MSG-168 Lecture Series on
Modelling and Simulation as a Service (MSaaS)

15b. M&S Ecosystem Implementation Guidance

Dr. Keith Ford
Thales UK
Crawley, RH10 9HA
UNITED KINGDOM

keith.ford@uk.thalesgroup.com

ABSTRACT

This paper describes the lessons learnt from experimenting with an implementation of MSaaS in the UK. It covers a range of issues including MSaaS roles, governance, discovery, metadata, resource management, reuse of resources, cloud technologies, security and resilience.

1.0 INTRODUCTION

Even though MSaaS hasn't currently achieved an Initial Operating Capability (IOC) a lot of experience has been obtained by NATO and nationally as a result of experimentation. This paper describes the lessons learnt from implementing an MSaaS capability in the UK.

2.0 MSAAS ROLES

The Ecosystem Administrator is one of the key people for successfully implementing MSaaS and is responsible for;

- Publicising the MSaaS Ecosystem;
- Access control to the MSaaS Ecosystem;
- Harvesting metadata from industry and coalition partner MSaaS registries/repositories;
- Federating registry with industry and coalition partner MSaaS registries/repositories;
- Verifying that M&S Resources submitted to the Registry are compliant with the metadata requirements and that it is an accurate description of the resource;
- Maintaining the registry e.g. install software upgrades;
- MSaaS Ecosystem security;
    - Cyber protection;
    - Production and updating accreditation documentation e.g. SyOps;
    - Supporting penetration testing;
    - Preparing for security audits;
    - Installing security bug fixes;
    - Verifying security clearance of prospective users;

- Integration of MOD, Industry and coalition partner repositories.

In addition to the Ecosystem Administrator, for an enterprise MSaaS implementation the following roles should also be considered:

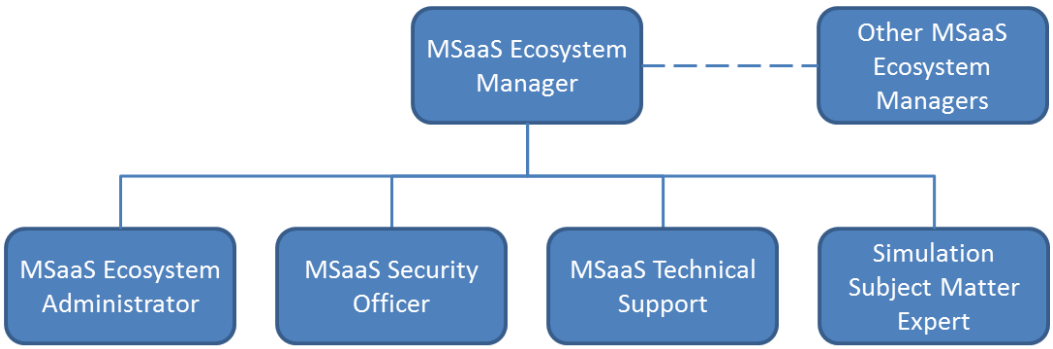

Figure 1 MSaaS Roles

- MSaaS Ecosystem Manager – Overall responsibility for MSaaS Ecosystem, line manager for MSaaS team, managing budget, purchasing, reports into organisation, liaises with other MSaaS Ecosystem managers and M&S Resource Providers;
- MSaaS Administrator – responsible for approving users with access to the different parts of the MSaaS Ecosystem, accepting that metadata accurately describes M&S Resource;
- MSaaS Security Officer – responsible for all aspects of MSaaS Ecosystem security;
- MSaaS Technical Support – ensuring all the tools in the MSaaS Ecosystem are functioning, performing updates to tools, ensuring anti-virus protection is up to date, connecting registry with registries with registries from other MSaaS Ecosystems (where appropriate), providing technical support to M&S Developers;
- Simulations Subject Matter Expert: Provides technical advice on using and integrating M&S Resources and best practice.

Depending on the size of the MSaaS capability, these roles could be managed by one or multiple people.

3.0 GOVERNANCE

A successful implementation of MSaaS will require stong governance. Organisations implementing a discovery capability at the enterprise level need to be fully committed to it for the long term. This is because there have been many initiatives for promoting the reuse of simulation resources and history has shown most have failed. Repositories for storing simulation resources are like Wiki's, there is an initial flurry of activity, which then slows down. Once the people responsible for setting-up the repository/Wiki move on, that usually signals the end of the initiative. A successful implementation of MSaaS in an enterprise requires a senior person to take responsibility to ensure that the initiative is properly funded and resourced, and that all parts of the organisation buy into it.

A board for managing the governance of MSaaS should be drawn up from different layers in the organisation's structure to ensure that all aspects are addressed from incorporation of MSaaS into the organisations processes and culture to practical issues with adoption at the user level. One of the responsibilities of the governance board is to ensure that MSaaS is being properly and effectively applied across the organisation. For UK MOD, this role is being performed by DMaSC.

To maximise the reuse in an organisation, a change in culture may be required to encourage the different parts of the organisation to share the information about the simulation resources they own (noting that due to security or commercial reasons, there may be a good case not to). This is because people are often reluctant to share knowledge/resources as this is perceived as losing 'power', and engineers are often very independent and resist using something designed by somebody else. Also, as MSaaS enables complex distributed simulations to be designed and deployed by non-technical users, engineers who have these skills may feel that their position is threatened.

To overcome any resistance when setting-up an MSaaS Ecosystem, proven change management techniques should be employed. A comprehensive plan should be made for introducing the new capability and metrics need to be produced to ensure that the benefits are being realised.

A key aspect of change management is that of communication. People need to understand:

- Why the change is being made;
- Vision and benefits of employing MSaaS;
- Effect on groups and individuals;
- Training for new skills e.g. use of MSaaS tools;
- Impact on wider business.

It is also important to give people a chance to respond to what they have been told. This not only gives them a sense of 'buying-in' to the change but their knowledge could improve the overall implementation. The MSaaS Ecosystem Manager is key to the successful introduction and management of MSaaS. The person responsible will need good management and communication skills as they need to ensure the governance processes are efficiently applied and they need to liaise with other MSaaS Managers and resource providers.

4.0 DISCOVERY IMPLEMENTATIONS

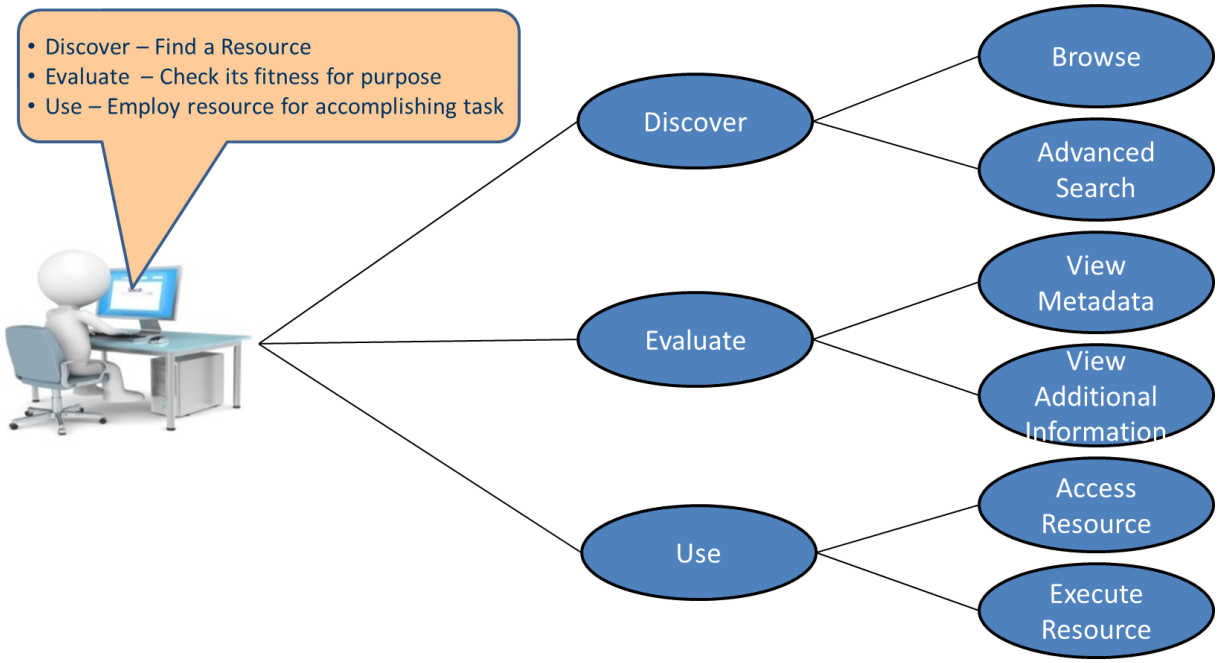

Figure 2 Steps in Discovering and Using a Resource

Figure 2 shows the steps in discovering and using a resource. The discovery activity can be performed in several ways as the approach used depends how well the requirement is defined. A user i.e. Simulation Developer or Simulation User, can just browse through what is available by filtering on a keyword e.g. A400M, or use some specific search criteria to perform an 'Advanced Search' e.g. What Events used the Tornado simulator at RAF Marham in July 2018?

Once a user has identified some resources of interest they will evaluate their suitability by viewing the metadata. In some instances, the metadata may also point to additional information. For physical simulators, this could be an Interface Control Document (ICD). For services and applications, it could be a user manual and for Events it could be lessons learnt from using the simulation environment.

When a suitable resource has been identified, the metadata will provide details to as to how to obtain it. For applications and data, this may be a URL for a repository for where the resource is stored; for services, it may be a URL for accessing the service; and for physical simulators, a point of contact for reserving a slot on the simulator.

There are many ways of implementing a discovery capability and the approach used depends on how many M&S Resources are being managed. When there are only a few tens of M&S Resources, the information could be contained in a spreadsheet. This approach was successfully used in the UK by the Defence Simulation Centre (DSC) for a number of years. The DSC also demonstrated that it was possible to store information in PDF files and used the 'Find' capability to search for appropriate M&S Resources. However, as the number of M&S Resources increases, more sophisticated search techniques are required to discover appropriate resources.

Most repository systems provide a discovery/search capability. If only a few hundred M&S Resources are being used, this may provide a convenient implementation as it combines the functionality of a Registry and Repository in one application. The downside of this approach is that typically, proprietary formats for storing the metadata are used for describing the M&S Resources, which makes it more difficult to share the information.

Where thousands of resources are to be managed the search capability of a registry is required to improve the chance of discovering appropriate resources.
The design of a discovery implementation should be scalable or needs to at least take into account the number of resources that will need to be managed over the long-term.

5.0 METADATA

The biggest risk to the success of MSaaS is poor quality metadata as this inhibits the Discovery process. The creation of metadata is typically performed manually and as such it is prone to errors and ambiguities. To overcome this, some form of automation tool or editor is required for producing the metadata. As a minimum, a tool should be provided to guide a user so that the desired information is entered. Such a tool ensures that all mandatory fields are populated with acceptable values and that keywords are selected from appropriate lists as defined by controlled vocabularies. Ideally all metadata should be produced with the minimum human involvement to ensure that the information provided is complete and consistent. Research by Thales in the UK has demonstrated the ability to automatically create metadata for scenarios. Where possible, MSaaS tools that produce information for reuse e.g. composition tool, should also create the metadata associated with the resource automatically. This will provide consistent quality of the metadata and ensure that it complies with the agreed standards.

A key responsibility of the MSaaS Administrator is to verify that the metadata correctly describes the

simulation resource it relates to and that the information in the registry/catalogue is accurate and up to date.

5.1 UK MSAAS METADATA

The Thales led UK selected the ISO 19000 series as the family of standards to be used by the MSaaS research. This is because the standards support all the elements of Dublin Core, they are formally extensible and have an XML encoding standard to support machine interpretation. The ISO 19000 series standard is also compatible with the use of a registry for providing a discovery capability.

The UK research concluded that although simpler 'catalogue' like implementations were probably sufficient for managing MOD's current simulation resources i.e. comprising simulators, applications and tools, once all the data associated with running M&S Events across MOD was included, the amount of data generated would increase exponentially and a more sophisticated implementation as provided by a registry would be required. For the purpose of the research, the UK used Envitia's GeoRegistry for implementing the registry capability.

GeoRegistry is a tool for managing and discovering geospatial information and natively supports the ISO 19000 series standard. To support the UK requirements, GeoRegistry was modified to enable the user interface to receive and display information about M&S Resources and it was configured with a bespoke Registry Information Model (RIM) that defined the relationship between different simulation objects. This ability is useful if say a Simulation Developer finds a Composition they would like to reuse, by traversing the RIM, they can find out which Deployment objects are associated with it.

The metadata is stored as XML with data structures mapped from existing standards already implemented by the GeoRegistry software. This enables the data to be harvested and stored as searchable fields, enabling machine-to-machine communication as well as human interactions with registry objects.

The approach for managing information proposed by the UK was influenced by and supports the desire to provide a future automated capability for composing and deploying a simulation environment.

6.0 RESOURCE MANAGEMENT

To maintain credibility, the information stored in any catalogue/registry capability should be accurate and up to date. Users that consistently find that the information provided is wrong will soon stop using the capability. This is particularly important where a point of contact is provided for obtaining a resource. Where possible the contact details for a role should be provided rather than a person's name, so if they leave the post, the contact details are still valid.

One of the responsibilities of the MSaaS Administrator is to ensure the validity of the information provided in the catalogue/registry. This will include performing audits to confirm that any URLs provided in the metadata for accessing the resources are still valid.

7.0 RESOURCE STORAGE

The UK research concluded that the MSaaS Ecosystem may have different repositories that are optimised to the type of information being stored. The type of repository used is also dependent on the type of catalogue/registry that is being used. As most repositories will provide some kind of search capability, implementations should not duplicate this functionality. Thales demonstrated that GitHub was a good tool for storing simulation resources where it is not possible to visualise the resource e.g. executable code for services, or where the tool used to perform the search provides a visualisation capability. Repositories like

AtoM provide the ability to visualise different types of media e.g. PDF files.

8.0 REUSE OF RESOURCES

Many simulation resources can be reused exactly as they were initially designed. As an example a VBS3 visual database of Salisbury Plain is likely to satisfy the requirements of multiple simulation environments. Even if the reuse does not exactly meet a requirement, it is usually more efficient to make changes to it rather than starting from scratch. If a high-resolution insert is required for a particular area, in addition to storing the high-resolution insert with the simulation environment it was created for, it should also be linked to the visual data base that it can be used with.

For some resources, it may be known that the requirements of a project may require them to evolve over the lifecycle of the project. As an example, for Synthetic Environment Based Acquisition (SeBA), a simple low fidelity simulation of a platform or sensor may be sufficient when exploring initial concepts which will mature through the programme's lifecycle. This may include improving the fidelity, functionality or interoperability of the resource.

The most efficient way to develop the resource is to consider known future requirements during its initial development. In this way, the architecture will support the future requirements and 'hooks' provided for implementing it. This will impact the way these resources are procured as the cost/timescales will be greater/longer for the initial procurement. When the resource could potentially be used in a different project, where the requirements have not been completely defined, the potential cost savings may be outweighed by the risk that the other potential uses do not materialise, so the extra effort is wasted.

9.0 CLOUD TECHNOLOGIES

Historically simulation capability has been installed on dedicated hardware. However, there is a move in the simulation industry to exploit the use of cloud technologies to make more efficient use of computing platforms.

Virtual machines provide a way of deploying simulation services and applications in cloud environments. The UK research demonstrated that although cloud providers use standards, it is still not always possible to transfer virtual machines from one cloud provider to another. To ensure compatibility, the UK research exploited the use of Infrastructure as Code to build virtual machines (VMs) as they were required.

For windows based applications and services, each virtual machine will require its own operating system licence. This can be provided by the cloud provider on a PAYG basis or installed by the user. In the latter case, if the VMs are not being used, some means of transferring the licence is required. Although the VMs can be stored in a repository because they also contain the operating system, they can be very large, which increases storage and download times.

Care should be taken when using applications stored in VMs to ensure that the number of VMs downloaded does not exceed the number of licences that have been purchased. This requires some form of licence manager to keep track of the number of licences being used at any one time. Ideally the MSaaS Ecosystem should also provide a scheduler that can 'book' the use of resources so that conflicts can be identified and resolved during the planning phase of an Event.

The use of container technologies overcomes some of the issues of using VMs. Each container consists of an entire runtime environment bundled into one package: an application, plus all its dependencies, libraries and other binaries, and configuration files needed to run it. A big advantage of containers is that multiple containers can share one operating system, network connection and base file system. Containers enable a

provider to run the app or service consistently and reliably when moving between clouds or from one computing environment to another e.g. from development rig to live rig.

This ability to transfer containers between different environments makes them ideal for storing and deploying MSaaS services and applications. It is recommended that each container comprises just one service or application. Also, the smaller size of containers compared to VMs reduces the storage requirement and download time.

10.0 CLOUD PROVISION

Most MSaaS ecosystems will have access to a cloud environment as it eliminates the need for dedicated hardware. An advantage of running the MSaaS Tool suite in a cloud means that the tools can be accessed by anyone without having to install software locally. Also, it ensures that all users are using the latest version of the software and no programme to roll out of software updates is required if changes are made to the software. The provision of generic computing resources provided by clouds facilitates being able to dynamically create the infrastructure for executing the services and applications required by a simulation environment.

Care should be taken when choosing a cloud provider to ensure that they meet all the requirements for the MSaaS Ecosystem. Things to consider should be:

- Security – does the cloud have the desired security accreditation, and does it provide appropriate firewalls and antivirus software?
- Data Centre Location – will it allow the MSaaS Ecosystem to obtain accreditation i.e. to be accredited for UK MOD use it should be located in the UK?
- Capability – e.g. graphics support, containerisation, OpenStack?;
- Availability of resources: do they provide the desired capability and in sufficient numbers?;
- Cloud models: do they provide the desired cloud models e.g. IaaS, PaaS, SaaS?
- Resilience – do they have multiple data centres with a mirroring capability, are the data centres geographically separated by an appropriate distance?
- Cost – is charging policy compatible with MSaaS requirements, is it easy to monitor costs?
- Service Level Agreement (SLA) – is the SLA compatible with MSaaS requirements e.g. availability, quality of service?
- Support – are the response times compatible with the requirements of the MSaaS Ecosystem?

One of the advantages of using a cloud is that virtual machines can be spun up and down as required, which can enable significant cost savings if the capability is provided on a Pay As You Go (PAYG) basis. However, experience in the UK has shown that the number of resources available from cloud providers is not limitless and that occasionally they are not accessible when required. This is particularly true of specialised resources such as high-performance Graphic Processing Units (GPUs) if a basic service is adopted.

Cloud providers typically have different levels of service and the confirmed availability of a service needs to be balanced against the extra cost.

11.0 SECURITY

MSaaS has conflicting requirements in that it wants to publicise the availability of simulation resources as

widely as possible whilst protecting protectively marked data and intellectual property. An appropriate balance needs to be struck between the needs of cyber security and accessibility of the MSaaS Ecosystem.

It is recommended that a person in the MSaaS delivery team is nominated to be the MSaaS Security Officer (MSO) and is made responsible for all aspects of security. The duties of the MSO include:

- Security solution;
- Accreditation audits;
- Maintaining accreditation documentation;
- Maintaining audit trail to comply with accreditation processes;
- Ensuring the security processes are strictly adhered to;
- Accreditation of Event networks they are responsible for;
- Providing advice on the accreditation of networks to other MSaaS users;
- Security clearance and authorisation of prospective users.

The implementation of a catalogue/registry must take account of the protective marking of the data it contains. There is a trade-off between making the information as accessible as possible and compromising security. Also, the issue of data aggregation must be considered i.e. the protective marking of the aggregated metadata in the registry may be higher than the classification of the metadata for individual resources. Operating the registry at a system high level will potentially limit the diversity of users having access to the information. Alternatively, a cross-domain security solution could be implemented; however, more research is required to determine how feasible this would be.

A more pragmatic solution to the problem is to only use metadata that is not protectively marked and ensure that the aggregation of the metadata remains unclassified. Any protectively marked information can be provided as additional information in a repository, which can be accessed by users with the appropriate security clearance.

12.0 RESILIENCE

Although not being able to access an MSaaS Ecosystem may be inconvenient whilst designing and testing a simulation environment, it could be disastrous when running a large exercise.

Even if a cloud provider has been selected that provides the required degree of availability, it will count for nothing if the design of the MSaaS Ecosystem and Event simulation environments is not robust. Resilience needs to be designed into the architecture of the MSaaS Ecosystem and simulation environment. However, this needs to be balanced against the extra cost due to the complexity of designing redundancy into the architecture e.g. use of different network bearers, or specifying the SLA for cloud services with a higher availability. A pragmatic approach is to only provide high resilience where the extra cost and timescales warrant it.

The following points should be addressed when considering how much resilience should be designed into an MSaaS Ecosystem implementation:

- Where do the technical and operational risks reside?
- Consequences should something happen?
- Cost if the system fails

- Reputational damage if the system fails
- How quickly must the operations be resumed