NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(MSG-131)TP/608

www.sto.nato.int

STO TECHNICAL REPORT **TR-MSG-131**

Modelling and Simulation as a Service: New Concepts and Service-Oriented Architectures

(Modélisation et simulation en tant que service : Nouveaux concepts et architectures orientés service)

Final Report of Specialist Team MSG-131.

Published May 2015

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(MSG-131)TP/608

www.sto.nato.int

STO TECHNICAL REPORT **TR-MSG-131**

Modelling and Simulation as a Service: New Concepts and Service-Oriented Architectures

(Modélisation et simulation en tant que service : Nouveaux concepts et architectures orientés service)

Final Report of Specialist Team MSG-131.

The NATO Science and Technology Organization

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

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

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

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

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

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

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

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

Published May 2015

ISBN 978-92-837-2006-5

Table of Contents

List of Figures

List of Tables

MSG-131 Membership List

Full Name	Nation	Organization Type	Email	Role
ALLEN Gary (Dr.)	USA	Government	gary.w.allen3.civ@mail.mil	Member
BEHNER Horst (TRDir.)	DEU	Government	horstbehner@bundeswehr.org	Member
BELINCHON Carlos (Maj.)	ESP	Government	cbelpin@et.mde.es	Observer
BERRY Daniel (Mr.)	USA	NATO Staff	daniel.berry@act.nato.int	Observer
BERTSCHIK Michael (Dr.)	DEU	Government	MichaelBertschik@bundeswehr.org	Member
CALVEZ Pierre (Mr.)	FRA	NATO Staff	pierre.calvez@ncia.nato.int	Observer
CARNELL Joseph (Mr.)	USA	Government	joseph.a.carnell.ctr@mail.mil	Observer
COURETAS Jerry (Dr.)	USA	Industry	jerry.m.couretas.ctr@mail.mil	Observer
CRAMP Anthony (Dr.)	AUS	Government	Anthony.Cramp@dsto.defence.gov.au	Member
DAVID Walter (Maj.)	ITA	Government	walter.david@esercito.difesa.it	Observer
DIEHL Andreas (Dr.)	DEU	Government	andreasdiehl@bundeswehr.org	Member
FERNANDEZ-VEGA José B. (Maj.)	ESP	Government	jbvega@ea.mde.es	Member
FORD Keith (Dr.)	GBR	Industry	keith.ford@uk.thalesgroup.com	Observer
GALAN Sergio (Mr.)	ESP	Other	sgcubero@isdefe.es	Observer
GIACOMOZZI Stefano (Lt. Col.)	ITA	NATO Staff	mscoe.ds02@smd.difesa.it	Observer
GOMEZ-RAMOS Francisco (LtCol.Dr.)	ESP	NATO Staff	francisco.gomez-ramos@cso.nato.int	Wise Observer
GONZALEZ GODOY Sabas (Mr.)	ESP	Government	Sabas.Gonzalez@act.nato.int	Observer
HANNAY Jo (Dr.)	NOR	Government	jo.hannay@ffi.no	Member
HAUSSMANN Stephen (Mr.)	USA	Industry	stephen.j.haussmann.ctr@mail.mil	Observer
HODICKY Jan (LTC.)	CZE	NATO Staff	jan.hodicky@unob.cz	Observer
HUISKAMP Wim (Mr.)	NLD	Industry	wim.huiskamp@tno.nl	Member
JENSE Hans (Dr.)	NLD	NATO Staff	hans.jense@ncia.nato.int	Observer
KOSTOFF John (Mr.)	USA	Government	John.s.kostoff.civ@mail.mil	Observer
KRARUP-HANSEN Niels (Mr.)	DEN	Government	nkh@mil.dk	Member

Full Name	Nation	Organization Type	Email	Role
MANDA Vladimir (Mr.)	CZE	NATO Staff	vladimir.manda@ncia.nato.int	Observer
MAUGET Régis (Mr.)	FRA	Industry	regis.mauget@capgemini.com	Observer
MILLER Brian (Mr.)	USA	Government	brian.s.miller116.civ@mail.mil	Co-Chair
MOCK Sherrel (Mr.)	USA	Government	sherrel.w.mock.ctr@mail.mil	Observer
MURSIA Agatino (Ing.)	ITA	Industry	agatino.mursia@selex-es.com	Member
NASCA Francesco (LtCol.)	ITA	Government	mscoe.cd04@smd.difesa.it	Member
OBERNDORFNER Michael (Mr.)	DEU	NATO Staff	Michael.Oberndorfner@ncia.nato.int	Observer
PATEL Bharatkumar (Mr.)	GBR	Government	bmpatel@dstl.gov.uk	Member
PICOLLO Marco (Mr.)	ITA	Industry	marco.picollo@selex-es.com	Member
PIERZCHALA Dariusz (Dr.)	POL	Academia	dpierzchala@wat.edu.pl	Member
ROACH Scott (Kevin John) (Maj.)	CAN	Government	SCOTT.ROACH1@forces.gc.ca	Member
ROTHER Martin (Dr.)	DEU	Industry	rother@iabg.de	Member
SAN JOSE MARTIN Angel (Mr.)	ESP	NATO Staff	Angel.SanJoseMartin@act.nato.int	Member
SIEGEL Barry (Mr.)	USA	Government	Barry.Siegel@navy.mil	Observer
SIEGFRIED Robert (Dr.)	DEU	Industry	robert.siegfried@aditerna.de	Co-Chair
SMITH Neil (Mr.)	GBR	Government	nsmith@dstl.gov.uk	Member
TARD Laurent (Col.)	FRA	Government	laurent.tard@defense.gouv.fr	Member
TIMMONS Colin (Capt.)	CAN	Government	COLIN.TIMMONS@forces.gc.ca	Observer
VAN DEN BERG Tom (Mr.)	NLD	Industry	tom.vandenberg@tno.nl	Observer
VAN GEEST Jan (Mr.)	NLD	NATO Staff	Jan.vanGeest@ncia.nato.int	Observer
VOICULET Adrian (Mr.)	ROM	NATO Staff	adrian.voiculet@cso.nato.int	Wise Observer
ZAMOUN Philippe (LtCol.)	FRA	Government	philippe.zamoun@intradef.gouv.fr	Member

Modelling and Simulation as a Service: New Concepts and Service-Oriented Architectures

(STO-TR-MSG-131)

Executive Summary

Modelling and Simulation (M&S) is a key enabler for the delivery of capabilities to NATO and Nations in the domains of training, analysis and decision-making. M&S solutions have to be integrated seamlessly in future computer information systems capabilities to ensure increased efficiency, affordability, interoperability and reusability. Technical developments in the area of Service-Oriented Architectures (SOAs) may offer opportunities for providing M&S solutions that address current NATO critical shortfalls.

The application of a "services" model to Modelling and Simulation, henceforth called "Modelling and Simulation as a Service" (MSaaS), promises to greatly reduce the barriers of cost and accessibility and to result in greater utility of M&S throughout NATO and the Nations.

MSG-131 responds to a request by Nations and ACT to investigate a "NATO MSaaS" technical concept, and to investigate a supporting Reference SOA.

The general approach taken by MSG-131 is to collect experience from Member Nations regarding the use of cloud solutions and service-oriented approaches within the M&S domain. This survey is used to develop a shared understanding of "M&S as a Service" in the NATO context. In addition, the survey provides a comprehensive documentation of MSaaS case studies and provides an overview of existing service-oriented (reference) architectures in the M&S domain. Based on these existing experiences and architectures, conclusions and recommendations are derived on the way forward.

A main conclusion of MSG-131 is that M&S is a critical technology for NATO and the Nations, independent of whether it is provided "as a service" or not. However, service-based approaches to M&S offer many potential benefits. Therefore, an alignment of "M&S as a Service" with the Connected Forces Initiative (CFI) is required, as the primary objective of the CFI (i.e., sharing and pooling of resources) is closely reflected in MSaaS. Similarly, it is required to align M&S and MSaaS with the NATO C3 Classification Taxonomy as this is the primary tool used by NATO to chart the NATO Consultation, Command and Control (C3) landscape.

MSG-131 identified various open issues with regards to MSaaS, spanning a broad range from technical to organizational questions. In accordance with its Technical Activity Description, MSG-131 recommends investigation of MSaaS in more detail. A Technical Activity Proposal for a follow-on Research Task Group was developed by MSG-131 and endorsed in June 2014. The Task Group MSG-136 ("Modelling and Simulation (M&S) as a Service (MSaaS) – Rapid Deployment of Interoperable and Credible Simulation Environments") will start its 3-year term in November 2014.

The NMSG has a formal Technical Cooperation Agreement with SISO on the development of M&S interoperability standards. MSG-131 strongly recommends that MSG-136 continues to engage with the SISO community to investigate areas where MSaaS-related standardization efforts are needed. The hands-on experiences with case studies will provide guidance and candidates for architectures, data models and interfaces that could become future SISO standards.

Modélisation et simulation en tant que service : Nouveaux concepts et architectures orientés service

(STO-TR-MSG-131)

Synthèse

La modélisation et simulation (M&S) est un facilitateur clé en vue de la fourniture de capacités à l'OTAN et aux pays en matière d'entraînement, d'analyse et de prise de décision. Les solutions de M&S doivent être intimement intégrées dans les futurs systèmes informatiques afin de garantir une plus grande efficacité, un moindre coût, une meilleure interopérabilité et une plus grande possibilité de réutilisation. Les progrès techniques dans le domaine des architectures de service (SOA) peuvent être l'occasion de proposer des solutions de M&S palliant les actuelles insuffisances critiques de l'OTAN.

L'application d'un modèle de « services » à la modélisation et simulation, désormais désigné par l'expression « modélisation et simulation en tant que service » (MSaaS), promet de réduire considérablement le coût, d'améliorer l'accessibilité et de rendre la M&S plus utile au sein de l'OTAN et des pays membres.

Le MSG-131 répond à la demande qu'ont exprimée les pays et l'ACT d'étudier un concept technique de « MSaaS de l'OTAN » et une SOA de référence qui s'y rattache.

La démarche générale adoptée par le MSG-131 a consisté à recueillir l'expérience des pays membres en matière d'utilisation des solutions de « cloud » et des approches orientées service dans le domaine de la M&S. La présente étude vise à développer une compréhension commune de la « M&S en tant que service » dans le contexte de l'OTAN. Elle fournit de plus une documentation complète composée d'études de cas et donne un panorama des architectures (de référence) orientées service dans le domaine de la M&S. Ces expériences et ces architectures permettent de tirer des conclusions et de formuler des recommandations sur la marche à suivre.

L'une des principales conclusions du MSG-131 est que la M&S est une technologie cruciale pour l'OTAN et les pays, indépendamment du fait qu'elle soit ou non proposée « en tant que service ». Cependant, les approches de M&S orientées service présentent beaucoup d'avantages potentiels. Par conséquent, un alignement de la « M&S en tant que service » sur l'initiative des forces connectées (CFI) est nécessaire, car la MSaaS reflète assez fidèlement l'objectif premier de la CFI (à savoir, le partage et le groupement des ressources). De même, il convient d'aligner la M&S et la MSaaS sur la taxonomie de classification C3 de l'OTAN, puisqu'il s'agit de l'outil principal qui encadre la consultation, le commandement et le contrôle (C3) de l'OTAN.

Le MSG-131 a identifié plusieurs sujets à débattre au sujet de la MSaaS, qui balaient un large spectre allant des aspects techniques aux questions d'organisation. Conformément à la description de son activité technique, le MSG-131 recommande d'étudier la MSaaS plus en détail. Le MSG-131 a élaboré une proposition d'activité technique en vue d'un groupe de recherche ultérieur, proposition qui a été approuvée en juin 2014. Le groupe de travail MSG-136 (« Modélisation et simulation (M&S) en tant que service (MSaaS) – Déploiement rapide d'environnements de simulation crédibles et interopérables ») entamera son mandat de trois ans en novembre 2014.

Le NMSG a conclu un accord de coopération technique officiel avec la SISO à propos du développement de normes d'interopérabilité de la M&S. Le MSG-131 recommande vivement que le MSG-136 poursuive son

engagement auprès de la communauté de la SISO pour étudier les domaines dans lesquels des efforts de normalisation liés à la MSaaS sont nécessaires. Les expériences pratiques des études de cas fourniront des orientations et des solutions d'architecture, de modèles de données et d'interfaces susceptibles de devenir de futures normes SISO.

Chapter 1 – INTRODUCTION

1.1 MOTIVATION

Modelling and Simulation (M&S) is already a key enabler for the delivery of capabilities to NATO and Nations in the domains of training, analysis and decision-making. However, M&S is still not being exploited to its fullest. Capabilities such as high fidelity training by units on station, en-route mission rehearsal and highly accurate real-time decision aides for Commanders in the field are within reach – but two of the main barriers are cost and accessibility. The hardware, software and personnel necessary to implement models and simulations can be both costly and difficult or impossible to deploy.

Recent developments in computing and networking are making it possible for a customer to benefit from the products of computing without the full investment in hardware, software, personnel and infrastructure. This is the main idea behind cloud computing. In this case, hardware, software and expert personnel can be centrally located and the "services" they provide are accessed over the network. This leads to enhanced flexibility, better accessibility and scalability, and also higher reliability in service provisioning from which both service customer and service provider will benefit. It is also assumed that this reduced footprint will reduce costs by pooling resources and allowing providers to serve multiple customers more efficiently at the same time. A further benefit is that individual services can be easily combined to efficiently form new, more complex services (proper design of the service landscape provided), leading to a reduction in development cost and time.

NATO and Nations are already implementing this concept to support non-M&S requirements. NATO is developing the Federated Mission Networking and supporting the Connected Forces Initiative (CFI) using cloud-based solutions. Nations are also working independently on cloud-based initiatives, e.g., Joint Information Enterprise (USA).

The application of the "services" model to Modelling and Simulation henceforth called "Modelling and Simulation as a Service" (MSaaS) promises to greatly reduce the barriers of cost and accessibility and to result in greater utility of M&S throughout NATO and the Nations.

The background documents for this technical concept are:

- 2013 NATO S&T Strategy;
- NATO M&S Master Plan (NMSMP) v.2.0 [31];
- The NAF (NATO Architecture Framework) v3 [27];
- NNEC (NATO Network-Enabled Capability) Concepts; and
- ACT's M&S Vision.

This technical concept also considers the relevant M&S architecture and interoperability work developed under NMSG until now.

1.2 OBJECTIVES

The objectives of this technical concept are:

- To define MSaaS and supporting terminology in NATO;
- To identify and describe MSaaS programs within participating Nations;

- To identify and describe MSaaS architecture efforts within participating Nations; and
- To provide conclusions and recommendations regarding MSaaS.

This is in agreement with the objectives of the MSG-131 Specialist Team (ST) on MSaaS as defined by its Technical Activity Description (TAD):

- To define the problem to be solved under the Nations and ACT demands, and to agree on a common understanding of the terminology, also important for future implementations of MSaaS in NATO.
- To develop a primer on M&S shortfalls regarding training and exercises and other M&S applications areas as identified in the NMSMP.
- To develop a primer of the NATO technical concept for MSaaS. This document will have to be sufficient to support the other objectives, and will be further elaborated later, if needed.
- To provide additional consolidated knowledge, if required, informed by standards and technical documentation on MSaaS, which serves as a basis and permits development of a specific concept and architecture to be used by NATO Nations and bodies.
- To develop a draft Reference Services-Oriented Architecture which will allow conducting improved training and exercises and other applications areas as identified during the first phase of the project.

The results from this ST provide the baseline for a follow-on Research Task Group (RTG). This RTG will analyze possible solutions for the rapid deployment of interoperable and credible simulation environments. The ST and the follow-on RTG support ACT in developing the NATO concept to operationalize modelling and simulation as part of NATO Communication and Information Systems (CIS) capabilities and the NATO M&S Reference Architecture. The NMSG is closely involved in that effort as NATO's Delegated Tasking Authority for standardization in the M&S domain.

1.3 GENERAL APPROACH

The general approach taken by MSG-131 is to collect experience from NATO bodies and Nations regarding the use of service-oriented approaches within the M&S domain. The resulting document contains a shared understanding of what "M&S as a Service" is in the NATO context and provides a comprehensive documentation of MSaaS case studies. In addition, existing service-oriented reference architectures in the M&S domain have been identified by MSG-131 and are documented in this technical concept. Based on these existing experiences and architectures, MSG-131 has derived conclusions and recommendations on the way forward.

Chapter 2 – M&S AS A SERVICE

2.1 DEFINITION

In the literature, several authoritative definitions for "Service" can be found that are applicable to the concept of "M&S as a Service".

OASIS (Organization for the Advancement of Structured Information Standards) is a non-profit consortium that has developed an abstract framework (see Ref [32]) for understanding significant entities, and relationships between them, within a service-oriented environment, and for the development of consistent standards or specifications supporting that environment. Within this framework a service is defined as:

> *"A service is a mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description."*

The *Open Group* developed a reference architecture for a service-oriented architecture (see Ref [36]). In OG2014 [37], a service is defined as:

> *"A service is a logical representation of a repeatable activity that has a specified outcome. It is self-contained and is a 'black box' to its consumers."*

The *Object Management Group* (OMG) is an international standards organization that has developed a specification for a Service-oriented architecture Modeling Language (SoaML). In this specification (see Ref [38]), a service is defined as:

> *"A service is value delivered to another through a well-defined interface and available to a community (which may be the general public). A service results in work provided to one by another."*

The above three organizations have written a joint white paper to help the service-oriented architecture community to navigate the technical products produced by these organizations (see Ref [35]).

And finally, two more definitions are provided by ITIL and ISO/IEC 20000, as described next.

The *Information Technology Infrastructure Library* (ITIL) is a set of practices for IT service management and defines service as follows:

> *"A service is a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks."* [16]

A good explanation and analysis of this definition is given in Ref [39].

ISO/IEC 20000 is an ISO standard for IT service management that was originally developed to reflect best practice guidance contained within the ITIL framework. This standard has adopted the ITIL definition, and defines service as:

> *"A service is a means of delivering value for the customer by facilitating results the customer wants to achieve."* [15]

More definitions may be found in the literature. As can be seen, the ITIL, ISO/IEC and OMG definitions are quite similar. Actually, many of the definitions share the same thoughts.

With regards to Modelling and Simulation (M&S), this technical concept bases its definition for "M&S as a Service" on the ITIL definition for service:

> *"**M&S as a Service (MSaaS)** is a means of delivering value to customers to enable or support modelling and simulation (M&S) user applications and capabilities as well as to provide associated data on demand without the ownership of specific costs and risks."*

What exactly "value" is, is defined by the customer. The value of a service is determined by what it enables the customer to do. One type of service in the MSaaS context is, for example, a professional service, such as a Verification and Validation (V&V) service, where an organization or human provides a service to a customer. Another example is an Information Technology (IT) or technical service, such as a weapon effects service, where the service is integrated within a larger simulation environment.

As such, MSaaS is an architectural and organizational approach that promotes abstraction, loose coupling, reusability, composability and discovery of M&S services. The objective of MSaaS is to effectively and efficiently support operational requirements (e.g., executing an exercise) and to improve development, operation and maintenance of M&S applications.

2.2 PERSPECTIVES ON THE MSAAS DEFINITION

The definition of MSaaS provides a high-level view of the topic. There are many different perspectives arising from this general definition of MSaaS.

This technical concept takes the following perspectives on MSaaS:

1) MSaaS as a cloud service model;
2) MSaaS using cloud service models;
3) MSaaS as a service-oriented architecture; and
4) MSaaS as a business model.

Perspective 1 (MSaaS as a cloud service model) is concerned with the question of how an M&S application is deployed and accessed by a user. Perspectives 2 and 3 are concerned with the architecture of an M&S application with Perspective 2 making use of general cloud services and Perspective 3 focusing on the construction of an M&S application via the SOA paradigm. In Perspective 2, interfaces to cloud services or cloud applications are dictated by the services or applications themselves. In Perspective 3, services have interfaces created in accordance with a defined service-oriented architecture developed to support the construction of the M&S application. Perspective 4 is primarily concerned with the provision of M&S applications as an organizational or professional service.

The four perspectives are orthogonal to each other, meaning they do not exclude each other. For example, an M&S application can both be provided as a cloud service model, as well as being designed as a service oriented architecture.

Perspectives 1, 2 and 3 are illustrated in Figure 2-1. All perspectives are described in detail in the following sections.

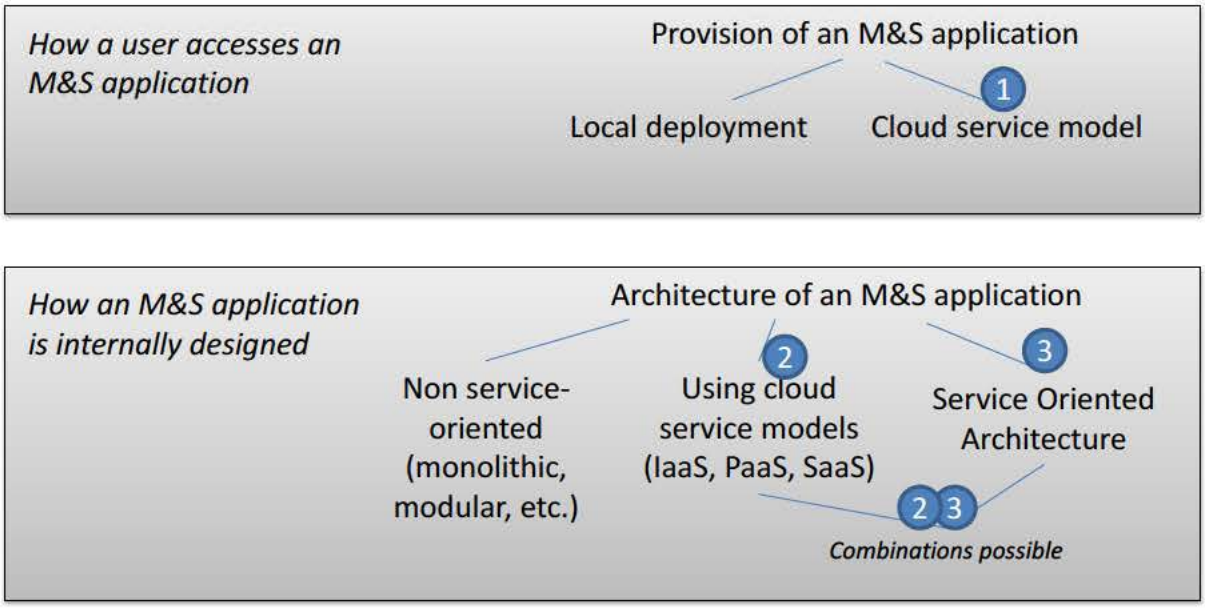

Figure 2-1: Perspectives on MSaaS.

2.2.1 MSaaS as a Cloud Service Model

The first perspective is to "servicize" M&S. That is, to bring to M&S all the characteristics attributed to Cloud Computing and the Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models.

Cloud computing is defined by NIST2011 [30] as:

> *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*

Cloud computing is composed of five essential characteristics:

- On-demand self-service;
- Broad network access;
- Resource pooling;
- Rapid elasticity; and
- Measured service.

As such cloud computing is not a service, but an IT mechanism or approach for providing a service to a customer, it can also be called "service model". Cloud computing supports the three service models mentioned previously:

- Software as a Service (SaaS);
- Platform as a Service (PaaS); and
- Infrastructure as a Service (IaaS).[1]

[1] http://en.wikipedia.org/wiki/Cloud_computing.

Each service model varies what capability is provided to a consumer and what aspects are removed from the consumers need to manage and control. The SaaS model allows the consumer to use the provider's applications running on a cloud infrastructure without the consumer needing to manage or control the underlying hardware and software infrastructure. The IaaS model allows the consumer to utilize processing, storage, networks and other fundamental computing resources, allowing the consumer to deploy and run arbitrary software. In the middle, the PaaS model allows the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.

Therefore, from this perspective, the goal of MSaaS is to provide M&S applications as a cloud-computing service model so that they are available on-demand, over the network, with the ability to charge per-use rather than needing to purchase entire M&S products. This approach reduces cost of ownership for the consumer (pay per use, no maintenance of local installations, less effort for deployment and maintenance).

However, this approach also comes with the disadvantage that the consumer does not own the service or any software involved. The consumer only purchases the right to use a service according to a specific service contract. Depending on the service contract, the consumer may not have full control of the service or the data processed by the service. In addition, the service consumer depends on a reliable, broadband and secure network connection.

This perspective on MSaaS is illustrated in Figure 2-2.

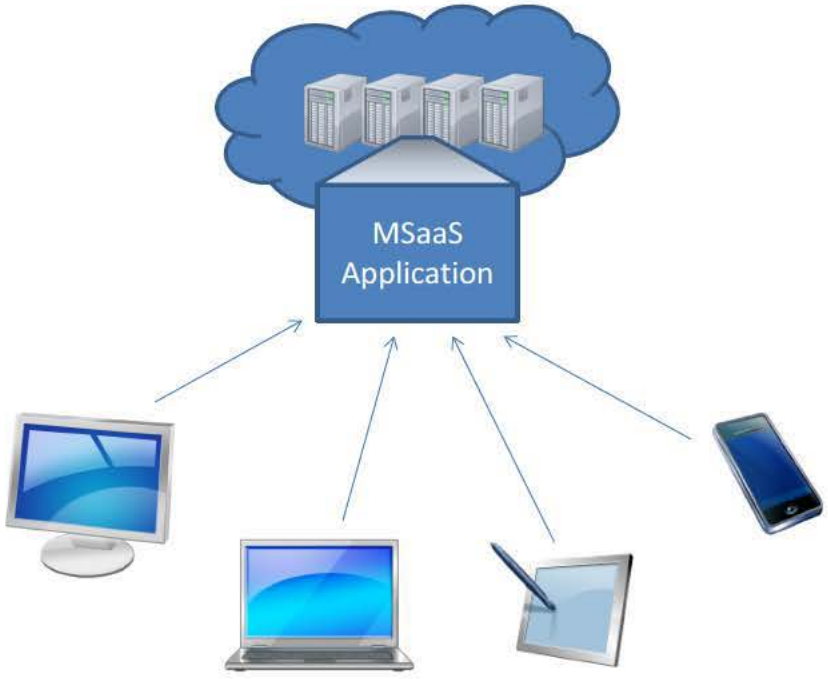

Figure 2-2: MSaaS as a Cloud Service Model.

2.2.2 MSaaS Using Cloud Service Models

This perspective is slightly different from the first and is illustrated in Figure 2-3. The desire here is for M&S to make effective use of existing cloud-computing service models. It focusses on how cloud-computing components, in particular the IaaS, PaaS, and SaaS models, can best be used in support of M&S. For example, how can IaaS be used on-demand in support of running distributed simulations so as to reduce

the need for the simulation owner to also own and maintain the simulation computing resources? Similar to the previously introduced approach, this perspective raises a number of questions, e.g., regarding security implications or regarding availability of cloud resources, which are particularly important in the military domain.

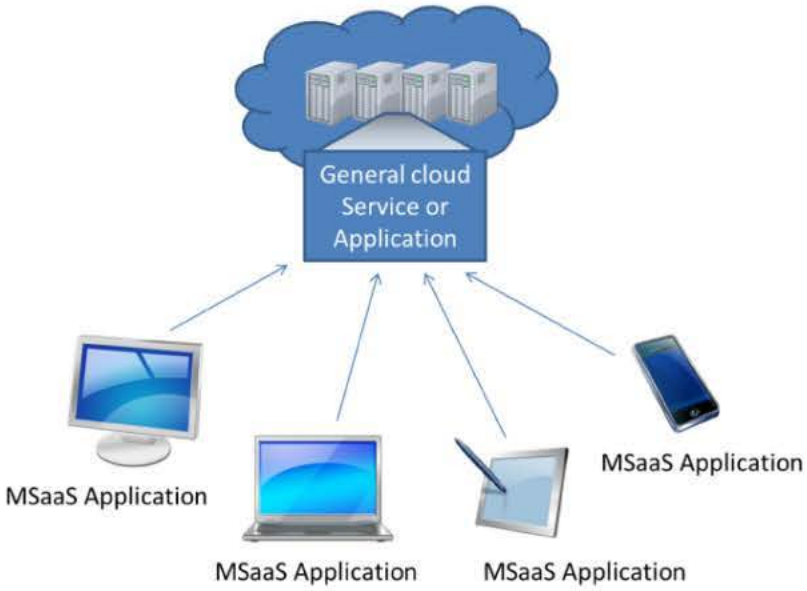

Figure 2-3: MSaaS Using Cloud Service Models.

2.2.3 MSaaS as a Service-Oriented Architecture

This perspective looks to use Service-Oriented Architecture (SOA) as the architectural approach for connecting and combining M&S services (see Figure 2-4). Ref [38] describes SOA as an architectural principle for defining how people, organizations, and systems provide and use services to achieve results.

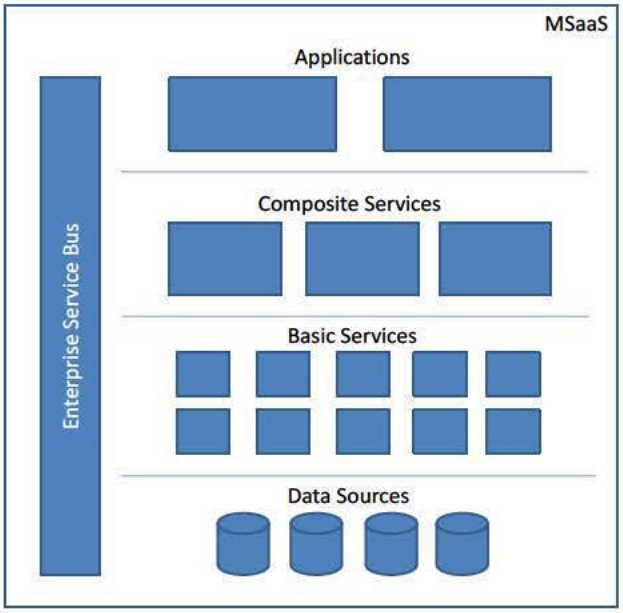

Figure 2-4: MSaaS as a Service-Oriented Architecture.

Meaningfully combining services requires a SOA that captures details on the service infrastructure, restrictions on the data model, types of allowed services, processes for developing services, and the governance of maintaining services. Following a system-of-systems approach, services may be combined to form new (possibly, more complex) services. An example is a CGF service that consumes a line-of-sight service. Each service requires an interface definition that defines how the service is technically accessed by a consumer, and requires a Service-Level Agreement (SLA) that provides a consumer with non-technical quality-of-service aspects such as cost, timescale, uptime guarantees, etc., of the service.

Service orientation is a design paradigm supporting the development of services according to certain design principles, within the context of a service-oriented architecture. Design principles include service abstraction, loose coupling, reusability, composability and discovery. Service orientation has a myriad of definitions and "purities", but for MSaaS, three central aspects of service orientation are:

1) Communication following standards so that service contracts can be declared and processed over a range of actors (components);
2) Loose coupling in the sense that components are usable in a wider context; and
3) Interoperability in the sense that components may function together to generate a larger/different piece of total functionality.

Service discovery is in the essence of SOA, but at present, service discovery is in effect possible only at design time; except for very mature systems. MSaaS should enable service discovery and service composability in the sense that components are ready for a pre-defined set of service types and may call upon these services at need.

This perspective potentially requires the definition of multiple, different SOAs. Integrating M&S services relevant to the M&S business domain will require a SOA different from a SOA used to integrate military domain specific simulation services in order to create a distributed simulation to support a training or analysis activity.

2.2.4 MSaaS as a Business Model

This perspective focuses on organizational and professional M&S services, including their underlying business models, such as Distributed Networked Battle Labs (DNBL) [33], [34], that provide a framework for registering, identifying and contracting providers of M&S services in order for a client to fulfil an M&S need (human-to-human or organization-to-organization). Services that can be contracted from this perspective are, for example:

- Model development services;
- Verification and validation services;
- Certification services; and
- Training services.

These services are typically provided by an organization/human to another organization/human.

2.3 ACTORS

MSaaS (whether technical or organizational) includes three main actors (see Ref [11] for more detailed information):

1) A **Service Consumer** accesses services provided by a service provider to achieve its own objectives. A service consumer relies completely on the service contract offered by a service provider and does not care about how a service provider actually performs its service delivery.

2) A **Service Provider** provides services on an on-demand basis. Each service is specified in a service contract that details scope, usage requirements and quality of the provided service.

3) A **Service Broker** acts as neutral platform that provides a catalogue and facilitates access to available services and service providers. Strictly speaking, a service broker can be considered as a special type of service (namely, a service for finding other services).

Actors may be realized differently:

- An actor may be a technical system (e.g., an implementation of a terrain service, line-of-sight service, or weather service).
- An actor may be a system-of-systems (e.g., a simulator or a battlelab providing M&S capabilities). A system-of-systems can be viewed from outside the system to be a self-contained system.
- An actor may be a person (e.g., a soldier operating a user application).
- An actor may be an organization (e.g., training, test and evaluation, planning).

2.4 SERVICE CATEGORIZATION

There are many ways to categorize services and often services fit into multiple categories at the same time. One possible service categorization uses the type of consumer and provider of the service. Given the types “Human”, “Machine” and “Organization”, possible service categories are:

- Machine-to-Machine;
- Human-to-Machine;
- Human-to-Human; and
- Organization-to-Organization.

Other service categorizations are service application area and service domain. An application service concerns the use of a service for a kind of application, for example a weapon-effects service for engagement simulations. A domain service concerns the use of a service in a certain domain or problem space, across a group of applications, for example a simulation data recording service.

Other categorizations may take into account other aspects of a service, such as time. Examples are a real-time service or a non-real-time service.

This technical concept is primarily focusing on the category of services that include a machine, i.e., machine-to-machine and human-to-machine services. These services may be combined with other services to a form a new service, or may be integrated into a simulation environment. MSaaS examples in this context are a weapon effects service within a simulation environment (machine-to-machine), planning support services, and scenario development services (both human-to-machine).

The professional type services in the form of human-to-human and organization-to-organization services are not in the focus of this technical concept – but it is possible for these services to be supported by machine services, either as enabling or intermediate services. For example, a V&V service is initiated by a human/ organization and the service is performed by a human/organization, but the process is facilitated by technical systems like a request for V&V Service and V&V progress tracking service.

2.5 ALIGNMENT WITH NATO C3 CLASSIFICATION TAXONOMY

Another categorization scheme that may be used for service categorization is the NATO C3 Classification Taxonomy. The taxonomy is a layered categorization scheme of capabilities in support of Consultation, Command and Control (C3).

The NATO C3 Classification Taxonomy provides a tool to synchronize all capabilities and their activities for C3 in the NATO Alliance. The purpose of the NATO C3 Classification Taxonomy is to capture concepts from various communities and map them for item classification, integration and harmonization purposes. Recognizing dependencies and relationships, it links political and military ambitions, mission-to-task decomposition, capability hierarchy, statements and codes, operational processes, information products, applications, services and equipment to reference documents, standards, implementation programs and fielded baselines [3].

Figure 2-5 gives an overview of the top levels of the NATO C3 Classification Taxonomy, connecting the top-level military operational ambitions all the way down to 'the wire', within the context of a service landscape.

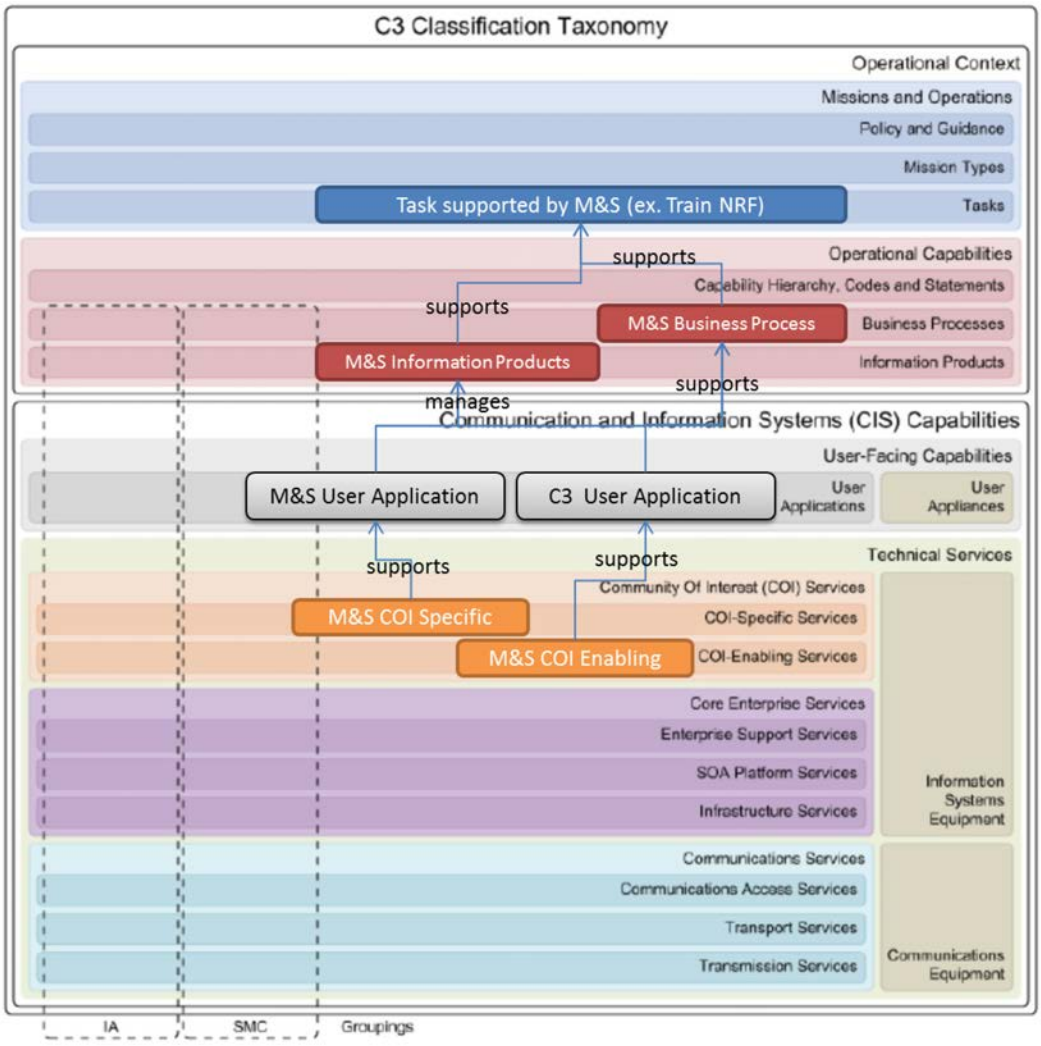

Figure 2-5: Integration of M&S Capabilities and Services into the NATO C3 Classification Taxonomy.

M&S may be integrated into the NATO C3 Classification Taxonomy as specialization of existing domain-independent components (see Table 2-1, and also Figure 2-5).

Table 2-1: Integration of M&S into NATO C3 Classification Taxonomy.

Domain-Independent Component of NATO C3 Classification Taxonomy	**M&S-Related Specialization**
Tasks	Tasks supported by M&S
Business Processes	M&S Business Processes
Information Products	M&S Information Products
User Applications	M&S User Applications (i.e., simulation systems, simulators) M&S CoI Applications
CoI-Specific Services	M&S CoI Services
CoI-Enabling Services	M&S Services

Each level of the C3 Classification Taxonomy and its relation to M&S is explained in detail in the next sub-sections.

2.5.1 Missions and Operations

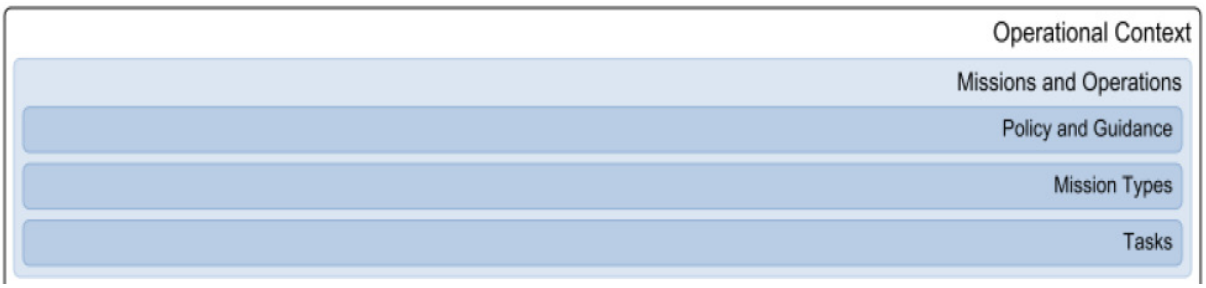

Figure 2-6: Missions and Operations in NATO C3CT.

Missions and Operations capture NATO's political and military Level of Ambition (LoA) as derived from the Strategic Concept and Political Guidance. These ambitions are expressed as a series of possible mission types and related tasks, as well as references to relevant concepts, guidance, policies, and publications.

Given a specific "Task" (see Figure 2-7 for a list of possibilities), one can choose the underlying services more specifically. For example, a "Train NRF" Task (as illustrated in Figure 2-5) may have implications like "use sensors", "do sensor fusion", and "do analysis" that have to be taken into account for fulfilling this specific task.

Figure 2-7: Mission Types and Tasks from the NATO C3 Classification Taxonomy (Sample).

2.5.2 Operational Capabilities

Figure 2-8: Operational Capabilities in the NATO C3 Classification Taxonomy.

Operational Capabilities capture everything required by NATO to successfully complete mission types and achieve stated Levels of Ambition (LoAs). Operational Capabilities are linked to established Business Processes. To support the implementation of C3 capabilities, information products that are identified during Business Process Analysis (BPA) are captured separately and linked to these mission types and key tasks.

With regards to M&S, M&S-specific Business Processes and Information Products may be defined.

2.5.3 User-Facing Capabilities and User Applications

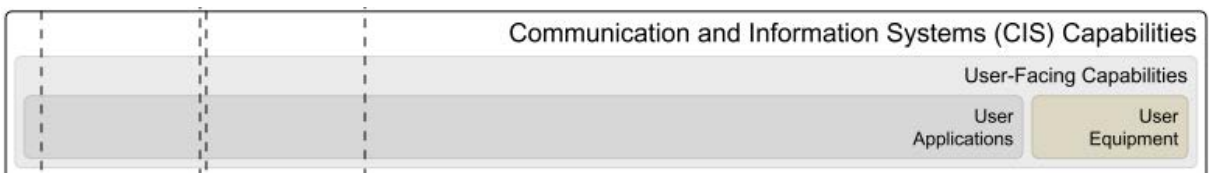

Figure 2-9: User-Facing Capabilities in the NATO C3 Classification Taxonomy.

User-Facing Capabilities express the requirements for the interaction between end-users and all CIS Capabilities, in order to process Information Products in support of Business Processes. User-Facing Capabilities incorporate the User Equipment, as well as the User Applications that runs on this equipment.
User Applications – also known as application software, software applications, applications or “apps” –

provide the computer software components designed to help an end-user perform singular or multiple related tasks.

Examples of User Applications are illustrated in Figure 2-10. The NATO C2 Classification Taxonomy explicitly defines “Modelling and Simulation CoI Applications” (which, for example, may be simulation systems or simulators).

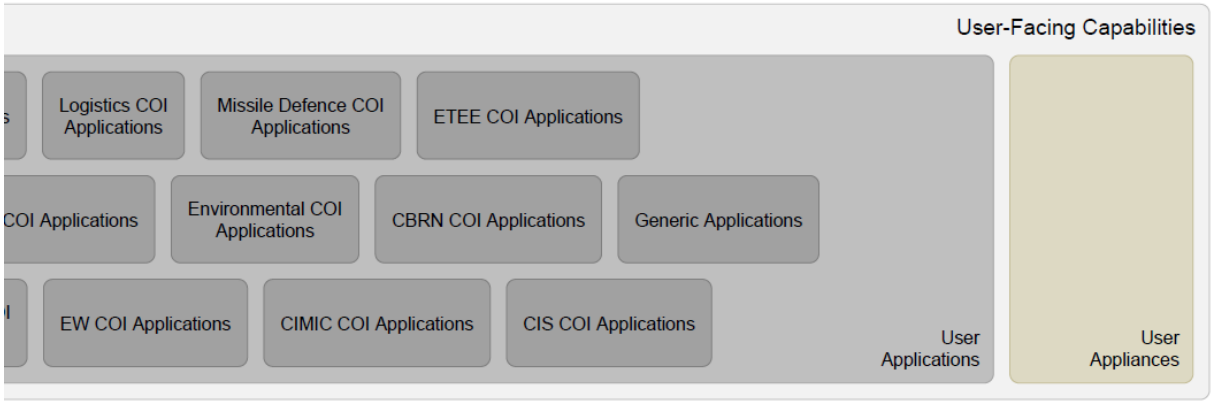

Figure 2-10: User Applications in the NATO C3 Classification Taxonomy (Sample).

2.5.4 Technical Services

Technical Services express the requirements for a set of related software and hardware functionalities that can be reused for different purposes, together with the policies that should control their usage. These requirements are derived from the operational needs expressed by the collection of User-Facing Capabilities. Inherently, the Technical Services must support all NATO mission types.

As illustrated in Figure 2-11, the Technical Services are further sub-characterized into:

- CoI-Enabling Services; and
- CoI-Specific Services.

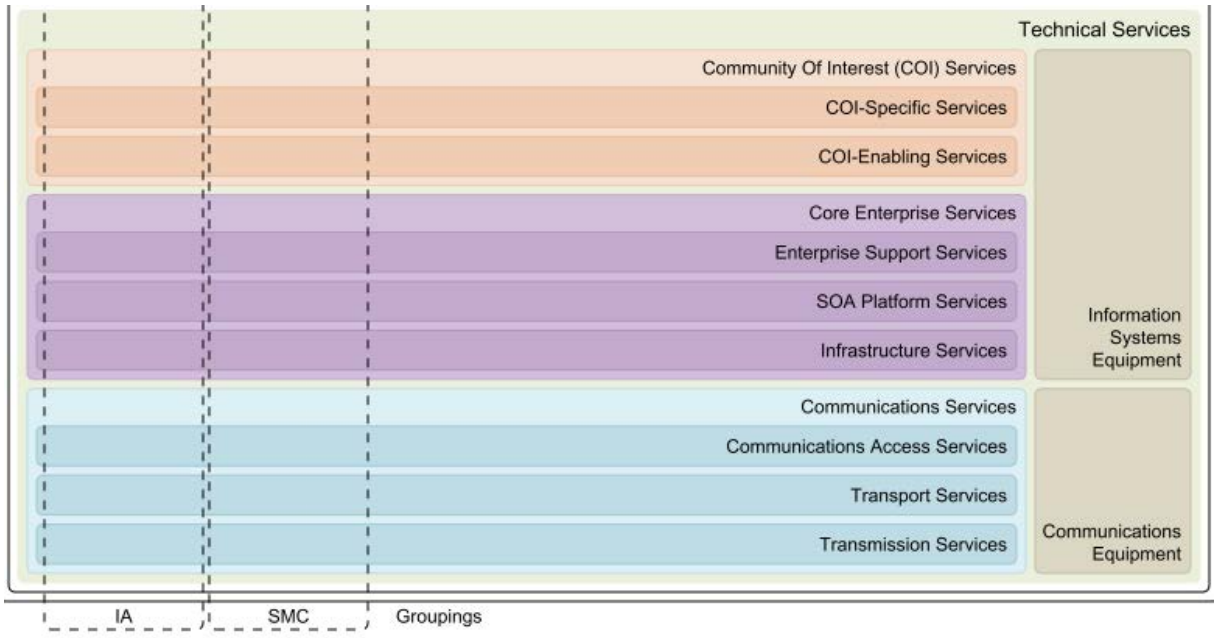

Figure 2-11: Technical Services in the NATO C3 Classification Taxonomy.

Whereas CoI-Enabling Services provide functionality that is required by more than one community of interest, CoI-Specific Services provide specific functionality that is required by a particular user community.

Both CoI-Enabling Services and CoI-Specific Services may be specialized as M&S Services and M&S CoI Services (see Figure 2-11).

Figure 2-12 and Figure 2-13 show more details on M&S Services and M&S CoI Services.

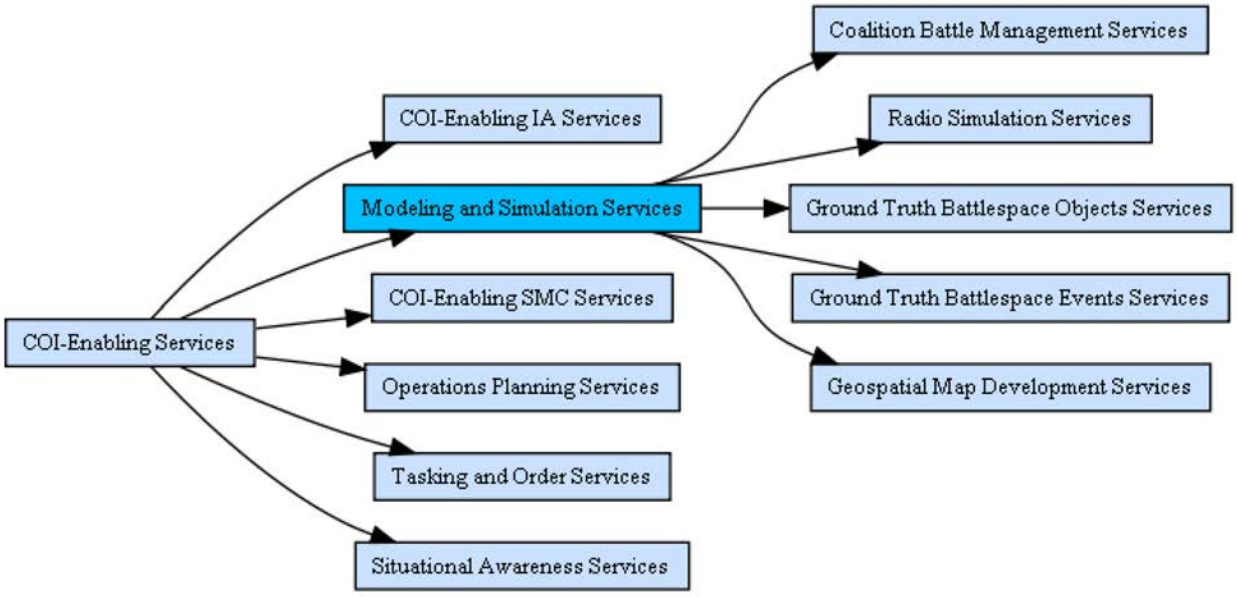

Figure 2-12: M&S Services as Specialization of COI-Enabling Services.

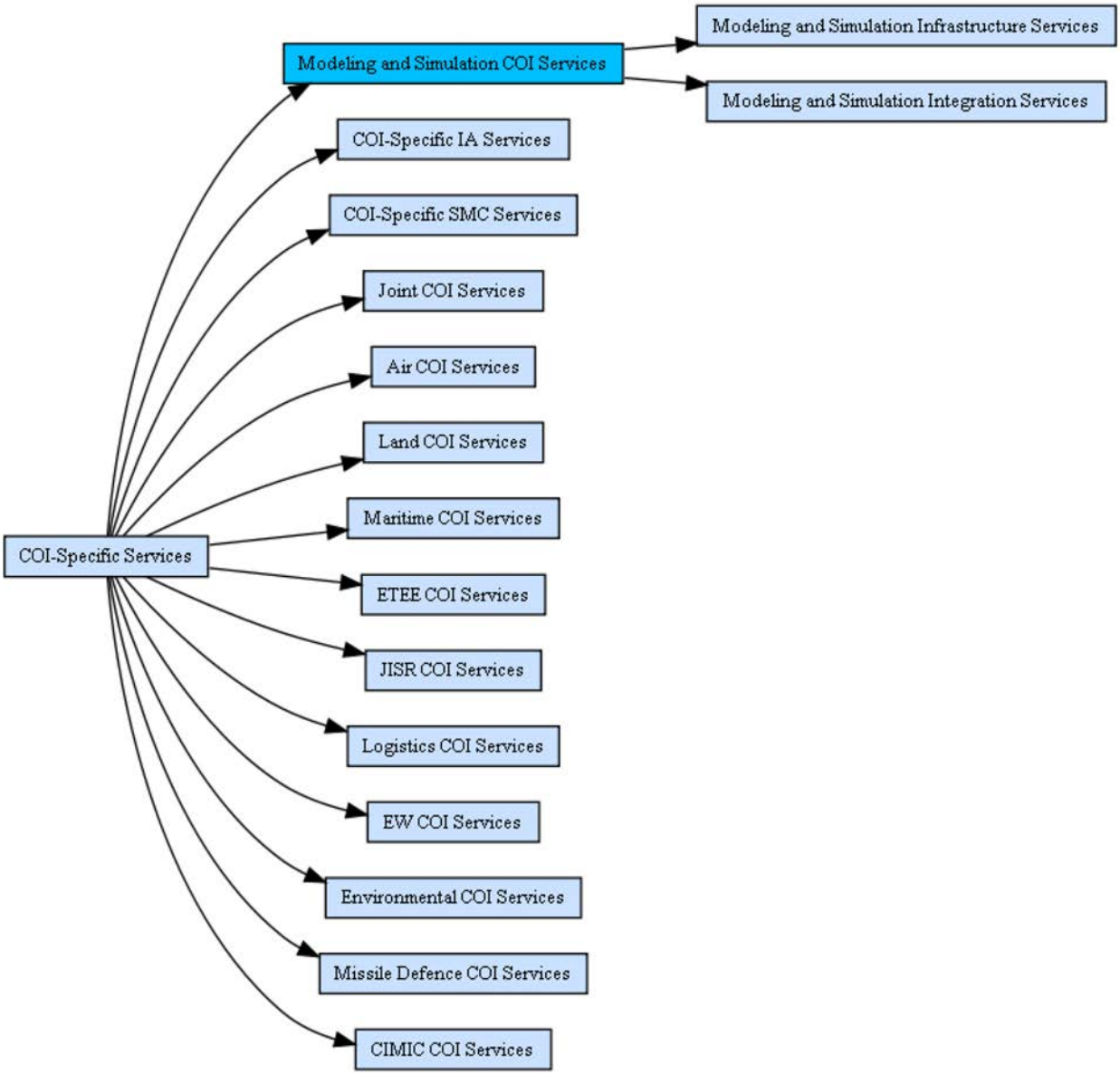

Figure 2-13: M&S COI Services as Specialization of COI-Specific Services.

2.6 ADVANTAGES AND DISADVANTAGES OF MSAAS

The use of MSaaS can have several advantages and disadvantages. The discussion below is based on [48], [49], [50] and discussions within MSG-131.

First general advantages and disadvantages are presented, followed by military M&S specific and disadvantages.

Note that some of the MSaaS properties provide advantages that are mainly locally (e.g., managerial and financial), while other MSaaS properties only provide advantages for applications such as distributed training.

Note that some of the MSaaS advantages are realized by also having relevant Data as a Service (DaaS). This includes not only data used in simulation (e.g., terrain databases), but also data used in military operations (e.g., standard data on how fast troops can move), and on top of that, data of current operations.

Another critical aspect that can be seen as a disadvantage if not properly addressed is Quality of Service (QoS). The ability to properly manage the QoS in service-oriented systems is critical to meet non-functional requirements in terms of, e.g., performance and reliability.

Managing the QoS means being able both to predict the QoS at design-time, when the selection of the services to be orchestrated has to be defined, and to dynamically reconfigure the system at operation time, when a performance downgrade may occur.

The advantages of decoupling interface and implementation and of avoiding the cost of ownership become critical in terms of QoS management, since the QoS properties of the networks and platform resources devoted to the invocation and execution of services may not be known from the orchestrator point of view.

This is exacerbated in the distributed simulation field, in which the ability to guarantee a given QoS level is of significant relevance for several applications.

Appropriate methods and languages are needed in order to extend the service description, which typically only covers the functional properties of services, and to exploit such an extended description at service discovery time.

2.6.1 General Advantages

This section briefly summarizes some of the advantages of using “as a Service” and cloud computing. They are not M&S specific and not tailored towards military use of MSaaS. Some of these advantages apply specifically to the user, some specifically to the provider, and some advantages work for both. Many of the listed advantages are general benefits attributed to cloud computing and are thus most relevant to MSaaS Perspectives 1 and 2:

- **On-Demand Self-Service** – Users can provision computing capabilities, such as server time and network storage, as needed, automatically without requiring human interaction. Quick deployment of the customer solution is possible since the used services are already installed, configured and on-line.
- **Broad Network Access** – Capabilities are available over the network and accessed through standard mechanisms via thin or thick client platforms (e.g., mobile phones, tablets, laptops, workstations).
- **Resource Pooling** – Computing resources are pooled to serve multiple consumers using a multitenant model. Different physical and virtual resources are dynamically assigned and reassigned according to consumer demand.
- **Rapid Elasticity** – Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. This can be computing hardware, data storage, network bandwidth, etc. One of the advantages is less environmental impact since assets are usually switched off if not needed.
- **Measured Service** – Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. This pay-per-use model may cost less than other licensing schemes. The administration that comes with licenses may also become simpler and removes the need for long-term investments in applications.
- **Automatic Upgrades** – The MSaaS provider has to apply updates. This is performed transparent to the user. The latest software versions are available.

- **Improved Composability** – Services can be composed into larger services as needed (requires standardized interfaces and service contracts).
- **Reusability** – Services tend to be provided by smaller building blocks using well-defined service interfaces, and thus facilitating reuse.

All in all, MSaaS promises more convenient and quicker access to M&S resources and at considerable cost reduction.

2.6.2 General Drawbacks

- Managing security, privacy, accountability, risk and trust become more complex in a distributed, heterogeneous environment with multiple service owners.
- Advanced aspects of composability of M&S services are still an open area of research (e.g., service discovery, service binding).
- Dependency on network connections makes M&S applications vulnerable to network effects out of the control of an M&S user.
- Adapting existing M&S applications with a service interface or for hosting in the cloud may be complex and/or costly. Not everything fits in the cloud, especially if it hadn't been designed for the cloud.
- Non-localized control over consumed services creates a dependency and reliance on a service provider to fulfil their service-level agreements and removes the possibility of manually modifying the service should the provider not do so.
- If a composed MSaaS service is validated for some use, updates to individual services may require re-validation. Mitigating this requires well-defined service management and governance to allow service users to continue using validated services while newer updates go through the validation process.

2.6.3 Military User-Specific Advantages

From the military user point of view, there are a number of (perceived) advantages of MSaaS. The advantages are grouped by most relevant perspective.

MSaaS as a cloud service:

- No major hardware necessary (e.g. on front-line) where you do not want it (it could be in a back-office);
- Less end-user maintenance of complex, military M&S assets (typically in large distributed training: version differences requiring upgrades, technical problems, etc.);
- Accessible from around the world (allowing, e.g., training wherever you are);
- Flexibility: adaptable depending on the training audience or selected scenario and required assets, solutions can be made to fit due to elasticity at the provider or by selecting another provider; and
- Scalability: adaptable depending on size of the training audience, solutions can be made to fit due to elasticity at the provider.

MSaaS as a SOA:

- Level playing field if all users access the same services (e.g., communication effects or weapon effects modules).

2.6.4 Military User-Specific Drawbacks

There are also several (perceived) drawbacks, again grouped by most relevant perspective.

MSaaS as a SOA:

- Adaptation of existing software is needed (e.g., replace internal weapon effects calculation of a simulation system with an interface to a service providing the same functionality). This may prove difficult or impossible in the case of COTS products. Note that it may be possible for some legacy/ COTS products to act as an MSaaS by encapsulating it in a wrapper.
- In current distributed M&S applications, often significant tailoring of gateways, etc., is required before use.
- Validation of specific services may be more difficult when they are more remote and internal operation is shielded to a large degree.

MSaaS as a cloud service:

- Poor performance of network infrastructure available to military users, especially those deployed – may make access to and use of M&S services difficult or impossible.
- Dependency on remote infrastructure and services increases vulnerability in front-line/combat situations and makes local fall-back options and back-up systems necessary, thus cancelling out the major advantages of MSaaS for these situations.
- There is less face-to-face contact if M&S assets are no longer needed locally since an exercise can be executed distributed. If there is an advantage of face-to-face meetings, they have to be held anyway.

Chapter 3 – CASE STUDIES FOR M&S AS A SERVICE

This chapter summarizes national case studies that utilize MSaaS ideas or that borrowed ideas from service-oriented architectures in general. Detailed descriptions of all case studies may be found in Annex B.

3.1 DOCUMENTATION SCHEMA

All case studies that have been identified by MSG-131 (see Annex B) are described according to the schema shown in Table 3-1.

Table 3-1: Documentation Schema for MSaaS Case Studies.

Nr	Title	Description and Possible Values
1	Description of case study	Description (text and figures) of case study.
2	M&S business process supported by the case study	• Concept development. • War fighting experimentation. • Support to acquisition life-cycle. • Analysis of possible alternatives in procurement decisions. • Life-cycle cost and logistics analysis (prediction tools). • Test and evaluation in capability development and interoperability. • M&S embedded in CIS and weapon systems (e.g. mission planning / mission preparation). • Emergency and rescue services (prediction models). • Exercise and training (individual/collective/joint).
3	Role of end-user	• Technical/tactical/operational/strategic level. • Operational military user. • Defence procurement/acquisition community. • Other types of user, e.g. supplier base. • M&S technical user.
4	Security classification	• Level of classification of information. • Support for cross-domain/Multi-Level Security (MLS).

5	Type of services provided	• Services:
		  • Weather forecast services.
		  • Decision support/prediction services.
		  • AAR (and in action review) services.
		  • Live data service (e.g. live air picture), etc.
		  • Health monitoring services.
		• Categorization of service consumer and provider:
		  • Machine;
		  • Person; and
		  • Organization.

Nr	Title	Description and Possible Values
5 (Cont'd)	Type of services provided (Cont'd)	For general M&S applications – refer to the 27 classes in the DNBL service catalogue (see Annex B, Section B.13.5, Figure B-11).
6	Properties of the service environment	• Technology Readiness Level (TRL). • Level of fidelity. • Level and type of control. Level and type of control refers to what the developers of the simulation and the users of the simulation are able to do. Proposed levels are: • No control: Simulation system is monolithic, has to be used as it comes; • Limited control: Few parts of the simulation can be changed or modified, few parameters can be changed; and • Full control: Simulation system comes in modules or with source code, usage is up to the user/operator.
7	Capacity/Availability	• Frequency of access (e.g., once in a week or less). • Availability and support hours of operation. • Quality of service (availability and response time to issues). • Instantiations of service (how many different users can be supported). • Level of scalability, e.g., a CGF farm that replicates capability and "grows" to support surge demand.
8	Authorization (Who/How)	• Who is able to access the service environment and how are they authorized to do so.
9	Type of delivery / quality of service	• Use of web services, including cloud-based infrastructures possible. • Other services.
10	Related costs	• Development costs (separating initial vs. through life costs – spend once, reuse many times). • Cost of using/providing capability.
11	Expected and observed benefits	• Benefits arising from taking a service-oriented approach in the case study.

3.2 SUMMARY OF CASE STUDIES

The following Table 3-2 provides a summary of the case studies documented by MSG-131. A reference to Annex B is provided for further information on each case study.

Table 3-2: Overview of MSaaS Case Studies.

Title	Nation	Reference
RUDI	DEU	B.1
SD VINTEL	DEU	B.2
NOGESI	ESP	B.3
CGF Provision	GBR	B.4
Mission Planning Support	NLD	B.5
Scenario Generation	NLD	B.6
Validation	NLD	B.7
SIM SOA	NOR	B.8
Collective Training and Exercise Functional Services	NCIA	B.9
C2 Interoperability Verification Testing	NCIA	B.10
Joint Training Enterprise Architecture (JTEA)	USA	B.11
TIES	M&S COE, NCIA	B.12
Table-Top Exercise	NCIA	B.13
Services Over Needs (SONS)	ITA	B.14
Multi-Resolution Integration HLA Cloud M&S Environment	POL	B.15
Semi-Automated Forces System Architecture for Cloud-Computing Environment	USA	B.16

3.3 SUMMARY OF SERVICES FROM CASE STUDIES

One of the purposes for exploring Nation case studies is to identify M&S services in common. The following table extracts from the case studies some of these common services and provides an initial categorization for each. Further categorization (e.g., application area and domain, C3 classification) and structuring of these services according to an architecture will need to be done in MSG-136, the follow-on activity of MSG-131.

Table 3-3: Overview of Services from MSaaS Case Studies.

Service	Case Study	Provider Category (Machine, Human, Organization)	Consumer Category (Machine, Human, Organization)	Classification (M&S Business, Simulation Domain, Enterprise, Infrastructure)	Perspective
Weapon Effects Service	SD VIntEL, SONs	Machine	Machine	Simulation	SOA
Communication Effects Service	SD VIntEL, SONs	Machine	Machine	Simulation	SOA
Exterior Ballistics Service	SD VIntEL, SONs	Machine	Machine	Simulation	SOA
Synthetic Environment Service	SD VIntEL, SONs	Machine	Machine	Enterprise	SOA
Synthetic Dynamic Service	SD VIntEL, SONs	Machine	Machine	Simulation	SOA
Init Service	SD VIntEL	Machine	Machine	Infrastructure	SOA
Weapon	NOGESI, SONs	Machine	Machine	Simulation	
CGF	CGF Provision, Scenario Generation, SONs	Machine	Machine/Human	Business/Simulation	
Weather Forecast	Mission Planning	Machine/Human/ Organization	Machine/Human	Enterprise	SOA
Live Data	Mission Planning	Machine	Machine/Human	Business/Simulation	
Terrain Generation	Scenario Generation, SONs	Machine/ Organization	Machine	Enterprise	
Weather Generation	Scenario Generation	Machine/ Organization	Machine	Enterprise	
V&V	V&V	Organization	Human/Organization	Business	Cloud

Service	Case Study	Provider Category (Machine, Human, Organization)	Consumer Category (Machine, Human, Organization)	Classification (M&S Business, Simulation Domain, Enterprise, Infrastructure)	Perspective
Monitoring Service	SONs	Machine	Machine	Simulation	
Recording, Analysis and AAR Services	SONs	Machine	Machine	Simulation	
Sensor and C2 Systems Simulation and Stimulation services	SONs	Machine	Machine	Simulation Infrastructure	

Chapter 4 – SURVEY OF EXISTING REFERENCE ARCHITECTURES FOR M&S AS A SERVICE

This chapter presents a survey of existing (national- and/or domain-related) reference architectures for MSaaS and reference architectures that utilize MSaaS ideas.

The existing reference architectures form the starting point for development of a draft Reference Services-Oriented Architecture (as defined in the TAP) which will allow conducting improved training and exercises and other applications areas.

4.1 DEFINITION AND TERMINOLOGY

4.1.1 Architecture

A good definition of 'architecture' is given in IEEE 610.12-1990 Standard Glossary of Software Engineering Terminology:

> *"The structure of components in a program/system, their interrelationships, and the principles and guidelines governing their design and evolution over time."* [13]

Typical design requirements, which influence the architecture of a specific system, are:

- Maintainability;
- Possibility for future upgrades;
- Scalability;
- Reusability; and
- Low life-cycle costs.

To achieve specific design requirements, developers should exploit proven design patterns and human expertise. The key is to 'think ahead' and reuse things that work. An architecture should support the intended application domain as much as possible. Architectures should be based on re-usable and interoperable components. The components themselves should have strong internal coherence and loose couplings between them. Interfaces between the components should comply with open, international standards as much as possible.

As reference architectures have a lot in common with reference models, the next section first looks at "reference models" and then defines "reference architectures".

4.1.2 Reference Models

A common definition of a model is the following:

> *"A **model** is a physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process."* [1],[6]

According to Schmidt [40], reference models are development guidelines providing standardized solutions for certain modeling problems of a (homogeneous) class of real systems. Reference models are usually characterized by the two main attributes *universality* and *recommendation character* [45]:

- *Universality* refers to the idea that a reference model should be applicable not only in one special case, but to a certain class of problems; and

- *Recommendation character* refers to the idea that a reference model should serve as a blueprint or even as a default solution for certain problems.

This characterization of reference models is similar to 'design patterns' (see Ref [10] for an excellent discussion, and also Refs [24] and [26]).

Another very simplistic and pragmatic definition for reference models is given by Modi et al. [21]:

> *"Any generic model that has specific examples can be considered to be a reference model."*

According to Modi et al., the purpose of reference models is "to enable others to practice their discipline with a solid foundation" [21]. Another pragmatic definition of the term reference model is given in Ref [45]:

> *"A **reference model** is a model used for supporting the construction of other models."*

Reference models have a lot in common with standardization activities – they:

- Create a common understanding of terms and concepts;
- Help to clarify (or even define) the semantics of systems; and
- Increase comparability among models defined or documented this way.

The applicability of a reference model is determined by the number of problems for which it may be used [40]. Of course, universality of a reference model depends crucially on the degrees of freedom a model developer has for adapting a reference model to problem-specific needs. Common major aims for using reference models are to reduce the complexity of a modeling task at hand and to simplify development processes. In general, a reduction of effort in time and cost is expected, although well-founded field reports are not available.

4.1.3 Reference Architectures

In general, reference architectures can be considered to be similar to a reference model. Reference architectures may be characterized in the same way, i.e., using the attributes *universality* and *recommendation character*.

Therefore, reference architectures are considered to be generic blueprints that may be used as a basis for deriving specific architectures. In this sense, reference architectures are recommendations on how to approach a certain architecture development task. Obviously, a different architecture development approach may be selected if no reference architecture is available, or no reference architecture seems suitable. Once a reference architecture has been selected, it becomes a boundary condition for developing the derived architecture.

Similarly, the NATO Architecture Framework (NAF) defines reference architectures as the linking element between overarching architectures and target architectures (see Figure 4-1). According to the NAF:

> *"Reference architectures reflect strategic decisions regarding system technologies, stakeholder issues, and product lines. They render user requirements, processes, and concepts in a high-level solution from which individual projects can be identified and initially programmed. Their primary focus is on services, processes and component functionality, and they provide the basis for the development of Target Architectures (TA)."* [27]

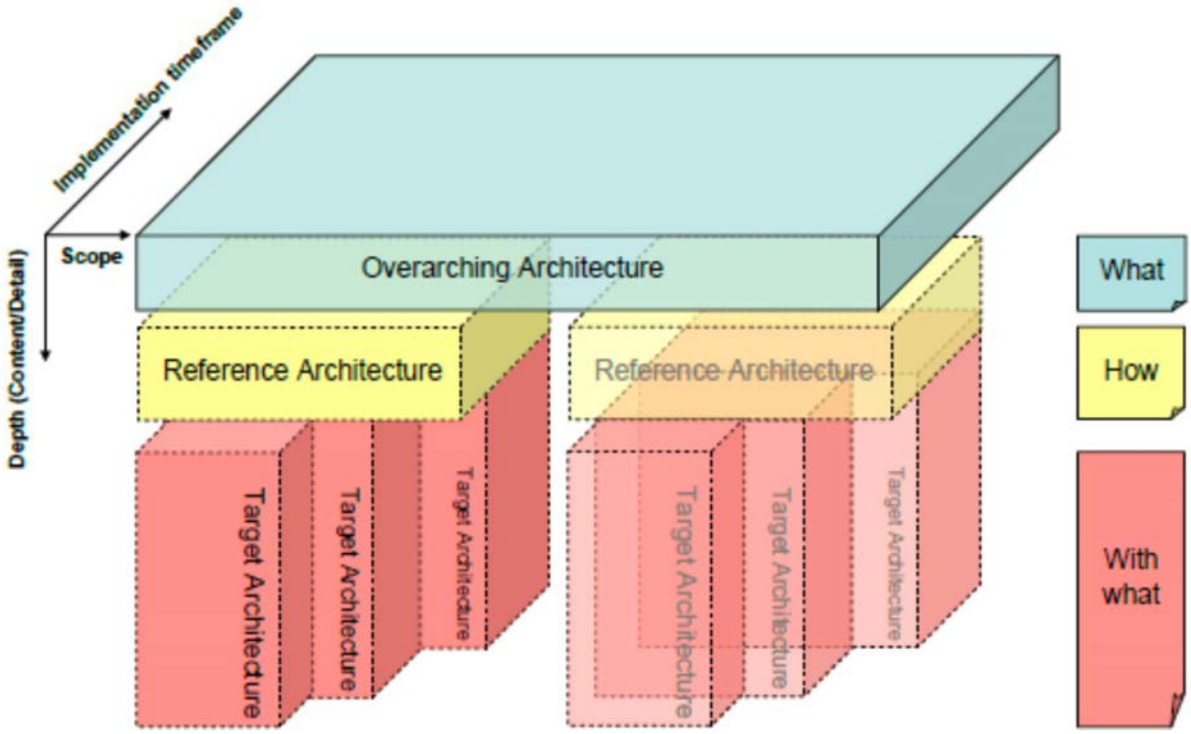

Figure 4-1: Relationships Between NATO Architectures [27].

The NAF states that target architectures are normally derived from the related reference architecture. They specify a system design at a detail sufficient to direct the acquisition and integration of components to achieve a desired capability. Target architectures focus on specifications for systems and services and are usually valid for the duration of the system acquisition and initial design. In contrast, reference architectures are expected to cover the entire planning cycle for a typical NATO system development, which is normally six years.

Within its investigation of simulation interoperability issues, NATO MSG-086 “Simulation Interoperability” came to the conclusion that comprehensive reference architectures for simulation environments are currently missing [25 – Annex A, Section A.2.6].

Established simulation architectures (e.g., the DSEEP considers DIS, HLA, and TENA to be simulation architectures) provide run-time infrastructure services or agreements for the exchange of data between simulation systems. However, full interoperability of simulation systems requires more and includes also the alignment of data models, the use of simulation services, the integration of operational systems, etc. Comprehensive reference architectures (in the sense of NAF) which treat all these aspects are currently missing and part of the Technical Activity Program of several NATO MSGs (especially MSG-068, MSG-106 and MSG-128, see Chapter 4, Sections 4.6 and 4.7).

Table 4-1 provides a mapping of the different kinds of architectures as defined by the NAF to the M&S domain. The mapping is not an exact science, but it indicates that a similar structuring of architectures as in the NAF may be defined for the M&S domain.

Table 4-1: Mapping of NAF Architectures to Simulation Environments.

NAF Terminology	Description	Examples
Overarching architecture	Architectures which are used for long-term planning. These architectures may include visionary concepts and ideas. Overarching architectures are often defined as goals or constraints which have to be applied when designing and implementing new systems.	"Our next-generation simulation framework shall be service-oriented." "Our long-term goal is to use only open (i.e., freely available) standards and protocols."
Reference architecture	Architectures which are used as a reference for a large set of applications. The following qualifiers may be used to distinguish domain-specific and domain-independent architectures: • Domain-specific: Architectures that target a very specific application domain, e.g., land-based entity level simulation. • Domain-independent: Architectures that are (at least to some degree) independent of a specific application domain. Additionally, architectures may be qualified as "comprehensive" if they define additional services, service agreements, and/or service components.	Domain-independent reference architectures: • HLA. Domain-specific reference architectures: • DIS; and • TENA. Comprehensive domain-specific reference architectures: • VIntEL (= HLA + VIntEL-FOM + services + etc.), see Chapter 4, Section 4.5. • NETN (= HLA + NETN-FOM + etc.), see Chapter 4, Section 4.6. • MTDS (= HLA + NETN-FOM + accreditation requirements + etc.), see Chapter 4, Section 4.7.
Target architecture	Architecture of a specific simulation environment.	Any specific development and execution of a simulation environment (e.g., MSG-068 demonstration at I/ITSEC).

Building target architectures for specific simulation systems or simulation environments on foundations from established reference architectures will increase not only the efficiency of work in time and budget, but also the quality of the results, and will lead to improved interoperability. A reference architecture states for example that HLA Evolved IEEE1516-2010 has to be used; the target architecture states which version, which data model and which version of that model are actually used, and which vendor provides the RTI and in which version, etc. The reference architecture is the general blueprint while the target architecture makes it very specific.

4.2 OVERVIEW OF EXISTING REFERENCE ARCHITECTURES

Figure 4-2 gives an overview of existing reference architectures within the M&S domain as identified by MSG-131.

Figure 4-2: Overview of Existing Reference Architectures and Their Scope.

Figure 4-2 also tries to give an indication of the scope or level that is addressed by each reference architecture. Each reference architecture is described in more detail in the following sections.

In addition to the reference, architectures shown in Figure 4-2, MSG-131 points out the need to integrate M&S reference architectures with C2 reference architectures, e.g., as described by the Multi-lateral Interoperability Programme (MIP).

4.3 JOINT TRAINING ENTERPRISE ARCHITECTURE (USA)

See detailed description in Annex B, Section B.11.

4.4 ETEE REFERENCE ARCHITECTURE (NCIA)

ETEE (Education, Training, Exercises and Evaluation) is defined in NATO policy as follows:

> *"ETEE are the core functions conducted by nations and NATO to prepare the NATO Command Structure (NCS) and NATO Force Structure (NFS) for its current and future missions. Additionally, NATO's exercise programme serves the dual purpose of conveying a clear and strong message of the alliance's capabilities while simultaneously demonstrating Alliance resolve. Further, ETEE supports the continuous transformation of the Alliance and its partners as an important basis for Lessons Identified (LI) and Lessons Learned (LL) and by supporting experimentation and development of new capabilities. ETEE also offers opportunities to validate interoperability within the Alliance Command and Force structure."* [8]

The ETEE Reference Architecture is being been defined by NATO Allied Command Transformation (ACT), supported by the NATO Communications and Information Agency (NCI Agency) to collect the operational user requirements for functional services in this area and to document already fielded capabilities.

The core concept of the ETEE Reference Architecture is the User Application. This is a logical grouping of functionality as recognised by the user. Each user application can be further developed into underlying

activities. For ETEE, the user applications are grouped as ETEE Community Of Interest (COI) applications. Note that the user applications are not related to any technical architecture for implementation of the functionality.

The user operational requirements are mainly defined in terms of:

- References to the outcomes of the NATO Defence Planning Process (when available) and other NATO documents such as the NATO Task List;
- Functional requirements;
- Non-functional requirements;
- Information products used and processed; and
- Links to currently fielded systems.

The top-level user applications for ETEE are the following, based on NATO policy and directives.

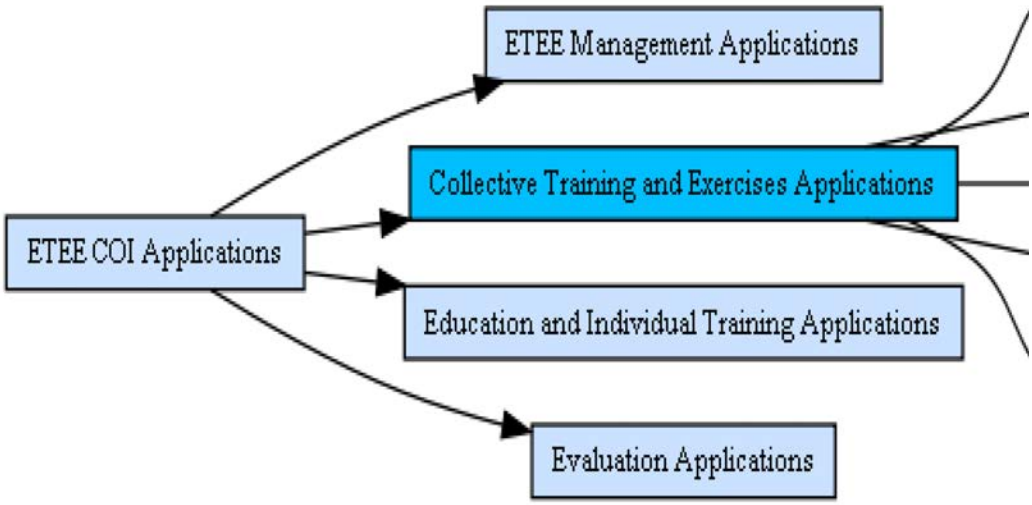

Figure 4-3: Top-Level User Applications for ETEE.

The ETEE Reference Architecture is being developed in the Enterprise Mapping Wiki, a password-protected collaborative work environment managed by ACT.

The user applications for ETEE are available here:

https://tide.act.nato.int/em/index.php?title=ETEE_COI_Applications

The elements of the ETEE Reference Architecture are part of the NATO C3 Classification Taxonomy available here:

https://tide.act.nato.int/em/index.php?title=C3_Classification_Taxonomy

M&S is highly relevant for ETEE, and M&S-specific sub-categories to ETEE COI Applications have been declared in the taxonomy. For example, a sub-category of ETEE COI Applications is Collective Training and Exercises (CTE) Applications, which in turn, has CTE M&S Applications; which “enable users to develop, maintain and execute models in order to provide a coherent, realistic and timely representation of information across Exercise Control (ExCon) and the training audience” (https://tide.act.nato.int/em/index.php?title=CTE_Modelling_and_Simulation_Applications).

4.5 SD VINTEL REFERENCE ARCHITECTURE (DEU)

4.5.1 General Description

A comprehensive reference architecture for service-oriented simulation environments has been developed in the German "SD VIntEL" project. Figure 4-4 shows the basic elements of the VIntEL reference architecture. The VIntEL reference architecture defines services in an implementation-independent way, e.g., the VIntEL reference architecture specifies a Weapon Effects Service (WES) with regards to syntax, semantics and pragmatic aspects, but does not specify the actual implementation.

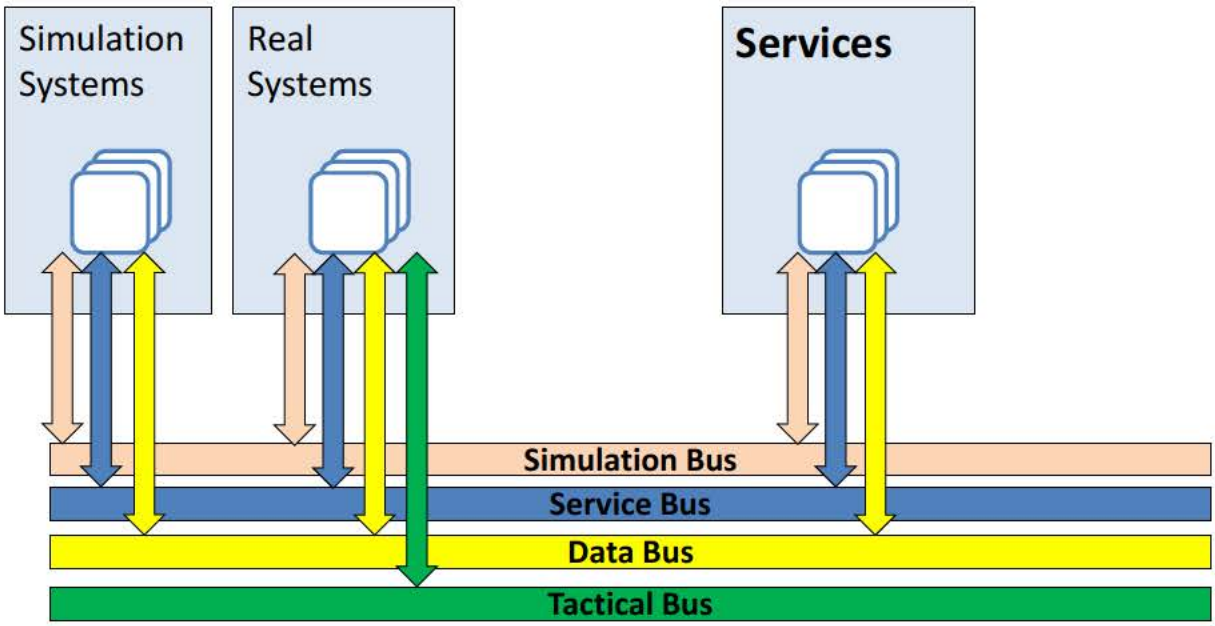

Figure 4-4: VIntEL Reference Architecture.

From this *VIntEL reference architecture*, several *Target architectures* for a series of evaluations and exercises were derived. An example of such a target architecture is shown in Figure 4-5. In contrast to the VIntEL reference architecture shown in Figure 4-4, the target architecture shown in Figure 4-5 specifies the actual implementations that are used for each service. For example, the Communications Effects Service (CES) is provided by the system KESS from Thales.

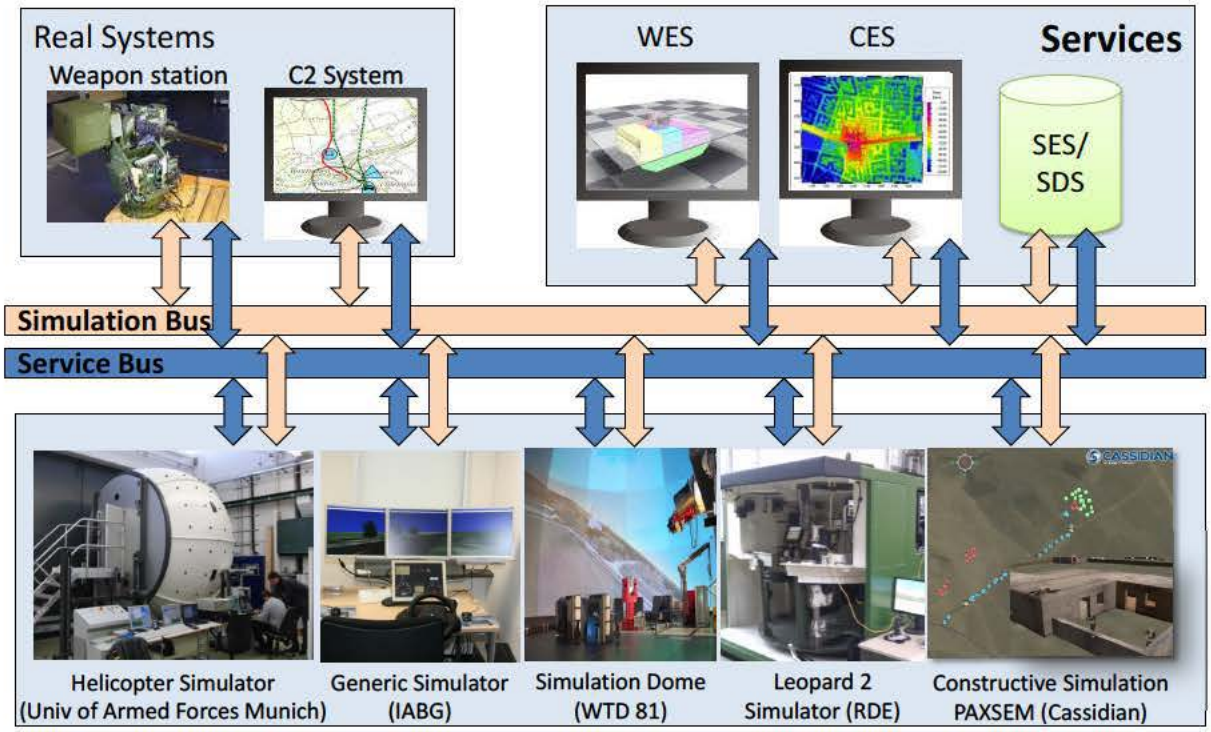

Figure 4-5: VIntEL Target Architecture (Example) as it Was or Would be Used in a Specific Simulation Environment.

4.5.2 Data Exchange Mechanism

The SD VIntEL Reference Architecture contains various data exchange mechanisms:

- **Simulation Bus**: For exchange of simulation data, currently HLA Evolved is used.
- **Service Bus**: Services may be integrated in different ways (e.g., as HLA federate but also via a separate service bus). Initial evaluations using an Enterprise Service Bus (RUDi) were made.
- **Data Bus**: For exchange of high-volume data (e.g., video links from a UAV), a dedicated data bus is use.
- **Tactical Bus**: For connection to C2 systems.

4.5.3 M&S-Specific Services

The SD VIntEL Reference Architecture contains various M&S-specific services:

- Weapon effects service (provided by IABG);
- Communication effects service (provided by KESS of Thales);
- Exterior ballistic service (provided by IABG);
- Synthetic environment service (provided by Rheinmetall and CPA); and
- Synthetic dynamic service (provided by Rheinmetall and CPA).

4.5.4 NAF Documentation

The architecture of SD VIntEL was modeled with NAF v3.1. Figure 4-6 shows the NAF views that have currently being described. This modeling of the architecture of SD VIntEL is an ongoing work. Presented here are some of the first steps of the modeling process.

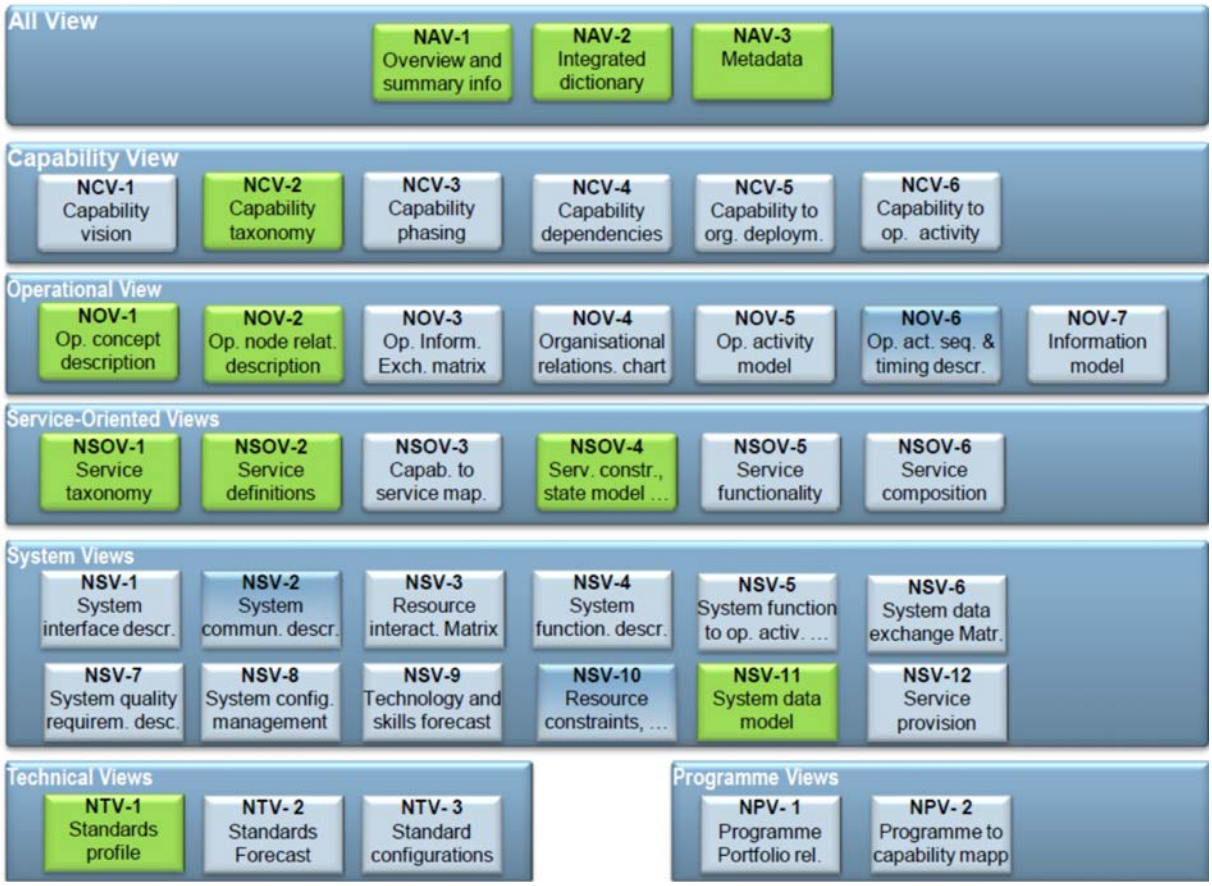

Figure 4-6: Overview of NAF v.3.1. The boxes marked in green are the views that have been described for the NAF model of the SD VIntEL Reference Architecture.

As an example, and because MSG-131 is focusing on the service domain, we pick the service-oriented views and have a closer look on them.

Figure 4-7 shows the NSOV-1/2 view on the existing services of SD VIntEL. As one can see, services are divided into three different types:

- Domain Services (services that fulfill a specific task within the simulation);
- Infrastructure Services (services that help to control the infrastructure); and
- Adaptor Services (services that connect features outside the infrastructure).

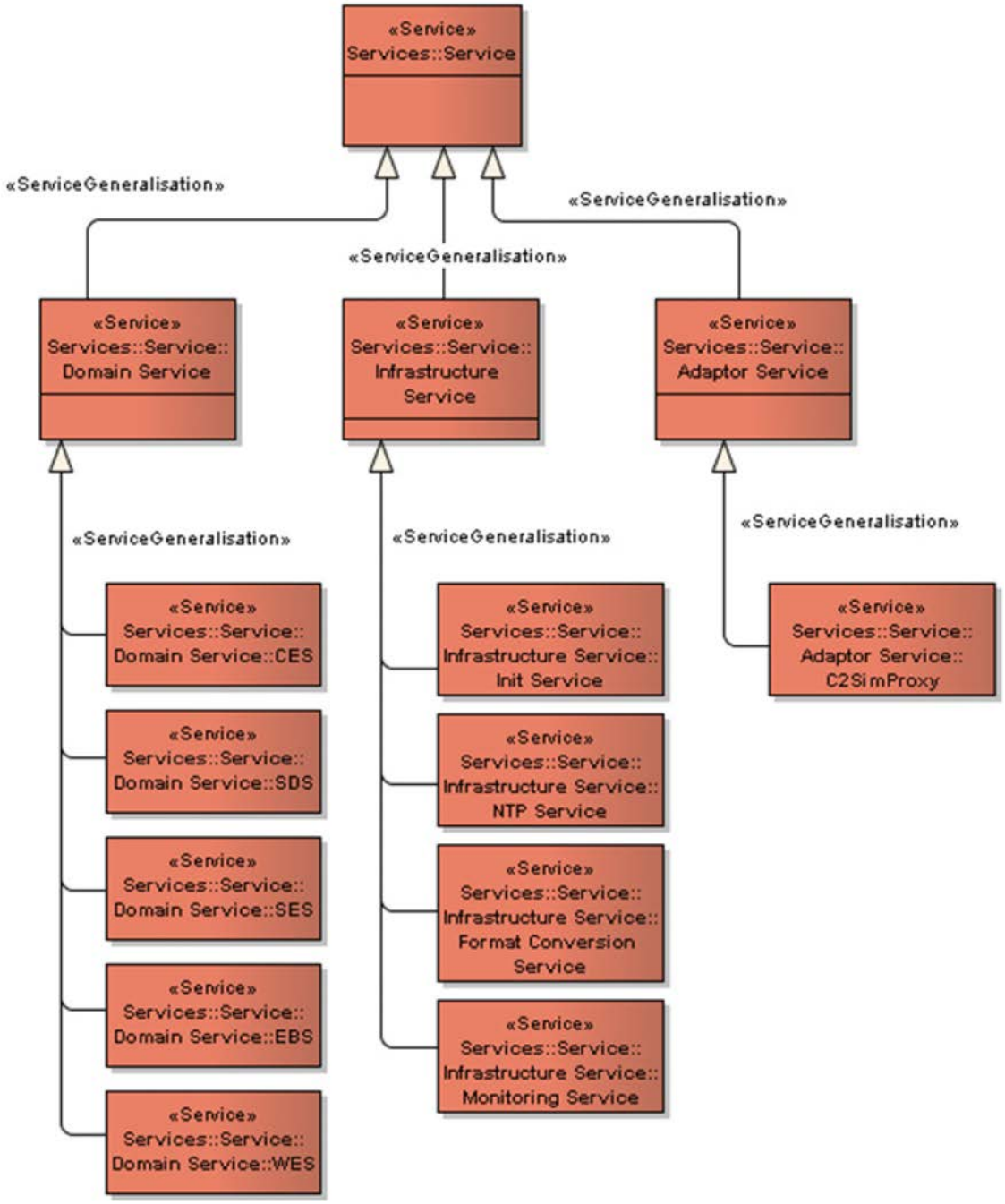

Figure 4-7: NSOV-1/2 (Service Taxonomy and Definitions) View on the Services of SD VIntEL.

The views of the NAF are used to separate all the components and describe them. The views also show the dependencies between the components. We give another example for this modeling in Figure 4-8 where dependencies and realizations in NSV-11 of SD VIntEL are shown.

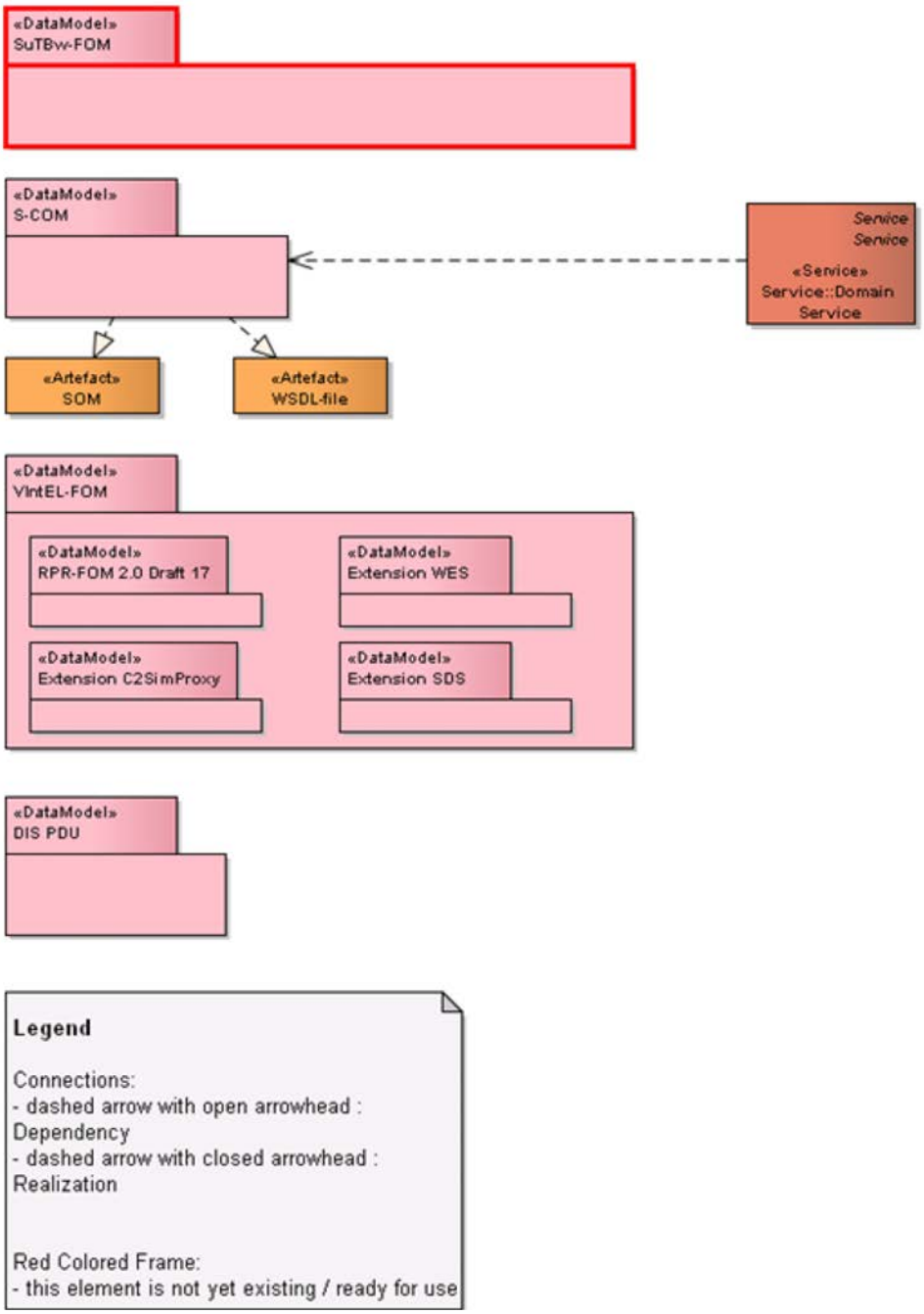

Figure 4-8: NSV-11 (System Data Model) View in SD VIntEL, Dependencies and Realizations.

Within the NAF modeling process, the SD VIntEL is handled as a reference architecture according to NAF terminology. Therefore, specific realizations of SD VIntEL in exercises or experiments are target architectures (see Figure 4-5).

4.6 NETN REFERENCE ARCHITECTURE

The NATO Education and Training Network (NETN) Federation Architecture and FOM Design (FAFD) document is a reference document intended to provide architecture and design guidance for developing distributed simulation and training systems in the context of Computer-Assisted Exercises (CAX).

The first version of the FAFD was developed by NATO Modelling and Simulation Group (NMSG) Task Group MSG-068 NETN. This Task Group was initiated to support the ACT Snow Leopard Program with M&S recommendations for establishing a NATO-wide Network for Education and Training (NETN), also known as "Snow Leopard".

A technical sub-group of MSG-068, Federation Architecture and FOM Design (FAFD), was created with representatives from the participating NATO and Partner Nations. This group represented a broad community of practice with respect to federation architecture and design. Major systems, federations and training networks were represented in the FAFD group. The input provided and the harmonization of federation architecture and design agreements formed the first version of the NETN FAFD.

The second version of the NETN FAFD was developed by a second NMSG Task Group, namely the MSG-106 "Enhanced CAX Architecture, Design and Methodology – SPHINX" technical (TEK) sub-group. This group modified the original agreements based on practical experiences in using the NETN recommendations in major exercises and experiments and included clarifications, recommendations and agreements resulting from work accomplished during the tenure of MSG-106.

Key recommendations of NETN include:

- Use of NATO STANAG 4603 (High-Level Architecture);
- Use of NATO NETN FOM and associated standard and NATO NETN developed FOM modules;
- Use of RPR-FOM v2.0 (modularized);
- Use of German maritime FOM modules;
- Use of Link16 BOM;
- Use of transfer of modelling responsibilities design pattern;
- Use of MSDL to support initialization;
- Use of CBML to support simulation-to-C2 interoperability;
- Design recommendations to support multi-resolution modeling;
- Design recommendations for fail-over and fault management;
- Design recommendations to optimize performance; and
- Design recommendations for federation execution control.

More detailed information is available in Refs [24] and [9].

The NETN reference architecture is still under development, but has seen applications already on a national level (e.g., NLD) as recommended interoperability 'backbone'. The NETN reference architecture has also been used in the major multi-national exercise in Scandinavia 'Viking 14'. The NETN reference architecture was tailored into a target architecture to meet the specific set of applications that participated in Viking 14.

4.7 MTDS REFERENCE ARCHITECTURE

NATO AWACS and Nations have a common need for training of air combined and joint collective tactical training, referred to in NATO as Mission Training through Distributed Simulation (MTDS).

Based on the work of previous NATO and (multi-)national studies and projects, NATO MSG-128 "Incremental Implementation of NATO MTDS Operations " is tasked to establish essential elements for a NATO MTDS environment, including:

- Concept;
- Standards and agreements;
- Legal and security framework;
- Services infrastructure; and
- Standing operating procedures.

One deliverable of NATO MSG-128 at the end of its term in 2016 will be the “MTDS Reference Architecture and Design” (MRAD).The MRAD will specify a reference architecture for the MTDS domain.

The resulting Reference Architecture (RA) will be the blueprint for specific exercises (target architectures) that may involve new participants for specific training needs. The solutions that are developed for a specific exercise may later be integrated into the RA when they are sound and considered to have value beyond a specific case. The experiences gained through these exercises will also result in new requirements for the RA that must first be investigated and developed.

Chapter 5 – REQUIREMENTS ON FUTURE SERVICE-ORIENTED ARCHITECTURES FOR M&S

Based on findings presented in Ref. [43] and discussions within MSG-131, requirements and recommendations on future simulation environments are presented.

The requirements and recommendations apply to simulation environments in general and are not specific to MSaaS. However, service-based approaches are very promising for realizing such future distributed simulation environments. Service-based approaches are well suited to directly satisfy many of the recommendations outlined in the following sections (e.g., SD-2 “Modularity”, IN-1 “Harmonize Critical Data and Algorithms”) and provide a good technical basis for satisfying recommendations like IN-2 “Establish Permanent Simulation Infrastructure” and DA-1 “Enforce Single Source of Truth Principle”.

5.1 REQUIREMENTS ON FUTURE SIMULATION ENVIRONMENTS

The M&S vision as stated by NATO [31] needs to be operationalized and broken down into measurable requirements. Taking into account recent results of national and international research projects, the high-level requirements on future simulation environments are as noted in Table 5-1.

Table 5-1: Requirements on Future Simulation Environments.

RE-1	Improve development of effective simulation environments, i.e., ensure that a simulation environment satisfies the users’ needs (related to DSEEP Step 1). In terms of measurable requirements this requires that the users’ needs (i.e., the requirements on a simulation environment) are completely known, consistent, and documented.
RE-2	Enable efficient preparation, development, integration, and maintenance of simulation environments. In terms of measurable requirements, the time required for executing the activities defined in DSEEP Steps 2 to 5 should be less than one month for average simulation environments.
RE-3	Enable efficient initialization and execution of simulation environments (as specified by DSEEP Step 6). In terms of measurable requirements this requires: (RE-3.1) Provide capability for centrally coordinated initialization of a simulation environment without manual interaction. (RE-3.2) Enable full initialization of a typical simulation environment within 15 minutes.
RE-4	Enable simulation environments that achieve fair fight. In terms of measurable requirements, this requires an objective and automatic assessment whether a simulation environment and its member applications comply with the specified fair fight requirements.

RE-5	Enable simulation environments that deliver credible simulation results. In terms of measurable requirements, this requires: (RE-5.1) Provide traceable documentation of the simulation environment engineering process (requirements, assumptions, constraints, agreements, version control, compliancy certification, etc.). Related to application of formal methods such as DSEEP. (RE-5.2) Provide traceable documentation of the simulation environment validation process (requirements, assumption, constraints, agreements, evidence, etc.). (RE-5.3) Provide automated control mechanisms for assessing the quality requirements of a simulation environment during execution. Typical quality requirements may include performance metrics, fair fight conditions, security violations, etc. (RE-5.4) Provide automated control mechanisms for assessing the quality requirements of a simulation environment after its execution. Typically this includes analysis of recorded generated simulation data and other output of a simulation environment (e.g., log files).
RE-6	Enable simulation environments that consistently deliver identical simulation results when initialized with identical data and executed under identical conditions. In terms of measurable requirements this requires: (RE-6.1) Full documentation of a simulation environment (participating systems, software versions, configuration, etc.). (RE-6.2) Full documentation of initialization data and execution data (initial state, course of events, etc.). (RE-6.3) If required, long-term storage of configuration files, software applications, etc. The degree of reproducibility may vary greatly for different simulation environments (e.g., basic reproducibility may only require using the same data, while full reproducibility may require using the exact same versions of participating systems) and may not always be fully achievable (e.g., in simulation environments with manual interaction). Depending on the required degree of reproducibility, the requirements defined above may need to be extended.

5.2 NON-FUNCTIONAL REQUIREMENTS AS DRIVERS FOR FUTURE SIMULATION ENVIRONMENTS

In software engineering, non-functional requirements (e.g., regarding security or scalability) are regularly considered as major impact factors for software architecture and software design. The same is true with regards to simulation environments – while functional requirements (like RE-3.1) are relatively easy to satisfy, non-functional requirements like RE-2 and RE-3.2 are considered to require substantially more effort to be achieved.

MSG-131 was hesitant to specify actual objectives for non-functional requirements RE-2 (preparation time for a simulation environment should be less than one month) and RE-3.2 (full initialization of a simulation

environment in less than 15 minutes) as simulation environments vary greatly in terms of size, complexity, and available resources. Nevertheless, due to the paramount importance on non-functional requirements on architecture and design of future simulation environments, actual objectives are specified. The requirements RE-2 and RE-3.2 are considered as major drivers and as such they are intentionally ambitious.

5.3 RECOMMENDATIONS FOR FUTURE SIMULATION ENVIRONMENTS

5.3.1 Recommendations on System Design

The following recommendations are concerned with simulation systems (and other member applications) that are likely to be part of distributed simulation environments. These recommendations target an easier integration of new or adapted systems into a next-generation distributed simulation environment.

The recommendations made below align with NATO's and NMSG's principles as covered in the NMSMP: Interoperability, Reuse and Synergy. These principles are achieved by advances towards:

- Develop Common Technical Framework (technical and methodology);
- Develop Common Services;
- Develop Models;
- Deploy Models; and
- Implement Technological Advances.

The adoption (or development) of common standards is a major aspect of improving interoperability. NATOs policy is to apply open standards whenever feasible.

5.3.1.1 Recommendation SD-1: Design and Document for Interoperability

Probably the most important recommendation is to design and document a simulation system (or any other member application) for interoperability. 'Interoperability' as a requirement needs to be considered from the very beginning when developing or adapting a simulation system. To design for interoperability requires advocating for modularity and changing execution conditions. Hard-coded algorithms, fixed configurations, and tacit assumptions need to be avoided.

Documentation for interoperability requires thoroughly documenting assumptions and limitations of simulation systems. Documenting assumptions and limitations is of great importance as this information is absolutely required for achieving interoperability on higher levels (i.e., from pragmatic to conceptual level). Furthermore, interoperability experiences made with a simulation system should be documented (e.g., lessons learned from past simulation environments and experiments) to avoid repeating work and allowing faster evaluation as to whether a specific integration of a simulation system into a simulation environment is feasible.

5.3.1.2 Recommendation SD-2: Design and Document for Modularity and Composability

Usually simulation environments are composed of multiple simulation systems (member applications), i.e., simulation systems are components of a simulation environment. Similarly, simulation systems themselves should be designed in a modular way and built from smaller components. Modularity and composability are two sides of a coin and need to be considered jointly. These two terms are often used synonymously and express the fact that a system is composed of other systems (modules) and that exchanging single modules is rather the rule than the exception.

To design for modularity and composability requires planning for exchangeability of algorithms, calculations, data, etc. Typical approaches towards modularity are object-oriented decomposition of a system (e.g., a cruise missile consists of guidance system, payload, and propulsion system) or functional decomposition of a system (e.g., a cruise missile has to execute functions for imaging or path finding). Although object-oriented approaches are more common, functional decomposition might be better in terms of modularity and reusability of modules [22],[28].

To document for modularity and composability requires documenting interfaces and relationships between modules. This documentation has to span all levels of interoperability (see Refs [46] and [47] for an in-depth discussion of interoperability levels). Furthermore, the decomposition strategy has to be documented to allow evaluating the pragmatic interoperability of simulation systems.

5.3.1.3 Recommendation SD-3: Favour Open Standards

Simulation systems that are intended to be used within distributed simulation environments should use open standards wherever possible. In general, compliance of a system with standards (not necessarily open standards) allows easier integration into a simulation environment. Also, it is more likely that additional tools (e.g., gateways, data analyzer) are available for established standard protocols and formats (see also Ref [1] for more reasons).

Open standards should be favoured compared to closed or de facto standards (see Ref [1] for details on terminology). The openness provides the additional benefit that a standard may be implemented more easily and avoids the danger of vendor lock-in that is immanent to closed standards. Furthermore, open standards are usually developed and maintained by a standards development organization – like the Simulation Interoperability Standards Organization (SISO) or the Open Geospatial Consortium (OGC) – which encourages participation in the development process, safeguards against undue influence on the standard development direction and ensures long-term availability of a standard.

Examples for potential use of open standards are:

- Use open interface standards for initialization of systems like OGC Web Feature Service (WFS), OGC Web Map Service (WMS), or Military Scenario Definition Language (MSDL);
- Use open data models like SEDRIS;
- Use reference data exchange models like RPR-FOM (open standard) or NETN FOM (potential future NATO standard [24],[26]);
- Use open simulation execution control patterns as proposed by MSG-052 [23] (to be standardized); and
- Use open control mechanisms like Distributed Debrief Control Architecture (DDCA) that is currently under development by SISO.

5.3.1.4 Recommendation SD-4: Design for Securability

As simulation environments are often faced with security concerns (e.g., due to processing classified data), components that are intended for use within future simulation environments need to be designed for securability. In this context, securability is defined as the extent to which a component or simulation system (member application) is securable. This especially addresses the ability of a simulation system to interoperate on different security levels without unintentional disclosure of information. Similarly, security aspects of connecting systems on the same levels of security have to be considered where different information is allowed to passed, i.e., from a tactical bus (C2) to a simulation bus.

Many approaches are currently used when connecting differently classified systems, like “System high”, “Multiple single levels of security”, or “Multiple independent levels of security” [4]. As these approaches come with many drawbacks, they are not recommended for future simulation environments. Instead future simulation environments require an approach that enables a flexible combination of differently classified systems.

Designing for securability includes:

- Enabling a simulation system to use differently classified data (e.g., via different data sets that are provided by removable disk drives or usage of different service implementations) and differently classified algorithms. This recommendation is tightly related to SD-2 “Modularity”.
- Enabling a simulation system to connect to differently classified networks. This may also affect physical infrastructure issues (e.g., building).

5.3.2 Recommendations on Simulation Environment Infrastructure

The following recommendations are concerned with infrastructure issues regarding next-generation distributed simulation environments. These recommendations target at faster set-up processes and more credible simulation environments.

5.3.2.1 Recommendation IN-1: Harmonize Critical Data and Algorithms

Currently, many problems are caused by incompatible data or algorithms of participating simulation systems (e.g., different visual representation of critical assets, different algorithms for computing weapons effects). To overcome these problems, critical data and algorithms have to be harmonized. Obviously, the decision which data and algorithms are critical depends on the application area of a simulation environment and cannot be generally determined. However, most military simulation environments have commonalities that are regularly considered critical (e.g., synthetic natural environment data, weapons effects calculation, communication effects calculation).

As a first step, a harmonization of the identified critical data and algorithms is required. This may be achieved by providing (free-text) specifications for identified critical data and algorithms. Every simulation system may implement these critical components separately as long as the specifications are satisfied.

In a second step, dedicated components may be provided (e.g., as software libraries) such that redundant implementation efforts are reduced or eliminated. Taking this a step further, these components may be treated as services that are centrally deployed and utilized by many simulation systems (i.e., software as a service).

Finally, the components and services need to be standardized (on the technical, syntactical, semantic, and pragmatic level). This allows different implementations of components and services (e.g., a classified weapons effects service and a non-classified one) and goes hand-in-hand with recommendations SD-2 “Modularity”, SD-3 “Favour Open Standards”, and SD-4 “Design for Securability”.

5.3.2.2 Recommendation IN-2: Establish Permanent Simulation Infrastructure

Significantly improving preparation and set-up times requires the establishment of a persistent NATO simulation infrastructure. This includes:

- Network connections (e.g., between different sites or Nations);
- Simulation environment control facilities;

- Provision of shared components and services in a “Defence Cloud” (e.g., Nation-wide or NATO-wide); and
- Provision of an information management system that supports the whole simulation environment engineering process (e.g., with regards to documentation, execution planning, file sharing).

Depending on the actual requirements (especially RE-2 and RE-3) the extent of the persistent simulation infrastructure may vary. As the permanent simulation infrastructure is an essential part of future simulation environments, it has to be documented thoroughly (see PO-2 “Use a Systems Engineering Process and Document Decisions”).

Experiences from many national simulation environments have shown that a permanent simulation infrastructure is a key to achieving significantly faster and more reliable set-up processes. It has to be stressed that establishment of a permanent simulation infrastructure does not only concern technical issues, but also establishment of a permanent support organization with skilled and experienced personnel.

5.3.2.3 Recommendation IN-3: Establish Member Application Compliance Testing

Fast and reliable development processes for future simulation environments require automated compliance testing of participating simulation systems and other member applications (e.g., command and control systems). The automated compliance testing has to include test cases on all interoperability levels:

- **Technical Level**: Test compliance with TCP/IP, HLA interfaces, etc.;
- **Syntactical Level**: Test compliance with interface syntax specifications;
- **Semantic Level**: Test compliance with data exchange model (e.g., with a specific FOM in HLA-based simulation environments); and
- **Pragmatic Level**: Test compliance with conceptual models (e.g., with the service consumer-provider pattern [18]).

Regarding federates for HLA-based simulation environments, this topic was investigated by ET-35 (“HLA Federation Compliance Test Tool”) and will probably be continued by MSG-134 (“NATO Distributed Simulation Architecture and Design, Compliance Testing and Certification”).

In national research projects, the experimental tools FACTS (Federation Agreements Conformance Test Service) and FIERS (Federation Integration and Experimentation Rehearsal Surrogate) are used to verify a specific sub-set of federation agreements and to easily provide mock-up federates for test purposes. A similar approach for testing simulation gateways is described in [20].

Configuration of such a compliance testing tool should be via a standardized data format (ideally defined in an open standard). Reuse of parts of this configuration is required (e.g., in form of “configuration modules”) for efficient handling of recurring test cases (e.g., testing compliance with RPR FOM).

5.3.2.4 Recommendation IN-4: Establish Simulation Environment Execution Compliance Testing

Achieving reliable and credible simulation results requires continuous monitoring of a simulation environment execution. Deviations from specified behaviour, errors, etc., need to be detected and assessed as to whether they influence the simulation execution and simulation results.

Due to the distributed nature and the manifold data exchange between participating simulation systems and other member applications, such a monitoring and assessment cannot be done manually but has to be done in an automated fashion. Execution compliance testing is similar to member application compliance testing as

described in IN-3, but takes this one step further. Continuous monitoring and assessment of a simulation environment execution is required, especially for ensuring credibility in simulation results.

Configuration of such a compliance testing tool should be via a standardized data format (ideally defined in an open standard). Reuse of parts of this configuration is necessary (e.g., in form of "configuration modules") for efficient handling of recurring test cases (e.g., that only RPR-FOM compliant interaction messages are used, or that specific fields within a message are used correctly).

5.3.3 Recommendations on Simulation Environment Engineering Processes and Organization

The following recommendations are concerned with organizational issues regarding future simulation environments. These recommendations target more reliable processes and more credible simulation environments.

5.3.3.1 Recommendation PO-1: Enforce Requirements Specification

Although seemingly obvious, the recommendation to enforce good requirements specifications is explicitly made. This includes all types of requirements (e.g., regarding desired terrain, required terrain fidelity, participating units) and includes also quality and fair fight requirements. The last two are often not specified explicitly, but taken for granted or implicitly assumed. The resulting problem is: How to assess quality or fair fight if they are not specified and agreed upon?

Besides organizational measures (procedures, etc.), it is recommended to assist the user as much as possible. Good experiences were made using checklists for elicitation of typical quality or fair fight requirements. Also documentation templates have proven to be useful for ensuring more complete requirements specifications.

Talking about future simulation environments, dedicated information management systems should be established that further assist users during the requirements specification process and throughout the whole simulation environment engineering process (see IN-2).

5.3.3.2 Recommendation PO-2: Use a Systems Engineering Process and Document Decisions

Setting up a simulation environment is a complex task and requires professional management. Therefore, the recommendation is to use an appropriate systems engineering process to ensure that all persons involved in the process have a common understanding of ongoing activities and expected deliverables.

The Distributed Simulation Engineering and Execution Process (DSEEP) is an obvious choice for such a systems engineering process [7]. As it provides a generalized, high-level framework DSEEP has to be adapted to the individual needs of an organization. The VEVA process model is an example of such an organization-specific adaptation of the DSEEP that is used by the German Armed Forces [41]. Some initial work has also started towards addressing service-oriented architecture approaches in DSEEP.

Besides the choice of a systems engineering process, a decision has also to be made regarding its documentation. Several approaches and standards may be used for documenting simulation environments (e.g., Base Object Models [42] or the NATO Architecture Framework [27]).

5.3.3.3 Recommendation PO-3: Establish Simulation Repository

In alignment with IN-2 (provision of an information management system that supports the whole simulation environment engineering process), it is recommended to establish a simulation repository.

Such a simulation repository (or information management system) should support the user throughout the whole simulation environment engineering process (e.g., using the DSEEP) and should provide a central repository for all kind of documentation, data, and file storage.

5.3.4 Recommendations on Simulation Environment Data

The following recommendation is concerned with all types of data that are likely to be part of simulation environments. This recommendation targets a faster set-up process of future simulation environments and more credible simulation environments.

5.3.4.1 Recommendation DA-1: Enforce "Single Source of Truth" Principle

Many data-related interoperability problems are caused by different simulation systems (or components thereof) using different data that is uncorrelated (although it is expected to represent the same facts). A typical example is a simulation environment with two simulators that use individually manufactured terrain databases of the same area. Although the same area is represented by the terrain databases, differences between the terrain databases are often large enough to cause severe interoperability problems and fair fight violations.

The "single source of truth" principle requires that each source data item is stored only once and that all application-specific data items or data formats are derived from this source data item. Figure 5-1 illustrates the "single source of truth" principle for terrain data.

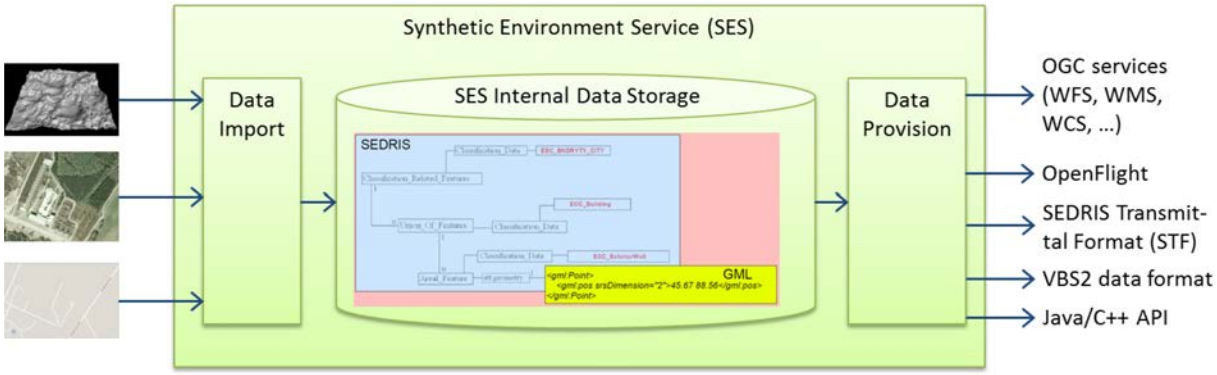

Figure 5-1: Basic Idea of a Synthetic Environment Service (SES) that Realizes the "Single Source of Truth" Principle for Terrain Data.

This recommendation is tightly related to SD-2 (Modularity) and SD-3 (Favour Open Standards). Realizing the "single source of truth" principle is ideally accompanied by establishing a permanent infrastructure for storage and maintenance of the original source data (see IN-2 "Establish Permanent Simulation Infrastructure").

Chapter 6 – CONCLUSIONS AND RECOMMENDATIONS

6.1 CONCLUSIONS

Modeling and Simulation (M&S) in general is widely utilized by NATO and the Nations in various domains. Although a seemingly new approach, the survey done by MSG-131 shows that M&S as a Service (MSaaS) is already widely utilized by NATO and the Nations. However, this survey of national case studies also revealed a large diversity with regards to MSaaS in NATO and the Nations.

To a great extent, future military training capabilities will be provided by simulation systems (either stand-alone or via distributed simulation environments). This is a consequence of limited or decreasing budgets, restrictions due to security and safety regulations, and shorter response times as well as increasingly faster changing mission profiles and operational needs. Accordingly, the main challenges regarding the use of M&S are to provide operational solutions faster and better; and to enable a more efficient development, usage and maintenance of M&S solutions.

Based on the survey of existing MSaaS case studies, MSG-131 concludes that service-based approaches can contribute towards more efficient M&S. To focus discussions, MSG-131 defined four perspectives on MSaaS that describe different application scenarios.

Some applications of MSaaS may be relatively easy to introduce and gain benefit from, but it will be a challenging task to map service orientation to simulation architectures in general. For example, if the goal is to have distributed simulation systems interact in a service-oriented manner rather than have the simulation systems interact with the simulation infrastructure as if it were a service. In terms of HLA, the goal may be for federates to see each other as service providers and to interact as such instead of purely interacting with the simulation infrastructure.

To put MSaaS in a proper context of related NATO activities, MSG-131 shows how M&S and MSaaS may be aligned with the NATO C3 Classification Taxonomy that is the primary tool used by NATO to chart the NATO Consultation, Command and Control (C3) landscape.

The survey done by MSG-131 also revealed a large diversity in existing MSaaS reference architectures. The identified reference architectures are located on very different levels (from technical level to overarching enterprise level) and thus are not directly comparable.

MSG-131 identified various open issues with regards to MSaaS, spanning a broad range from technical to organizational questions.

6.2 RECOMMENDATIONS

In accordance with its Technical Activity Description, MSG-131 recommends investigation of MSaaS in more detail. A Technical Activity Proposal for a follow-on Research Task Group was developed by MSG-131 and endorsed in June 2014. The Task Group MSG-136 (“Modelling and Simulation (M&S) as a Service (MSaaS) – Rapid deployment of interoperable and credible simulation environments”) will start its 3-year term in November 2014.

MSG-131 recommends further that the NMSG as NATOs delegated tasking authority for M&S interoperability standards investigates how to establish permanent/persistent M&S services within the Alliance. This task should be addressed in the approved follow-on Task Group MSG-136 by specialists from NATO organizations and Nations. The focus should be on the training domain and the decision support domain as the leading application areas. The Task Group should research the topic in more detail through

multi-national experimentation and develop recommendations regarding service-oriented methodology and possible extensions of a future iteration of the DSEEP and HLA standards. The hands-on experiences with multi-national case studies will provide guidance and candidates for architectures, data models and interfaces that could become future SISO standards. NMSG should work closely with SISO and IEEE as the custodians of HLA and DSEEP. SISO should lead the investigation with respect to the application of SOA in the M&S domain in general.

Furthermore, an alignment of “M&S as a Service” with the Connected Forces Initiative (CFI) is required, as the primary objective of M&S in the CFI (i.e., sharing and pooling of resources) is closely reflected in MSaaS. This alignment should be done jointly by NMSG and ACT.

Chapter 7 – REFERENCES

[1] NATO: NATO Modelling and Simulation Standards Profile. AMSP-01, Edition (B), Version 1, June 2011.

[2] Bocciarelli, P. and D'Ambrogio, A. (2011) "A Model-Driven Method for Describing and Predicting the Reliability of Composite Services", Software and System Modeling, Vol. 10, No. 2, pp. 265-280.

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

[4] Croom-Johnson, S., Huiskamp, W. and Möller, B. (2013) "Security in Simulation – A Step in the Right Direction", SISO 2013 Fall SIW, Orlando, FL, USA, 13F-SIW-009.

[5] D'Ambrogio, A. (2006) "A Model-Driven WSDL Extension for Describing the QoS of Web Services", 2006 IEEE International Conference on Web Services (ICWS 2006), 18-22 September 2006, Chicago, IL, USA.

[6] US Department of Defense (DoD) Modeling and Simulation (M&S), "DoD M&S Glossary", July 2013, http://msco.mil/MSGlossary.html.

[7] Institute of Electrical and Electronics Engineers, "IEEE Recommended Practice for Distributed Simulation Engineering and Execution Process (DSEEP)", IEEE Standard 1730-2010.

[8] MC 458/2, NATO Education, Training, Exercise and Evaluation (ETEE) Policy (Final), 12 October 2009.

[9] NATO: "NETN Federation Architecture and FOM Design v2.0", as of 4 July 2014 available as DRAFT.

[10] Gamma, E., Helm, R., Johnson, R. and Vlissides, J. (1994) "Design Patterns – Elements of Reusable Object-Oriented Software", Addison-Wesley.

[11] Hannay, J., Bråthen, K. and Mevassvik, O.-M., (2013) "Simulation Architectures and Service-Oriented Defence Information Infrastructures – Preliminary Findings", Norwegian Defence Research Establishment (FFI), FFI-rapport 2013/01674, 30 August 2013.

[12] RUDi: "IT Security Architecture", R&T Report, 2012. Available via Sharepoint.

[13] IEEE Standard Glossary of Software Engineering Terminology, IEEE Std 610.12-1990, December 31 1990, doi: 10.1109/IEEESTD.1990.101064.

[14] Iqbal, M., Nieves, M. and Taylor, S. (2007) "Service Strategy"; TSO (The Stationery Office); Published for the Office of Government Commerce (OGC).

[15] ISO/IEC 20000. http://www.iso.org, ISO/IEC 20000-1:2011.

[16] ITIL Glossary: http://www.itil-officialsite.com, ITIL glossary and abbreviations, AXELOS Limited 2011.

[17] Josuttis, N.M. (2007) "SOA in Practice: The Art of Distributed System Design", O'Reilly Media Inc.

[18] Khayari, R., Neumann, K.-H., Devaud, S., Faye, J.-P., Desert, D., Ruiz, J. and Löfstrand, B. (2011) "NATO Education and Training Network (NETN): Logistics and Transfer of Control FOM Modules Harmonization", SISO 2011 Fall SIW, Orlando, FL, USA, 11F-SIW-012.

[19] Krückhans, M. (2012) "ISO and OGC compliant Database Technology for the Development of Simulation Object Databases", Winter Simulation Conference 2012, Berlin, Germany.

[20] Lutz, R., Drake, D., Brunton, R., O'Connor, M., Lessmann, K. and Cutts, D. (2013) "A LVCAR-I Retrospective: Tools, Processes, and Specifications for Gateway Selection and Configuration", SISO 2013 Fall SIW, Orlando, FL, USA, 13F-SIW-011.

[21] Modi, P.J., Regli, W.C. and Mayk, I. (2006) "The Case for a Reference Model for Agent-Based Systems", In Proceedings of the IEEE Workshop on Distributed Intelligent Systems: Collective Intelligence and Its Applications. DIS 2006, pp. 321-325. IEEE Computer Society, June 2006. 10.1109/DIS.2006.69.

[22] Moynihan, T. (1996) "An Experimental Comparison of Object-Orientation and Functional-Decomposition as Paradigms for Communicating System Functionality to Users", Journal of Systems and Software, Vol. 33, Issue 2, May 1996, pp. 163-169.

[23] NATO: Final Report of MSG-052 "Knowledge Network for Federation Architecture and Design", TR-MSG-052, November 2011.

[24] NATO: Final Report of MSG-068 "NATO Education and Training Network". RTO Technical Report RTO-TR-MSG-068 AC/323(MSG-068)TP/407, February 2012.

[25] NATO STO: Final Report of NATO MSG-086 "Simulation Interoperability". STO Technical Report STO-TR-MSG-086-Part-I, January 2015.

[26] NATO: MSG-106 "Enhanced CAX Architecture, Design, and Methodology – SPHINX".

[27] NATO Consultation, Command and Control Board (NC3B): NATO Architecture Framework. Version 3, AC/322-D(2007)0048-AS1, 2007.

[28] Narbel, Ph. (2009) "Functional Programming at Work in Object-Oriented Programming", in Journal of Object Technology, Vol. 8, No. 6, September-October 2009, pp. 181-209, http://www.jot.fm/issues/issue_2009_09/article5/.

[29] Neugebauer, E., Nitsch, D. and Henne, O. (2009) "Architecture for a Distributed Integrated Test Bed", NATO RTO Modelling and Simulation Group Symposium (MSG-069), Brussels, Belgium, October 2009, RTO-MP-MSG-069 Paper 19.

[30] Mell, P. and Grance, T. "The NIST Definition of Cloud Computing", National Institute of Science and Technology, U.S. Department of Commerce, Special Publication 800-145, September 2011.

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

[32] OASIS, Reference Model for Service Oriented Architecture 1.0, OASIS Standard, 12 October 2006. https://www.oasis-open.org.

[33] Oberndorfer, M., van Geest, J. (2011) "Modelling and Simulation Events Enabled by the Distributed Networked Battle Labs Framework", RTO-MP-MSG-087: Enhance or Replace: Finding the Right Live vs Synthetic Balance, Paper 6, October 2011.

[34] Oberndorfner, M. (2012) “The Distributed Networked Battle Labs Framework (DNBL) as the Operating and Business Model for Experimentation, Test and Evaluation”, STO-MP-MSG-094: Transforming Defence Through Modelling and Simulation – Opportunities and Challenges, Paper 16, October 2012.

[35] “Navigating the SOA Open Standards Landscape Around Architecture”. Joint White Paper from OASIS, OMG, and The Open Group, July 2009, https://www2.opengroup.org/ogsys/catalog/w096.

[36] The Open Group, SOA Reference Architecture, document number C119, November 2011. http://www.opengroup.org.

[37] The Open Group, Service Oriented Architecture Ontology, Version 2.0. Document number C144, April 2014. http://www.opengroup.org.

[38] Object Management Group. Service oriented architecture Modeling Language (SoaML) Specification, Version 1.0.1, May 2012. http://www.omg.org/spec/SoaML/1.0.1/.

[39] Probst, J. (2009) “ANATOMY OF A SERVICE – A Practical Guide to Defining IT Services”, Pink Elephant.

[40] Schmidt, B. and Schneider, B. (2004) “Agent-Based Modelling of Human Acting, Deciding and Behaviour - The Reference Model PECS”. In Graham Horton, editor, Network Simulations and Simulated Networks, pages 378–387. SCS Europe, 2004. Proceedings of the 18th European Simulation Multiconference 2004.

[41] Siegfried, R., Herrmann, G., Lüthi, J. and Hahn, M. (2011) “VEVA as German approach towards operationalizing the DSEEP: Overview and first experiences”, SISO 2011 Spring SIW, Boston, MA, USA, 11S-SIW-044.

[42] Siegfried, R., Laux, A., Rother, M., Steinkamp, D., Herrmann, G., Lüthi, J. and Hahn, M. (2012) “Components and Reuse in Scenario Development Processes for Distributed Simulation Environments”, SISO 2012 Fall SIW, Orlando, FL, USA, 12F-SIW-046.

[43] Siegfried, R., Bertschik, M., Hahn, M., Herrmann, G., Lüthi, J. and Rother, M. (2013) “Effective and Efficient Training Capabilities through Next Generation Distributed Simulation Environments”, 2013 NMSG Multi-Workshop, Sydney, Australia, Paper 7.

[44] Stüber, R. and Krückhans, M. (2012) “Increased sustainability of Simulation Object Databases using international norms and standards”, NATO MSG Conference 2012, Stockholm, Sweden, Paper 15.

[45] Thomas, O. (2006) “Understanding the Term Reference Model in Information Systems Research: History, Literature Analysis and Explanation”, In Christoph Bussler and Armin Haller, Editors, Business Process Management Workshops, Volume 3812 of Lecture Notes in Computer Science, pp. 484-496, Berlin, Heidelberg, 2006. Springer-Verlag.

[46] Tolk, A. and Muguira, J.A. (2003) “The Levels of Conceptual Interoperability Model”, SISO 2003 Fall SIW, Orlando, FL, USA, 03F-SIW-007, September 2003.

[47] Tolk, A., et al., (2006) “Ontology Driven Interoperability – M&S Applications”, White paper for Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2006.

[48] Cayirci, E. (2013) “Modeling and simulation as a cloud service: A survey”, Proceedings of the 2013 Winter Simulation Conference, 8-11 December 2013, doi: 10.1109/WSC.2013.6721436.

[49] Taylor, S.J.E., Khan, A., Morse, K.L., Tolk, A., Yilmaz, L. and Zander, J. (2013) “Grand Challenges on the Theory of Modeling and Simulation”, In Proceedings of the 2013 Symposium on the Theory of Modeling and Simulation, SCS, Vista, CA, USA.

[50] Drake, D., Martins, I.X., Roca, R.A. and Carr, F. (2011) “Live-Virtual-Constructive Service-Oriented Architecture, Service-Oriented Architecture, Application to Live-Virtual-Constructive Simulation: Approach, Benefits, and Barriers”, NSAD-R-2011-025.

[51] “Systems and software engineering – vocabulary”, ISO/IEC/IEEE 24765:2010(E), 2010.

Annex A – GLOSSARY

The terms in this glossary are presented in approximately the same order as they appear in the main body of this technical concept document.

Term	Definition	References
Service	A **service** is a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks.	Ch. 2, [16]
	A service is a means of delivering value for the customer by facilitating results the customer wants to achieve.	Ch. 2, [15]
	A service is a means of delivering value for the customer by facilitating results the customer wants to achieve.	Ch. 2, [38]
	A **service** is a mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description.	Ch. 2, [32]
M&S as a Service	**M&S as a Service** (MSaaS) is a means of delivering value to customers to enable or support Modelling and Simulation (M&S) user applications and capabilities as well as to provide associated data on demand without the ownership of specific costs and risks.	Ch. 2
MSaaS Perspective	A conceptual understanding of MSaaS in terms of a solution space. This technical concept identifies four perspectives: • MSaaS as a cloud service model; • MSaaS using cloud service models; • MSaaS as a service-oriented architecture; and • MSaaS as a business model.	Ch. 2, Section. 2.2
Cloud Computing	Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.	[30]
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.	[30]

Term	Definition	References
Platform as a Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.	[30]
Infrastructure as a Service (IaaS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).	[30]
Cloud Deployment Models	Private cloud, community cloud, public cloud, hybrid cloud.	[30]
Service-Oriented Architecture (SOA)	SOA is an architectural paradigm for dealing with business processes distributed over a large landscape of existing and new heterogeneous systems that are under the control of different owners.	[17]
	An architectural principle for defining how people, organizations, and systems provide and use services to achieve results.	[38]
Service Orientation	A design paradigm to develop services according to certain design principles within the context of a SOA. Design principles include service abstraction, loose coupling, reusability, composability and discovery.	Ch. 2, Section 2.2.3
Enterprise Service Bus (ESB)	Part of SOA is the infrastructure that allows you to use services in a productive system landscape. Its purpose is to provide interoperability (connectivity, data transformation, and routing) combined with some additional services such as security, monitoring and so on.	[17]
Service Consumer	Accesses services provided by a service provider to achieve its own objectives. A service consumer relies completely on the service contract offered by a service provider and does not care about how a service provider actually performs its service delivery.	[11]
Service Provider	Provides services on an on-demand basis. Each service is specified in a service contract that details scope, usage requirements and quality of the provided service.	[11]
Service Broker	Acts as a neutral platform that provides a catalogue and facilitates access to available services and service providers. Strictly speaking, a service broker can be considered as a special type of service (namely, a service for finding other services).	[11]

Term	Definition	References
Service Categorization	A means of grouping services according to common characteristics. This technical concept identifies categories of human, machine and organization as classifiers for the actor providing or consumer a service. The NATO C3 Classification Taxonomy provides an alternative means of categorization.	Ch. 2, Section 2.4
Architecture	The fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution.	[51]
Model	A model is a physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process.	[1], [6]
Reference Model	Any generic model that has specific examples can be considered to be a reference model.	[21]
	A reference model is a model used for supporting the construction of other models.	[45]
Overarching Architecture	Architectures which are used for long-term planning. These architectures may include visionary concepts and ideas. Overarching architectures are often defined as goals or constraints that have to be applied when designing and implementing new systems.	Table 4-1, Ch. 4, Section 4.1.2
Reference Architecture	Reference architectures reflect strategic decisions regarding system technologies, stakeholder issues, and product lines. They render user requirements, processes, and concepts in a high-level solution from which individual projects can be identified and initially programmed. Their primary focus is on services, processes, and component functionality, and they provide the basis for the development of Target Architectures (TA).	Ch. 4, Section 4.1.2, [27]
Domain-independent Reference Architecture	An architecture that is independent (to some degree) of any particular application domain.	Table 4-1, Ch. 4, Section 4.1.2
Domain-specific Reference Architecture	An architecture designed for a specific application domain, e.g., entity level simulation.	Table 4-1, Ch. 4, Section 4.1.2
Comprehensive Reference Architecture	A reference architecture is further qualified as “comprehensive” if it defines additional services, service agreements, and/or service components.	Table 4-1, Ch. 4, Section 4.1.2
Target Architecture	Target architectures are normally derived from a related reference architecture. They specify a system design at a detail sufficient to direct the acquisition and integration of components to achieve a desired capability. Target architectures focus on specifications for systems and services and are usually valid for the duration of the system acquisition and initial design.	Ch. 4, Section 4.1.2

Term	Definition	References
DSEEP	The Distributed Simulation Engineering and Execution Process (DSEEP) is a process model for the development and execution of a distributed simulation environment.	[7]

Annex B – CASE STUDIES FOR M&S AS A SERVICE

B.1 CASE STUDY "RUDI" (DEU)

B.1.1 Description of Case Study

RUDi offers a generalized service-oriented infrastructure for different military-focused applications. It is not focused on M&S, but the support of M&S applications is basically possible.

Figure B-1 shows the principle structure of RUDi. RUDi is based on common standards and open-source products. At the moment the main military application domain of RUDi is focused on C2 systems. RUDi provides different services in the tactical domain for the military user.

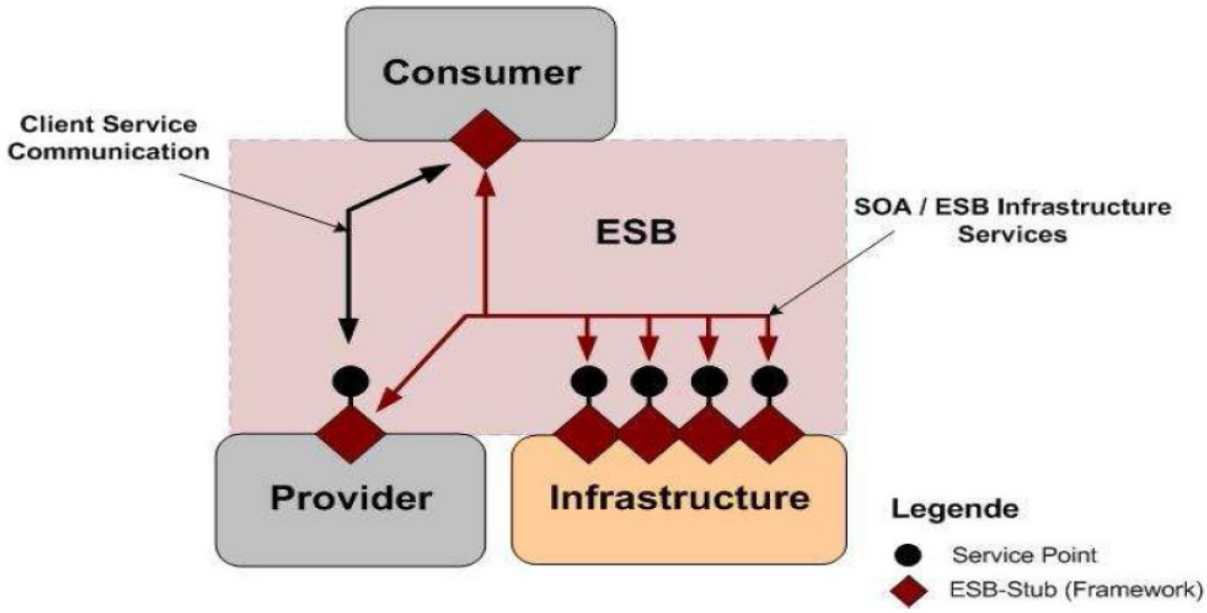

Figure B-1: Basic Structure of RUDi: Consumer/Provider Schema Using an Enterprise Service Bus (ESB).

RUDi is an ongoing project of the German Armed Forces.

B.1.2 M&S Business Process Supported by the Case Study

- Test and evaluation of new C2 configurations.
- Training (including joint/collective).
- Tactical, operational.

B.1.3 Role of End-User

- Operational military user.

B.1.4 Security Classification

The security classification within RUDi depends on the application domain. Because real C2-systems are involved, the security level is up to NATO SECRET (see Section B.1.5).

Support for cross-domain/Multi-Level Security (MLS) is provided by RUDi [12].

B.1.5 Type of Services Provided by RUDi

- QoS mechanisms.
- SOAP-over-UDP.
- Data compression for the case of limited bandwidth.
- Security services, e.g. token-, authorization-, key-management services.

B.1.6 Properties of the Service Environment

RUDi has a Technology Readiness Level (TRL) of 7 (“System prototype demonstration in an operational environment”).

B.1.7 Capacity/Availability

- **Frequency of Access:** RUDi was used for several experiments in the last two years, and is still in use in different experimental environments.
- **Level of Scalability:** Granted for RUDi in the sense of copying/multiplying the environment.

B.1.8 Type of Delivery / Quality of Service

- Use of web services; cloud-based infrastructures are possible to include.
- Distributed enterprise service bus.

B.1.9 Related Costs

- **Development Costs:** Since RUDi has TRL 7, most development costs have been spent already.
- **Cost of Use/Providing Capability:** Not known.

B.1.10 Authorisation (Who/How)

RUDi provides different authorization and authentication techniques and schemes (see Section B.1.5, “Services”).

B.1.11 Expected and Observed Benefits

RUDi is/was used in tests and experiments to investigate new concepts of C2 systems. In these tests RUDi proved to be useful in following cases:

- Quick installation, easy-to-learn;
- Easy access and authorization management; and
- High flexibility when responding to additional or new requirements.

B.2 CASE STUDY "SD VINTEL" (DEU)

B.2.1 Description of Case Study

Performing distributed simulation for multi-purpose (training, procurement, test of materiel, etc.).

Starting in 2006, the German Armed Forces initiated a project named SuTBw (German: "Simulations- und Testumgebung der Bundeswehr", Engl. "Simulation and Test Environment of the German Armed Forces") to provide the infrastructure for the coupling of simulation systems. The SuTBw provides networks, network services, software tools and technical support to all military simulation projects within the German Armed Forces.

Built on this infrastructure distributed all over Germany at sites working on military simulations, the so-called "SD VIntEL" (German: "Systemdemonstrator Verteilte Integrierte Erprobungslandschaft", Engl. "System Demonstrator for a Distributed Integrated Test Environment") is developed as a generic testbed for distributed simulation environments. Based on a service-based architecture, the SD VIntEL offers a variety of methods, tools, and databases to achieve simulation interoperability and to improve fair fight (see Ref [29] for more details).

SD VIntEL is based on HLA and uses centralized application services for critical aspects (e.g., for calculating weapon effects). Currently the SD VIntEL contains the following M&S-specific services:

- Weapon effects service (provided by IABG);
- Communication effects service (provided by KESS of Thales);
- Exterior ballistic service (provided by IABG);
- Synthetic environment service (provided by Rheinmetall and CPA); and
- Synthetic dynamic service (provided by Rheinmetall and CPA).

In the following, the SES and SDS are described in more detail.

In addition to M&S-specific services, the SD VIntEL contains so-called infrastructure service:

- Init-service (used for initialization of simulation systems with simulation-specific configuration and data files, as well as for collecting simulation results from simulation systems).

The Synthetic Environment Service (SES) allows:

- Centralized standards-compliant storage of synthetic environment data; and
- The SES allows initialization of simulation systems before run-time through various interfaces (OGC services, OpenFlight, etc.) with correlated data.

The SES uses internally an OGC- and SEDRIS-compliant database and allows export of synthetic environment data in various data formats (e.g., OpenFlight, STF, VBS2). Therefore all simulation systems may be initialized from a common synthetic environment database. Figure B-2 illustrates the SES.

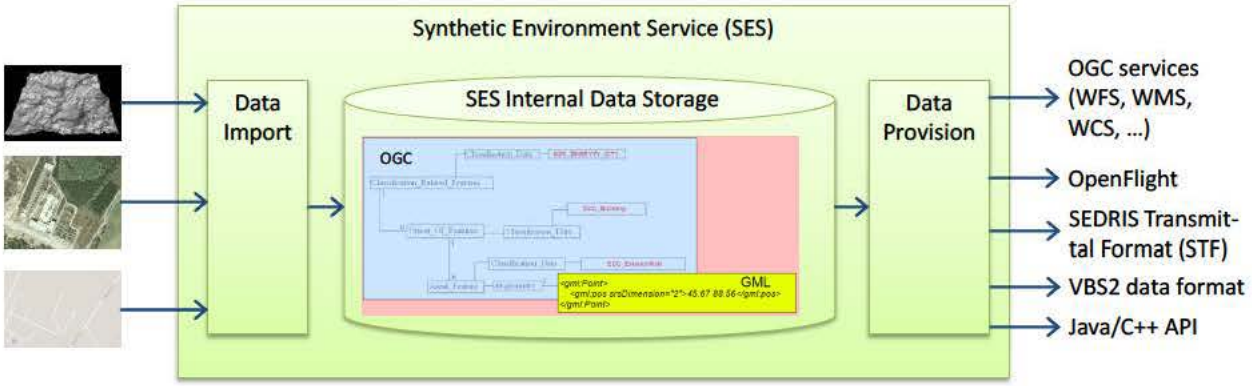

Figure B-2: Basic Idea of DEU Synthetic Environment Service (SES).

The Synthetic Dynamic Service (SDS) is an extension of the SES and allows to change/update certain objects and environmental features during run-time (execution) of a simulation environment. This is done via manipulations on the environment database which is distributed to the connected simulation systems (using the SES). While run-time updates of environmental data and features are quite easy for simple objects like buildings (e.g., opening a gate), manipulations on the terrain itself are complex and take some time, even for simpler actions (i.e., several seconds for imprinting a crater into the terrain).

B.2.2 M&S Business Process Supported by the Case Study

Giving a set of models (FOM) to the provider and scenarios with necessary instructions; performing vignettes and analyze the results to extract benefit for the way ahead. Besides, SD VIntEL offers an own process model which is based on the DSEEP and helps improving M&S projects throughout the German Army.

B.2.3 Role of End-User

Military and associated governmental organizations.

B.2.4 Security Classification

Depends on the involved networks and simulation assets. Experiments and exercises have been done from NATO UNCLASSIFIED (NU) to NATO SECRET (NS).

B.2.5 Type of Services Provided

M&S-specific services:

- Weapon effects service (provided by IABG);
- Communication effects service (provided by KESS of Thales);
- Exterior ballistic service (provided by IABG);
- Synthetic environment service (provided by Rheinmetall and CPA); and
- Synthetic dynamic service (provided by Rheinmetall and CPA).

Infrastructure services:

- Init-service (used for initialization of simulation systems with simulation-specific configuration and data files as well as for collecting simulation results from simulation systems).

B.2.6 Properties of the Service Environment

The Technology Readiness Level (TRL) of the SD VIntEL testbed is at least 6 (“System/subsystem model or prototype demonstration in a relevant environment”).

B.2.7 Capacity/Availability

VIntEL defines a reference architecture for distributed simulation environments. As such it is usually used for dedicated evaluations and experiments. It is not designed for 24/7 use (although it should be technically possible).

Typical applications of the VIntEL reference architecture include multiple simulation systems, real systems (e.g., C2 systems) and various services. General capacity constraints were not observed, although the underlying simulation infrastructure (e.g., HLA Runtime Infrastructure) may limit the maximum number of federates or entities.

The services (e.g., WES, CES) have been used in various distributed simulation environments as well as in data farming set-ups. General scalability issues were not observed in tactical-level scenarios. Dedicated evaluations with large-scale scenarios have not been executed.

B.2.8 Type of Delivery / Quality of Service

Different alternatives have been evaluated as to how the services can be integrated into a HLA-based distributed simulation environment (see also Figure 4-4 in Chapter 4, Section 4.5):

- Services as federates;
- Integration of services via a proxy; and
- Integration of services through web service interfaces (e.g., OGC WFS).

Depending on the specific type of service and its requirements, the integration into the simulation environment is realized differently. For example, the Weapon Effects Server (WES) needs access to the state of the simulation environment (e.g., positions of units) and is therefore integrated into the simulation environment as a federate.

Due to the different nature and requirements of the services within SD VIntEL, different bus systems are used for integration into the simulation environment (see also Figure 4-4 in Chapter 4, Section 4.5).

Also, simulation systems need to be adapted tom make use of the services. Again, depending on the type and complexity of a service and characteristics of the simulation system (e.g., system architecture, modularity) necessary adaptations may be rather simple or very hard.

B.2.9 Related Costs

Main development activities will be finished by 2015. No assessment of cost of operation available.

B.2.10 Authorisation (Who/How)

The VIntEL reference architecture does not define specific methods or techniques for authorization. Standard HLA mechanism, etc., are used.

If a simulation environment requires classified data (e.g., real weapon effects data) appropriate IT security mechanisms have to be put in place (e.g., use of encrypted data transfer, use of accredited sites and hardware).

B.2.11 Expected and Observed Benefits

The benefits expected by SD VIntEL and its service-oriented architecture are:

- Time reduction (for setting up a distributed simulation environment);
- Quality improvement (by using tested infrastructure, services, processes, etc.); and
- Cost reduction and recommendations for further, similar cases.

Practical experiences with SD VIntEL in general show the following results:

- Repeated use of a tested and partially pre-integrated simulation environment reduces test and integration efforts; and
- Improved quality by using services for critical simulation aspects.

Practical experiences with the Weapon Effects Server (WES) and Exterior Ballistics Server (EBS) show the following results:

- Unfair fight situations due to different damage computation algorithms used by different simulation systems are eliminated; and
- Adoption of existing simulation systems and simulators required moderate efforts.

Practical experiences with the Communication Effects Server (CES) show the following results:

- Unfair fight situations due to different handling of communication effects (i.e., the decision whether two units may actually communicate with each other via radio) by different simulation systems are eliminated; and
- Adoption of existing simulation systems and simulators requires moderate efforts.

Practical experiences with the Synthetic Environment Service (SES) show the following results:

- The SES allows centralized standards-compliant storage of correlated synthetic environment data for all simulation systems.
- The SES allows initialization of simulation systems before runtime through various interfaces (OGC services, OpenFlight, etc.).
- The SES significantly reduces interoperability problems due to uncorrelated synthetic environment data and allows time-saving automated initialization of simulation systems. (Obviously, the SES cannot solve problems related to conceptual differences in simulation systems, e.g. flat earth representation in one simulation system vs. round earth representation in a second system.)
- More details can be found in Refs [44] and [19].

B.3 CASE STUDY “NOGESI” (ESP)

B.3.1 Description of Case Study

One of the research lines at the Simulation Department at the Instituto Tecnológico ‘La Marañosa’ (ITM), sponsored by the Spanish Ministry of Defence, is the creation of a distributed simulation framework based on DDS (Data Distribution Service), HLA (High-Level Architecture) and C-BML (Coalition Battle Management Language).

Over the last four years, ITM and NADS have been working together in two related projects in order to create a simulation framework as a platform for open and interoperable distributed simulation, introducing

some disruptive concepts like using DDS as a simulation data bus or open interfaces between simulation components.

NOGESI (NOdo GEnerico de SImulacion, Simulation Generic Node) puts together simulators and COTS (Commercial-Off-The-Shelf) connecting with HLA (High-Level Architecture) or DIS (Distributed Interactive Simulation) in order to create a real-time laboratory for distributed simulation.

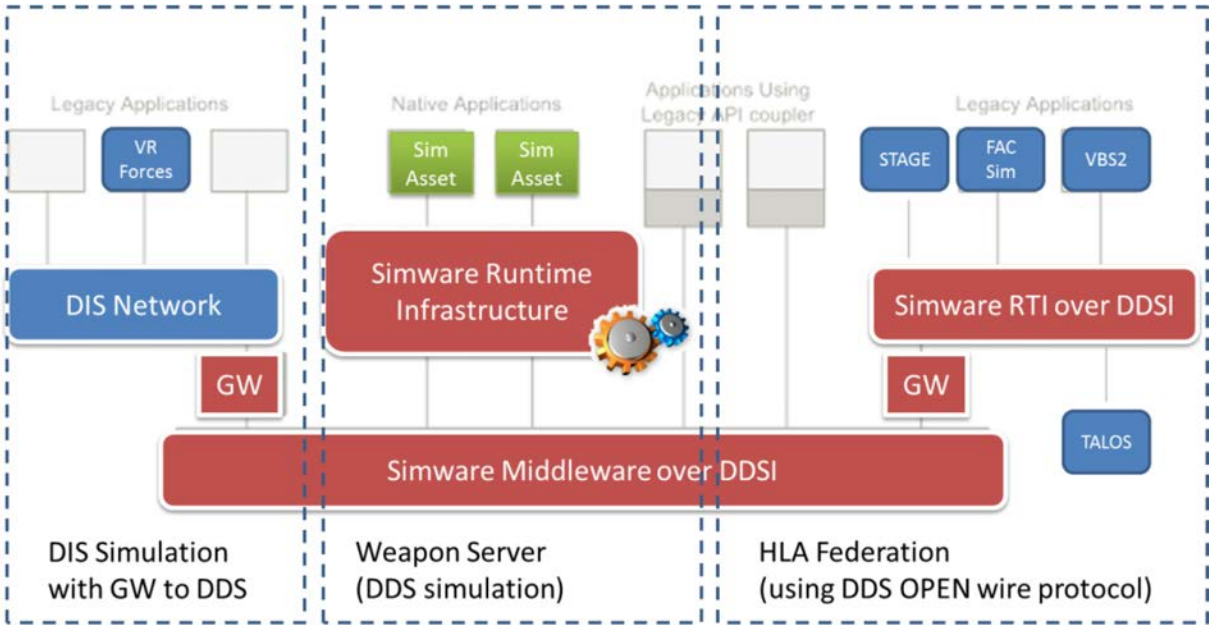

Figure B-3: NOGESI Architecture.

NOGESI's main capabilities are:

- Interoperability between simulated and operational systems using DDSI (DDS Interoperability Protocol) open wire protocol;
- Development and maintenance of simulation assets using MDA (Model-Driven Architecture) paradigm;
- Deployment of simulation assets as services into an HLA federation;
- HLA interoperability to a wire protocol level; and
- DIS interoperability using a gateway DIS and DDS data models.

An exercise for this case study, a Forward Air Controller (FAC) virtual simulator, developed by Indra Sistemas for the Spanish Air Force in 2010, has been integrated into NOGESI supporting some advanced simulation services like ownership management. By using HLA ownership services over DDSI wire protocol, FAC virtual simulator can interoperate in real time with a simulation server in uses cases like Close Air Support or Call for Fire. In this exercise, friendly forces simulated by VRForces or Stage can call for air support to a FAC that it is going to engage foes simulated by VBS2 with missiles or bombs that are been simulated by another HLA federate, the "Weapon Server". The following figure shows the systems involved in this exercise.

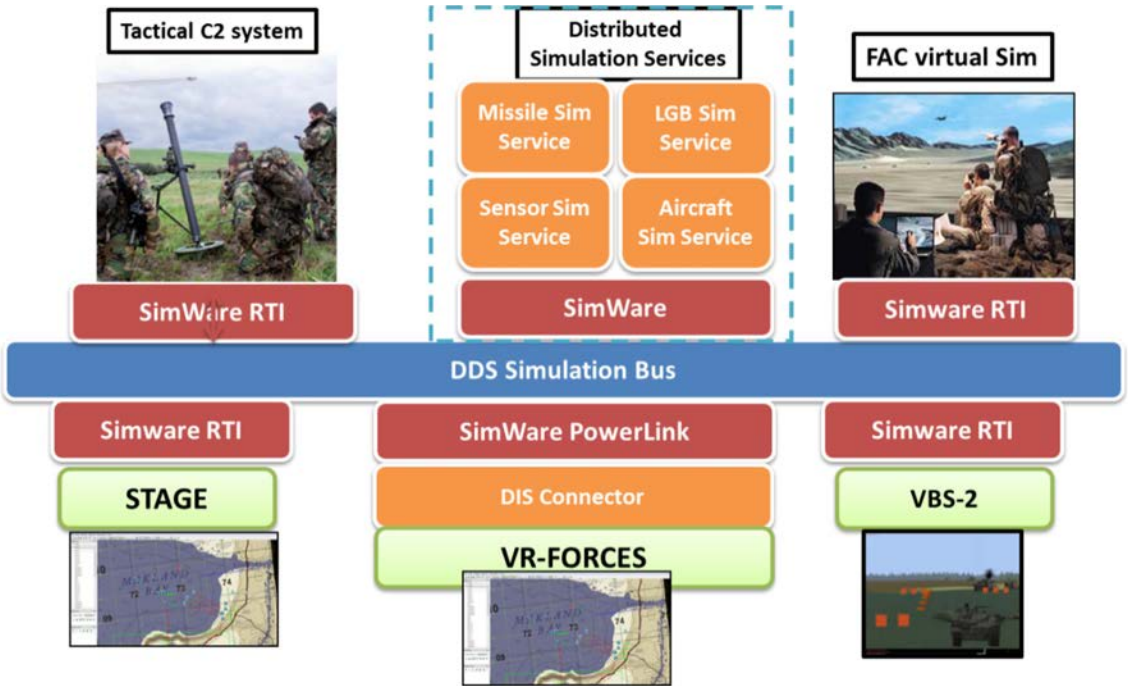

Figure B-4: NOGESI Case Study (Example).

NOGESI use a data-centric simulation middleware called Simware which is a commercial-off-the-shelf platform to do distributed simulation with an open architecture. Simware proposes a new way to integrate and interoperate simulation systems, with an open layered architecture based on OMG DDS standard for distribution of data.

Dynamical simulation of the "weapon services" is managed by Simware run-time infrastructure (based on Simulink from Mathworks), which is a fully compliant DDS distributed infrastructure and is composed of four main components:

- **Scheduler:** It is a real-time scheduler which manages the execution of the simulation and the state machine during run-time. All the configuration is based on a XML files.
- **SimEngine:** Manages cyclical execution of the simulation assets during run-time. In a fully distributed architecture, like Simware, a SimEngine instance is required in each node that it is running simulation assets.
- **ACS:** Tool to manage weapon server and its instances. Allows interacting with instances of the simulation services on run-time.
- **Simulation Assets:** Dynamical models of simulated entities. In NOGESI deployment there are simulation models for infrared missile, sensor, aircrafts and LGB.

B.3.2 M&S Business Process Supported by the Case Study

A scenario where FAC simulator calls the weapon service, as mentioned above. To be more general, any simulator that needs to request a weapon service (guided bomb/missile) could call this service, like for example, any aircraft, helicopter or ship.

B.3.3 Role of End-User

Military and associated governmental organizations.

B.3.4 Security Classification

Depends on the involved networks and simulation assets. Usually NATO UNCLASSIFIED.

B.3.5 Type of Services Provided

Weapon service (guided bomb/missile).

B.3.6 Properties of the Service Environment

NOGESI has a Technology Readiness Level (TRL) of 6 (“System/subsystem model or prototype demonstration in a relevant environment”).

B.3.7 Capacity/Availability

NOGESI is used in demonstrations to show the use of distributed services using HLA. It has not been tested to support 24/7 use.

NOGESI could be replicated to provide services to more clients at the same time; also it is prepared to support more guided bomb/missile to be developed.

B.3.8 Type of Delivery / Quality of Service

Service is provided using HLA, though it is possible to develop a web service for the use of the weapon service.

B.3.9 Related Costs

Main development activities were finished in 2013. It does not have cost of use, but if it is necessary to make changes in the service, it will be discussed with the developer company.

B.3.10 Authorisation (Who/How)

There are no defined specific methods of authorization. NOGESI works as a federate in a HLA federation in which is used RPR-FOM 2.0 Draft 17 as FOM.

B.3.11 Expected and Observed Benefits

With NOGESI it is possible to improve interoperability and reusability of simulation assets. This can be achieved with a low budget and low technical risk by the simulation community. Taking advantage of new data exchange technologies, like DDS, successfully applied in many others domains, into a new architecture, structured by layers and based on open interfaces, is a very good solution to the many pains that exist right now in the simulation industry.

B.4 CASE STUDY “CGF PROVISION” (GBR)

B.4.1 Description of Case Study

Computer Generated Force (CGF) systems are computer programs that simulate human behaviours, units, systems and platforms. They provide the ‘C’ element of ‘LVC’ (Live, Virtual, Constructive) simulations and are used to provide the background context to an exercise such as Blue Force (including coalition) and Red Force tactics and doctrine, civilian pattern of life, etc., for creating realistic scenarios.

Typically, simulation federations only employ one CGF application. However, it is becoming increasingly common to utilise multiple CGFs in a federation. The reason for this is two-fold:

1) Some federations require a large number of entities, which cannot be simulated on a single computing platform; and
2) Some CGFs are becoming more specialized, i.e., domain specific.

Elements of CGFs (e.g., the simulation 'engine') could conceivably be provided by a service which is remote from the host simulation (e.g., training establishment), and controlled using a Reconfigurable User Interface (RUI). The development of a RUI which can be used to control multiple CGFs remote from the simulation engine(s) is being investigated as an enabler for providing 'CGFs as a Service' (see Figure B-5).

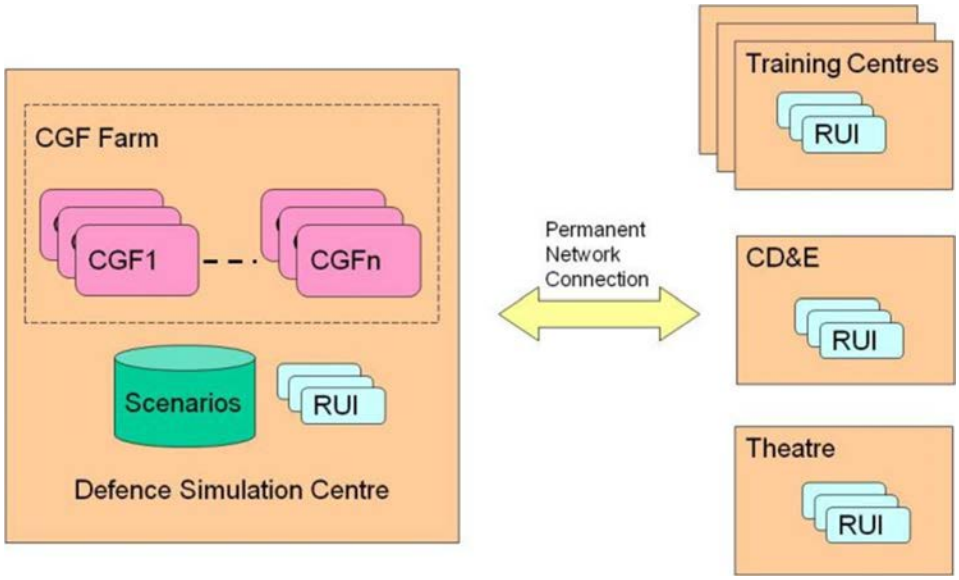

Figure B-5: CGF Provision.

B.4.2 M&S Business Process Supported by the Case Study

CGFs can support all levels of command representation and are used in a variety of defence applications including training, mission planning and mission preparation.

B.4.3 Role of End-User

Delivering CGFs as a service based on a common RUI is aimed at providing benefits to the operational military users, the supplier base and technical users.

B.4.4 Security Classification

Delivering CGFs as a service will be required to support different security classifications on the same simulation network, including NATO UNCLASSIFIED.

B.4.5 Type of Services Provided

The aim is to investigate mechanisms for providing improved control and visualisation of CGF Systems executing on the same simulation network, to facilitate a mechanism route for Common CGF interfaces, i.e., client/server based implementation.

B.4.6 Properties of the Service Environment

No information provided.

B.4.7 Capacity/Availability

CGF systems to be available as an 'on demand' service, managed as part of a UK Defence Simulation Centre (DSC). The UK DSC is planned to be implemented as an enduring capability in April 2016.

B.4.8 Type of Delivery / Quality of Service

The future delivery mechanism being considered for CGFs is through the use of web services, e.g. UK G-Cloud service.

B.4.9 Related Costs

No information provided.

B.4.10 Authorisation (Who/How)

UK MOD through a future enduring Defence Simulation Centre (DSC).

B.4.11 Expected and Observed Benefits

The future availability of CGFs delivered as a service, based on a common reconfigurable user interface, will support an aim of the UK MOD to achieve a step change in the exploitation of future simulation systems as part of a Defence Training and Education Capability (DTEC) implementation programme:

- Simulations must be more agile and reconfigurable to meet future changing operational requirements; and
- Simulations must be supported by common infrastructure and services to reduce overall life-cycle cost.

In addition, this capability will significantly reduce the training and education burden relevant to using one or more CGFS, either within a given application (e.g., training system), or across multiple simulation applications.

B.5 CASE STUDY "MISSION PLANNING SUPPORT" (NLD)

B.5.1 Description of Case Study

Imagine the following situation: a military unit (battalion/brigade) at the front of an operation has to decide exactly how and when they will deploy their troops. Based on the actual situation and the tasks to be performed, the Commander wants to 'run through' a large number of what-if scenarios in order to help to choose the 'best' course of action. Detailed questions within the what-if scenarios are in the following fields:

- Optimization of (deployment) routes;
- Optimization of (defensive) positions;
- Inventarisation and identification of possible ambush locations;
- Determination of POL (Petrol/Oil/Lubrication);

- Synchronizing activities of sub-units; and
- Making C3I information available.

All of these activities are wanted/necessary at the level given. M&S can be helpful in answering the questions above. However, the resources for performing M&S actions at the level identified are not available. Thus, offering these tools 'as-a-service' will enlarge the problem solving capabilities at the battalion level.

Detailed solution:

- Front-line troops send their current situation, plans, etc., to a service;
- The service calculates the routes, timing, etc., and makes sure that the plans of the front troops are synchronized and in line with the Commander's intent; and
- It integrates all existing information on, e.g., daily patterns of life, hot-spots for IEDs, to make the calculated routes as effective, efficient and safe as possible.

B.5.2 M&S Business Process Supported by the Case Study

The following processes can be supported:

- War fighting experimentation;
- M&S embedded in CIS and weapon systems (e.g., mission planning / mission preparation); and
- Emergency and rescue services (prediction models).

B.5.3 Role of End-User

End-user roles are:

- Technical/tactical/operational/strategic level;
- Operational military user:
  - The front-line troops; and
  - Mission Commander.
- Other types of user, e.g., supplier base.

B.5.4 Security Classification

High: The transmission of current status and plans/orders, etc., must be secure!

B.5.5 Type of Services Provided

For decision aid systems:

- Weather forecast services; and
- Complete spectrum of prediction tools.

Other services:

- AAR (and in action review) services; and
- Live data service (e.g., live air picture), etc.

Services to support planning, synchronizing, de-confliction, integration of all extant information (i.e. hot-spots of IEDs). This service actually consists of many smaller parts:

- Getting data on the front line and sending it to the back office.
- Back-office services consisting of:
  - Analysing data from front-line troops.
  - Analysing Commander's intent.
  - Analysing special objects/situations/history of affected areas/enemies, etc.
  - Planning for front-line troops (joint, combined, all front-line troops):
    - Synchronized;
    - Deconflicted;
    - Effective, efficient and as safe as possible; and
    - SME and mission Commander user interfaces (showing the right information in the right way and responding to user actions).
- Sending data to front-line troops.
- Front-line troop user interfaces (showing the right information in the right way and responding to user actions).

B.5.6 Properties of the Service Environment

These are all planned services, i.e., the service environment does not exist at this point.

B.5.7 Capacity/Availability

- Availability and support hours of operation.
- Quality of service (availability and response time to issues).
- Instantiations of service (how many different users can be supported).
- Level of scalability, e.g., a CGF farm that replicates capability and "grows" to support surge demand.

B.5.8 Type of Delivery / Quality of Service

Likely mode of delivery is service provision via a cloud backend, able to scale in and out on demand, accessed over a secure network by the types of devices typically available at the front. There are important QoS implications so that services access is reliable and trust worthy.

B.5.9 Related Costs

- Development costs (separating initial vs. through life costs – spend once, reuse many times).
- Cost of use/providing capability.
- Infrastructure:
  - High bandwidth networking (between front-line troops and back office);
  - Computing power available for front troops;

  - Computing power/storage available for back office;
  - UI for front troops; and
  - UI for mission Commander.
- Other:
  - Standards for information exchange.

B.5.10 Authorisation (Who/How)

Appropriate authorization and security mechanisms are vital to ensure the service is used only by those that need to know. Access by unauthorized users would lead to leakage of operational information.

For front-line troops, authorization would probably need to take the form of time-limited certificates issued from a trusted source in a secure manner.

B.5.11 Expected and Observed Benefits

- Optimization, synchronization, de-confliction, safe planning.

B.6 CASE STUDY "SCENARIO GENERATION" (NLD)

B.6.1 Description of Case Study

A (military) user wants to generate a scenario for a specific situation. This could be, e.g., for a training scenario or an operational research question.

Example: Steps for a user wanting to create a training scenario:

- Determines learning objectives;
- Prep-phase;
- From that, determines requirements on terrain and environment (weather, patterns of life, etc.);
- Create a sketch in the online tool;
- Tool generates a (geo-typical) landscape (small) adjustments interactively; and
- Terrain created available for all students and scenario users.

Example: Running a scenario:

- People are dynamically represented in the training, generated by the pattern-of-life service;
- The weather is generated by the weather service;
- CGF tools are used;
- Note that this requires interaction between the different services; and
- All actions are logged for DAR and AAR purposes.

B.6.2 M&S Business Process Supported by the Case Study

Exercise and training.

B.6.3 Role of End-User

Trainer/trainee.

B.6.4 Security Classification

Can range from unclassified to highly classified.

B.6.5 Type of Services Provided

- Terrain generation (off-line).
- Weather generation (on-line).
- Pattern-of-life (i.e., crowd generation) (on-line).
- CGF (on-line).
- Logging, DAR and AAR services.

B.6.6 Properties of the Service Environment

Service environment does not exist at this point.

B.6.7 Capacity/Availability

Real-time requirement.

B.6.8 Type of Delivery / Quality of Service

Scenario generation could be naturally delivered via MSaaS as a cloud application. It also requires the definition of a SOA to meaningfully orchestrate the component services employed.

B.6.9 Related Costs

Potentially substantial development costs would be required to build this from scratch. However, this cost would be mitigated via the employment of services written and maintained by third parties.

B.6.10 Authorisation (Who/How)

Multi-level authorization would allow different users access to different models depending on need-to-know/security considerations. Authorisation could also be restricted based on financial grounds whereby only users who have paid for use can gain access.

B.6.11 Expected and Observed Benefits

All of the general advantages mentioned in Section 2.6.

B.7 CASE STUDY “VALIDATION” (NLD)

B.7.1 Description of Case Study

Support to the Verification and Validation (V&V) of models and simulations. V&V is important to ensure models and simulations provide appropriate representations of the systems they are representing. Providing

V&V as a service allows for centralization of V&V expertise for use by many users, especially important for distributed exercises to ensure all components experience the same quality of V&V.

Note that a range of services can be offered – the two extremes being:

- **Fully Distributed:** All tests have to be executed by the various manufacturers/user of the M&S. The service only checks (by independent SMEs) the results of the V&V work already done, and suggests further work; and
- **The V&V is Performed On-site:** The V&V tests are executed by independent SMEs on-site.

The needed V&V for a specific case can be a mix of the above two extremes: the less critical parts can be checked by studying material sent by the manufacturer/user, while the parts that contribute the most to the risk can be check by independent V&V. The optimal mix depends on the overall risk (and available resources).

B.7.2 M&S Business Process Supported by the Case Study

V&V of M&S is important in all types of case studies as long as there is a risk involved in application of the results in the real world.

Before distributed exercises:

- SMEs do V&V on documentation sent by the manufacturers/users or perform on-site tests.

During analysis studies:

- SMEs check the validity during execution and if necessary make changes.

B.7.3 Role of End-User

In general, all end-users mentioned in the table at the beginning of this annex.

The real-world risk is a problem for the user of the simulation results. However, many problems can be detected early in the development. Both the end-user as well as the builder and executer of a simulation are relevant roles for this case study.

B.7.4 Security Classification

Depends on the simulation itself. A classified simulation will require security mechanisms rated at that classification in order to support the V&V of the simulation.

B.7.5 Type of Services Provided

Two services:

Before Use of the M&S

- In this service the M&S (the components, data and proposed execution) is V&V-ed.
- The Dutch Society for Simulation in Healthcare (DSSH) approach is one possibility:
    - The group executing and using the simulation has to answer a number of questions and provide evidence. A group of independent experts then judges the provided data and responds with an OK or with possible problems that require more attention.

During Use of the M&S

- During execution of a scenario, especially with CGF or many distributed partners, it may happen that the course the simulation as a whole takes is not valid anymore. This is especially a problem with analysis using only CGFs. One or more SMEs can be chosen to monitor the execution and can change the execution such that it remains valid; and
- The SME should have the means to follow the simulation and they should have the means to change the running simulation.

B.7.6 Properties of the Service Environment

Service environment does not exist at this point.

B.7.7 Capacity/Availability

The frequency of access is likely to be low since large-scale M&S activities do not occur regularly. Before the use of M&S, the availability and support hours of operation are not critical and can be scheduled as need by the M&S project manager. During an M&S activity, the V&V service must be available through the simulation lifetime.

Q-tility (a V&V expertise centre for simulation developers and users) can organize this process:

- SME network must be set up (and maintained);
- Independent V&V is important -> not all SMEs can be used for all parts of the M&S; and
- The needed capacity depends on risk, complexity, already available information, etc.

B.7.8 Type of Delivery / Quality of Service

V&V conducted before the use of M&S could be delivered via a web service. During an M&S event, V&V needs to be online with access to streaming data from the event in order to be able to continually monitor the V&V of the event.

B.7.9 Related Costs

Depends on risk involved in application of the simulation results. If no risk is involved, then no V&V is necessary. If there is risk, the required certainty and complexity of the M&S is of importance to estimate the costs.

B.7.10 Authorisation (Who/How)

Before use of the M&S, authorization to use a V&V service requires a service contract between the service provider and consumer.

During use of the M&S, there is the additional authorization requirement that the V&V service provider has the appropriate credentials to be able to monitor the live data streams being generated by the M&S event.

B.7.11 Expected and Observed Benefits

If there is substantial risk involved in using the simulation results in the real world, the user needs to lower this risk as much as possible. V&V helps in doing this.

VVaaS potentially reduces the need for distributed participants to travel to a central location periodically in order to perform integration and V&V activities.

B.8 ARCHITECTURAL CASE STUDY "SIM-SOA" FOR INTEGRATING C2 AND SIMULATION SYSTEMS WITH SERVICES (NOR)

B.8.1 Description of Case Study

This is a demonstrator for the Norwegian Armed Forces that shows the usefulness of service orientation for rapidly and readily combining systems and services for specific operational needs; in particular M&S for training and exercise, and for planning. It is also an architectural study investigating the feasibility of a hybrid SOA, wherein HLA resides intact. Emphasis will be laid on using important operational systems at the User Applications level. Figure B-6 shows a sketch of the system. (Colours follow the C3 Classification Taxonomy's candy colour chart http://tide.act.nato.int/em/index.php?title=Candy_Color_Chart.)

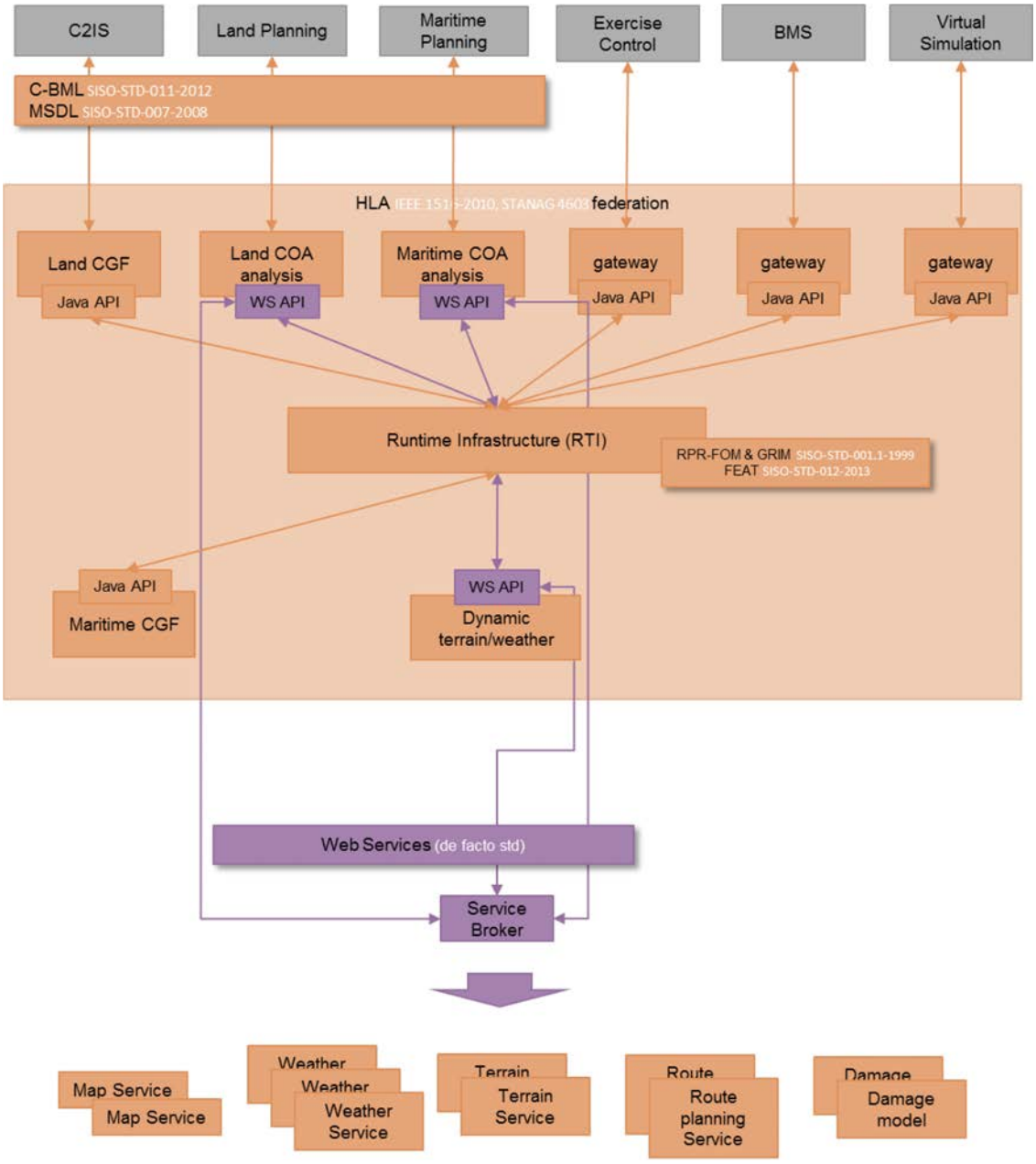

Figure B-6: SIM-SOA.

In agreement with Chapter 2, Section 2.2.3, the three central aspects of service orientation are:

1) Communication following standards so that service contracts can be declared and processed over a range of actors (components);
2) Loose coupling in the sense that components are usable in a wider context; and
3) Interoperability in the sense that components may function together to generate a larger/different piece of total functionality.

We view HLA as fulfilling these three aspects to a certain degree; in particular, universal FOMs (RPR-FOM, NETN-FOM, etc.) with guidelines enable what amount to service contracts to be declared *relative to a given* FOM. This enables one to view a HLA federation as having a service-oriented sub-architecture relating to a wider federation of systems which may have a different service-oriented target architecture (e.g., based on WS*).

Further, the existence of communications standards such C-BML enable service contracts to be declared between simulation systems and operational systems, and interfaces – both into HLA federations (e.g., WebLVC) and within federations (e.g., WS APIs in HLA Evolved, but also general service connectivity for federates) – based on de facto standards such as WS*, REST, WebSockets, enable federations and federates to join in a wider SOA system.

The totality of this picture corresponds, in essence, to the VIntEL reference architecture (above), in that we integrate several communication and interoperability standards to produce service-oriented systems. Our reference architecture is a straight-forward generalization of Figure B-6.

Turning to our specific case, the objective is to have simulation systems and operational systems interoperate over standards and to enable coupling components readily and rapidly. For example, a land planning user application can ask (using MSDL/C-BML) for a land COA analysis COI-specific service, which in turn uses (over HLA/RPR-FOM) a land CGF COI-specific service to simulate its battle orders. COA analysis can use COI-enabling services maintain and accessing common data repositories for maps, weather, terrain, route finding and damage. These latter services may be consumed over one of several SOA-associated de facto standards such as WS*, and various QoS modes and formats can be chosen on the fly. This enables fair fight based on a common operational picture across systems and dynamic terrain environment modelling, Thus, SIM-SOA shares objectives with several other cases in this report. Another example is LVC simulation for exercises, where all three modes of simulation interoperate, and where the combined result is reflected in operational applications such as C2IS, BMS and Exercise Control (ExCon). The exact configuration of systems in both these examples must be easily changeable.

We explicitly use the C3 Taxonomy to structure architecture, system and development; see Ref [11]. For conceptual integrity, we include systems in the taxonomy that are not necessarily service-oriented at present. In particular, we include legacy (silo) systems in the C3 Taxonomy's User Applications area; with the understanding that, in time, these should be refactored into/replaced by thin clients calling on services. In the meantime, such systems may have to be "service-enabled" by linking them via gateways to the rest of the system. Also, COI-specific services such as land COA analysis and Maritime COA analysis may be made thinner when common functionality is factored out and placed in COI-enabling services.

B.8.2 M&S Business Process Supported by the Case Study

- Concept development.
- Test and evaluation in capability development and interoperability.

- M&S embedded in CIS and weapon systems (e.g. mission planning / mission preparation).
- Exercise and training (individual/collective/joint).

B.8.3 Role of End-User

- Technical/tactical/operational/strategic level.
- Operational military user.
- Exercise Control (ExCon).

B.8.4 Security Classification

Support for cross-domain/Multi-Level Security (MLS) since operational systems (e.g., BMS) are stimulated by simulations.

B.8.5 Type of Services Provided

- Weather (forecast), terrain data/modelling, maps, damage data/modelling, route planning services.
- Decision support/prediction services.
- AAR (and in action review) services.
- Live data service (e.g., live air picture), etc.

In line with the C3 Taxonomy, consumers of services are other services and user applications. Consumers of user applications are military personnel.

B.8.6 Properties of the Service Environment

- Technology Readiness Level: 6 (prototype, demonstrator).
- Level of fidelity: High; in particular for fair fight conditions. Must have feel of operational systems.
- Level and type of control 3 – 4: Simulations can be readily and rapidly included in system and configured both at design time and run-time; the latter by operational personnel.

B.8.7 Capacity/Availability

For deployed system (after prototype):

- **Frequency of Access:** For large-scale exercises, a few times a year. For small-scale training, several times a week.
- **Availability and Support Hours of Operation:** Must be supported by persistent hardware and software environment, with support staff.
- **Quality of Service for System as a Whole:** 24-hour availability and uptime during exercise and training. Crashes and downtime are very detrimental to training and exercise objectives.
- **Instantiations of Services and System:** Should support full-scale military exercises and operations. The number of simulation systems may be limited, but the number of operational systems (e.g., BMS) may be large.

- **Level of Scalability:** Flexibility from small to large is important, and is a reason for going service oriented.

B.8.8 Type of Delivery / Quality of Service

HLA, other standards (e.g., C-BML, MSDL), de facto industry standards (e.g., WS*, WebSockets, WebLVC).

B.8.9 Related Costs

Prototype covered by research funding. Deployed system unknown cost.

B.8.10 Authorisation (Who/How)

Operational personnel as consumers of user applications authorized via their usual security regimes. Access from user applications and technical services to (other) technical services must be controlled depending on nature and classification of service.

B.8.11 Expected and Observed Benefits

Expected benefits are:

- Flexible and rapid orchestration of services and applications into system for training, exercise and planning, so that operational needs can be addressed properly. Often, operational plans for exercise and training are finalized immediately before training starts, and the simulation/C2 system environment must adapt quickly. Rapid orchestration should enable one to launch anything from simulations for a single MUAS team to a large-scale battalion exercise pulling from the same suite of services and applications.
- Common data sources services and modelling services for environment enables fair fight conditions and enables dynamic environment modelling and rendering.
- Service-orienting functionality should diminish the need for substantial development and integration efforts during orchestration. This enables one to move the task of assembling the systems needed for a specific operational task closer to the end-user. For example, a goal of this prototype is to show that an exercise commander can orchestrate his/her own exercise to a certain degree.

B.9 CASE STUDY "COLLECTIVE TRAINING AND EXERCISE FUNCTIONAL SERVICES" (NCIA)

B.9.1 Description of Case Study

Exercise Control Information Services (ExCon Services, ES) offer advanced information management in preparation, execution, and analysis of exercises.

The complexity and dynamics of information flows in Exercise Control (ExCon) organizations make it difficult to maintain situational awareness and control. This is mainly due to the fact that critical information is distributed in various Functional Systems (FS) and not correlated to provide a consistent picture in the FS that ExCon use. The complexity of maintaining a common operational picture for the whole ExCon will increase even further with the need to connect other, e.g., national, training organizations who may use their own, different, systems. These issues give rise to a requirement for an information system solution that is operationally relevant, supports legacy systems, enables the connection of 3rd party systems, and is "future

proof." A Service-Oriented Architecture (SOA) provides the enhanced flexibility and allows the incremental development of an effective and extensible set of Exercise Control Information Services. The aim is to take a pragmatic approach that preserves the investment in staff training of existing systems, while providing meaningful operational benefits through improved information sharing and fit-for-purpose presentation of information through configurable dashboards.

ExCon Information Services is a SOA-based information system used in planning and execution of CAX. The services provide a technical solution that enables continuity of service for legacy systems, but also allows the integration of a variety of additional systems via information providers (mediation modules). It currently supports, among others, the JTLS and JCATS simulations, the JEMM exercise management tool, and various C2 systems. As a common framework, the Exercise Control Information Services enable the Education, Training, Exercise and Evaluation (ETEE) community to reuse as much as possible the operational procedures associated with the use of existing (legacy) systems and share training and maintenance cost, while maintaining flexibility to adapt the training environment to meet new and emerging exercise requirements. The capability provides enhanced situational awareness to ExCon by providing access to all information from relevant sources in a consistent manner. The use of web services enables rapid production of customized reports, views and dashboards, configured for specific roles in the ExCon organization.

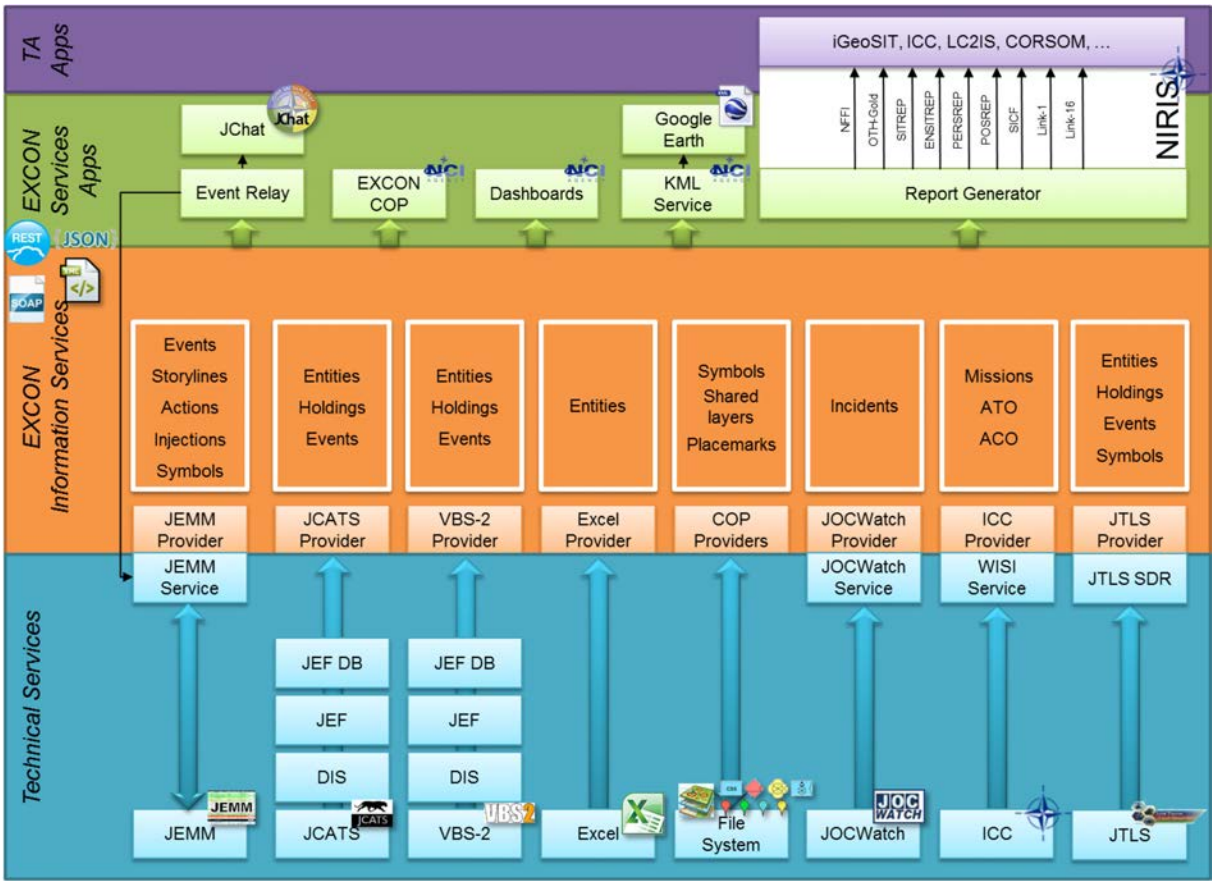

Figure B-7: Overview ExCon Services.

B.9.2 M&S Business Process Supported by the Case Study

- Exercises (collective training).

- Development of exercise operational concepts.
- Development of technical architecture.
- Interoperability.

B.9.3 Role of End-User

- Tactical, operational, strategic level.
- Operational military user.
- M&S technical user.

B.9.4 Security Classification

- Up to Mission SECRET.
- Currently not on AFPL.
- Support for cross-domain.
- Support for Multi-Level Security (MLS).

B.9.5 Type of Services Provided

- Services:
  - Entity service (Simulations, MEL/MIL, …) – ORBAT, Entities, Holdings;
  - Symbology service;
  - Events service;
  - Media service;
  - Object relation service;
  - Recording and replay service;
  - History service;
  - Integration service;
  - Reporting (e.g., ADatP-3) and track (e.g., Link 1, Link 16, NFFI) service;
  - Bridge service (bridge between service instances);
  - Monitoring and management service; and
  - Configuration service.
- Technology Readiness Level (TRL): TRL 7 (“System prototype demonstration in an operational environment”).

B.9.6 Properties of the Service Environment

No information provided.

B.9.7 Capacity/Availability

- Instantiation typically on user's network, can be provided over CFBLNet – depends on location of the users vs. technical systems.
- Example: Service instantiation at JFTC:
  - Periods with intensive access once every ~ 2 months;
  - Available 24/7 with help-desk, local and/or remote support; and
  - Response time immediate in case of local support, otherwise within 2 hours during working hours (can be extended to working hours of the exercise).
- Scalability by stacking of services.

B.9.8 Type of Delivery / Quality of Service

- Web services (SOAP, REST).
- Intended to be part of JEMM installation.

B.9.9 Related Costs

- Existing components:
  - Service definition and basic infrastructure; and
  - Set of information providers.
- For currently unsupported systems: creation of service adapter(s); and
- Installation and configuration.

B.9.10 Authorisation (Who/How)

Will be introduced in iteration 3 (2014).

B.9.11 Expected and Observed Benefits

- Easy and unified way of accessing information, access ExCon information in a consistent manner from exercise to exercise.
- Solution can be tailored to the required level of detail and the available ExCon augmentation.
- Allowing maximum re-use of ExCon ways of working and supporting applications from exercise to exercise.
- No need to re-configure ExCon end-user environment.
- Enabler for wider collaboration: connect other exercise support providers into architecture.
- Clearly defined capability to conduct exercises.
- Deliberate control on information released to TA: injects, automated flows including intel.
- Share ExCon information and combine relevant aspects from multiple sources.

- Shorter ExCon augmentation training.
- Better response cell management of all reportable/reported data.
- Access to information across different networks and locations.
- Share experience between exercise planning teams and apply for different exercise types.
- Expect more rapid response to change requests or emerging requirements for application features or expansion with new sources of data.
- Simple installation and configuration.

B.10 CASE STUDY "C2 INTEROPERABILITY VERIFICATION TESTING" (NCIA)

B.10.1 Description of Case Study

The NATO Nations agreed to the C3 Interoperability Testing Policy in December 2012. The access to the systems and facilities for interoperability testing will be arranged through DNBL services. A corresponding CIS testing service package is available on the DNBL Service Catalogue.

B.10.2 M&S Business Process Supported by the Case Study

Capability development.

B.10.3 Role of End-User

NATO and Nations are the end-users of the interoperability testing services.

B.10.4 Security Classification

NU to NS depending on the level of scenario. The use of operational data requires higher classification of the test environment.

B.10.5 Type of Services Provided

The DNBL CIS service package is structured along the C3 Classification Taxonomy and the list of standards provided by the NATO Interoperability Standards and Profiles (NISP). Services are available for the compliance testing of systems against services and standards and the interoperability testing between systems.

B.10.6 Properties of the Service Environment

No information provided.

B.10.7 Capacity/Availability

The testing services are persistently available during local office hours. Single service capacity is defined in the DNBL Event Support Agreement (ESA) of the specific service.

B.10.8 Type of Delivery / Quality of Service

The access to the services is typically provided in a distributed way via a Wide-Area Network (WAN).

B.10.9 Related Costs

The cost to subscribe to the specific CIS testing service are provided by the service providers ESA and subject to be tailored to the size of the test event.

B.10.10 Authorisation (Who/How)

CIS testing services can be requested by any NATO or national organization with a responsibility for CIS and C2 systems development and deployment to operational theatres.

B.10.11 Expected and Observed Benefits

With the CIS testing services the level of interoperability between NATO and Nations CIS and C2 systems is expected to rise. This will help to become more agile on coalition troop operation and save lives.

B.11 CASE STUDY "JOINT TRAINING ENTERPRISE ARCHITECTURE (JTEA)" (USA)

B.11.1 Description of Case Study

JTEA will provide the Combatant Commands (COCOMs) and services with affordable distributed joint training capabilities at the point of need, tailored to their respective missions, and provision a training environment that emulates the complexity, and dynamic nature of the projected Joint Force 2020 operating environment to support operation, maintenance and accessibility of M&S applications. JTEA is an ongoing initiative of the US Department of Defense, under the direction of the Joint Staff J7.

B.11.2 M&S Business Process Supported by the Case Study

JTEA will provide all operational, functional, and technical aspects of joint training from the strategic to the tactical level in support of joint force development. Joint training events are developed using the process described in the Joint Exercise Life-Cycle (JELC). The JELC is a sub-process contained within the Joint Training System (JTS) Phase III (Execution) and consists of five sub-stages to successfully execute a discrete training event:

1) Design;
2) Planning;
3) Preparation;
4) Execution; and
5) Analysis, evaluation, and reporting.

The JELC is the primary process supported by the JTEA capability and provides a well-defined use case for capability development. The life-cycle of a simulation-supported training exercise is divided into three phases:

1) Pre-Exercise;

2) Exercise execution; and

3) Evaluation and reporting.

These three phases are a simpler way of describing the five stages of the JELC, which is defined in CJCSM 3500.03 series, Joint Training Manual for the Armed Forces of the United States.

B.11.3 Role of End-User

- Strategic/operational/tactical level.
- Operational military user.
- Exercise planning and Control (ExCon).
- M&S technical user.

B.11.4 Security Classification

- JTEA security classification is dependent upon domain and application. Concepts for use extend across multiple security domains up to and above NATO SECRET.
- Support for cross-domain/Multi-Level Security (MLS).

B.11.5 Type of Services Provided

Multiple services will be provided that support all aspects of the JELC. Here are some examples currently under design.

Design:

- Force development mission process modeling;
- Exercise design wizard;
- Joint mission model editor; and
- Joint concept map editor.

Planning:

- Force management service; and
- Staff inject manager.

Preparation:

- Exercise network planner; and
- Admin planning tool.

Execution:

- Tactical decision-making service;
- Logistics service; and
- Convoy simulation service.

Analysis:

- After action review service.

The suite of services will allow JTEA trainers and other users to create their own joint exercises, mission rehearsals, combatant Commander wargames and/or other events like joint staff section training at the strategic and operational levels.

JTEA will also provide capabilities for current and legacy US simulations to join the framework and interact with it, allowing for seamless integration of the existing US military simulation base until those legacy systems are replaced with services that are designed for JTEA.

JTEA will also provide the ability for exercise control and technical support personnel to operate their systems remotely, yielding efficiencies for size of staff and logistics operations. Simulation legacy service/agency components federating with JTEA, as well as some components of JTEA, require operators in order to function. JTEA will provide a virtual connection between operator and simulation to reduce travel, reduce space and hardware requirements, and eliminate reconfiguration costs. The operator's environment will represented in a 3D virtual environment that is web-enabled to provide the display and control for the computer systems running model or simulation applications/services to allow operators to control a simulation and execute events, regardless of location. JTEA will provide a virtual environment accessible from any location that will allow the creation of virtual Exercise Control Group (ECG) that will enable participants to effectively manage the event from their home station, thereby accruing the same savings with regard to travel, space, and reconfiguration costs. The environment will leverage collaboration environment services to enable virtual meetings and related events (e.g. synchronization meetings, shift changeover briefs, etc.) required to collectively support the daily ECG "battle rhythm" and deconflict it from the Training Audience (TA) battle rhythm. It will allow the ECG to monitor TA briefings to stay abreast of TA plans and perceptions. It will support simulation control functions (start, stop, pause, rewind, flag, simulation speed, etc.) to allow management of the simulated environment based on scripted event requirements. The environment will have various communications capabilities, such as chat, telephony voice, intercom, tactical radio (live and virtual), and avatar voice. The virtual environment can be tailored to support specific functions (white cell, response cells, role players, etc.), displaying the same information to the ECG as is provided to the training audience.

B.11.6 Properties of the Service Environment

- Technology Readiness Level (TRL): Given that JTEA is a framework, it of itself does not have a TRL; there are multiple TRLs across the framework each associated with individual components of the architecture. Most components are at TRL 3 – 5.

B.11.7 Capacity/Availability

JTEA is a framework under development; contributing pieces are individually available today in both operational and training domains. In some cases access is limited by current policy with respect to identity management and control, and workarounds have been institutionalized to support coalition and interagency training event participation.

B.11.8 Type of Delivery / Quality of Service

- Use of web services and cloud-based infrastructure is part of the objective architecture framework.
- User interface and auto-provisioning of training enablers to support planning and distribution of collective training.
- Ubiquitous access to force development information and services is planned.

B.11.9 Related Costs

Under development.

B.11.10 Authorisation (Who/How)

- Objective access will be available to combatant command and service trainers.
- Access control and demand for services and apportionment of “capacity” is to be determined.
- Access rights will likely be managed by the Joint Staff J7.

B.11.11 Expected and Observed Benefits

- Accessibility.
- Adaptability.
- Scalability.
- Persistent availability.
- Operationally representative.
- Supports application of innovative thoughts and exploration in warfighting.
- Reduced touch labor costs associated with the planning and conduct of collective training events.
- Collaboration.
- Discoverable services.
- Standards-based.
- Sustainable.

B.12 CASE STUDY “TIES” (M&S CoE, NCIA)

B.12.1 Description of Case Study

Aim of this case study is to test the interoperability of simulation systems and C2 systems focusing on federated Identity Access Management (IdAM), information sharing in SOA environment and messaging services. This case study has been tailored to test NATO M&S CoE Scenario Generator and Animator (SGA) capability within the Tactical Infrastructure Enterprise Services (TIES) Coalition Warfare Program (CWP) of Mission Partner Environment (MNE) (US national Federated Mission Network) in Coalition Warrior Interoperability eXploration, eXperimentation and eXamination eXercise (CWIX) 2014 SOA Focus Area.

TIES is meant to improve interoperability between different national Tactical C2 system Information Technology (IT) services by securely identifying and authorizing users for access (IdAM). NATO M&S CoE SGA is a simulation system able to interoperate with the C2 systems and perceived as another C2 system.

NATO M&S CoE SGA is a M&S capability for constructive simulations, focused on interoperability with other LVC simulation assets and with real C2 systems. SGA environment is composed by the following sub-systems:

- SGA engine allows creation and management of object (platforms, sensors, weapons, etc.) libraries, scenario generation, defining gaming area, entities' kinematics, planning missions and events and scenario animation using artificial intelligence algorithms to perform complex behaviours and missions.

Figure B-8: SGA Engine Function Overview.

- SGA Trials Monitoring (TM) allows to visualize and to monitor exchanged data among the systems involved in the exercise both on simulation bus and on real systems bus.

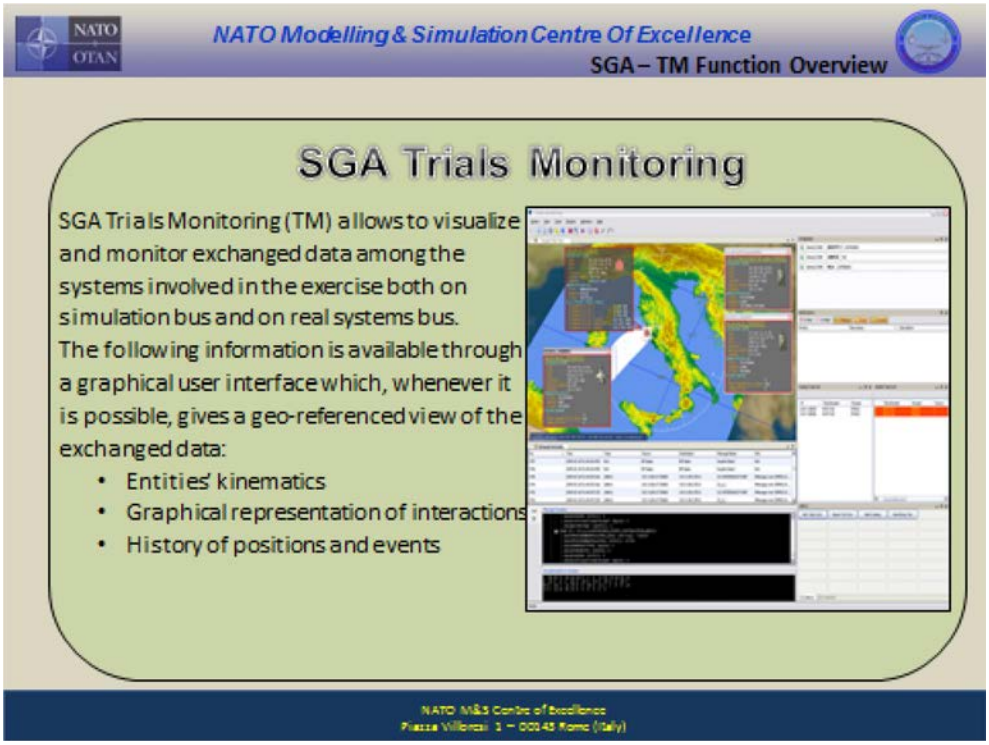

Figure B-9: SGA Trials Monitoring Function Overview.

- SGA Gateway SimReal translates simulation data into real systems and C2 data, to stimulate them, managing different formats at the same time. In particular, GTW is a web application with single sign on capability in an enterprise/federated environment. It exposes web services to allow the exchange of NIEM messages. NIEM messages can also be transmitted with XML labelling feature.
- VCS Gateway LVC bridges the simulation to other live virtual and constructive environments, connecting them at the same time for enhancing interoperability, reducing different configuration issues.

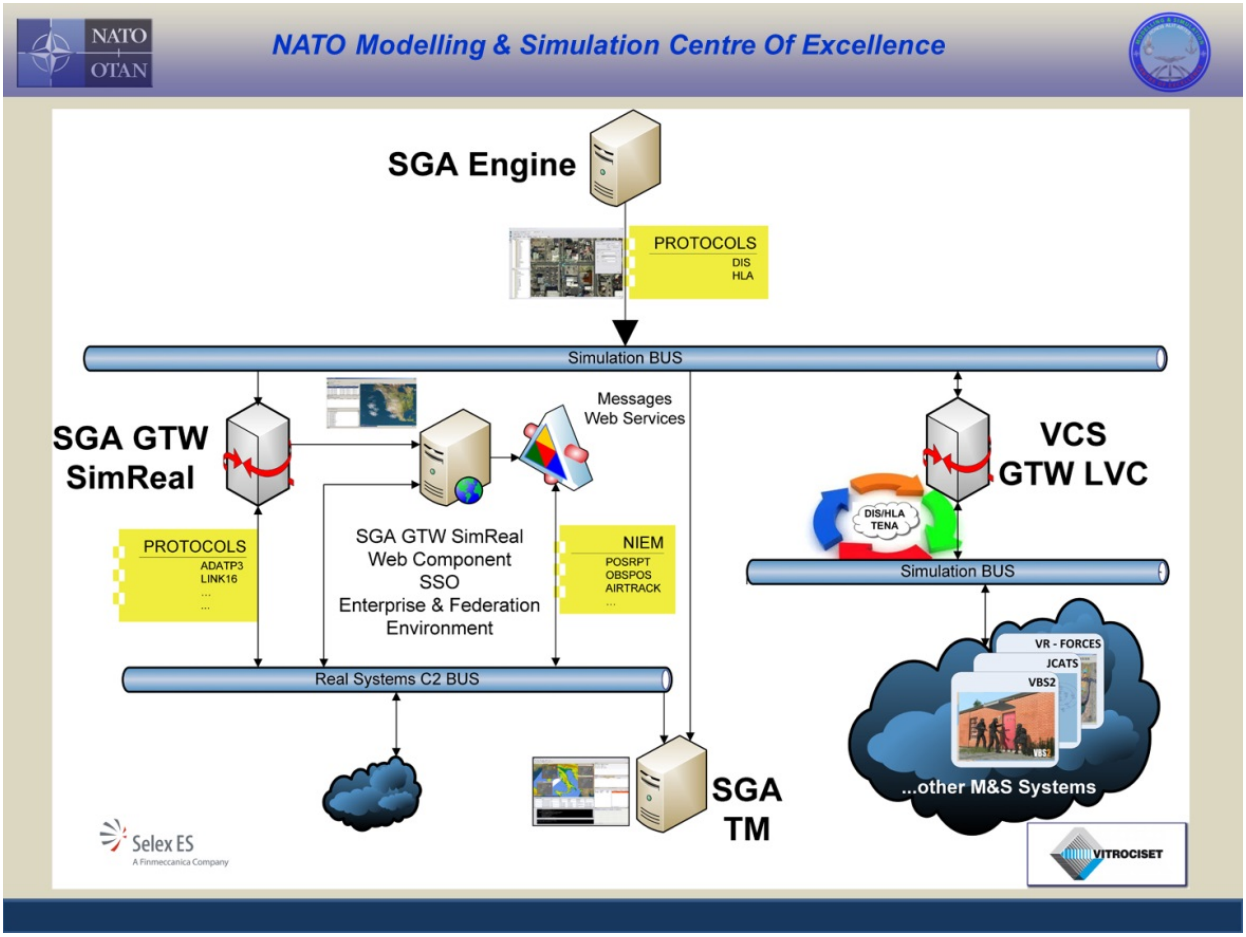

Figure B-10: SGA Capability Overview.

The information sharing is based on NIEM Request-Response Message Exchange. Producers must expose a WSDL web service endpoint(s) compliant with the Coalition Adapter WSDL. Producers must expose their Coalition Adapter WSDL web service endpoint(s) for discovery on an HTTPS URL. Coalition Adapter Compliant WSDL Consumers must query each Coalition Adapter Web Service with one or more desired Categories and cut-off time, as specified in the Coalition Adapter WSDL, to receive NIEM messages. The consumers must be able to parse the query response, which is composed of a list of updates and deletes for a given category. The consumers must then be able to parse each update and delete to determine the type of NIEM message received. The consumer must then be able to process (e.g. translate) into their systems' native format for display. Multiple runs are conducted to assess accuracy, consistency, and completeness.

The information assurance in SOA environment is based on Federated Mission Network Configuration Template for Web Authentication Services (SAML 2.0 Security Token, WS-Federation, WS-Trust). Tests are conducted through Web Application Single Sign-On with trusted consumer (Enterprise Scenario) or federated provider and consumer (federated scenario) Identity Provider using WS-Federation protocol or SAML 2.0 Protocol. During these tests, Provider provides its Web Application accessible via browser.

Consumer provides Identity Provider used to authenticate users in consumer domain.

The Web Application has a trust relationship with the Identity Provider in consumer domain, and is registered in Identity Provider as Relying Party. The trust relationship is established using PKI trust (exchange of Root/CA certificates or cross-certification).

User accessing the Web Application from consumer domain is redirected to the consumer Identity Provider for authentication (automatically using Home Realm Discovery or manually by following a link provided on Web Application home page).

After successful authentication, the Identity Provider redirects user back to the Web Application passing SAML Security Token containing agreed set of user attributes. Interaction between the Web Application and consumer Identity Provider used to exchange SAML Security Token is based on WS-Federation Passive Profile.

Based on the results of authentication and the user attributes provided in SAML Security Token, the Policy Enforcement Point protecting Web Application provides the user an access only to authorized Web Application parts/information (in extreme case denies an access to the Web Application at all).

The Web Service Security is based on X.509 Certificate or SAML 2.0 Assertions as primary protection, both for enterprise of federated scenario. Provider provides its Web Service accessible at given URL and the Identity Provider used to authenticate users in provider domain.

Consumer provides its Application able to invoke provider Web Service and the Identity Provider used to authenticate users in consumer domain.

The Web Service has a trust relationship with the consumer Application.

The Web Service has a trust relationship with the provider's Identity Provider.

Provider's Identity Provider has a trust relationship with the Identity Provider in consumer domain.

The trust relationships are established using PKI trust (exchange of Root/CA certificates or cross-certification).

In case access is granted, the Web Service processes the request and creates valid response.

The PEP signs response using the Web Service certificate and returns signed response to the consumer Application.

The Application validates the signature and processes response.

Finally, Confidentiality Labeling of information is compliant with AC/322 Directive and Guidance (Final Draft). Tests are conducted both for Confidentiality Label embedded within Data Objects and binding to SOAP message. Provider provides its Web Service providing information objects.

Consumer provides a client able to invoke Web Service.

A response SOAP message body contains one or more information objects with different classification labels attached to these objects.

The highest classification label value of these objects is mapped to the SOAP header to express the classification value of the whole SOAP message. In addition, based on the security policy of the originating domain, the SOAP body may or may not be encrypted during the message transportation phase.

B.12.2 M&S Business Process Supported by the Case Study

- Concept development.
- War fighting experimentation.

- Support to acquisition life-cycle.
- Analysis of possible alternatives in procurement decisions.
- Life-cycle cost and logistics analysis (prediction tools).
- Test and evaluation in capability development and interoperability.
- M&S embedded in CIS and weapon systems (e.g. mission planning / mission preparation).
- Exercise and training (individual/collective/joint).

B.12.3 Role of End-User

- Technical/tactical/operational level.
- Operational military user.
- Defence procurement/acquisition community.
- M&S technical user.

B.12.4 Security Classification

Unclassified.

B.12.5 Type of Services Provided

- Decision support/prediction services.
- AAR (and in action review) services.
- Distributed training.

B.12.6 Properties of the Service Environment

- Technology Readiness Level (TRL): 7.
- Level of fidelity: High.
- Level and type of control: Full control.

B.12.7 Capacity/Availability

Not yet available as a service.

B.12.8 Type of Delivery / Quality of Service

Use of web services, including cloud-based infrastructures possible.

B.12.9 Related Costs

Main development activities will be finished by 2015. No assessment of cost of operation available.

B.12.10 Authorisation (Who/How)

NATO M&S CoE is the owner of the SGA capability and has full access to the service.

B.12.11 Expected and Observed Benefits

The tests run during CWIX 2014 proved a relevant interoperability, flexibility and adaptability of SGA and its capability to interoperate with other simulation systems and C2 systems using different formats and protocols. The simulation environment proved also the capability to be published as a service.

This resulted into a high operational relevance, in terms of capability to stimulate C2 systems for training purposes, testing in virtual scenarios, development of new concepts, and decision support in operations.

B.13 CASE STUDY "TABLE-TOP EXERCISE" (NCIA)

B.13.1 Description of Case Study

The case study describes a table-top exercise with reference to the example developed for the Harbour Protection system assessment by CMRE for the NATO Harbour Protection Table-Top Exercise (HPT2E, Mar 2012) CMRE-MR-2013-004.

The exercise used red-on-blue serious gaming to:

- Exercise emerging technologies for maritime force protection countering small boat and underwater intruder threats in ports and harbours;
- Demonstrate the non-lethal capabilities envisioned for integrated surveillance and response using emerging technologies;
- Assess the vulnerability reduction afforded by analysis of red-on-blue engagements; and
- Demonstrate the role that gaming can play in capability development in counter terrorism.

B.13.2 M&S Business Process Supported by the Case Study

Table-top exercise for Harbour Protection supporting:

- Concept development;
- War fighting experimentation;
- Support to acquisition life-cycle;
- Analysis of possible alternatives in procurement decisions; and
- Test and evaluation in capability development and interoperability.

B.13.3 Role of End-User

The case study is supporting TTPs development in Harbour Protection area:

- Technical/tactical/operational/strategic level;
- Operational military user; and
- Defence procurement/acquisition community.

B.13.4 Security Classification

NATO UNCLASSIFIED.

B.13.5 Type of Services Provided

Services from the 134 services from 27 M&S CoI enabling set of the DNBL service catalogue.

No.	Service category
1	DNBL T&E Manager and Integrator
2	Battle Lab
3	C2 elements representation
4	Platform and System Elements representation
5	Life Form representation
6	Synthetic natural environment
7	Communication systems representation
8	Computer Generated Forces
9	Simulators
10	Information Assurance and Security
11	Networking Infrastructure
12	Collaboration support
13	Federation Development Services
14	Integration Tools
15	Global management
16	Integration Services
17	Federation management services
18	Scenario management services
19	Interface testing
20	Integration test
21	Federation system performance testing
22	Interoperability services C2 and Simulations
23	Interoperability Services LVC
24	Interoperability services Simulation-Simulation
25	Analysis services
26	Verification Services
27	Validation Services

Figure B-11: M&S CoI Enabling Classes of Services.

Provider/Category	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
AGI				X		X	X	X						X				X							X		
Cassidian SDC		X				X								X		X		X					X	X			
Havelsan						X								X													X
ITWL			X				X		X									X									
MBDA	X	X	X	X			X	X	X	X	X	X					X		X	X			X				
NADS		X						X	X				X		X		X						X	X			
NATO MSCO (via NRL)						X																					
NCIA Service Strategy	X										X	X															
OKTAL-SE				X		X			X					X							X						X
Pitch Technologies											X		X		X	X				X							
Rheinmetall Defense RDE		X	X	X	X	X	X	X	X				X	X	X	X	X	X	X			X	X	X	X		
RTI														X		X			X	X		X	X	X	X	X	
THALES NLD	X		X		X		X				X	X															
THALES Raytheon TRS																			X	X						X	X
THALES UK	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X				X	X	X	X	X	X
VT MÄK					X	X	X	X				X		X	X	X			X	X	X	X	X	X	X		

Figure B-12: Service Providers for the M&S CoI Enabling Services.

Such a table-top exercise can be supported with a range of services from the DNBL service catalogue.

Category	Short service description	Possible service provider
1	Event Manager – organising the event and orchestrating the service providers	CMRE
2	Battle Lab hosting the exercise	CMRE
3	C2	MBDA
4	Platform and Systems representation	AGI
6	Synthetic Natural Environment	CASSIDIAN
7	Computer generated forces/opponents	THALES
12	Collaboration support	NCI Agency
13,14,16,17,19,20,21,22,23,24,25,26,27	Simulation setup and operation – depending on size of the exercise	THALES
18	Scenario Generation	THALES CASSIDIAN

Figure B-13: Candidate Service Providers for the Table-Top Exercise for Harbour Protection.

B.13.6 Properties of the Service Environment

No information provided.

B.13.7 Capacity/Availability

Single event; 3 days, on-site, based on standardized services which can be repeated in same or different format.

B.13.8 Type of Delivery / Quality of Service

On-site set-up; could be organised distributed and federated.

B.13.9 Related Costs

Services coming from a range of service providers in accordance with their cost estimates provided on the DNBL service catalogue.

B.13.10 Authorisation (Who/How)

NATO Scientific Program of Work.

B.13.11 Expected and Observed Benefits

The table-top exercise provides awareness about the process to operate a Harbour Protection system and on the characteristics/performance of system options against a spectrum of threats.

B.14 CASE STUDY "SERVICES OVER NEEDS (SONS)" (ITA)

B.14.1 Description of Case Study

SONs (Services Over Needs) are achieved using an hybrid cloud-computing and net-centric architectures monitored and controlled by security middlewares.

SONs are a suite of applications (based on all modern architecture like SOA, WebGL, WebSockets) living in this architecture. Internal or external users belonging to different categories can access and use them.

Once the user has logged in to this "ecosystem" (spend less, do more), according to their login credentials and to the reliability of their identity (i.e., NATO SECURITY CLEARANCE), they can specify their needs. The infrastructure will offer a set of available services, a built virtual environment for them or allow them to enter an existing one, enabling also the creation of private cloud on demand and on-the-fly services over needs.

The actor can build an exercise (simulation to simulation / or simulation to C2) on the fly and stimulate its own system.

B.14.2 M&S Business Process Supported by the Case Study (Planned)

Possible application fields:

- Concept development;
- Test and evaluation;
- Training (including joint/collective);
- Technological, tactical, operational; and
- Decision support.

B.14.3 Role of End-User

- Operational military user.
- Other types of users/consumers.
- M&S technical user.

B.14.4 Security Classification

- Support for cross-domain / Multi-Level Security (MLS) / federated domain.

B.14.5 Type of Services Provided

- IaaS, PaaS and SaaS availability.
- Authentication and identity management, identity provider authentication.
- Technology Readiness Level (TRL) = 3.
- Specific M&S:
  - Computer Generated Forces (CGFs);

- Communication Visibility Services (SVC);
- Scenario/terrain generation services;
- Simulation monitoring and control services;
- Complex systems (C2, platforms, sensors, etc.) simulators;
- AAR (and in action review) services; and
- Real systems stimulation through simulation.

B.14.6 Properties of the Service Environment

- TRL 6, the system prototype for main capability was developed in laboratory.
- The systems controls have to be developed and improved.

B.14.7 Capacity/Availability

- SONs infrastructure dynamically scale up and it is always available.

B.14.8 Type of Delivery / Quality of Service

- Use of web services (SOA), including cloud-based infrastructures.
- Use of real-time web protocols (ex. WebSockets).
- Use of optimized graphical system (ex. WebGL).
- Use of standard simulation, C2 and so on protocols.

B.14.9 Related Costs

- Development costs: prototype still under development.
- Cost of use/providing capability: not yet available.

B.14.10 Authorisation (Who/How)

SONs provides different authorization and authentication techniques: database based, windows (domain) authentication, enterprise, federative.

B.14.11 Expected and Observed Benefits

Main benefits are:

- **Agility:** IT provisioning, like public cloud-enabling rapid development and delivering;
- **Cost:** Cloud is easier and cheaper than in-house infrastructure;
- **Control:** Data can be stored geographically, optimized environment;
- **Dev and Test:** Accelerate development and testing cycles while maintaining IT governance and control; and
- **Secure:** Advanced security solution allow use over Internet.

B.15 CASE STUDY "MULTI-RESOLUTION INTEGRATED HLA CLOUD M&S ENVIRONMENT" (POL)

B.15.1 Description of Case Study

The environment is the result of former and ongoing projects conducted by Military University of Technology (Warsaw, Poland) for the Polish Armed Forces. It has been evaluated how to integrate HLA-based simulation environment with services under cloud. The main offer is a service-oriented infrastructure for distributed multi-resolution simulation supporting: decision-making, COA (Course Of Action) verification, mission planning, training, testing (new doctrines, weapons, etc.). The environment is based on HLA as a communication backbone. Currently, the following M&S-specific goals are achieved:

- COA simulation, verification and recommendation;
- Complex operation and mission planning;
- Cyber-warfare influence analysing; and
- Quantitative assessment and planning of capabilities.

The concept schema of the multi-resolution integrated HLA-cloud M&S environment is presented in Figure B-14.

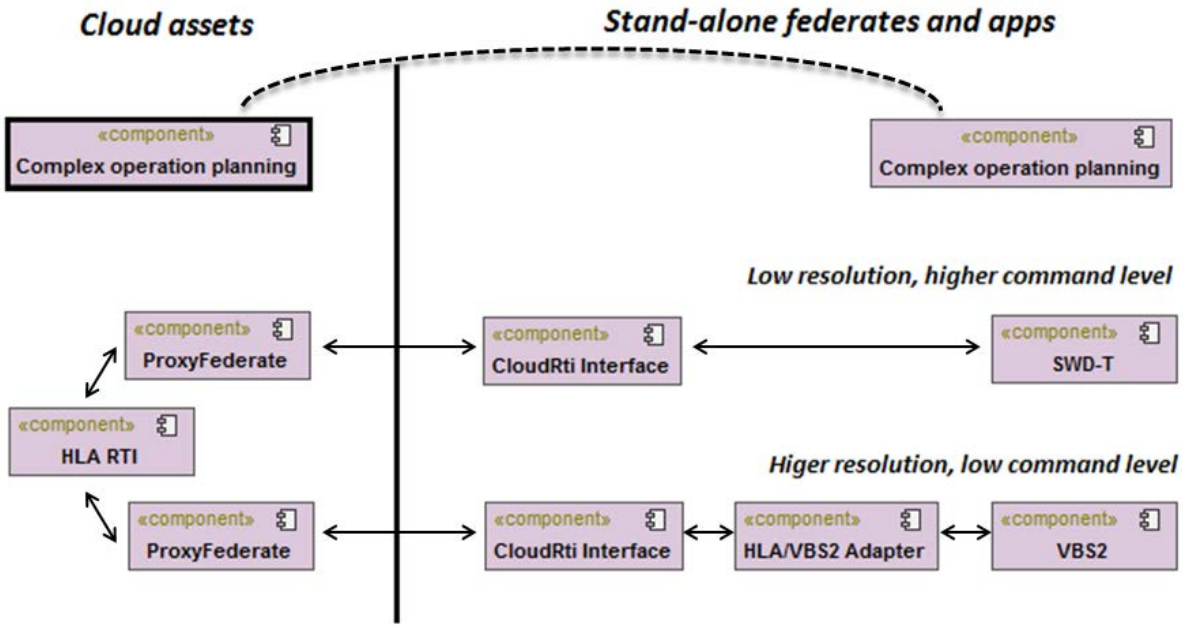

Figure B-14: Concept Schema of Multi-Resolution Integrated HLA-Cloud M&S Environment.

The left-side components are embedded inside a specific cloud. It offers services for connection with HLA RTI as well as for complex operation and mission planning. The right-side components are federate clients for cloud assets. The communications process between both sides demands specialized CloudRti Interfaces and ProxyFederates.

The Complex Operation Planning component offers quantitative evaluation of different variants of complex operation plan. The concept of CAST logic and stochastic PERT analysis to support military joint operation planning are applied. It could be applied not only for military joint operations, but for all complex operations where execution of many different and mutually dependent tasks leads us to a goal.

The SWD-T component is the Course of Actions Verification and Recommendation Simulator (discrete event driven, with random number generators). It is being used mainly for the following services:

- A variant verification (via simulation); and
- The variant recommendation.

In addition, it can be also useful for:

- Optimization of military units' command chains;
- Evaluation of the military operational rules and improving the C2 procedures;
- Research of military equipment's parameters which modify results of military actions; and
- Verification quality of battlefield models (shooting, target searching, movement, etc.).

The most recent functions are oriented to cyber-warfare influence analysing and to support estimation of required capabilities and identification of lacks.

The VBS2 is an interactive environment (well-known) for a military training of a single person or a small group of soldiers. In order to merge those two simulators into one coherent simulation space, the HLA/VBS2 Adapter component has been developed. In contrast to the gateway called *LVC Game* (supplied by the manufacturer of the VBS2), the HLA/VBS2 Adapter approach has been created in order to cooperate with constructive and event-driven simulations, and it does not exclude the possibilities of interactions with real-time simulations. Furthermore, a very important advantage is an ability to configure an exchanged data model, to work with different HLA federation object models, and to manage a logical simtime.

And finally, CloudRTInterface is a component that gives the ability to enrich the functionality provided by the distant federates (on the side of a cloud) – its basic function is to communicate with ProxyFederates. The last one is dual-goal component which encapsulates both web services and the HLA Federate Ambassador.

B.15.2 M&S Business Process Supported by the Case Study

- Decision-making.
- COA (Course Of Action) verification.
- Mission planning.
- Training (including joint/collective).
- Testing.

B.15.3 Role of End-User

Military and associated governmental users on different command levels. Commanders, staff personnel and M&S technical users.

B.15.4 Security Classification

The security classification is related to the security status of collaborated client applications or/and data processed in. Default: NATO UNCLASSIFIED.

B.15.5 Type of Services Provided

Multi-resolution M&S, interoperability, planning, forecasting, optimizing services.

B.15.6 Properties of the Service Environment

Technology Readiness Level (TRL) is 6 – 8. Some modules are prototypes ready to demonstration, while others are completed and qualified through tests and demonstrations.

B.15.7 Capacity/Availability

Generally – under operational testing. Partially – (SWD-T) deployed at universities in order to support education on military-based subjects 'on demand'.

B.15.8 Type of Delivery / Quality of Service

Use of web services and cloud-based infrastructures:

- HLA services for federates; and
- Integration of multi-resolution federates and services via a proxy.

B.15.9 Related Costs

Development costs have been refunded by the Polish National Centre for Research and Development. No assessment of prospective operational available.

B.15.10 Authorisation (Who/How)

To date, the authorization/authentication methods are based on the HLA restrictions.

B.15.11 Expected and Observed Benefits

The benefits are widely observed, particularly:

- Both speeding up and cost-time reduction:
  - When setting up or reconfiguring a multi-resolution distributed simulations; and
  - During decision-making process.
- Common flexible infrastructure for federates as well as services.
- Scalable environment based on cloud assets.

B.16 CASE STUDY "SEMI-AUTOMATED FORCES SYSTEM ARCHITECTURE FOR CLOUD-COMPUTING ENVIRONMENT" (USA)

B.16.1 Description of Case Study

This case study is for a Semi-Automated Forces (SAF) system architecture for cloud-computing environment and is from a concept developed by the University of Central Florida, MSCI, and Leidos for the US Army and was be presented at the 2013 Interservice/Industry Training, Simulation and Education Conference (I/ITSEC). In this project, an M&S as a Service Framework called the Cloud Simulation Infrastructure (CSI) was developed. The CSI consists of three main components (see Figure B-15):

- User application interfaces;
- Simulation services; and
- Physical hardware.

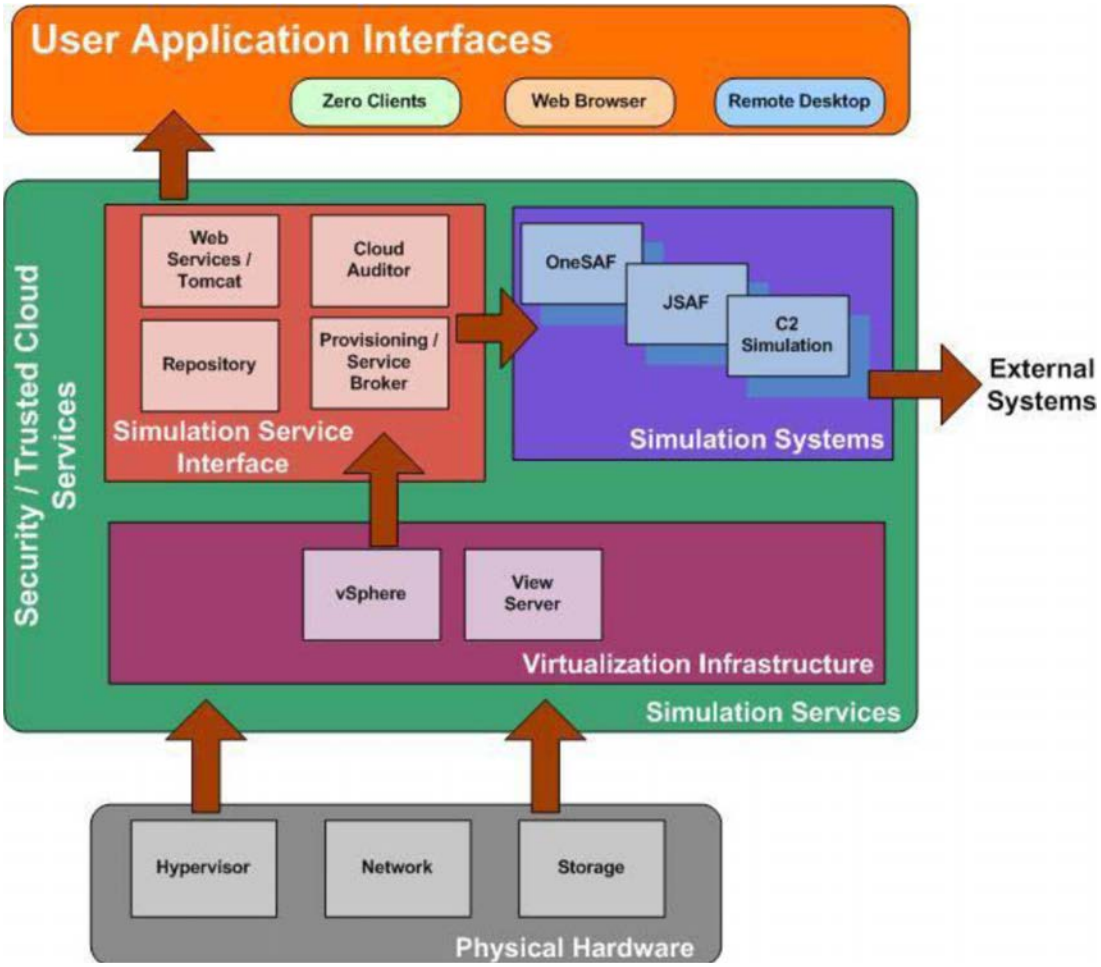

Figure B-15: Cloud Simulation Infrastructure.

The user application interfaces includes zero, thin or thick client interfaces that allow the end-user to interact with the simulation services. The physical hardware provides the CPU, memory, and network hardware infrastructure for hosting the simulation services component. The physical hardware implemented is a high-end network server utilizing virtualization for hosting simulation service components. Future work will explore how High-Performance Computing (HPC) hardware might be addressed in this framework or something similar. The simulation services component contains the actual simulations used for creating the simulation services being delivered. These simulations can interact locally with other locally hosted simulations or may connect to external systems. In addition, the simulation services component contains the virtualization infrastructure. In the case of an HPC not utilizing virtualization, this sub-component might instead provide a set of job scripts that will assign simulation component processes to specific nodes in the underlying HPC infrastructure.

This concept has been tested in real hardware using OneSAF.

B.16.2 M&S Business Process Supported by the Case Study

The cloud-based service for OneSAF enables the US Army to deploy simulation solutions directly to warfighter locations or to centralized simulation centers via enterprise networks. The result is a solution for providing training with lower operator overhead requirements, reduced exercise lead times, and lower overall hardware capital costs associated with legacy simulation approaches.

B.16.3 Role of End-User

Military training, experimentation, and mission planning.

B.16.4 Security Classification

May be hosted at any classification level.

B.16.5 Type of Services Provided

Semi-automated force simulation.

B.16.6 Properties of the Service Environment

Technology Readiness Level (TRL) 4. Proof of concept experiments have been done.

B.16.7 Capacity/Availability

This service would accommodate 24/7 on-demand availability. It is highly scalable and would be limited by cloud hardware and the environment it is hosted on. Proof of concept prototype ran on 40 available CPU cores.

B.16.8 Type of Delivery / Quality of Service

This service allows users to connect to service via zero, thin or thick client over a network connection to configure and execute SAF.

B.16.9 Related Costs

Unknown.

B.16.10 Authorisation (Who/How)

This is part of on-going research for the US Army.

B.16.11 Expected and Observed Benefits

Allows existing and new SAF software to achieve key cloud computing benefits such as on-demand self-service, broad network access, resource pooling and rapid elasticity.

Ultimately, this could result in enhanced training, mission planning and analysis capabilities available to tactical commanders in real time.

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TR-MSG-131 AC/323(MSG-131)TP/608	ISBN 978-92-837-2006-5	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: New Concepts and Service-Oriented Architectures

7. Presented at/Sponsored by

Final Report of Specialist Team MSG-131.

8. Author(s)/Editor(s)	9. Date
Multiple	May 2015
10. Author's/Editor's Address	**11. Pages**
Multiple	120

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
Connected Forces Initiative (CFI)
Distributed simulation
Interoperability
Live, Virtual, Constructive (LVC)
Modelling
Modelling and Simulation (M&S)
Modelling and Simulation as a Service (MSaaS)
NATO C3 Classification Taxonomy
Reference architecture
Service-Oriented Architecture (SOA)
Simulation
Validation and verification

14. Abstract

Modelling and Simulation (M&S) is a key enabler for the delivery of capabilities to NATO and Nations in the domains of training, analysis and decision-making. M&S solutions have to be integrated seamlessly in future computer information systems capabilities to ensure increased efficiency, affordability, interoperability and reusability. Technical developments in the area of Service-Oriented Architectures (SOAs) may offer opportunities for providing M&S solutions that address current NATO critical shortfalls. The application of a "services" model to Modelling and Simulation, henceforth called "Modelling and Simulation as a Service" (MSaaS), promises to greatly reduce the barriers of cost and accessibility and to result in greater utility of M&S throughout NATO and the Nations. In response to a request by Nations and ACT to investigate a "NATO MSaaS" technical concept, and to investigate a supporting Reference SOA, MSG-131 developed a set of conclusions and recommendations on MSaaS. These conclusions and recommendations along with a survey of the experiences of the Member Nations regarding the use of cloud solutions and service-oriented approaches within the M&S domain are included in this report.

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

SC ENCE 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. Zvetan Lazarov"
Blvd "Totleben" 34
1606 Sofia

CANADA
DGSlST
Recherche et développement pour la défense Canada
101 Colonel By Drive, 6 CBS
Ottawa, Ontario K1A 0K2

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

ESPAGNE
SDGTECIN (DGAM)
C/ Arturo Soria 289
Madrid 28033

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
Centro Gestione Conoscenza
Secretariat General of Defence
National Armaments Directorate
Via XX Settembre 123/A
00187 Roma

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 Knowledge and Information
Services
Building 247
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. Zvetan Lazarov"
Blvd "Totleben" 34
1606 Sofia

CANADA
DSTKIM
Defence Research and Development Canada
101 Colonel By Drive, 6 CBS
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
Centro Gestione Conoscenza
Secretariat General of Defence
National Armaments Directorate
Via XX Settembre 123/A
00187 Roma

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
SDGTECIN (DGAM)
C/ Arturo Soria 289
Madrid 28033

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

UNITED KINGDOM
Dstl Knowledge and Information Services
Building 247
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 978-92-837-2006-5