Overview of M&S as a Service

Tom van den Berg
TNO Applied Physics Laboratory
THE NETHERLANDS

tom.vandenberg@tno.nl

ABSTRACT

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

The concept of M&S as a Service (MSaaS) has been researched and evolved by various NATO Research Task Groups (MSG-131/136/164/195) with the aim to address the need to share and pool resources and provide greater flexibility in accessing resources. The Allied Framework for MSaaS defines the technical and organizational foundations to enable a service-based M&S ecosystem with M&S Services within NATO and Nations. The framework is designed to aid stakeholders to utilize state-of-the-art service-oriented and cloud-based methodology and technology to achieve interoperability between participating MSaaS Capabilities. This paper discusses the motivation and presents the Allied Framework for MSaaS.

1.0 INTRODUCTION

Modelling & Simulation as a Service (MSaaS) offers a different approach to providing a simulation capability by exploiting Service Oriented Architecture (SOA) and cloud-based infrastructures, as well as other business models to provide and consume M&S Services.

The following sections discuss motivation and needs, benefits, and challenges for MSaaS, based on the MSaaS Business Model.

1.1 Motivation and Needs

NATO and nations use simulation for various purposes, such as training, mission rehearsal, decision support, and acquisition. Consequently, Modeling and Simulation (M&S) has become a critical technology for the coalition and its nations. A technology that is increasingly integrated with computer information systems capabilities to ensure increased responsiveness, efficiency, affordability, interoperability and reusability.

Such an increase in M&S requirements must consider affordability, sustainability and maintainability as defence budgets are unlikely to increase or even be prioritised towards M&S capabilities. Increasing the efficiency and reusability of M&S capabilities across NATO and its nations is key to making M&S more affordable, and ultimately to achieve the vision of M&S being fully integrated into all operations. There will be the need within the NATO coalition and also within the national M&S communities for greater sharing of models and simulations to leverage investments and encourage greater interoperability to be able to execute the right simulations whenever needed.

Recent technical development in cloud computing technology and service-oriented architecture (SOA) offers opportunities to better utilize M&S capabilities in order to satisfy NATO critical needs. A new concept that includes service orientation and the provision of M&S applications via the as-a-service model of cloud computing. And a concept that has the potential to greatly reduce the barriers of cost and accessibility, and to result in greater utility of M&S throughout NATO and the nations. The application of a "services" model to Modelling and Simulation, became known as "Modelling and Simulation as a Service" (MSaaS).

More recently the motivation for MSaaS had been aligned to modernising defence through practices to match commercial practices (e.g., ecosystem, on-line on-demand at point of need) and exploiting commercial technologies (e.g. cloud computing, virtualization, smart phones, component and service based architectures).

1.2 Benefits and Achievability

The implementation of MSaaS and a resulting ecosystem has the potential to accrue significant benefits provided the challenges of achieving MSaaS can be met.

The benefits would be:

- Greater Agility to meet the demands of fast-changing and complex defence and security environment, in particularly rapidly representing the future operational environments, representing full-spectrum of effects, and integrating real world data feeds.
- Greater Effectiveness through using MSaaS to prepare agile force elements at high level of readiness, to carry out more comprehensive and immersive mission rehearsal, and to support operational decision when planning as well as during prosecuting missions or campaigns. In addition, MSaaS can better inform balance of investments amongst air, land, maritime, cyber, space, autonomous and information operations by supporting operational research or analysis, capability experimentation.
- Greater Efficiency through MSaaS taking advantage of commercial practices such as on-line on-demand service-based ecosystem, leveraging and adapting commercial technology much quicker, and de-risking capability development, test and evaluation and delivery. Potentially leading to time and efficiency savings through establishing and sustaining an on-line on-demand defence M&S ecosystem of models, simulations, scenarios, data, tools and application services.

MSaaS has the potential to not only provide significant enhancement to defence capability but also provides a faster, better and cheaper approach to the need of M&S for defence and security.

1.2 Implementation Challenges

Implementing MSaaS and creating a sustainable defence M&S ecosystem will have technical challenges. In addition to these technical challenges there are cultural, investment and reliance on commercial sector challenges:

- The culture change required will rely on innovative and creative thinking, novel approach to procuring capability.
- Defence budgets have not really recovered since "the peace dividend" divestments, and investment in M&S has to compete with other priorities, so the aim for MSaaS is to do even more with less money and people.
- Defence cannot compete for required technical skills with richer non-defence sectors, so defence M&S is dependent on leveraging technology developed by the commercial sector. Some of these technologies have short life span or morph into new technologies at rapid pace that cannot be

matched by traditional defence decision, development and procurement cycles. So, building resilience in adapting non-defence technology and preparing against adversaries with equal access to non-defence technology are both essential.

- Security challenges, both defence and commercial, are in line with those that defence needs to address more widely as it increasingly uses cloud-based or ecosystem approaches for defence business and operations.

2.0 ALLIED FRAMEWORK FOR MSAAS

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

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

From the definition it is clear that MSaaS is not merely a technical approach of executing simulations in a cloud environment using virtualisation and container technologies. Far from this! The definition stresses the fact that MSaaS is not only a technical solution, but also includes organizational aspects on the enterprise level (e.g., overarching management, governance, funding and oversight). The term "enterprise level" refers to the fact that MSaaS satisfies the needs of a broader community rather than individual service consumers. And the term "management" refers to governance and policies for implementation.

The Allied Framework for MSaaS is a reference architecture providing a common approach in the NATO coalition towards a federated MSaaS Ecosystem, consisting of national and NATO MSaaS implementations, and underpinned by a common technical reference architecture, common processes and a common business model. Figure 1 provides a high-level overview of the Allied Framework for MSaaS depicting a variety of suppliers/providers offering M&S services via amongst others registry and repository services, in a national cloud, a NATO cloud, or some coalition cloud. The M&S services are used by users/customers from thin clients, simulators, C2 systems, and other systems. Suppliers, providers, users, and customers can, depending on their role, use portal applications to discover, compose, and execute M&S services.

To allow easy sharing and to enable broad adoption, key aspects of the Allied Framework for MSaaS are provided as separate documents. The Allied Framework for MSaaS comprises the following four documents, summarized in the next sections:

- **MSaaS Operational Concept Document [1]:** describes the intended use, key capabilities, and application areas of the Allied Framework for MSaaS.
- **MSaaS Concept of Employment [2]:** identifies stakeholders and provides guidance for implementing and maintaining the Allied Framework for MSaaS.
- **MSaaS Business Model [3]:** discusses the concept of an MSaaS ecosystem from a business model perspective.
- **MSaaS Technical Reference Architecture [4]:** describes the architectural building blocks and patterns for realizing an MSaaS Capability.

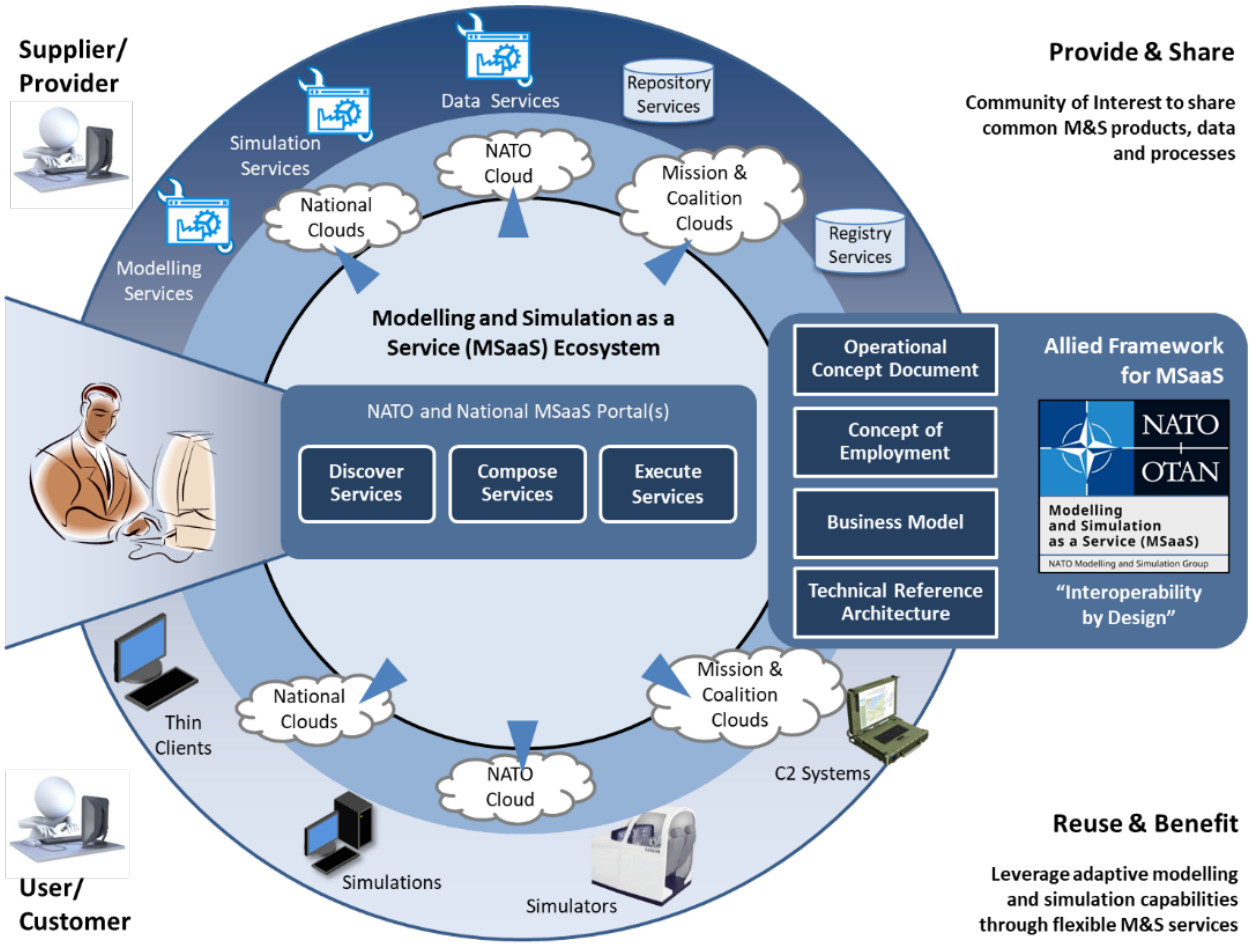

Figure 1: Allied Framework for MSaaS.

2.1 MSaaS Operation Concept Document

The purpose of the Operational Concept Document of the Allied Framework for MSaaS is to inform relevant stakeholders how the framework will function. The Operational Concept Document describes the capabilities and key characteristics of the proposed framework as well as how stakeholders will interact with the system.

2.1.1 Vision Statement and Goals

The North Atlantic Treaty Organization (NATO) Modelling and Simulation Master Plan (NMSMP) [5] defines the following vision regarding M&S:

> Exploit M&S to its full potential across NATO and the Nations to enhance both operational and cost effectiveness.

The MSaaS Vision Statement defines from a user's point of view the desired end-state of a future operational M&S environment.

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

To achieve the MSaaS vision statement the following MSaaS goals are defined:

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

2.1.2 Stakeholders and Relationships

Figure 2 shows the MSaaS stakeholders and their relationships. The identified stakeholders in MSaaS represent generic roles required for implementing MSaaS as a persistent capability. Each nation or organization that implements MSaaS should map these generic roles to its specific organizational structures. Depending on the actual organizational structures, it may be the case that some of the stakeholders identified are actually represented by the same organizational entity. Generic roles can be mapped onto one or more real people or organizational entities. Depending on the organisation size, one real person could fulfil multiple roles, unless prevented by other guidelines.

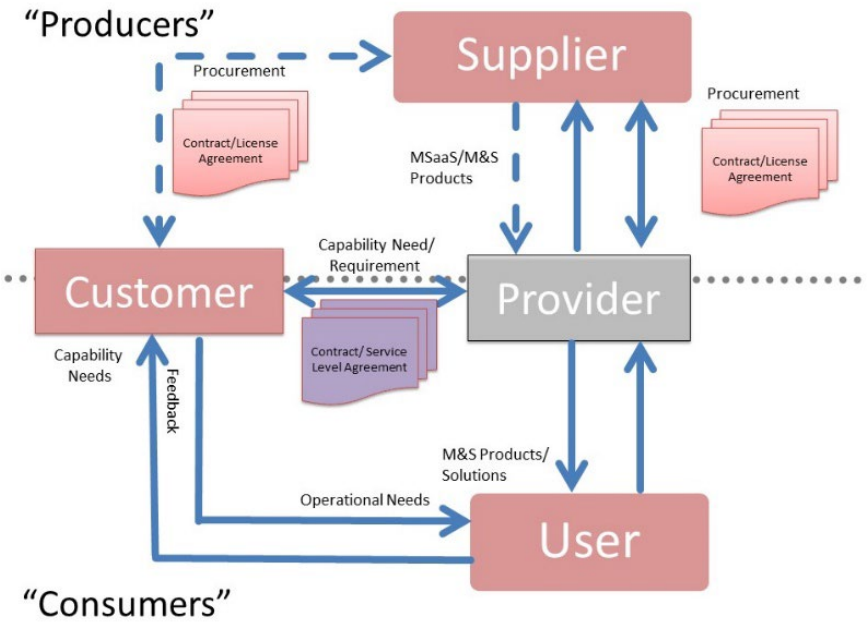

Figure 2: Stakeholders and Interactions.

2.1.3 Application areas and Key Capabilities

Identified application areas are defined in the NMSMP [5]:

- Training (collective training, individual training)
- Support to Operations Planning
- Capability Development
- Mission Rehearsal
- Procurement/Acquisition

The key capabilities supported by the Allied Framework for MSaaS and made available to the users through an MSaaS Portal are:

- **Discover Services.**

  The Allied Framework for MSaaS provides a mechanism for users to search and discover M&S services and assets (e.g., Data, Services, Models, Federations, and Scenarios). A registry is used to catalogue available content from NATO, nations, industry and academic organizations. This registry provides useful information on available services and assets in a manner that the user is able to assess their suitability to meet a particular requirement (i.e., user rating, requirements, simulation specific information, and verification and validation information). The registry also points to a repository (or owner) where that simulation service or asset is stored and can be obtained, including business model information (i.e., license fees, pay per use costs).

  Figure 3 illustrates the concept of distributed registries being able to search and discover simulation assets from various different repositories (i.e., those from industry, academic, NATO or national organisations).

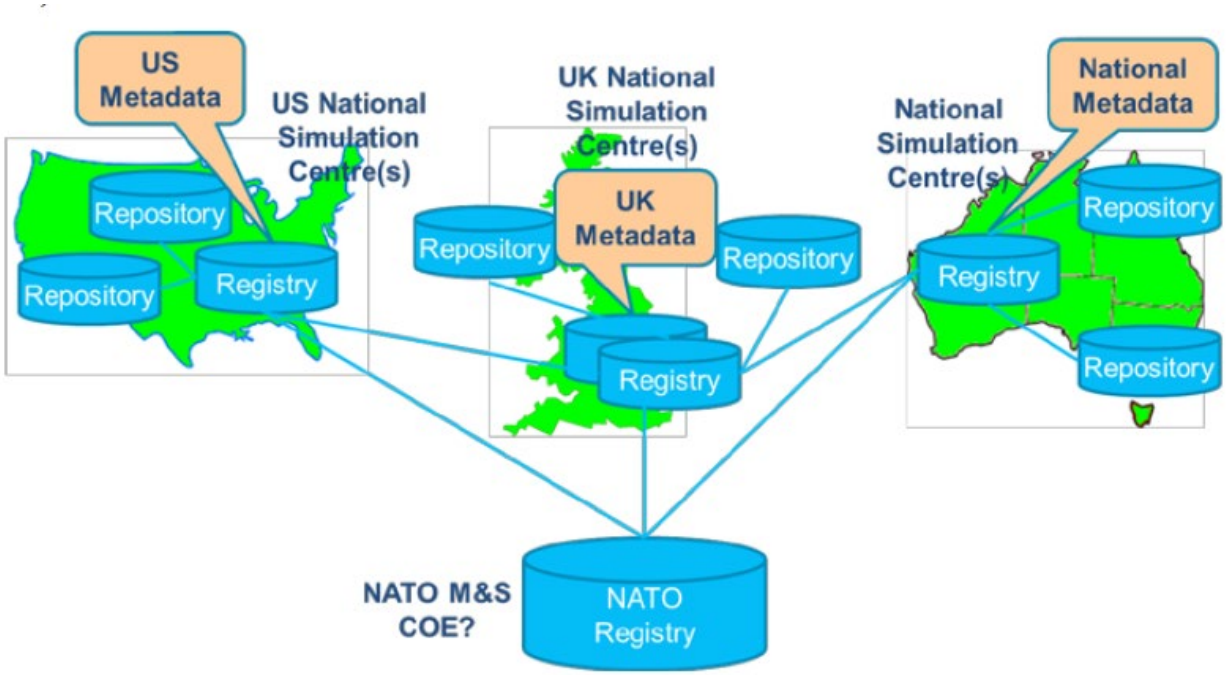

Figure 3: Sharing of registry content across nations.

- **Compose Services.**

  The Allied Framework for MSaaS provides the ability to compose discovered services to perform a given simulation use case. Initially it is envisaged that simulation services will be composed through existing simulation architectures and protocols and can be executed on-demand (i.e., with no set up time). In the longer term, distributed simulation technology will evolve, enabling further automation of discovery, composition and execution than is possible today.

- **Execute Services.**

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

2.2 MSaaS Concept of Employment

The purpose of the MSaaS Concept of Employment is to define policies for MSaaS implementations, and to define responsibilities on how to sustain (maintain and update) the Allied Framework for MSaaS. This ensures that all of the independent service-based efforts (i.e., design, development, deployment, or operation of a service) combined will meet customer requirements.

2.2.1 Terms and Definitions

The MSaaS Concept of Employment provides MSaaS-specific key terms used throughout the MSaaS documents. Some relevant terms are elaborated next.

2.2.1.1 Service

The term "*service*" is always in the sense of "M&S service", using the following definition:

> "An M&S service is a specific M&S-related capability delivered by a producer to one or more consumers according to well defined contracts including Service Level Agreements (SLA) and interfaces."

2.2.1.2 Service Lifecycle

The ability to effectively manage all stages of the service lifecycle is fundamental to the effectiveness of MSaaS. The MSaaS Concept of Employment uses the "*service lifecycle stages*" from [6], see Table 1.

2.2.1.3 MSaaS Implementation

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

An "*MSaaS Implementation*" is the specific realization of M&S as a Service by a certain stakeholder. An MSaaS implementation includes both technical and organizational aspects.

Table 1: Service Lifecycle Stages.

Lifecycle Stage	Description
Proposed	The need for a specific service has been identified and it has been assessed whether existing services satisfy this need. If this is not the case, a new service may be proposed.
Definition	The service's requirements are gathered, and the service design is produced based on these requirements.
Development and Maintenance	The service specifications are developed, and the service is built or maintained to include Verification and Validation.
Compliance	The service is inspected and/or tested to confirm that the service complies with the prescribed set of standards and regulations and is approved for use.
Production	The service is available for use by its intended users.
Deprecated	The service will no longer be available to new users or supported to existing users and will be phased out until retired.
Retired	The service is disposed of and is no longer used.

2.2.1.4 MSaaS Solution Architecture

An "*MSaaS Solution Architecture*" is the architecture of a specific MSaaS implementation and is derived from the Operational Concept Document and the Technical Reference Architecture

2.2.1.5 Stakeholders

The stakeholders in MSaaS are defined by their roles as described by the MSaaS Operational Concept Document, and based on their MSaaS business and operational needs and interactions.

2.2.2 General Policies

The Concept of Employment defines both general and detailed policies for MSaaS implementations. General policies are:

- An MSaaS implementation SHALL conform to the principles as identified and established in the NATO M&S Master Plan [5].
- An MSaaS implementation SHALL be aligned with the NATO M&S Standards Profile AMSP-01 [7]. The AMSP-01 includes recommended M&S standards and STANAGs/STANRECs.
- An MSaaS implementation SHALL conform to the practices, architectural principles, and operating procedures as identified and established by this document.
- An MSaaS solution architecture SHALL comply with the MSaaS Technical Reference Architecture. This includes access to the services through a Portal (or a federation of Portals) and support for a federated MSaaS ecosystem with multiple solution architectures.
- Any M&S service from a NATO MSaaS implementation that is provided or consumed by a NATO body, Nation or Organization SHOULD comply with the policies defined in this document as formalised by its related STANREC.
- The federated MSaaS ecosystem SHALL include a NATO MSaaS Portal provided by a NATO assigned organization.

2.2.3 Organizational Policies

Organizational Policies are more detailed policies and concern amongst others Service Level Agreements, Service Descriptions, and Business Model.

The Service Level Agreements define the conditions under which a service may be used. These are documented according to a template provided in the Concept of Employment.

The Service Description provides a description of the service according to a template as defined in the Technical Reference Architecture. Amongst others, a service is classified in accordance with the C3 Classification Taxonomy, facilitating service discovery via a registry.

The Business Model provides information about how an MSaaS implementation will manage and enable its intended use. Each MSaaS implementation must define a business model covering the topics provided in the MSaaS Business Model.

2.2.4 Security Policies

The Concept of Employment includes more detailed policies related to security. These policies address security concerns of all MSaaS stakeholders by employing a secure environment, for their services, data, account information and personally identifiable information.

The approach to securing an MSaaS implementation is intrinsically related to the underlying infrastructure which may utilize different cloud computing service models (SaaS, PaaS, or IaaS) and deployment model (Public, Private, Hybrid, or Community). For each component it is necessary to evaluate the particular security requirements in the specific MSaaS solution architecture, and to map them to proper security controls and practices in technical, operational, and management classes.

The policies in this section address security concerns and the safeguard of all MSaaS stakeholders (Suppliers, Providers, Customers, and Users) by employing a secure environment, for their services, data, account information and personally identifiable information.

- Any MSaaS implementation SHALL be compliant with the hosted security environment measures.
- All products and services developed by industry SHALL provide the required nation certifications as fit for use and adhere to NIST best practices.
- Any MSaaS implementation SHOULD adhere to the MSaaS Technical Reference Architecture, to provide specific end-to-end data flow examples of where specific security controls (e.g., Cross Domain Security solutions) shall be imposed.
- The stakeholders involved in managing an MSaaS implementation and in providing technical services SHALL be responsible for ensuring they address the users' areas of concern regarding security and secure hosting infrastructure.
- All MSaaS data, data exchanges, data transfers, output (ex. After Action Review) in the same security domain SHALL be at the same classification level. Aggregation of data may result in a higher classification and needs to be examined and re-classified before execution.
- The stakeholders involved in managing an MSaaS implementation and in providing technical services SHALL apply best practices for security and comply with specific regulations from involved accreditation authorities.
- The practices to be implemented SHALL be selected by the MSaaS provider based on the national or other specific organisational security requirements. Selected practices and compliance with them SHALL be documented by the MSaaS provider and SHALL be provided upon request to other parties.

2.3 MSaaS Business Model

The purpose of the MSaaS Business Model (BM) is to define the topics for a Business Model for an MSaaS implementation. The purpose of a Business Model for an MSaaS implementation is to inform relevant stakeholders on how the MSaaS implementation will operate in the multi-government business space for the sharing of M&S technologies. The Business Model for an MSaaS implementation describes how the implementation will manage and enable the intended use, key capabilities and desired effects of the Allied Framework for MSaaS. It also defines methods and means to enable MSaaS as demand-supply ecosystem. The following subsections summarize the main topics to be addressed in the Business Model for an MSaaS implementation. The topics are provided through an MSaaS Business Model Canvas.

2.3.1 MSaaS Business Model Canvas

The BM makes use of an MSaaS Business Model Canvas, based on the Osterwalder and Pigneur's Business Model Canvas [8]. The Business Model Canvas is a strategic management template for developing a new or documenting an existing business model. It is a visual chart with elements that describe the organizations value proposition, infrastructure, customers and finances. It assists organizations in aligning their activities by illustrating potential trade-offs.

Figure 4 provides the visual chart of the MSaaS Business Model Canvas. It shows typical defence and security perspectives that must be considered for the Business Model of an MSaaS implementation.

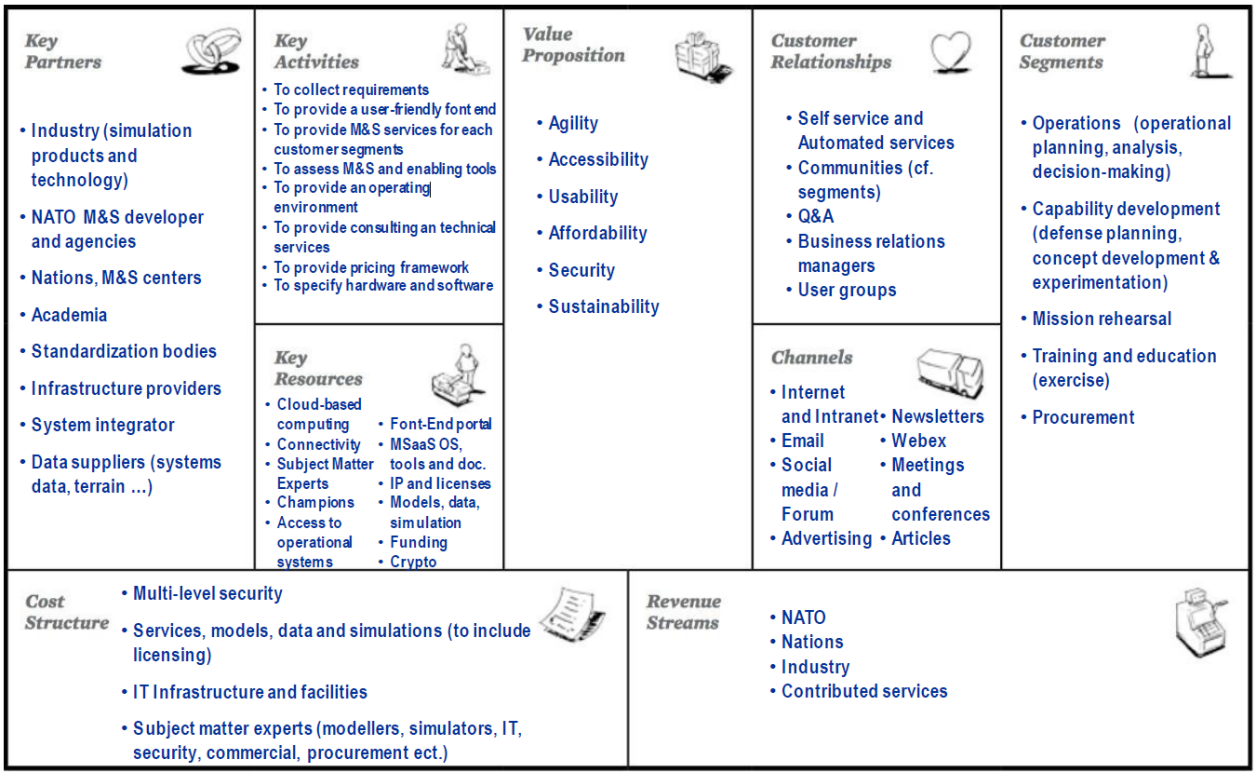

Figure 4: MSaaS Business Model Canvas.

2.3.2 MSaaS Business Model Canvas Elements

2.3.2.1 Key Partners

Stakeholders can be segmented into distinct groups (roles) based on needs, behaviours and other traits that they share. The stakeholder segment is defined by their roles as described by the MSaaS Operational Concept Document based on their MSaaS Business and operational needs interactions. At the top level, the Stakeholders can be classified as Service Producers and Service Consumers. These two categories can be further divided into respectively, Suppliers / Providers and Customers / Users.

2.3.2.2 Key Activities

Key activities are considered relevant in order to satisfy the value propositions. The activities will be performed by one or more stakeholders. For instance, continuous collection of customer and/or user requirements, provide consulting and technical services, and provide pricing framework.

2.3.2.3 Key Resources

Lists the key resources required to deliver the MSaaS Value proposition. For instance, cloud-based computing (public, private or hybrid clouds), connectivity, and subject matter experts.

2.3.2.4 Value Proposition

The MSaaS value proposition is stated as follows:

> Agile and user-friendly services that are readily accessible to compose and execute the required modelling and simulation environment that is sustainable, affordable, scalable and secure.

To deliver MSaaS to the stakeholders, the values needed are further specified and detailed in the terms as listed in the canvas.

2.3.2.5 Customer Relationships

Identified customer relationships are those listed in the canvas. The MSaaS Portal will be an important access point enabling Customers to communicate and engage with other stakeholders and communities.

2.3.2.6 Channels

While various channels of communication will be available, the highly encouraged means to communicate within the MSaaS ecosystem will be through the MSaaS Portal. Main communication channels include for instance:

- Emails, Newsletters (on MSaaS Portal);
- Video or Telcons (e.g., Webex, Skype);
- Social Media.

2.3.2.7 Customer Segments

The customer segments and their operational needs are recognized in accordance with the NATO M&S Masterplan (NMSMP) application areas:

- Operations (Operational Planning, Analysis, Decision-Making);
- Capability Development (Defence Planning, Concept Development & Experimentation);

- Mission Rehearsal;
- Training and Education (Exercises);
- Procurement.

The different application areas will all be able to benefit from the MSaaS proposition. Specific needs or constraints may be different or stricter (e.g., security requirements for mission rehearsal) depending on the domain.

2.3.2.8 Cost Structure

There is an inherent cost to doing business when adhering to the MSaaS construct. Key cost drivers are listed in the canvas and include:

- Cost to maintain an open architecture;
- Cost to adhere to standard communications protocols;
- Cost to Maintain Continuous Security Accreditation;
- Cost of ensuring compatibility with off-line/on-premises implementations;
- Cost of services, models, data and simulations;
- Cost of IT Infrastructure and facilities;
- Cost of Subject Matter Experts;
- Cost of Local Implementations for Execution;
- Cost of Modernization and Maintenance.

While there are many costs to be considered when implementing MSaaS within an organization, many of these costs are not unique to MSaaS.

2.3.2.9 Revenue Streams

The MSaaS sources of revenue (includes money and services) are:

- NATO;
- Nations;
- Industry (B2B); and
- Contributed services.

These revenue streams are more or less the same as in the current situation. Current Customers of M&S products pay for the product (including tailoring, integration, interest charges, acquisition and contracting), lifecycle maintenance (licenses, technical support), hardware, facilities (including energy & cooling) and cost of operators (e.g., instructors, maintainers).

Payment models include:

- Fixed pricing: list price, product feature dependent, customer segment dependent, volume dependent.
- Leasing: fixed price or pay-per-use, product feature dependent, customer segment dependent, volume dependent.
- Cost plus incentive: either including or excluding facility and operator costs.

2.4 MSaaS Technical Reference Architecture

The purpose of the MSaaS Technical Reference Architecture is to provide technical guidelines, recommended standards, architecture building blocks and architecture patterns that should be considered in realizing an MSaaS Capability. The Technical Reference Architecture uses the NATO C3 Classification Taxonomy as a tool for describing capability concepts and as a source for architecture building blocks and patterns.

2.4.1 MSaaS Architecture Framework

Architectures can be designed at various levels of abstraction and different types of architecture can be distinguished. The MSaaS Architecture Framework identifies three types of architecture and methods need to be applied for refining an architecture at one abstraction level to the next, see Figure 5.

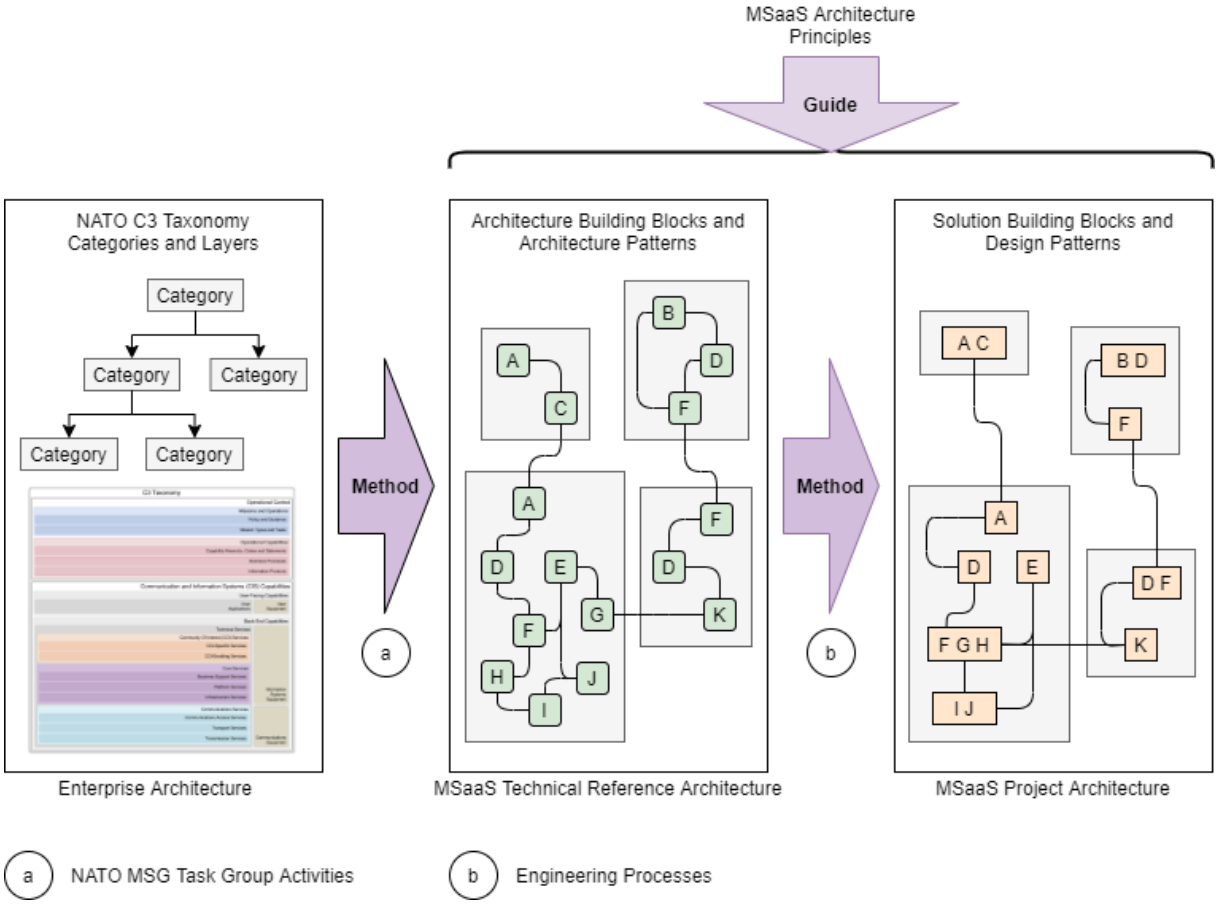

Figure 5: MSaaS Architecture Framework.

- **Enterprise Architecture**. The NATO Consultation, Command and Control (C3) Taxonomy is considered as the Enterprise Architecture. The NATO C3 Taxonomy provides a categorization of NATO C3 capabilities (including standards and requirements), organized in a hierarchy by supertype-subtype relationships. The taxonomy is developed and maintained by NATO ACT and can be viewed and modified through the C3 Taxonomy's Enterprise Management Wiki site. The C3 Taxonomy informs the Technical Reference Architecture on required capabilities.
- **Technical Reference Architecture**. The MSaaS Technical Reference Architecture (TRA) is developed and maintained under the umbrella of the NMSG through Task Groups. The TRA defines the architecture building blocks that should be considered for the realization of an MSaaS

Capability. This concerns both process building blocks as well as technical building blocks. The notions Architecture Building Block (ABB) and Architecture Pattern (AP) are used to describe building blocks and to describe how building blocks may be combined. An architecture building block in this type of architecture defines a capability.

- **Project Architecture**. The architecture of a MSaaS implementation is called a Project Architecture (also called solution architecture). Since the MSaaS TRA provides the architecture building blocks for an MSaaS Capability, many of the requirements for the solution building blocks used in the project architecture can in principle be derived from the building blocks in the TRA. Still, refinement is generally needed to meet the requirements and constraints of the project. A solution building block in this type of architecture defines a solution, related to an MSaaS implementation.

MSaaS Architecture Principles are general rules and guidelines, intended to be enduring and seldom amended, that inform and support the way in which an organization applies the MSaaS Technical Reference Architecture and implements MSaaS.

Technical Reference Architecture is the focus of this chapter.

2.4.2 Architecture Building Blocks and Architecture Patterns

The notion **Architecture Building Block** (ABB) is used to describe the building blocks in the MSaaS Technical Reference Architecture. A similar notion **Solution Building Block** (SBB) is used to refer to the elements in the Project Architecture. These notions are derived from TOGAF, see figure below.

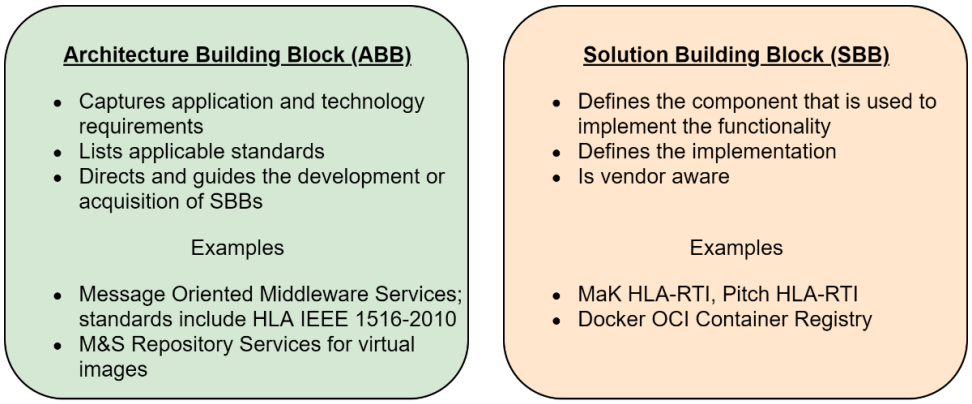

Figure 6: Architecture Building Block and Solution Building Block.

An ABB defines a capability to support the use cases in terms of requirements and standards, whereas an SBB specifies a solution that conforms to the requirements of the related ABB. An ABB represents a component of the Technical Reference Architecture and describes a logical aspect of the overall architecture. An SBB represents a component in the Solution Architecture. An Architecture Pattern (AP) shows one way (of several) of combining an ABB with other ABBs.

2.4.3 MSaaS Capability

The vision of MSaaS within NATO context is to establish an MSaaS ecosystem, where MSaaS Capabilities from different nations are federated, see Figure 7. An MSaaS ecosystem is a network of organizations with MSaaS Capabilities that drives the creation, delivery and use of M&S services in NATO context. An MSaaS Capability consists of operational capabilities as well as technical capabilities needed to achieve this.

The operational capabilities consist of the *MSaaS Operational Concept Document*, the *MSaaS Concept of Employment*, the *MSaaS Business Model*, and the *MSaaS Engineering Process*. The Concept of Employment provides the recommended operating procedures and technical references to promote M&S service sharing and interoperability between MSaaS Capabilities. The Business Model informs relevant stakeholders with a template on how the MSaaS ecosystem should operate in the multi-government business space for the sharing of M&S technologies and services. And the MSaaS Engineering Process informs organizations on the recommended engineering activities for development and use of services, and compositions of services. The MSaaS Engineering Process is addressed in the Technical Reference Architecture.

An MSaaS Capability support the discovery, composition, and execution of M&S services by defining technical requirements in the form of Architecture Building Blocks. The Architecture Building Blocks are organized in several layers (user-facing and back-end) and clusters (within each horizontal layer or cross-cutting layer), in line with the C3 Taxonomy, as illustrated in Figure 8. This figure also shows the operational capabilities mentioned earlier. The scope of the Technical Reference Architecture concerns the detailed stakeholder Use Cases, the Engineering Process, User-Facing Capabilities, and Back-End Capabilities.

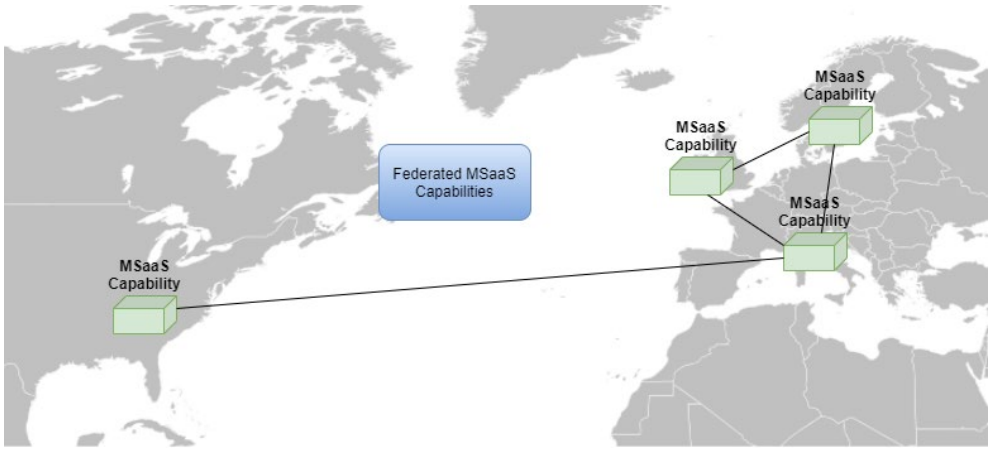

Figure 7: Federated MSaaS Capabilities.

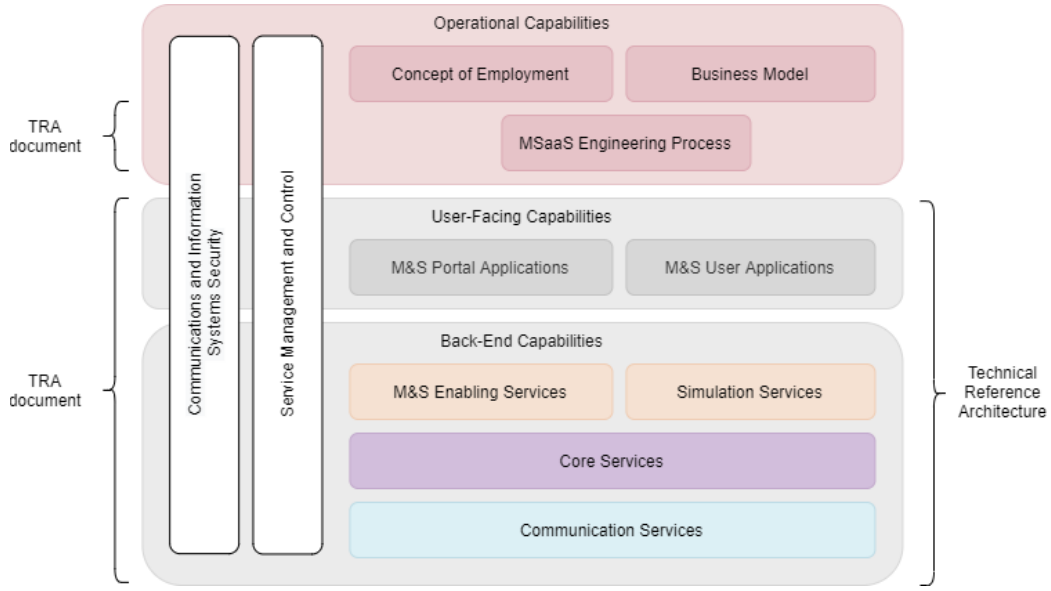

Figure 8: MSaaS Capability: Architecture Building Blocks clustering.

Clustering:

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

The following sections summarize the most relevant ABBs of an MSaaS Capability.

2.4.4 M&S Portal Applications and M&S Enabling Services

M&S Portal Applications and M&S Enabling Services are ABBs that define capabilities that enable the discovery, composition, and execution of Simulation Services and M&S User Applications within a MSaaS Capability.

Portal and Enabling Services capabilities include:

- Integrator Portal Applications (for creating compositions and deployment descriptions).
- Supplier Portal Applications (for providing M&S Resources and associated metadata).
- M&S Repository Services (for managing and exchanging M&S Resources).
- M&S Registry Services (for managing and exchanging M&S Resource Metadata.)
- M&S Message Oriented Middleware (MOM) Services (for distributing simulation data) and M&S Mediation Services (for connecting external services and applications).
- Simulation Scenario Services (for managing simulation scenarios).

2.4.5 M&S User Applications and Simulation Services

M&S User Applications and Simulation Services are ABBs that define capabilities for the synthetic representation of (real-world) objects and events:

- For these there are many. The NATO C3 Taxonomy provides a categorization of potential Simulation Services.

Following are just a few examples of Simulation Services for which one or more solutions can be provided. These capabilities can be linked to categories in the C3 Taxonomy. Recall that the term “Simulation Services” concerns an ABB and refers to a capability. The term does not refer to a solution or a software implementation.

- Route Planning Services;
- Weapon Effects Services;
- Tactical Data Link Services;
- Radio Communication Services;
- Cyber Effects Services;

- Electronic Warfare Services;
- Vantage Point Services;
- Track Generation Services;
- Platform Generation Services;
- Meteo Services;
- C2 Mediation Services.

Solutions for Simulation Services are provided by Suppliers in the form of virtual images (Virtual Machine image, Container image) or datasets, and stored by M&S Repository Services, ready for deployment within the MSaaS Capability.

The description (or the content) of the ABB for Simulation Services includes the following, see Figure 9:

For the Supplier:

- Requirements or specifications, for the benefit of the Supplier who will realize the service as an executable software implementation, supplied in the form of a virtual image.

For the Provider in the role of Integrator of Simulation Services:

- An interface with functional and operational signatures for syntactic interoperability;
- A contract with elaborations of what the functions; and operations declared in the interface do in terms of functional and operational semantics, for a degree of semantic interoperability, as well as a specification of contractual non-functional requirements;
- A model for simulation services of that which is being simulated in the form of limited information (white-box view) on internal workings of the simulation functionality provided by the simulation service, necessary for determining what assumptions in the environment the simulation service uses, for pragmatic interoperability.

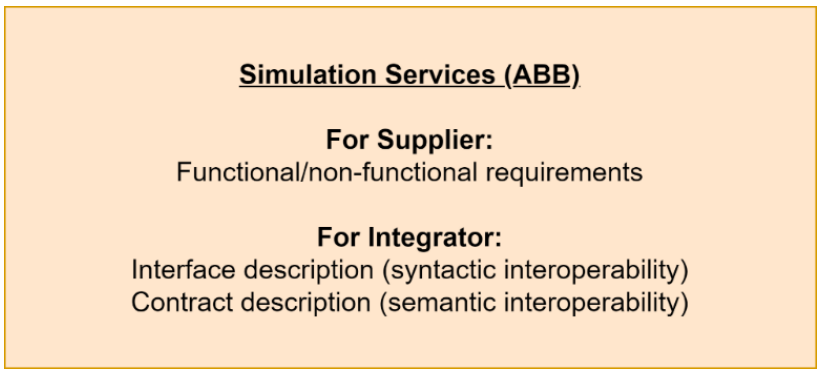

Figure 9: Content of the ABB for Simulation Services.

2.4.6 Service Management and Control

Service Management and Control (SMC) is a collection of ABBs to coherently manage components in a federated service-enabled information technology infrastructure. SMC is a cross-cutting capability that generally affects each building block in the architecture in terms of SMC-related requirements.

Examples of SMC building blocks are:

- Metering Services measure the levels of resource utilization by Simulation Services and M&S Enabling Services, such as number of service/application requests, CPU cycles/time used to process requests, number of messages transmitted or received, number of message queue requests, incoming and outgoing network bandwidth (total size of incoming and outgoing messages), data storage volume used over various periods of time (e.g., second, hour, week, month, year).
- Monitoring Services provide information on the actual utilization and performance of monitored components. These services monitor component communication based on service calls and message exchange to identify performance issues and determine current availability in order to ensure that any failures are detected proactively, isolated, analyzed, and resolved with as little impact on the end user as possible.
- Logging Services are essential for problem analysis, auditing, performance optimization, etc. These services provide facilities for capturing, filtering and saving information about message exchanges between components or important events raised by components in the environment.
- Verification Services verify the correct functioning of M&S User Applications and Simulation Services. For instance, on service in-take from a Supplier, or during the Development and Maintenance stage of the service.

2.4.7 CIS Security

The MSaaS Provider is responsible for the security of an MSaaS Capability. In practice, the MSaaS Provider could be a NATO organization and/or a national organization. It is expected that the MSaaS Provider will have to follow the cybersecurity protocols that are required by the organization/nation. Given the diversity of NATO organizations and national security protocols, it would be impossible to standardize security across the MSaaS Capabilities. Instead, the MSaaS TRA discusses some considerations, specific to MSaaS.

First, the MSaaS Capability itself must be secured by the Provider. Considerations are:

- Security Classification Level of an M&S execution event;
- Access to M&S resources;
- Security of M&S Mediation and Message Oriented Middleware Services;
- Security Monitoring of Service Management and Control.

If the MSaaS Capability is to be federated with another MSaaS Capability, the Federated group of Providers must coordinate security. Also, the federated MSaaS Providers need to have a Memorandum of Agreement or Understanding for the Federation. Considerations are:

- Authentication and authorization between MSaaS Capabilities;
- Trust between MSaaS Capabilities;
- Networking and Encryption;
- Cross Domain Security solutions.

3.0 SUMMARY

M&S as a Service (MSaaS) is a new concept of providing and consuming M&S Services. The concept includes service orientation and the provision of M&S applications via the as-a-service model of cloud computing, and has both an organizational dimension as well as a technical dimension. The concept has the potential to greatly reduce the barriers of cost and accessibility, and to result in greater utility of M&S throughout NATO and the nations.

The concept is described in four documents, collectively called the Allied Framework for MSaaS, covering different areas: operational concept, concept of employment (AMSP-02), business model, and technical reference architecture. The concept has been defined, refined, and further matured by a series of NATO Research Task Groups (MSG-131, 136, 164, and 195).

4.0 FURTHER READING

The MSG-168 Lecture Series on M&S as a Service provides more information on the topic MSaaS. The Lecture Series notes and presentations are available from the NATO STO website [9] (search for MSG-168).

ACKNOWLEDGEMENTS

The author would like to acknowledge the contribution of NATO Research Task Group (RTG) MSG-136 (MSaaS-1), RTG MSG-164 (MSaaS-2) and RTG MSG-195 (MSaaS-3) in relation to the content of this paper. This paper provides a summary of the documentation produced by these RTGs. The author is co-chair/member of these RTGs.

5.0 REFERENCES

[1] "MSaaS Operational Concept Document (MSG-164)," CSO, 2023.

[2] "MSaaS Concept of Employment (AMSP-02)," NSO, 2023.

[3] "MSaaS Business Model (MSG-164)," CSO, 2023.

[4] "MSaaS Technical Reference Architecture (MSG-164)," CSO, 2023.

[5] "NATO Modelling and simulation Master Plan – Strategic Plan," AC/323/NMSG(2012)-015, 14 September 2012.

[6] F. A. A. (FAA), "System Wide Information Management (SWIM) Governance Policies, version 3.1," 2020.

[7] NMSG, "AMSP-01 NATO Modelling and Simulation Standards Profile. Edition (E), Version 1," NSO, 2021.

[8] Osterwalder, Business Model Generation: A Handbook For Visionaries, Game Changers, and Challengers, John Wiley & Sons. ISBN 9780470876411. OCLC 648031756, 2010.

[9] "NATO STO," [Online]. Available: https://www.sto.nato.int/publications/Pages/default.aspx