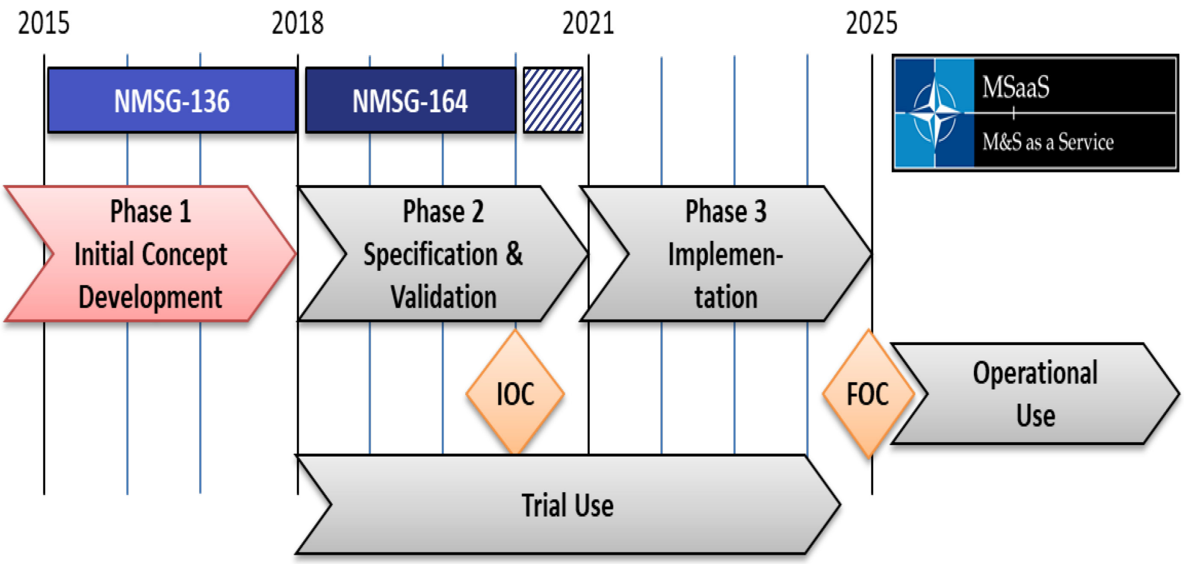

Figure 4-1: MSaaS Implementation Strategy.

MSG-136 developed a Technical Activity Proposal (TAP) to address Phase 2. The TAP was approved by the NSMG in Fall 2017, and accordingly MSG-164 will focus on two main work streams:

1) To advance and to promote the operational readiness of M&S as a Service.

2) To investigate critical research and development topics to further enhance the benefits of M&S as a Service.

Service-based approaches rely on a high degree of standardization and automation in order to achieve their goals. Therefore the development and implementation of a recommended set of supporting standards is critical. MSG-136 research has identified the importance for the following capabilities:

- M&S Composition Services: create and execute a simulation composition. A composition can be created from individual simulation services or from smaller compositions.
- M&S Repository Services: store, retrieve and manage simulation service components and associated metadata that implement and provide simulation services, in particular metadata for automated composition.
- M&S Security Services: implement and enforce security policies for M&S services.

MSG-164 will continue to participate in the SISO Cloud-based M&S Study Group and share its approach and experiences. The goal is that MSG-164 will contribute to a set of open standards and recommendations for MSaaS.

4.3 RECOMMENDATIONS

In alignment with the conclusions and the proposed way forward, MSG-136 makes the following recommendations:

1) NATO and nations should implement the Allied Framework for MSaaS. Especially it is recommended to permanently establish the required infrastructure (e.g., cloud computing resources) and to establish a permanent governance body (including required personnel).
    a) For NATO it is recommended to adapt Core Sim 2020 Capability Package to fully align with the Allied Framework for MSaaS and to cover required infrastructure and personnel.
2) NATO and nations should conduct activities to increase the operational readiness of MSaaS through participation in MSG-164:
    a) NATO and nations should start using MSaaS in operational environments (e.g., exercises).
    b) In the spirit of "pooling and sharing" it is strongly recommended that NATO and nations share information and provide access to M&S resources through the interim Allied Framework for MSaaS as provided by MSG-164.
    c) Conduct research activities to increase the Technology Readiness Level of the supporting services and tools. Example topics to be addressed include cyber security, service composition and business models.

Chapter 5 – REFERENCES

[1] NATO: NATO Modelling and Simulation Standards Profile. AMSP-01, Edition (D), Version 1. September 2017.

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

[3] IEEE 1730.1-2013: IEEE Recommended Practice for Distributed Simulation Engineering and Execution Process Multi-Architecture Overlay (DMAO).

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

[5] NATO STO: MSaaS Concept and Reference Architecture Evaluation Report. STO Technical Report STO-TR-MSG-136-Part-II. To be published.

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

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

[8] NATO STO: Modelling and Simulation as a Service, Volume 3: Reference Engineering Process. STO Technical Report STO-TR-MSG-136- Part-VI. To be published.

[9] NATO STO: Modelling and Simulation as a Service, Volume 4: Experimentation Report. STO Technical Report STO-TR-MSG-136-Part-VII. To be published.

[10] NATO: Final Report of MSG-131 "Modelling and Simulation as a Service: New Concepts and Service Oriented Architectures". STO Technical Report TR-MSG-131, Document AC/323(MSG-131)TP/608. May 2015.

[11] NATO Consultation, Command and Control Board (C3B): "NATO Cloud Computing Policy", AC/322-D(2016)0001, 7 January 2016.

[12] NATO: NATO Modelling and Simulation Master Plan, Version 2.0, 14 September 2012, Document AC/323/NMSG(2012)-015.

[13] NATO STO: Final Report of NATO MSG-134 "NATO Distributed Simulation Architecture & Design, Compliance Testing and Certification". To be published.

[14] NATO C3 Classification Taxonomy, Baseline 1.0, NATO Allied Command Transformation (ACT) C4ISR Technology and Human Factors (THF) Branch, 15 June 2012.

[15] National Institute of Standards and Technology: NIST Cloud Computing Security Reference Architecture, NIST Special Publication 500-299, Draft, 15 May 2013.

[16] SOA Reference Architecture, C119, Open Group Standard, 2011.

[17] STANAG 4603 Edition 2, Modeling and Simulation Architecture Standards for Technical Interoperability: HLA, NATO Standardization Office, 17 February 2015.

[18] T.W. van den Berg, A. Cramp, B. Siegel, "Guidelines and best practices for using Docker in support of HLA federations", 2016-SIW-031; SISO SIW Fall 2016.

[19] T.W. van den Berg, A. Cramp, "Container orchestration environments for M&S", 2017-SIW-006; SISO SIW Fall 2017.

Annex A – MEETINGS

MSG-136 held 10 face-to-face meetings. Dates and locations are recorded in Table A-1.

Table A-1: MSG-136 Face-to-Face Meetings.

Nr	Host	Location	Dates
1	CSO	Neuilly-sur-Seine, FRA	10-12 November 2014
2	TNO	The Hague, NLD	23-26 February 2015
3	Dstl	London, GBR	15-18 June 2015
4	ACT	Virginia Beach, USA	26-30 October 2015
5	TNO	Leiden, NLD	8-12 February 2016
6	JWC	Stavanger, NOR	6-10 June 2016
7	Lockheed Martin	Orlando, USA	7-11 November 2016
8	M&S COE	Rome, ITA	20-24 February 2017
9	M&S COE	Rome, ITA	19-23 June 2017
10	Danish Defence Acquisition and Logistics Organization	Copenhagen, DNK	6-10 November 2017

In addition to the above mentioned face-to-face meetings MSG-136 extensively used web meetings in between these meetings. Especially, the TEK sub-group conducted web meetings every 2 weeks to track progress and discuss current issues.

Annex B – DISSEMINATION

MSG-136 members were very active in promoting task group results and interacting with all potentially relevant communities of interest. This annex tries as much as possible to provide an overview about all MSG-136 related dissemination activities.

B.1 JOURNAL PUBLICATIONS

1) Tom van den Berg, Barry Siegel, Anthony Cramp, “Containerization of High Level Architecture based simulations: A Case Study”, The Journal of Defense Modeling and Simulation (JDMS), Vol 14, Issue 2, pp. 115-138, First Published September 15, 2016. https://doi.org/10.1177/1548512916662365.

2) Jo Erskine Hannay, “Architectural work for Modeling and Simulation combining the NATO Architecture Framework and C3 Taxonomy”, The Journal of Defense Modeling and Simulation (JDMS), Vol 14, Issue 2, pp. 139-158, First Published November 14, 2016. https://doi.org/10.1177/1548512916670785.

3) Saikou Y. Diallo, Ross Gore, Jose J. Padilla, Hamdi Kavak, Christopher J. Lynch, “Towards a World Wide Web of Simulation”, The Journal of Defense Modeling and Simulation (JDMS), Vol 14, Issue 2, pp. 159-170, First Published December 29, 2015. https://doi.org/10.1177/1548512915621974.

4) Erdal Cayirci, Lütfü Özcakir, “Modeling and Simulation Support to the Defence Planning Process”, The Journal of Defense Modeling and Simulation (JDMS), Vol 14, Issue 2, pp. 171-180, First Published November 7, 2016. https://doi.org/10.1177/1548512916675433.

5) Jose-Ramon Martinez-Salio, “Sandbox deployment model for services in modeling and simulation as a service”, The Journal of Defense Modeling and Simulation (JDMS), Vol 14, Issue 2, pp. 181-191, First Published December 16, 2016. https://doi.org/10.1177/1548512916680916.

6) Jo Hannay, Karsten Brathen, Ole-Martin Mevassvik, “A Hybrid Architecture Framework for Simulations in a Service-Oriented Environment”, Systems Engineering 20(3), pp. 235-256, Wiley, 2017.

7) Jo Hannay, Karsten Brathen, Ole-Martin Mevassvik, “Agile requirements handling in a service-oriented taxonomy of capabilities”, Requirements Engineering 22(2), pp. 289-314, Springer, 2017.

B.2 CONFERENCE PAPERS

1) Robert Siegfried, “Von isolierten Anwendungen zur allgegenwärtigen Trainings-Cloud”, Presentation at DWT Symposium on Simulation and Training, March 2015, Bad Godesberg, DEU.

2) Robert Siegfried, Tom van den Berg, “An overview of the standards landscape for M&S as a Service”, 4th SISO seminar at ITEC 2015, 27 April 2015, Prague, CZE.

3) Robert Siegfried, “M&S as a Service: Expectations and Challenges”, Workshop at SimTecT 2015, 17 August 2015, Adelaide, AUS.

4) Robert Siegfried, Tom van den Berg, “M&S as a Service: Emerging Approach and Standards Activities”, Invited Presentation at SISO Fall SIW 2015, 01 September 2015, Orlando, FL (USA).

5) Tom van den Berg, Robert Lutz, “Simulation environment architecture development using the DoDAF”, SISO Fall SIW 2015, Paper 15F-SIW-019, September 2015, Orlando, FL (USA).

6) Robert Siegfried, Tom van den Berg, “M&S as a Service: Paradigm for Future Simulation Environments”, Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2015, December 2015, Orlando, FL (USA).

7) Robert Siegfried, Michael Mifsud, “NATO MSG-136: M&S as a Service”, Demonstration at Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2015, December 2015, Orlando, FL (USA).

8) Robert Siegfried, “Switching to a New Paradigm – Modelling & Simulation as a Service”, Military Technology, Issue 04/2016.

9) Robert Siegfried, “NATO MSG-136: M&S as a Service”, Briefing at ITEC 2016, 18 May 2016, London, GBR.

10) Katherine Morse, Michael Bertschik, Andy Bowers, Marco Picollo, “Developing Service Discovery Metadata to Support Modeling and Simulation as a Service”, SISO Fall SIW 2016, Paper 2016-SIW-011, September 2016, Orlando, FL (USA). Best Paper Award (SIWzie).

11) Tom van den Berg, Anthony Cramp, Barry Siegel, “Guidelines and best practices for using Docker in support of HLA federations”, SISO Fall SIW 2016, Paper 2016-SIW-031, September 2016, Orlando, FL (USA).

12) Tom van den Berg, Jo Hannay, Barry Siegel, “Towards a Reference Architecture for M&S as a Service”, SISO Fall SIW 2016, Paper 2016-SIW-011, September 2016, Orlando, FL (USA).

13) Robert Siegfried, “M&S as a Service to meet Increasing Training Demands”, Presentation at NATO CAX Forum 2016, 20 September 2016, Ottobrunn, DEU.

14) Anthony Cramp, Tom van den Berg, “An Introduction to Using Docker in Support of HLA Federations”, SimTecT, September 2016, Melbourne, AUS.

15) Billings, Amy Grom, Barry Siegel, Mike Douklias, Andy Bowers, Blount, “Joint Training Implementation of Modeling and Simulation (M&S) as a Service (MSaaS)”, Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2016, December 2016, Orlando, FL (USA).

16) Jon Lloyd, Keith Ford, Simon Skinner, “Common non run-time simulation services – lessons from UK MOD research”, Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2016, December 2016, Orlando, FL (USA).

17) Marco Biagini, Michele La Grotta, Fabio Corona, Forconi, Marco Picollo, Christian Faillace, “NATO MSaaS – A Comprehensive Approach for Military Operational Requirements Development”, Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2016, December 2016, Orlando, FL (USA).

18) Erdal Cayirci, Hakan Karapinar, Lütfü Ozcakir, “hTEC: A Layered MSaaS Architecture for Training and Experimentation Cloud”, Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2016, December 2016, Orlando, FL (USA).

19) Hammar, Peter Lindskog, “MSaaS – Automated Support for Producing Reports in Command Post Exercises”, Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2016, December 2016, Orlando, FL (USA).

20) Andrea D'Ambrogio, Paolo Bocciarelli, Antonio Mastromattei, A PAAS-Based framework for automated performance analysis of service-oriented systems, Proceedings of the 2016 Winter Simulation Conference, T.M.K. Roeder, P.I. Frazier, R. Szechtman, E. Zhou, T. Huschka, and S.E. Chick, eds., pp. 931-942, Washington, DC (USA), December 11-14, 2016.

21) Tom van den Berg, Wim Huiskamp, Robert Siegfried, Jon Lloyd, Amy Grom, Robbie Phillips, "Modelling and Simulation as a Service: Rapid deployment of interoperable and credible simulation environments – an overview of NATO MSG-136", SISO SIW 2017, 11-15 September 2017, Orlando, FL (USA).

22) Erdal Cayirci, Hakan Karapinar, Lütfü Özcakir, Erdem Yazgan, "Joint Military Space Operation Services for NATO MSaaS", NATO MSG Symposium 2017, MSG-149, 19-20 October 2017, Lisbon, PRT.

23) Erdal Cayirci, Hakan Karapinar, Lütfü Özcakir, "Joint Military Space Operations Simulation as a Service". In Proceedings of the 2017 Winter Simulation Conference, edited by W.K.V. Chan, A. D'Ambrogio, G. Zacharewicz, N. Mustafee, G. Wainer, and E. Page. Las Vegas, NV (USA).

24) Dalibor Procházka, Jan Hodický, "Modelling and Simulation as a Service and Concept Development and Experimentation", 2017 International Conference on Military Technologies (ICMT), May 31 – June 2, 2017, Brno, CZE.

25) Jo Hannay, Tom van den Berg, "The NATO MSG-136 Reference Architecture for M&S as a Service", NATO MSG Symposium 2017, MSG-149, 19-20 October 2017, Lisbon, PRT.

26) Keith Ford, Jon Lloyd, Neil Smith, "NATO Aligned UK Approach to Modelling & Simulation as a Service", NATO MSG Symposium 2017, MSG-149, 19-20 October 2017, Lisbon, PRT.

27) Daniel Kallfass, Michael Bertschik, Stefan Vrieler, Jo Hannay, Kvernelv, "Proof of concept demonstrator of MSG-136 for using and providing simulation as a service within NATO environments", NATO MSG Symposium 2017, MSG-149, 19-20 October 2017, Lisbon, PRT.

28) Ralf Stüber, "SEDRIS on the Test Bench – The Future of Exchanging Environmental Data to become Part of M&S as a Service", NATO MSG Symposium 2017, MSG-149, 19-20 October 2017, Lisbon, PRT.

29) Paolo Bocciarelli, Andrea D'Ambrogio, Andrea Giglio, Antonio Mastromattei, "Automated development of web-based modeling services for MSaaS platforms", Proceedings of the 2017 SCS Spring Simulation Multi-Conference, Simulation Series, 49 (7), pp. 80-91, Virginia Beach, VA (USA), April 23-26, 2017.

30) Paolo Bocciarelli, Andrea D'Ambrogio, Andrea Giglio, Antonio Mastromattei, Emiliano Paglia, "Business process modeling and simulation: State of the art and MSaaS opportunities", Proceedings of the 2017 SCS Summer Simulation Multi-Conference, Simulation Series, 49 (9), pp. 261-272, Seattle, WA (USA), July 9-12, 2017.

B.3 SPECIAL EVENTS, WORKSHOPS, DEMONSTRATIONS, ETC.

1) Robert Siegfried, "Bringing training specialists and M&S experts together: MSG-136 Workshop on M&S as a Service", Workshop at NATO CAX Forum 2016, 20 September 2016, Ottobrunn, Germany.

2) Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2016, December 2016, Orlando, USA:
   - Robert Siegfried, "Cloud-Based Simulation: Fiction or Future?", 2016 Special Event (Panel Debate).
   - MSaaS demonstration at NATO booth.

3) TIDE Sprint Fall 2015, Virginia Beach, VA, USA:
   - Various workshops with different communities of interest and TIDE Sprint tracks.

4) MSaaS Industry Outreach Day, 08 November 2016, Orlando, FL (USA).

5) TIDE Sprint Spring 2017, St. Malo, FRA:
   - Presentation of MSaaS Portal.
   - Presentation of MSaaS Operational Concept.
   - Workshop on MSaaS Governance Policies.

6) NATO Air Force Armaments Group (NAFAG) Topical Meeting, June 2017, Ramstein, DEU:
   - Robert Siegfried, Briefing about NMSG and MSaaS.

7) NATO CAX Forum 2017, Florence, ITA:
   - Live demonstration of MSaaS for operational target audience.

8) TIDE Sprint Fall 2017, Virginia Beach, VA, USA:
   - Joint session with IT Service Management track to discuss MSaaS governance policies and IT service management aspects.

9) Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2017, November 2017, Orlando, USA:
   - Robert Siegfried, "Cloud-Based Simulation: Hype or Reality?", 2017 Special Event (Panel Debate).
   - Six MSaaS demonstrations (partially, live demonstrations) at NATO booth.

Annex C – SHARED M&S SERVICES AND RESOURCES

In the spirit of "pooling and sharing resources", MSG-136 members shared M&S services and resources, thus contributing to a joint set of resources and capabilities following the MSaaS concept. The following list provides an overview of services and resources shared by MSG-136 members. The container images are described in Ref. [9].

Table C-1: MSaaS Resources Contributions by MSG-136 Members.

Nr	Nation	Provider	M&S Service / Resource Description
1	AUS	DSTG	Containerized images for: • Ship Simulation, Ship User Interface, Munition Simulation, MaK CRC, MaK LRC
2	DEU	aditerna GmbH	aditerna SRP
		CPA ReDev GmbH	Containerized images: • Synthetic Environment Service and data for Meppen area and Gulf area
3	DNK	IFAD	Containerized images: • Symbol services, DIS/HLA Gateway, Data Recorder
4	NLD	TNO	Containerized images for e.g.: • Damage Server, Sensor Server, KML Server, VR-Forces, Google Earth, Google Chrome, MSaaS Portal, Pitch CRC, Pitch LRC, Pitch Recorder, Pitch DIS/HLA Adapter, Time Pacer, XServer, System Logger, Portico LRC
		TNO	MSaaS Docker Registry
5	NOR	FFI	Route Planning Service
6	SWE	Pitch	Licenses for Pitch products
7	USA	LMCO	Containerized images: • EPIC
8	USA	Spawar	Private GitHub repository
9	NATO	CSO	Funding for AWS Cloud Computing infrastructure

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TR-MSG-136-Part-I AC/323(MSG-136)TP/826	ISBN 978-92-837-2154-3	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 (MSaaS) – Rapid Deployment of Interoperable and Credible Simulation Environments

7. Presented at/Sponsored by

Final Report of NATO MSG-136.

8. Author(s)/Editor(s)	9. Date
Multiple	October 2018

10. Author's/Editor's Address	11. Pages
Multiple	60

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

13. Keywords/Descriptors

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

14. Abstract

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

MSG-136 evaluated the MSaaS concept in various experiments. The experimentation results and initial 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-136 strongly recommends NATO and nations to advance and to promote the operational readiness of M&S as a Service, and to conduct required Science and Technology efforts to close current gaps.

NORTH ATLANTIC TREATY ORGANIZATION

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

SCIENCE AND TECHNOLOGY ORGANIZATION

DIFFUSION DES PUBLICATIONS
STO NON CLASSIFIEES

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

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

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

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

CENTRES DE DIFFUSION NATIONAUX

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

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

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

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

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

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

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

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

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

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

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

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

LUXEMBOURG
Voir Belgique

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

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

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

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

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

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

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

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

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

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

AGENCES DE VENTE

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

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

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

NORTH ATLANTIC TREATY ORGANIZATION

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

SCIENCE AND TECHNOLOGY ORGANIZATION

DISTRIBUTION OF UNCLASSIFIED STO PUBLICATIONS

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

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

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

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

NATIONAL DISTRIBUTION CENTRES

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

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

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

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

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

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

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

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

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

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

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

LUXEMBOURG
See Belgium

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

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

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

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

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

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

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

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

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

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

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

SALES AGENCIES

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

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

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

ISBN 978-92-837-2154-3