A National Approach to Achieve International Distributed Simulation Interoperability Certification.

Grant Bailey
UK Ministry of Defence
UK
grant.bailey127@mod.gov.uk

Daran Crush, Ian Page
Defence Simulation Centre
UK
dfcrush@qinetiq.com, iwpage@qinetiq.com

ABSTRACT

As the capability and utility of simulation across Defense grows, it is becoming increasingly important to understand if each simulation system is fit for purpose, well understood and meets distributed simulation interoperability requirements. To support this, the UK Ministry of Defence's (MoD) Defence Training and Education Coherence (DTEC) approach has developed a set of compliance rules and identified a number of international standards that must be employed, or at the very least demonstrate (from the Enterprise level Value for Money perspective) why they have been discarded. These rules compel system developers to investigate and employ the standards, best practices and resources in which UK MoD has invested. To further support these developments UK MoD is beginning to develop Defense-wide capabilities, delivered as services, to provide common simulation components and resources.

Distributed simulation offers increased opportunity to train collaboratively across national boundaries. With the High Level Architecture (HLA) the preferred NATO interoperability standard, initiatives (such as MSG-134 Distributed Simulation Architecture & Design, Compliance Testing and Certification) are investigating and developing tools for HLA certification. The MSG-134 output will support interoperability testing enabling national and international activities. There is also potential for the development of a UK Distributed Simulation Management Service for Defense that could, for example, manage interoperability software (e.g. the HLA Run Time Interfaces (RTIs)), network performance, interoperability exchange definitions (e.g. the NATO Education Training Network (NETN) Federation Object Model (FOM) modules) and the certification of HLA federations.

This paper describes a potential option that the UK MoD is investigating to develop a coherent testing capability that will support the evaluation of simulation components and the certification of simulation systems interoperability at a national and international participant level. The paper highlights key programs where certification would be required, outlines what a certification service might look like and identifies initiatives that will support the development of such a service.

ABOUT THE AUTHORS

Mr. Grant Bailey is a civil servant working for the UK MoD. Having served for 15 years as an engineering technician maintaining and developing flight simulators in the UK Royal Air Force (RAF), he has spent the past 20 years as a civilian in the UK MoD fulfilling various IT related engineering roles before returning to simulation 12 years ago. Grant is currently part of the Technical Design Authority for the simulation element of the Defence Training & Engineering Coherence approach.

Mr. Daran Crush is a skilled systems engineer, which has led to him working across a wide range of UK MoD programs throughout his 26 year career at QinetiQ and its former UK MoD organizations. Daran's expertise includes the application of simulation and modelling to training, experimentation, testing, battlespace architecture, secure networking and facility construction and operation. Currently Daran is the Technical Lead within the iDSC.

Mr. Ian Page is an accomplished systems engineer who has worked primarily in the area of simulation, modelling and synthetic environments for QinetiQ and its former UK MoD organizations. Ian has extensive experience applying simulation technologies to the training, analysis, trials, assessment, experimentation and equipment acquisition fields. Ian has developed and led many programs across the Defense Land, Sea, Air and Joint domains, frequently working with mixed industry and government teams.

A National Approach to Achieve International Distributed Simulation Interoperability Certification.

Grant Bailey
UK Ministry of Defence
UK
grant.bailey127@mod.gov.uk

Daran Crush, Ian Page
Defence Simulation Centre
UK
dfcrush@qinetiq.com, iwpage@qinetiq.com

INTRODUCTION

Like many other nations, and as a consequence of the 2010 UK Strategic Defence and Security Review (SDSR) which stated that "Defence should embrace a step change in its exploitation of modern simulation training systems" the UK MoD makes extensive use of simulation to support training, education and experimentation activities. Opportunities for live training exercises are increasingly challenging, due to cost, operational, environmental, safety and other drivers, but there is significant potential to undertake or augment these activities using distributed simulation. To ensure the simulation systems are integrated coherently and consistently, and the activities that they are used to undertake are ultimately effective, the individual simulation systems and the complete distributed systems must be thoroughly tested. Rather than testing each system repeatedly for every use, this paper explores how the certification of systems could enable the integration of the distributed systems more efficiently and effectively.

A certification capability offers the potential to test and accredit simulation systems. Such a capability would generate an understanding of how each system may be interfaced with other systems, including security considerations, and the degree to which they have implemented distributed interoperability standards. The capability could potentially offer significant benefits in reducing the time and cost for integrating distributed systems and reducing the overall risk to distributed exercises.

This paper investigates the drivers for a Systems of Systems Approach (SOSA) to developing distributed simulations; the UK MoD's approach to achieving technical coherence in simulation; the current approach to the testing of simulation systems and proposes a new approach: the development of a certification service. The paper discusses the national and international initiatives that would support the generation of such a service; what the service could comprise and key programs that would benefit. While aspirational, the paper concludes with a discussion and recommendation of what would need to be put in place to create the service and what benefits it would engender.

BACKGROUND

Improvements in how training and experimentation capabilities can be delivered to the User are available to Defense today, largely resulting from advances in distributed simulation that includes such things as continuous gaming technology advancements, how simulation is and can be delivered to the point of need, and more cost-effective networking capabilities. It follows that there is a strong argument that distributed simulation should be exploited as it has benefits that includes the following:

- Increasing harmony by minimizing disruption for personnel allowing them to conduct training and experimentation events closer to home, therefore not affecting family life;
- Cutting travel and subsistence costs;
- Allowing for greater participation all levels of UK Defense; and
- Allowing events to take place where assets may not be available.

It is recognized that distributed simulation is not without issues of its own, such as those experienced with differences in time zones and the technical and management challenges to ensure that each system can connect and understand the data that flows between them.

It follows that there is a growing need for technical coherence to ease interoperability and more effectively deliver the benefits of distributed simulation, not just nationally, but also internationally with Allies. Indeed, it is not unreasonable to state that due to resource challenges and safety issues, the use of distributed simulation allows activities to take place that would otherwise only be possible in wartime. For example, it could be argued that complex platforms such as warships can only be fully stress-tested by incorporating simulation. Further, it may only be desirable to test some aspects in simulation, such as those that would allow the exploration of different concepts and operations in a controlled environment that is measurable, safe and secure.

In order to allow individual simulation systems and components to be composed into more capable distributed simulations to reap the above benefits, systems must be developed and managed in a coherent manner. In a drive to ensure this delivery of technically coherent capability across UK Defense, the UK MoD has developed an approach for the acquisition and development of Modelling & Simulation (M&S) capabilities. In this approach, interoperability is promoted along with the ability to improve sharing and reuse. However, matters such as operating across a range of security domains (so called 'Cross Domain Security') and interoperating different technical architectures, particularly those from legacy systems, makes distributed simulation ever more challenging.

Currently, when looking to compose simulation systems and interoperate in a distributed manner, a number of questions arise. For example:

- How do we know what the technical status is for each system?
- Are the systems using approved standards as defined in UK MoD Defence Standard 03-50?
- What data model is being used?
- What is the technical architecture of the overall system of systems or for each individual system or both?
- What enumerations mappings have been employed?

A great deal of technical and coordination effort is needed in order to determine all the required information to create a distributed simulation event. This is where the benefits of certification can come into play, capturing (if it does not already exist) and bringing together all the metadata to describe each of the simulation components in a consistent form. This should both ease the process of answering the questions and also promote the reusability of simulations in multi-level security scenarios and across a disparate set of organizations and systems.

SOSA

SOSA represents an open system approach aimed at mitigating obsolescence issues that challenge the ability to upgrade and integrate into a system of systems. It champions a modular design with interfaces based on open standards that have been subjected to Validation and Verification (V&V) tests (UK MoD, 2015a). This open system approach:

- Promotes interoperability between systems, sub-systems and components;
- Allows the modification of a capability for different roles;
- Eases integration;
- Provides more opportunities for competition and innovation through the open approach; and
- Helps the management of technology refreshes, obsolescence and capability insertion.

By employing the SOSA principles to M&S in what is specifically known as the UK Defence Training & Education Coherence (DTEC) approach, it encourages a focus on those elements that both comprise and are used by each system that will need to be assured to deliver greater interoperability and cost efficiencies across the Enterprise.

Seen as an 'enabling capability' for Defense, there are 9 Principles with SOSA (UK MoD, 2015b) that are applicable to M&S designed to encourage coherence. These Principles spell out and promote goals that minimize diversity, optimize reuse, encourage the selection of proven solutions, direct the use of open standards, etc.

THE DEFENCE TRAINING AND EDUCATION COHERENCE (DTEC) APPROACH

Applying the SOSA principles, the DTEC approach helps to deliver technical coherence for M&S internally across UK Defense and externally with our Allies. It does this via the application of a number of rules with which each simulation-based capability change must demonstrate compliance. DTEC also provides the clear line of governance

that is required to make this coherent capability approach effective. Active engagement with the NATO M&S Group (NMSG) and its M&S Standards Subgroup (MS3) helps to achieve the external coherence requirement.

Underpinning the DTEC approach is the Defence Simulation Centre (DSC) that provides a single point of focus for all simulation within the Ministry of Defence. The DSC provides a number of tools and facilities to help manage technical coherence such as a M&S Catalogue that promotes reuse and sharing, repositories (where needed) to store data and resources, and management of capabilities such as that provided for the Defence Virtual Simulation (currently based around an Enterprise licence for Virtual BattleSpace 3). A DSC Front Door team manages all simulation enquiries in a triage manner providing assistance as required and is able to draw on many resources.

THE CURRENT APPROACH TO DELIVER ACCEPTED DISTRIBUTED SIMULATION INTEROPERABILITY

Types of Testing

A simulation system should never be accepted into operation until its capabilities are tested. A common reference for testing, be it of a system of systems, system, sub-systems or component, can be overlaid across the waterfall development[1] process in a v-type model where, for the purposes of this paper, a simulation is validated and accepted against user requirements, system verified and tested against system requirements, integration is tested against the architectural design and components are tested against a detailed design, see Figure 1.

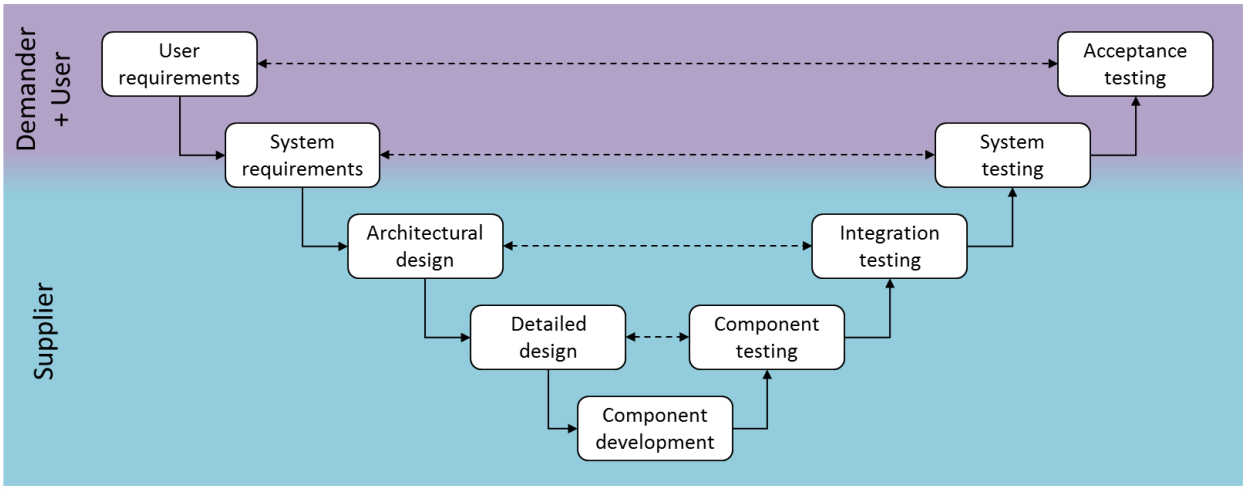

Figure 1. Waterfall process for system development and testing

In Figure 1 it is highlighted that there is both Demander and User (the separate body that sponsors the simulation capability and those that will use the simulation) involvement in system testing and the validation and acceptance processes (as shown by the purple area), but the majority of the testing is the responsibility of the Supplier (the blue area). The Demander and User tests are likely to be tied to a procurement activity (and may well be covered by contractual requirements), whereas the Supplier tests form part of the development activity. This complete process may take place multiple times if the simulation is being delivered in phases and this entire process may also take place a number of times over the life of the simulation as it is updated or upgraded. The overall process may also contain some specific forms of testing, such as interoperability testing.

Existing components (now possibly even complete simulation systems) can be further configured together to meet a particular proposal or purpose, rather than developed anew, and brought together in a specific composition to meet a specific requirement. This activity is likely to be after the original acceptance of the components / system and therefore the Users of the simulation may also be involved in the configuration of the components (simulation systems) as well as the Supplier.

[1] The waterfall development process is used rather than Distributed Simulation Engineering and Execution Process (DSEEP) for simplicity and to allow the clear distinction between the testing activities to be highlighted.

Limitations of the Current Approach

Where there is a clear requirement that specific tests should be generated and undertaken (as mentioned in the Background section), this can require significant levels of effort. This stems from the need to generate all of the data and information needed to successfully compose the simulations into a complete, tested, coherent, interoperating distributed system. But without appropriate action, this information generation and testing activity has to be repeated for each proposed composition as they arise.

Simulation Standards

In order to provide guidance on the selection and use of simulation standards to promote interoperability, best practice and reuse in the simulation domain, the NMSG has created (and maintains) the Allied Modelling and Simulation Publication (AMSP-01), the NATO Modelling and Simulation Standards Profile (NMSSP).

The DTEC M&S Standards Profile (DMSP) (UK MoD, 2015a), is a national subset of the NMSSP, that identifies the preferred M&S standards that should be used by the UK MoD. The content (standards) included in the DMSP are reviewed by UK MoD regularly (typically annually) in consultation with Industry and Academia, although the UK MoD reserves the right over any final content decisions. The DMSP is made publically available. This approach has been welcomed by Industry as it provides strategic customer direction.

Consideration of use of these identified M&S standards is mandated and tested to ensure Value for Money (VfM) at the Defense Enterprise level. It is done in this manner to avoid stifling innovation. So it is possible to obtain a waiver from DTEC if VfM at the enterprise level, and not the project level, can be demonstrated.

It is worth noting that in line with work ongoing with the NMSSP, the next version of the DMSP will include a maturity status for each identified standard and list those standards that are mandated for use in coalition operations. The NMSSP mandated standards will be covered by a STANAG[2] with the NMSSP itself becoming a STANREC[3]. Some of the pertinent standards in the current version of the DMSP are shown in Table 1.

Table 1. UK MoD DMSP Approved Standards

	Category	***Standard***
M&S methodology, architecture, processes and guides	Systems Engineering processes	DSEEP
		DMAO
		FEAT
	Verification and Validation	SISO-GUIDE-001-2013 GM-VV
	Conceptual modelling and scenarios	MSDL
	M&S interoperability	HLA Evolved
	Live simulation	UCATT
	Information exchange data model	NETN FOM
		C-BML
		SISO-REF-010-2015 Enumerations
Synthetic Natural Environments (SNEs)	Processed data sources and formats	Shapefile
		DTED
		GeoTIFF
		JPEG2000
	3D models	OpenFlight
	Production processes	RIEDP
	Visualization	CIGI
	Simulation analysis and evaluation	DDCA
	General	SEDRIS EDCS
		SEDRIS SRM
		CDB

[2] A Standardization Agreement (STANAG) is a NATO standardization document that specifies the agreement of member nations to implement a standard, in whole or in part, with or without reservation, in order to meet an interoperability requirement.
[3] A NATO recommended standard (STANREC), less prescriptive than a STANAG.

It therefore follows that any interoperability between distributed simulation systems in the UK must be seen to consider the HLAe standard and gain a DTEC Waiver before choosing any alterative.

PROPOSED APPROACH TO DELIVER ACCEPTANCE

Interoperability Testing

Interoperability testing is not simply a case of pass or fail, as there may be degrees of potential interoperability depending on the implementation chosen by each particular system. These include, but are not limited to, the following:

- The interoperability standard implemented, for example:
  - Distributed Interactive Simulation (DIS – IEEE 1278); or
  - The High Level Architecture (HLA – IEEE 1516).
- The version of the standard chosen:
  - DIS version 4, 5, etc.;
  - HLA or HLAe.
- The elements of the standard that are supported:
  - For DIS which Protocol Data Units (PDUs) are implemented;
  - For HLA which modules of the NATO Education & Training Network (NETN) or Real-time Platform-level Reference RPR Federation Object Model (FOM) are selected.
- The completeness and correctness of the implementation;
- The software used to support the implementation, particularly the Run-Time Infrastructure (RTI) chosen for an HLA implementation;
- Enumerations selected and mapped;
- The availability of Interface Control Documentation (ICD).

The above list includes old or retired versions of standards whereas the DMSP calls for the latest or preferred versions to be used (for example HLAe is preferred over DIS and the NETN FOM is preferred over RPR). This is because we would not wish to eliminate interoperability with legacy systems that may still use these older versions of standards.

Cross Domain Security

There is a growing requirement to interoperate federations of different security classifications resulting in a need for Cross Domain Security (CDS). Potentially, such federations could be asked to operate at different security levels themselves and interoperate with other federations that are at different and various security classifications, and this situation could change on a case by case basis. Each of these cases will require appropriate recording of configuration data for security accreditation purposes.

Work in this area (Hughes, 2014 and Möller, 2015) has proposed / suggested that required firewall and HLA data ‘guardian’ systems be configured before each federation exercise / experiment and this data can also be captured and recorded not just in the normal security accreditation documentation but made readily available with other interoperability information.

Other Specific Types of Interoperability-Related Tests

In addition to interoperability testing and testing against standards, other types of test could be undertaken and need to be selected as appropriate. Examples include:

- **Simulation performance tests**, i.e. do the simulation representations of the systems match the real world to the required level of fidelity / security classification / real-time performance?
- **Simulation robustness tests**, i.e. do the simulations continue to behave if they are passed invalid simulation data, such as mal-formed HLA messages?
- **Simulation endurance tests**, i.e. do the simulations continue to operate for the required length of time?
- **Simulation fair fight tests**, i.e. do the simulations conform to the laws of physics and do they respond in expected ways of other simulation activities, such as detonations?

- **Simulation consistency tests**, i.e. do the simulations perform the same way / give the same results in the same situations?
- **More general security / cyber aspects**, i.e. are the systems secure against malicious attacks that could come through simulation connections or information exchanges?

Interoperability Data Pack (IDP)

All of the above leads to an approach to generate and collate an Interoperability Data Pack (IDP) for each composed system that will support formal and (if needed) repeated interoperability testing as part of its development.

The IDP could include, but not be limited to, the following:

- The HLA version implemented;
- The RTI used (including version and any configuration information);
- The FOMs supported and the FOM modules implemented;
- The Enumerations supported and mapping information, such as to 3D models;
- The terrain files and configuration information;
- System (software and hardware) version and configuration information;
- The intended use of the system for which it has been tested;
- Other systems that have been connected to and when.

Once an IDP has been created by the federation or system, and approved as being complete, then it should be made readily available to those systems that may wish to have recourse to it in the future to allow preparation for a distributed simulation event.

A CERTICATION SERVICE

The Need for a Certification Service

As the requirement for distributed simulation increases, and the need for technical coherence delivering cost and interoperability benefits gathers pace under financial challenges, the requirement also increases for a certification service that would demonstrate and record testing to certify an IDP for each system/federation. This certification service would also address CDS testing and recording requirements for accreditation purposes.

When interoperability is required across international borders with Allies and Coalition partners, such certification is of equal importance helping to demonstrate that technical requirements have been met with the minimum amount of effort. Therefore, the certification service itself would need to be coherent with NATO plans as covered in MSG-134 to provide confidence in each system.

Triggering Testing Activity

The creation of any federation or system that could have a requirement to interoperate, either within the UK and/or with Allies and Coalition partners would require validation testing and certification. The DTEC Rules would be amended to support this directive. Before each distributed simulation event, checks that the certification certificate is current (within the IDP) and covers the planned exercise/experiment would need to be carried out.

What could a Certification Service look like?

What such a certification service could look like can be described from a number of perspectives, such as physical, governance, availability and the capabilities/functions.

Physical: While certification is ultimately about endorsing a specific system as compliant (or not) against a standardized approach, the user base is varied in terms of the environment and constraints in which they are operating. To meet such a varied user base, the Service needs to have multiple modes of operating to support the broad requirements and constraints of the community. From a physical perspective, this would comprise at least the following means of accessing the Service for a certification activity:

- **Remote access / cloud based service**. This would likely be the preferred means by which most users would access the Service. Users connect in over an appropriate Wide Area Network (WAN) (potentially the same WAN that will be used in the distributed activity), such as the internet, potentially requiring various classification levels to be supported;
- **Physical center**. A number of capabilities that require testing services will not be approved for network access or it may simply be impractical to conduct the certification remotely so a facility is required that can host users during a certification event, this would be expected to be located at the DSC; and
- **Deployable test capability**. There will be some users who, for various reasons, are constrained to their home site and so the Service needs to be able to deploy to the user with a mobile capability.

In addition to the above description of physical access for a certification activity, the Service should also be providing assistance to users during the development and preparation of a system for certification. Support tools to assist developers in testing interoperability at their local site should be available so that they have every opportunity to be best prepared for a certification event. Ideally this should be part of an integrated and pervasive process that results in the certification event being a final confirmation of a pass that is already expected by the user and Service due to the pre-certification activities. The final certification test result should not be a surprise to anyone involved in the process!

Governance: The governance of the Certification process (probably managed under DTEC) and the process itself, should be clear and made readily available to users. The assessment criteria should be clearly described so that users can plan accurately for its inclusion in the development costs of a system. The Certification Service should provide advice and support to users to help understanding of the process, what will be expected and the steps during development that will mitigate the final certification activity. A description of the key steps and recommended activities should be provided with use cases to aid understanding. As mentioned in the Physical section, the certification process should be closely embedded in the user's development of the system to be certified. As well as a clear description of the process, the roles involved should be clearly explained, potentially even having a Terms of Reference for the key roles to clarify what the user is expected to do and what they can expect from the Service.

Ultimately the governance and process needs to be scalable. Large, complex and high impact systems under test will require appropriately detailed certification tests. However, the same governance and process should scale to support an agile and 'light touch' for smaller, simpler and low impact systems. From an internal Service perspective, the governance and process should also include internal activities to identify if changes or updates are required to the certification service as a consequence of user feedback or changes to the standards. Similarly, the supporting test capabilities need to be maintained and developed to ensure they continue to meet what will be an ever-evolving requirement. This will provide a means to take on board lessons learned and apply best practice from the community.

Availability: While physical aspects, such as access to a Service center and the staff to support and provide advice, will necessarily be time constrained to normal working hours, other elements should be available on demand. For example, the provision of a (or several) persistent synthetic test environment to provide an automated reference environment to which users can connect and conduct preliminary tests. As discussed in the Physical section earlier, a range of remote, Service site-based and user site-based options should be available.

The Service would need to have performance indicators to support the governance, process and role descriptions so that users can plan against a known quality and quantity of service and the responsiveness that they can expect.

Capabilities: In order to deliver the forecast capabilities, this DTEC Distributed Simulation Certification Service (DSCS) would likely comprise of the following:

- A synthetic test environment that consists of both software and hardware;
- A physical location with remote access;
- A deployable capability;
- Scenarios to validate against;
- Reference systems to validate against; and
- Suitably skilled and experienced staff to support test activities.

Establishing and accessing the service: This would need support from a central MoD organization to drive it forward and provide initial funding. Ongoing funding could be provided by the customer base on a 'per use' basis, but this may be difficult to both implement and recover fees whereas central funding is a more pragmatic approach if available. If no security concerns are raised, then access to vendors and services outside the UK MoD supply chain could provide an additional revenue stream and help contribute towards the services operation while supporting a broader initiative for consistency and coherence.

Example Engagement: An engagement between a simulation system and the DSCS might take a number of steps:

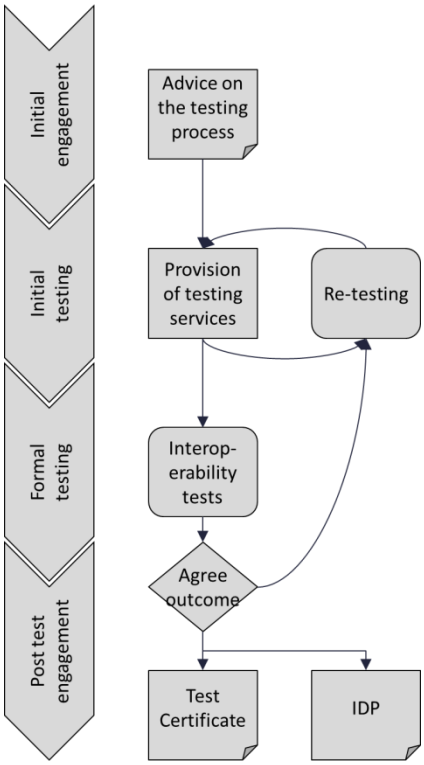

Figure 2. Example engagement

- Initial engagement with the DSCS, initiated by the simulation system manager, providing advice as required on:
  - The benefits in having the simulation certified;
  - The testing process that will be followed;
  - The types of tests available, mandatory and optional; and
  - What it means to have interoperability certified.
- Provision of deployable / remote test services, so that:
  - System developers can test their system as they are being built; and
  - Suppliers can prepare their own location.
- Formal tests and certification activities, where a supplier offers a specific version of their system for certification. These tests could include:
  - Interoperability tests;
  - Interface tests;
  - Validation and acceptance tests; and
  - Ultimately there would be tests for each standard named within the DMSP.
- Post-test engagement, where the outcome of the formal testing is agreed and certificates issued for inclusion in the systems' IDP;
- Ongoing activities:
  - Recording certified systems through their life;
  - Developing and maintaining a test suite; and
  - Evolving the test service as standards develop.

DTEC could continue to provide the mechanism that provides both the coherence and the governance required to promote this approach, but the DTEC Rules may need to be reviewed to ensure that this certification service would be used for distributed simulation federations. Day to day management and oversight of the Certification Service could be done by the Defence Simulation Centre.

EXAMPLES OF PROGRAMS THAT WOULD USE THE SERVICE

Each instance of the UK MoD programs listed below will have a need for each of its federations to be examined and certified should it wish to interoperate with any other federations in a distributed manner:

- **Land**: The Training and Education Architecture (Land) (T&EA(L)) will present a single enterprise definition that enables delivery of land forces T&E capability that is modular, scalable, interoperable and adaptable and able to deliver force elements at readiness for operations. T&EA(L) addresses the entire range of T&E media, including Computer-Based Training (CBT), simulation-based training (virtual and constructive), live training, and the various blends thereof, see Kent 2017;
- **Air**: The Defence Operational Training Capability (Air) (DOTC(A)) aims to provide the Air element of a Defence Live Virtual Constructive Training Capability. The DOTC(A) Program will establish a series of networked synthetic mission training capabilities (a system of systems) to support the development and sustainment of the UK Defense Capability across the full range of Air Power Effects (UK MoD, 2015c);

- **Maritime**: The Maritime Composite Training System (MCTS) enables the Royal Navy to train maritime warfare skills in the most cost effective manner. It consists of a holistic training system for Warfare Ops Room Officers / Ratings located at both HMS Collingwood and HMNB Devonport.

WHAT ALREADY EXISTS AND WHAT IS IN DEVELOPMENT

There are NATO projects and activities that have informed and remain applicable to this proposed approach that include the following:

- **MSG-025 "Implementation of HLA Compliance Certification within NATO and NATO/PfP Nations"**. In 2007 NATO concluded a 12 Nation study whose main aim was to specify and co-ordinate the implementation of a "NATO HLA Compliance Certification". By the end of this 4 year program 4 Nations (France, Spain, Sweden and the USA) had established a certification capability, (NATO, 2007);
- **MSG-134 "NATO Distributed Simulation Architecture & Design, Compliance Testing and Certification"**. Started in 2014 this ingoing 11 Nation study is developing an Integration Verification and Certification Tools (IVCT) to support compliance testing and certification of NATO Education and Training Network (NETN) Federation Architecture and FOM Design Document (FAFD) compliant simulation components. This program will test and demonstrate the IVCT in 2017 (NATO, 2017);
- **NATO Modelling and Simulation Centre of Excellence (M&S COE[4])**. The NATO M&S COE is the key body involved with the development of Standards and Interoperability. The COE is recognized as a key body within the MSG-134 program, involved with the certification process and the accreditation of laboratories that will undertake the certification of simulation systems.

GAPS IN CAPABILITY

To achieve the goal of successfully creating an internationally coherent national simulation interoperability certification service, a number of activities must be put in place. Not least of which is the creation of the national testing capabilities, the development of their governance structures and the routes through which they will be funded.

Alignment with and participation in MSG-134 are key to achieving the UK MoD's goals. Figure 3, reproduced from NATO 2017, shows the how an International certification organization could be set up and the various bodies within it. Aligning with this model the UK would expect to have at least one Accredited Test Laboratory and Certification Entity (CE). The challenge of International coherence would be achieved with each nation aligning itself with the central certification facility provided by the NATO M&S Centre of Excellence based in Rome.

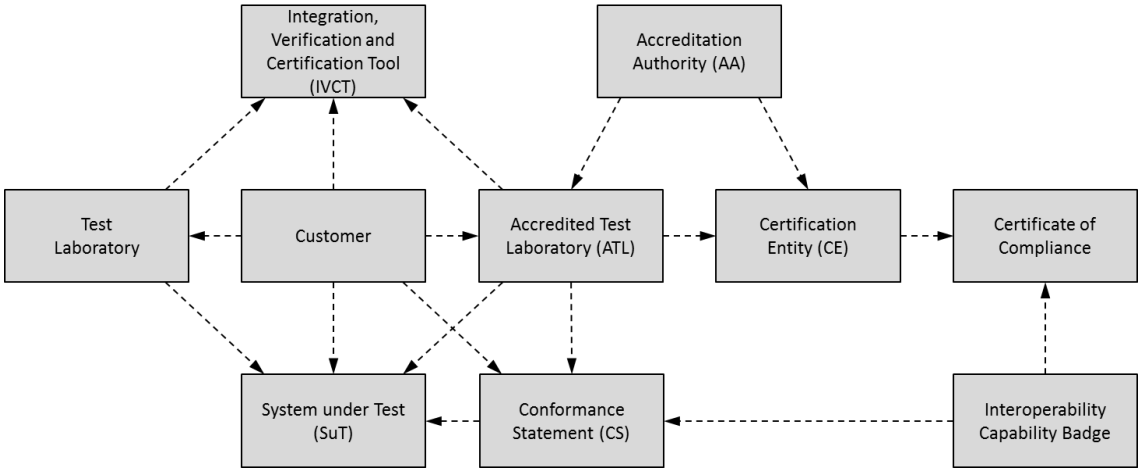

Figure 3. MSG-134 Simulation Interoperability Test and Certification Service - Organizational Relationships and Key Roles

[4] https://www.mscoe.org/

In addition to the certification of simulation interoperability, systems must also be appropriately accredited by the relevant security bodies. The configuration of the firewall and HLA data guardian systems must be suitably managed with the potential for tested and accredited configurations forming part of the IDP. In parallel to the creation of the certification service, the development of both the definition of the structure and the process for governance and implementation of the IDP must be supported to enable the collection of system configuration information.

BENEFITS

The primary benefits to the UK MoD from implementing a national simulation interoperability certification service are cost and delay avoidance. This is achieved through the reduction in the amount of testing required: testing a system for compliance rather than testing it against all of the other systems with which it is needed to interoperate, and having relevant system information readily available.

A certification service should allow a shorter turnaround for non-recurring events enabling quicker reactions as events and opportunities for participation present themselves. This in turn offers the potential for greater participation in training and experimentation activities. The certification service would ensure that a consistent approach is employed to testing, providing governance and coherence. In practical terms this means once a system, or a part of a system has been certified, it should not need to be tested again. As more systems become certified a point could be reached where a complete distributed system could be brought together without the need for extensive integration testing, focusing instead on testing specific exercise requirements.

The information collected through certification would increase understanding of individual capabilities and so increasing opportunities for re-use and informing lessons to be learned at the enterprise level. This experience and knowledge gained in applying such a service would benefit improved design of systems to improve productivity and reduce costs.

Accepting and applying the recommendations in MSG-134 would also help align the UK's distributed simulation capability with the remainder of Allies making distributed simulation-based events across international borders easier to set-up, run and be more effective (and so reduce costs).

CONCLUSIONS AND RECOMMENDATIONS

This paper has identified the need and value for a national simulation interoperability certification service. This capability would support the development and the validation of simulation systems and reduce the test burden when composing a distributed simulation activity. If implemented the capability would avoid the repeated costs of testing each system for each use, reduce integration time and de-risk the distributed activities. This avoidance of cost, reduction in time and overall de-risking, therefore providing enhanced and consistent capability, should offer and encourage increased opportunities to undertake distributed activities.

It is recommended that this concept is supported nationally and internationally to enable the benefits of distributed activities between nations to be achieved and within the UK programs are identified, such as those mentioned above, to support the development of a Distributed Simulation Certification Service. While the concept and approach outlined in this paper reflect UK MoD aspirations, the UK MoD welcomes views and requests to participate in any such future activities to support the development of the concept and to be involved with any potential future National and International interoperability certification activities.

REFERENCES

Crooks, A., Igarza, J., Staffan, L., Turrell, C. & Zimmerman P. (2004). *HLA Compliance Certification: Lessons learned from the US past activity and current developments within NATO and PfP nations.* (SISO paper ref. 04E-SIW-071). SISO.

Hughes, K. (2015). *Training Transformation DOTC(A) Cross Domain Security Project Approach.*

Igarza, J. (2007). *Implementation of HLA Compliance Certification within NATO and NATO/PfP Nations.* (NATO paper ref. RTO-TR-MSG-025). NATO.

Kent, J. (2017). *T&EA(L) WP-01-Strategy Paper*. (QinetiQ paper ref. QINETIQ/17/00693 – V.01). UK MoD.

Möller, B. (2015). Using HLA Object Models for the Analysis of Cross Domain Security Policies. 15F-SIW-038.

NATO. (2007). *Implementation of HLA Compliance Certification within NATO and NATO/PfP Nations. RTO Technical Report*. (NATO paper ref. AC/323(MSG-025)TP/29). NATO.

NATO. (2017). *NATO MSG-134 Simulation Interoperability Test and Certification Service – Concept of Operations (CONOPS)*. NATO.

UK MoD DTEC Publication (2015a). *Modelling and Simulation Standards Profile (Version 5).* Retrieved August 3, 2017, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/477180/20151113-DTEC_MS_Standards_Profile_v5.pdf. UK MoD.

UK MoD Joint Service Publication (2015b) *JSP 906 Defence Principles for Coherent Capability*. UK MoD.

UK MoD. (2015c). *DOTC(A) Core System and Services*. Retrieved August 3, 2017, from https://www.contracts.mod.uk/announcements/dotca-core-system-and-services-industry-engagement-event/. UK MoD.

ACRONYMS

AMSP	Allied Modelling and Simulation Publication
C-BML	Coalition Battle Management Language
CDT	Computer-Based Training
CDB	Common Data Base
CDS	Cross Domain Security
CIGI	Common Image Generator Interface
COE	Centre of Excellence
DDCA	Distributed Debrief Control Architecture
DE&S	UK Defence Equipment and Support
DIS	Distributed Interactive Simulation
DMAO	DSEEP Multi Architecture Overlay
DMSP	DTEC Modelling and Simulation Standards Profile
DOTC(A)	Defence Operational Training Capability (Air)
DSEEP	Distributed Simulation Engineering and Execution Process
DSC	Defence Simulation Centre
DSCS	Distributed Simulation Certification Service
DTEC	Defence Training and Education Coherence
DTED	Digital Terrain Elevation Data
DVS	Defence Virtual Simulation
EDCS	Environmental Data Coding Specification`
FEAT	Federation Engineering Agreements Template
GeoTIFF	Geographic Tagged Image File Format
FAFD	FOM Design Document
FOM	Federation Object Model
HLA	High Level Architecture
HLAe	High Level Architecture Evolved
HMNB	Her Majesties Naval Base
HMS	Her Majesties Ship
iDSC	Interim Defence Simulation Centre
IDP	Interoperability Data Pack

IEEE	Institute of Electrical and Electronics Engineers
IVCT	Integration Verification and Certification Tool
JPEG2000	Joint Photographic Experts Group
JSP	Joint Service Publication
M&S	Modelling and Simulation
MCTS	Maritime Composite Training System
MoD	UK Ministry of Defence
MS3	M&S Standards Subgroup
MSDL	Military Scenario Definition Language
MSG	Modelling and Simulation Group
NMSG	NATO Modelling and Simulation Group
NMSSP	NATO Modelling and Simulation Standards Profile
NATO	North Atlantic Treaty Organization
NATO SDI ITE	North Atlantic Treaty Organization Smart Defense Initiative Immersive Training Environment
NETN FOM	NATO Education Training Network Federation Object Model
Niteworks	A UK MOD-Industry partnership organization
OTS	Off The Shelf
PDU	Protocol Data Unit
RAF	UK Royal Air Force
REIDP	Reuse and Interoperation of Environmental Data and Processes
RPR FOM	Real-time Platform Reference Federation Object Model
RTI	Run Time Infrastructure
SEDRIS	Synthetic Environment Data Representation and Interchange Specification
SISO	Simulation Interoperability Standards Organization
SNE	Synthetic Natural Environment
SOSA	Systems of Systems Approach
SRM	Spatial Reference Model
STANAG	NATO Standardization Agreement
STANREC	NATO Recommended Standard
T&E	Training and Education
T&EA(L)	Training and Education Architecture (Land)
UCATT	Urban Combat Advanced Training Technology
UK	United Kingdom
V&V	Verification and Validation
VBS	Bohemia Interactive's Virtual Battlespace
WAN	Wide Area Network