

Joint Training Implementation of Modeling and Simulation (M&S) as a Service (MSaaS)

Lt Col Se'kou Billings
Lt Col, USAF
Development Chief, JS J7
Environment Architecture
Division
Suffolk, VA
sekou.t.billings.mil@mail.mil

Amy Grom
NAVSEA, JS J7 Environment
Architecture Division
Suffolk, VA
amy.m.grom.civ@mail.mil

Barry Siegel
SPAWAR PAC, JS J7
Environment Architecture
Division
San Diego, CA
barry.siegel@navy.mil

Efthimios (Mike) Douklias
SPAWAR PAC, JS J7
Environment Architecture
Division
Suffolk, VA
efthimios.d.douklias.civ@mail.mil

Andy Bowers
General Dynamics Information
Technology
Williamsburg, VA
francis.bowers@gdit.com

Dr. Elaine Blount
General Dynamics Information
Technology
Suffolk, VA
elaine.blount@gdit.com

ABSTRACT

The Environment Architecture Division, Joint Staff (JS) J7 Deputy Director for Joint Training (DDJT), supported by General Dynamics Information Technology under a support contract with the DoD is applying commercial and open source information technologies to the training environment for a proof-of-concept effort to evaluate cloud computing solutions for future Joint, Service, and US-supported Coalition training. Key components of this effort include:

1) JS J7 M&S Roadmap to direct the migration of the current Joint Live, Virtual, Constructive (JLVC) training federation to a Joint Training Synthetic Environment (JTSE) founded on a converged infrastructure using shared web services and on-demand computing;

2) JS J7 support for NATO Science & Technology Organization (STO) NATO Modelling & Simulation (NMSG) Task Group MSG-136 M&S as a Service (MSaaS);

3) Testing and experimentation with various services will occur during the Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX) series and in conjunction with integration tests in the JS J7 facility in Suffolk, VA.

MSG-136 support focuses on cooperative development of MSaaS standards with NATO coalition partners while concurrent experimentation and testing ensure practical and useful cloud computing strategies. Participation in the CWIX experimentation complements MSG-136 support and will enable M&S services with C2 systems which are critical components of the Joint and Coalition training environment. Integration events at JS J7 are planned monthly during FY16 and beyond to test and validate web services and associated APIs.

Finally, the JS J7 M&S Roadmap will need to follow the recent guidance by DDJT and previous strategies such as the 2011 DoD IT Strategy and Roadmap and the 2012 DoD CIO Cloud Computing Strategy in order to chart the course to the objective JTSE. This paper will introduce key components of the JTSE and MSG-136 efforts, discusses synergies achieved among JTSE and MSG-136, compare and contrast the results based on our testing and experimentation and summarize their influences on future support of US Joint Force training.

ABOUT THE AUTHORS

Lt Col Se'kou Billings is an Air Force Acquisition Officer assigned to the Joint Staff (JS) Joint Training Directorate (J7) Environment Architecture Division (EAD) as the Development Team Lead responsible for the managing the development of the Joint Training Synthetic Environment. He is a Defense Acquisition Workforce Improvement Act (DAWIA) Level III certified in Program Management. He has over 20 years of experience in managing various major acquisition programs for DoD and the USAF.

Amy Grom is an M&S Development Program Manager with Environment Architecture Division (EAD) at the US Joint Staff Joint Training Directorate. She is a US Army veteran with 15 years of service in the Signal Corps and Civil Affairs and has a bachelor degree in Computer Science from Western Connecticut State University. She has been involved with M&S and training with the Army and Joint Staff for 15 years.

Barry Siegel is a senior scientist at the Space and Naval Warfare Systems Center - Pacific in San Diego, California. He is currently enrolled as a PhD candidate in Systems Engineering at Colorado State University, and holds Masters Degrees in Economics and Computer Science. He has conducted R&D in the areas of Command and Control, software engineering and architectures, web technologies, predictive analytics using "big data", gaming, and anomaly detection algorithms. His current focus is the application of cloud-based computing to M&S in the military domain.

Efthimios (Mike) Douklias is a Principal Systems Engineer and Cybersecurity Engineer at the Space and Naval Warfare Systems Center - Pacific specializing in cybersecurity, high-performing IT, software architecture, and modeling and simulation technologies. He has a Bachelor's Degree in Computer Science from Old Dominion University and has multiple certificates in Cybersecurity, Engineering and Capability Maturity Model. He is presently applying his knowledge at Joint Staff J7 Environment Architecture Division with focus at cybersecurity in a wide-range of complex training environments and Modeling & Simulation designs and methodologies.

Elaine Blount, PhD is a Principal Scientist at General Dynamics Information Technology. She is currently serving as the development lead for Joint Training Data Services (JTDS) and data modeler for Joint Training tools at the Joint Staff (JS) Joint Training Directorate (J7) Environment Architecture Division (EAD). Elaine has a PhD from Old Dominion University in Modeling and Simulation, a Masters Degree from the College of William and Mary in Computer Science. Prior to her current work, Elaine has written software for real-time flight simulation and hospital services.

Andy Bowers is employed by General Dynamics Information Technology as a Senior Principle Systems Analyst. He is a retired United States Army officer, a graduate of the US Army Command and General Staff College and the US Air Force Air Command and Staff College, and has more than 20 years of experience in simulation and federation support of military training.. His interests include multi-resolution modeling and simulation interoperability. Mr. Bowers has a Bachelor of Science degree from the United States Military Academy and a Master of Science in Operations Research Systems Analysis and a Master of Science in Civil Engineering, both from Stanford University.

Joint Training Implementation of Modeling and Simulation (M&S) as a Service (MSaaS)

Lt Col Se'kou Billings
Lt Col, USAF
Development Chief, JS J7
Environment Architecture
Division
Suffolk, VA
sekou.t.billings.mil@mail.mil

Amy Grom
NAVSEA, JS J7 Environment
Architecture Division
Suffolk, VA
amy.m.grom.civ@mail.mil

Barry Siegel
SPAWAR PAC, JS J7
Environment Architecture
Division
San Diego, CA
barry.siegel@navy.mil

Efthimios (Mike) Douklias
SPAWAR PAC, JS J7
Environment Architecture
Division
Suffolk, VA
efthimios.d.douklias.civ@mail.mil

Andy Bowers
General Dynamics Information
Technology
Williamsburg, VA
francis.bowers@gdit.com

Dr. Elaine Blount
General Dynamics Information
Technology
Suffolk, VA
elaine.blount@gdit.com

Approaches that reduce costs and complexity for supporting exercises are needed. Joint Staff (JS) J7 is pursuing more efficient uses of Modeling and Simulation (M&S) and new technologies for Joint Training. The North Atlantic Treaty Organization (NATO) Science & Technology Organization (STO) NATO M&S Group (NMSG) MSG-136 M&S as a Service (MSaaS) is also exploring efficient M&S capabilities that stem from new technologies, cloud computing, consolidated data sharing, and web-enabled services. Both of these efforts share similar objectives, and though different in approach, there exists the potential to have mutually supportive outcomes.

JS J7 JOINT TRAINING SYNTHETIC ENVIRONMENT (JTSE)

The JTSE will replace the legacy Joint Live, Virtual, and Constructive (JLVC) Federation and support Joint force readiness to fulfill Combatant Commander (CCDR) (regional commands responsible for Joint Task Force training) and Service (Army, Navy, Air Force, Marines) Joint Training requirements. The web-enabled, enterprise-based JTSE will improve trainer access to capabilities; enhance ease of use through simplified user interfaces; and support discoverability and more rapid content delivery. It will provide scalable, modular simulation services supported by a cloud-based computing architecture providing on-demand, operationally relevant training for globally integrated operations. The JTSE will leverage existing collaborative environments and provide planning services that can be used to foster increased interaction among the Combatant Commands (CCMD), Services, and Agencies (C/S/A), and their mission partners. JTSE will provide planning and execution services that reduce manual processes and the tedious, repetitive tasks inherent to data processing, and database configuration and coordination. Commanders can use JTSE services to meet CCMD, Joint Task Force (JTF), Service, and Agency (C/J/S/A) high-interest training requirements to achieve Joint force readiness.

Commanders at all echelons are the primary trainers responsible for preparing their units to accomplish assigned missions. To assist Commanders in preparing for current and future conflicts, training, and exercises, mission rehearsal solutions must represent and adapt to rapidly changing operational environments. JTSE services will provide trainers the ability to represent operational environments, while reducing the amount of time and labor necessary to design, plan, execute, and access Joint Training across the full range of military operations. JTSE services will enable Joint forces to accomplish a diverse and complex set of missions that demand an ever-changing combination of military deterrence, security cooperation, and engagement.

JTSE's authority stems directly from the Chairman of the Joint Chiefs of Staff (CJCS) Joint Training Guidance that dictates, "The joint community must sustain training with joint, interagency, intergovernmental, and multinational partners."¹ This same collaborative focus is found in the Combatant Commanders Exercise Engagement and Training Transformation (CE2T2) Program Goals and Objectives (PGO), which targets "a realistic training environment for

CCDRs to maintain trained and ready forces, exercise their Theater Campaign Plans (TCP), and achieve joint and multinational training.”ⁱⁱ

The JTSE Operational Viewpoint (OV) (Figure 1) illustrates how trainers employ the JTSE to represent training domains that meet the needs of C/J/S/A training audiences. Capability Requirements (CRs) define desired JTSE services that must interoperate with C/J/S/A Live, Virtual, and Constructive (LVC) capabilities to conduct training. JTSE uses a Joint Information Environment (JIE)-compliant training network to deliver capabilities. JIE is the evolving [Department of Defense](#) (DoD) single, joint, secure, reliable and agile command, control, communications and computing enterprise information environment.

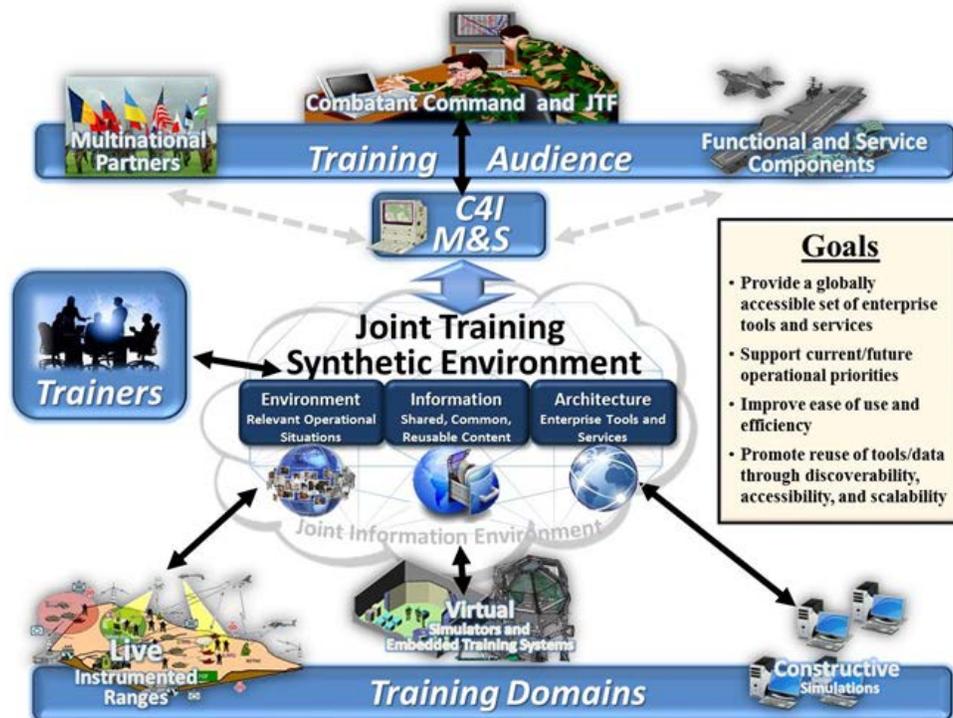


Figure 1. JTSE Operational Viewpoint (OV)

JS J7 MODELING AND SIMULATION (M&S) ROADMAP

The Deputy Director Joint Training (DDJT) approved the M&S Roadmap, which logically groups and sequences JTSE development activities. JTSE development focuses on constructive capabilities enabling Joint Training, exercises, and mission rehearsal while maintaining interoperability with instrumented live and virtual (i.e., simulators) and Command, Control, Communications, Computers, and Intelligence (C4I) systems. The M&S Roadmap supports senior leader decision-making, provides strategies to deliver required training enablers, applies disciplined program management to product delivery, and informs the Joint Training Enterprise (JTE) for better alignment with Service, Agency, and Coalition development.

The M&S Roadmap/JTSE development activities are grouped within eight Lines of Effort (LOEs):

1. **Event Management** – capabilities to specifically enhance or automate the management and synchronization of an event
2. **Scenario Development & Synthetic Environment** – capabilities to develop integrated scenario products
3. **Role-Player & User Presentation** – tools to allow military audience to directly use simulation throughout the Joint Event Life Cycle (JELC) for planning, training, and learning on demand via the web. The JELC is an event planning process with five stages: design, planning, preparation, execution, and after action evaluation / reports

4. **Data Model, Data Services, and Data Repository** – simulation and data manipulation to ingest/modify/correlate data for simulation use
5. **Simulation Services** – modular services to represent the Joint environment
6. **Training & Knowledge Management (KM)** – KM services required for Joint Training
7. **Cloud & Technical Infrastructure** – efforts to prepare simulations for use in virtual cloud environment
8. **Joint, Service, Coalition, and Agency M&S Integration** – Service simulations and architectures (legacy systems)

The DDJT's mission is inclusive of non-materiel as well as materiel Joint Training CRs. For instance, aspects of scenario development that add context and realism (e.g., production of the Road to War, development of intelligence products not produced by simulation, and production of media segments) may be difficult for technical solutions to replicate. However, it is possible to simplify manual processes to enable the trainer to focus on these human-dependent tasks in designing and executing training to meet objectives.

ENVIRONMENT ARCHITECTURE DIVISION (EAD) DEVELOPMENT ACTIVITIES

EAD designs, develops, and deploys Joint Training technical enablers comprised of Joint Training Tools that support planning, provisioning, and execution of Joint Training activities. These capabilities enable CCMD and Service training programs to support and align to military priorities by developing and fielding innovative, low-cost, small-footprint, net-centric Enterprise Joint Training capabilities to replace unsustainable (costly integration and manual labor activities) legacy capabilities. Joint Training Tools will represent the pace and complexity of today's simulated battlefield with coalition partners. These tools support the United States (US) defense strategy and enhance joint warfighting readiness by improving the relevance and realism of training through realistic threat environments, logistic constraints, and degraded information. Additional capabilities are improved access to the user point of need; interoperability with coalition partners; reusable data services; distributed exercise design, and maturation of modular services supporting scalable and adaptable M&S training capabilities.

JS J7 SUPPORT FOR MSG-136

JS J7 EAD's decision to join the NATO MSG-136 MSaaS project in October 2015 was driven by two factors. First, the US government established a "Cloud First" policy which requires agencies to use cloud-based solutions when a secure, cost-effective option exists. The second factor was based on the NMSG Specialist Team (ST-131) "M&S as a Service: New concepts and Service Oriented Architectures" involvement and final report, which collected national perspectives and experiences regarding MSaaSⁱⁱⁱ. As JS J7 validated its requirements for cloud solutions, it deemed cloud coalition interoperability vital to the continued success of military interoperability with strategic partnerships. Thus, JS J7 queried its strategic partners and discovered how many other nations were pursuing the same concepts as those alluded to by LOE 5, Simulation Services, and decided this could be the venue to develop future interoperability solutions and standards with our coalition partners.

EAD formulated the following objectives for its participation in MSG-136:

- Influence, adopt, and adapt partner-developed services that support JS J7 goals in the Joint Force Development mission.
- Ensure US interests are considered to enable JTSE interoperability with coalition architectures, services, and systems.
- Leverage M&S expertise and systems being developed under the MSG-136 charter.
- Influence M&S interoperability standards proposed for delivery by the group.

MSaaS REFERENCE ARCHITECTURE

The majority of EAD support to NATO MSG-136 is comprised of support to the MSG-136 Technical (TEK) subgroup. The TEK subgroup is responsible for authoring the MSaaS Reference Architecture (RA) and testing services to inform and support RA guidelines. The RA consists of four volumes, all authored in accordance with the NATO Architecture Framework:^{iv}

- Volume 1: Reference Architecture
- Volume 2: Reference Service Descriptions
- Volume 3: Reference Engineering Process
- Volume 4: Experimentation

Volume 1 Reference Architecture, the MSaaS RA provides a template for the development of one or more concrete Solution Architectures, and is based on the Open Group Service Oriented Architecture (SOA) RA^v and the NATO C3 Taxonomy. The C3 Taxonomy approach within NATO describes general capability concepts. Following the SOA RA, the MSaaS RA is described in nine layers as shown in Table 1.

Table 1. SOA Reference Architecture Layer Descriptions

SOA RA Layers	Description
Operational Systems	This layer describes the runtime and deployment infrastructure.
Service Component	This layer contains software components, each of which provides the implementation or realization for services and their operations, hence the name Service Component. The layer also contains the Functional and Technical Components that facilitate a Service Component to realize one or more services.
Services	This layer consists of all the services defined within the SOA.
Business Process	This layer covers process representation and composition, and provides building blocks for aggregating loosely-coupled services as a sequencing process aligned with business goals.
Consumer	This layer is the point where consumers interact with the SOA.
Integration	This layer provides the capability to mediate, which includes transformation, routing, and protocol conversion to transport service requests from the service requester to the correct service provider
Quality of Service (QoS)	This layer provides solution QoS management of various aspects, such as availability, reliability, security, and safety as well as mechanisms to support, track, monitor, and manage solution QoS control.
Information	This layer is responsible for manifesting a unified representation of the information aspect of an organization.
Governance	This layer ensures that the services and SOA solutions within an organization are adhering to the policies, guidelines, and standards that are defined as a function of the objectives, strategies, and regulations applied in the organization and that the SOA solutions are providing the desired business value.

The MSaaS RA makes the further distinction between stateless services and stateful services.

- Stateless services are memoryless; each invocation of the service is independent of the next invocation. Stateless services are relatively easy to scale and load balance. Most importantly, stateless services are not time synchronized and therefore need not be synchronized in time.
- Conversely, stateful services have memory. Each invocation of stateful services is dependent on the result of the previous invocation.

Based on the MSaaS RA, MSG-136 decided to pursue experimentation to better define the goals of MSaaS and to experiment with both stateless and stateful services. MSG-136 experimentation is described below.

Volume 2 Reference Service Descriptions provides an overview of methods and tools to describe services and their interfaces for MSaaS. TEK made rapid progress initially with a service description template based on a standardized SOA model for describing information technology and related business functions,^{vi} but has since slowed while evaluating the metadata necessary to support discovery by users or tools (so that one or more simulation services might be rapidly and accurately assessed and, when required, composed to meet the diverse simulation needs of NATO nations). A TEK “tiger team” was established to evaluate the applicability of several existing metadata specifications for capturing these needs, including:

- Department of Defense (DoD) Discovery Metadata Specification (DDMS) 5.0

- NATO Metadata Registry and Repository (NMRR)
- NATO Core Metadata Specification (NCMS)
- Modeling and Simulation Community of Interest Discover Metadata Specification (MSC-DMS)
- Federation Engineering Agreements Template (FEAT)
- Universal Description, Discovery, and Integration (UDDI)

The tiger team's conclusions thus far suggest that the existing schemas are insufficient to meet the MSaaS requirements. The team intends on proposing a modified schema to the wider M&S interoperability community for review and comment beginning with the Fall 2016 Simulation Innovation Workshop (SIW).

Volume 3 Reference Engineering Process leverages M&S community standards, including the Distributed Simulation Engineering and Execution Process (DSEEP)^{vii} and the FEAT^{viii}, and documents additions or extensions necessary in either standard to support MSaaS. The MSG-136 leadership intends to submit this documentation to the Simulation Interoperability Standards Organization (SISO)^{ix} and work with SISO to revise the standards.

In *Volume 4 Experimentation*, MSG-136 TEK experimentation has proceeded along two paths, one using a collection of private clouds and a common cloud to conduct experiments to test different aspects of the RA on a routine basis; the other to use established venues, most notably the Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX), to integrate MSaaS with other systems and services to gain perspective on use of MSaaS in other contexts.

MSaaS TESTING AND EXPERIMENTATION WITH COALITION PARTNERS

MSG-136 participants constructed a low-cost, vendor neutral experimentation virtual environment to explore multiple solution architectures that are conformant to the MSG-136 RA. This experimentation environment utilizes commercial cloud vendors, support for Infrastructure as a Service (IaaS) model with the ability to provision self-service, on-demand cloud resources. Each nation that participates in the experimentation environment must provide their own cloud resources. Various commercial web services, engines, and cloud capabilities have been federated by the MSG-136 experiment participants into a large experimental environment. In addition, on-premises private cloud infrastructure can be connected to the larger MSG-136 virtual experimental environment.

Routine testing has thus far used two solution architectures: a containerized High-Level Architecture (HLA)-based simulation environment and a containerized centralized storage simulation environment.

A critical component of MSG-136 experimentation is the use of Linux containers popularized by the open source "Docker" project. Containers are analogous to lightweight virtual machines, and include a self-contained file system, network stack, and process (execution) system. All services within the MSG-136 experimental environment are deployed as containers.

The MSG-136 experimentation architecture is depicted in Figure 2. The architecture consists of multiple distributed hosts; each host houses one or more containers and within each container is an MSaaS service. Containers are pulled from a centralized container registry within the cloud. As indicated in the figure, MSG-136 participants intend on experimenting with two container hosts, one of which will utilize containerized HLA services. The intent is twofold:

- To demonstrate reuse of existing HLA-enabled simulation capabilities, and,
- To explore differences in stateless and stateful services with a time-managed HLA federation providing federates for the stateful services implementation.

Command and Control (C2) systems and stateless non-HLA services are also located in the cloud. Hosts are globally connected in an HLA environment using the Run-time Infrastructure (RTI). Hosts can also be located within on-premises data centers and connected through the internet; no special network hardware or point-to-point Virtual Private Networks (VPNs) are required.

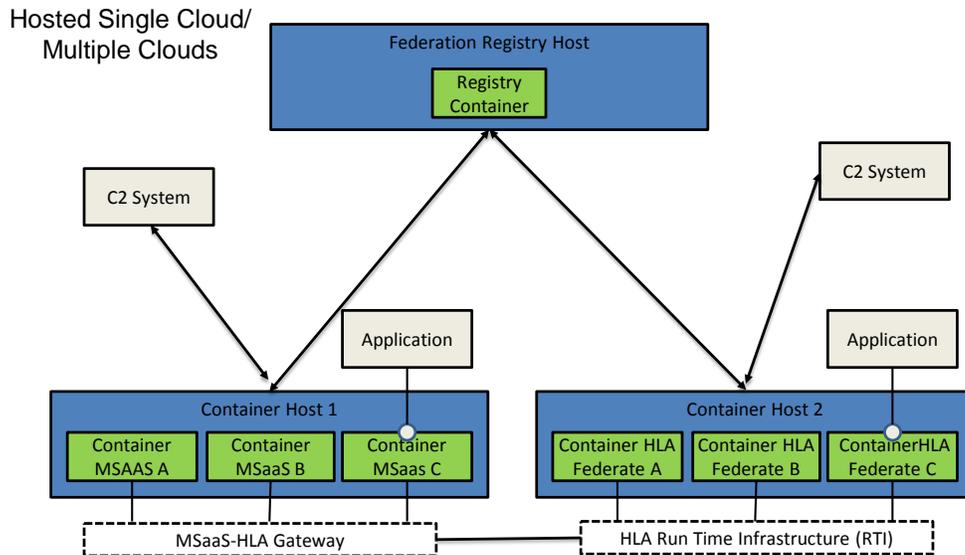


Figure 2. MSaaS Experimentation Architecture

For experimentation purposes, MSG-136 defined an example use case based on mission rehearsal of a maritime interdiction operation. Within this use case, a task group was deployed in the Gulf Region and surface track managers rehearsed coordination. The created simulation environment was deployed as containers and was distributed in the MSG-136 cloud. Services were pulled on-demand from a private service component registry/repository. Within the HLA federation, HLA federates included an Automated Information System (AIS) commercial vessel traffic simulator representing a constructive simulation that generated traffic based on previously recorded live traffic, a military surface ship simulator representing a virtual simulator, various HLA components including an RTI, and a commercial web-based mapping application to provide visualization of the scenario.

Two different solution architectures were mapped to the MSG-136 RA and the maritime interdiction use case.

- The first solution architecture is based on the use of hybrid HLA architecture.
- The second solution architecture is based on the Discrete Event System Specification (DEVS).

Each of these solution architectures are discussed below.

MSG-136 Solution Architecture #1: MSaaS Services in Hybrid HLA Architecture

Under the MSaaS services in hybrid HLA architecture, some services are provided through stateless RESTful (Representational State Transfer) Application Programming Interfaces (APIs), while other services are provided through stateful HLA federates. Figure 3 depicts Solution Architecture #1.

Note that this solution architecture was developed and implemented without a provisional infrastructure; only commercial cloud resources were used. Multiple open source products were used to support run-time discovery and orchestration of the scenario. Although there were multiple hosts involved with the scenario, multicast protocols were not used. Since multi-cast is prohibited in commercial cloud environments, services reverted to using point-to-point Transmission Control Protocol (TCP)/Internet Protocol (IP).

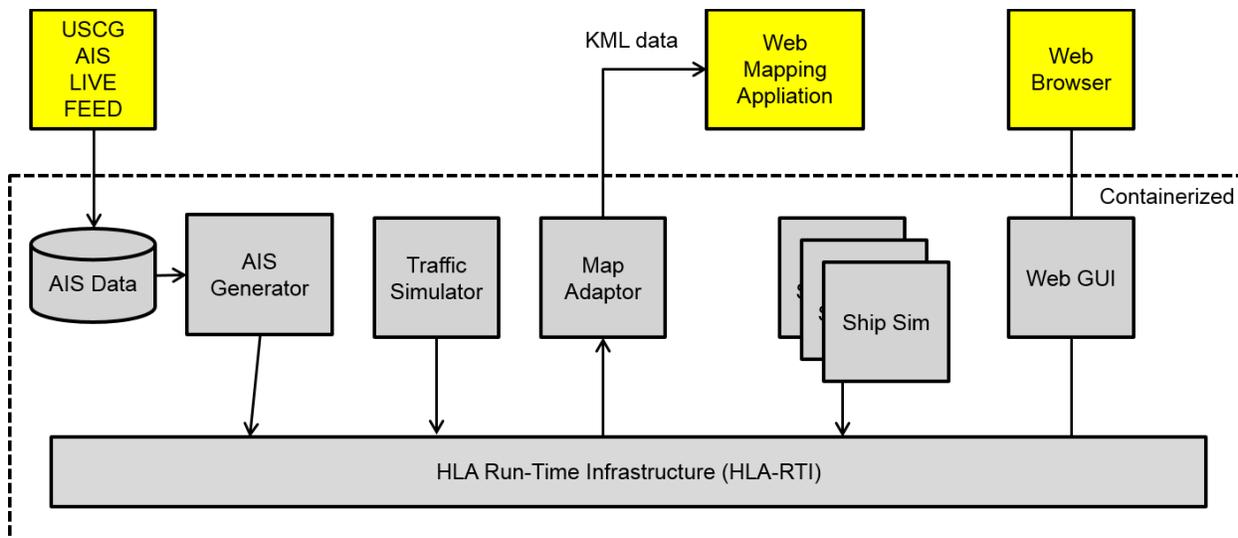


Figure 3. Services as Federates within HLA Federation

MSG-136 Solution Architecture #2: MSaaS Services Using DEVS

Figure 4 depicts the second solution architecture that is conformant to the MSaaS RA. In this architecture, HLA is not used but replaced by an implementation of the DEVS and the Redis open source, in-memory data structure store, database, cache, and message broker. All of the components of the maritime interdiction use case remained the same; however, the interfaces were changed to support DEVS and Redis APIs. The simulation executed identically to the HLA-based Solution Architecture #1 discussed above. This example illustrates that multiple technology stacks can support a given use case and be fully compliant with the MSaaS RA.

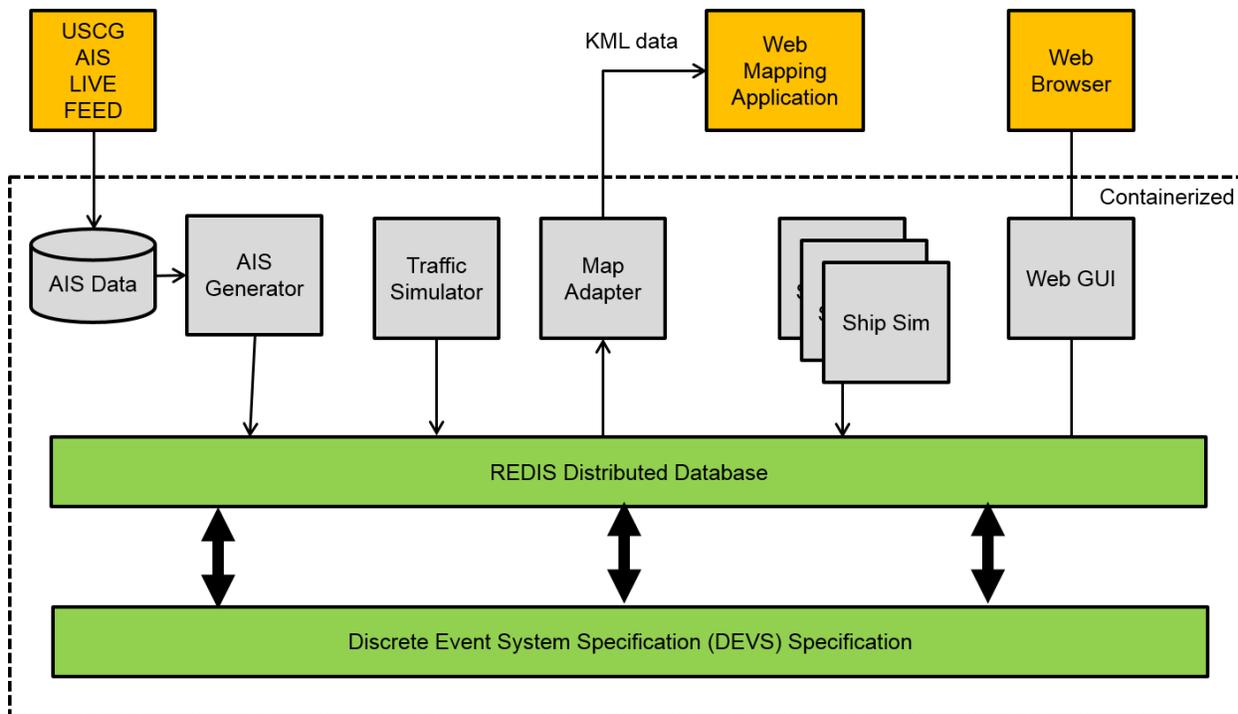


Figure 4. Pure Services Approach with DEVS and Data Structure Server

CWIX EXPERIMENTATION

CWIX participation, while not officially “sponsored” by MSG-136, includes MSaaS experimentation by several nations, including Canada, Italy, and the US, which are also MSG-136 participants. This paper confines itself to reporting on US lessons learned to date.

The US is sponsoring two M&S services to participate in CWIX 2016:

- The Air Tasking Order (ATO) Translator (ATO-T) Service is a simulation-enabling service designed to reduce simulation operator workload by automating the translation of an ATO and associated Air Control Order (ACO) from a C2 System to the simulation commands necessary to execute the ATO/ACO in the simulation.^x
- The ATO Generator (ATO-G) Service enables generation of a complete day-long ATO for Opposing Forces (OPFOR), Situational Forces (SITFOR) and, in the event an air staff is not available, Blue Forces (BLUFOR). The resulting ATO is then available for simulation or execution by Integrated Command and Control (ICC) or similar C2 system.^{xi}

Both services use Message Text Format (MTF) adhering to ADatP-3 B11 Standard.^{xii} Thus far, the primary “lesson learned” with respect to the two services is that while the standards for expressing the ATO and ACO in MTF are sufficient to support operational requirements, M&S community standards are inadequate to express the ATO and ACO in “a digitized form ... in support of the unambiguous exchange across C2, simulation and robotic systems”.^{xiii} This shortfall, and corresponding requirement, was recognized by NATO MSG-048 with a clear requirement, “Air Operations – [Coalition – Battle Management Language] C-BML should support air operations and therefore allow for constructing Air Tasking Orders (ATO) and Airspace Coordination Orders (ACO)” in the MSG-048 technical report dating from 2012.^{xiv}

MSG-085^{xv} and SISO Product Development Group (PDG) C2Sim have continued to progress C-BML and Military Scenario Definition Language (MSDL)^{xvi} as they relate to air operations, but some shortfalls remain. For example, while MSG-085 reached consensus for expressing air missions such as Close Air Support (CAS) or Defensive Counter Air (DCA), more complex missions involving coordinating different mission types, DCA with refueling for example, or missions involving sequential tasks, still need additional work.^{xvii}

Being involved in CWIX, has uncovered a number of programs or activities pursuing service-related objectives similar to those of both MSG-136 and JTSE. Chief among them is the NATO Federated Mission Networking (FMN), which already has service instructions for a variety of services including authentication, digital certificates, directory data synchronization, web hosting, and others, and procedural instructions for information management, service management, change management, and so on. Also, potential leveraging may exist for both JTSE and MSaaS efforts from a number of other CWIX 2016 SOA Focus Area experiments that include:

- Public Key Infrastructure (PKI)
- Service Monitoring and Control (Service Discovery, Service Monitoring)
- Information Sharing
 - Messaging (Publish-Subscribe, Request-Response)
 - Information Models (National Information Exchange Model (NIEM))
 - Information Discovery using Semantic Web Technologies
 - Information Access and Aggregation Services
 - eXtensible Markup Language (XML) Labeling (transport and data level)
- Federated Identity and Access Management (IdAM)
 - Federated Web Authentication
 - Web Service Security for Simple Object Access Protocol (SOAP) based messages
 - Web API Security
- Others (portlets: Web Services for Remote Portlets (WSRP) specification, service orchestration: Business Process Execution Language (BPEL), etc.)

The point in reporting these interactions with other programs and activities is that they, and many others, involve specification development, coordination, and agreement among Coalition partners. If JS J7 intends to support

interoperability with these partners, validating the instructions and specifications is necessary, as is participation in these venues in order to influence subsequent specification spirals.

JTSE TESTING AND EXPERIMENTATION WITH SERVICES

The M&S Roadmap services are implemented as the JTSE project along eight interdependent LOEs and are referred to as Joint Training Tools. These services follow general best practices for web services and meet Cyber Security criteria established within DoD.

All web service calls utilize REST. REST is stateless that enables service calls to be retried independently and aids in scalability. JavaScript Object Notation (JSON) is used as the primary transfer data format. While based upon a subset of JavaScript, JSON is an open standard format that uses human readable text to transmit data objects consisting of attribute-value pairs.^{xviii} JSON is language independent and supported by all of the technology stacks used by the developers. A style guide was created to aide developers in standardizing their design practices. The guide includes standards regarding browser support, client side software, server side technology and architecture, and API standards. Elements considered when designing APIs included versioning, Uniform Resource Identifier (URI) structure, pagination of request responses, data versioning, object identifier fields, and error codes. As a standard practice, each of the services provides an API reference describing available calls, input, response, and other service specific information to aid other developers. Services are developed according to priorities established by the M&S Roadmap. The data model and names used within the services are standardized so that variables used across the APIs have the same semantic meaning for the same name. If different data names are used, then the semantic components of the data are also different.

LOE #8 of the JS J7 M&S Roadmap is to guide the migration of the current JLVC training federation to a JTSE founded on a converged infrastructure using shared web services and on-demand computing. JTSE has already started the overall architectural design and experimenting with cloud solutions starting from virtual machine hypervisors to bare metal containers. It is a phased approach and multiple services are being tested in the hypervisor MSaaS environment. The created environment is a cybersecurity approved DoD n-tier environment that takes into account the Cyber Security controls required by Defense Information Systems Agency (DISA). We have analyzed some monolithic M&S systems to investigate their capabilities so there is isolation of specific functionalities that can be transported into services. All communication utilizes Transport Layer Security (TLS) and is Federal Information Processing Standard (FIPS) 140-2 encryption compliant.

A technology stack has been developed to aid the EAD Cloud Team in determining technologies to be supported within the infrastructure to include servlet containers, server proxy software, operating system versions, supported programming languages, supported databases, etc. Each of nine services of the JTSE tested to date are installed and maintained according to standard best practices and DoD Cyber Security requirements with respect to ensuring confidentiality, integrity, and availability of the systems being developed. The main consumer interface software is a campaign planning manager, which makes calls to each of the other services to obtain results requested by the user. The design of the systems called by campaign planning manager incorporates the following principles:

1. Services are each designed for a single purpose with no interdependencies - essential for parallel computing.
2. Services are designed to be stateless. Information needed to determine calculation is all sent to the service and results returned. Data stored within the service is used for the calculations on the input data, but does not change based upon the results. Information that changes is stored at the calling software. Stateful information is stored at one location to enable easier management of the world state. Statelessness facilitates easier scaling and load balancing of the services. Contention of a service is not an issue, as a new copy of a service can easily be added enhancing availability of the service. Stateful objects are difficult to regenerate, require backups to enable restoration, and are difficult to load balance as they change with each call leading to concurrency issues.
3. Consistent results are required for a service. Regardless of the number of times a service is called, the order of service calls, or the timing of the service calls, the results are the same for the same input.
4. Services do not rely upon hardcoded or set locations of other services. A service will be written to enable location of services that are dynamic and may have changing addresses to aid in scaling of the services

provided. Locations of services within the infrastructure are written without dependencies upon particular hostnames or IP addresses.

In the service architecture, we introduced IdAM for both person and system for accessing services in the environment through authentication, authorization user management, and central user repository. IdAM is the combination of technical systems, policies, and processes that create, define, govern, and synchronize the ownership, utilization, and safeguarding of identity information. Using IdAM, we achieved Single Sign On (SSO), which allows a user to enter their login credentials a single time to access multiple system and services without re-authenticating.

Our next step is to setup an internal cloud environment that will introduce container technology. Containerization is based on shared operating systems. Containers wrap up all software components and the complete filesystem to run. Since the software is inside the container, it guarantees that it will always run the same, regardless of the environment. Containers are much thinner and more efficient than hypervisors since it wraps up only the software entities it needs to run. Containers are on top of a single Linux instance and multiple containers can run simultaneously. This technology can relax the need of configuring different servers for different software requirements. One container server fits all.

JTSE AND MSaaS COMPARISONS

Table 2 compares the JS J7 JTSE initial implementation with the MSG-136 MSaaS experimental approaches using the nine layers of the SOA RA.

Table 2. Comparison of JTSE and MSaaS Approaches

SOA RA Layers	Layer Short Description	JTSE	MSaaS
Operational Systems	Runtime or deployment technologies	Virtual machines.	Containers and virtual machines.
Service Component	Design of services	Servlet containers organized by data calculated.	Small Services following micro-service design pattern.
Services	Services implemented in the solution	RESTful APIs return information needed by user for campaign planning. Services used and known, no current registry.	Exemplar service prototypes supporting a maritime interdiction use case.
Business Process	Support for mission processes and workflows	Campaign planning manager performs actions and calls systems for computations based upon user requests. Message API informs subscribed systems of updates. Some process calls have criteria for early exit; example decision points reached during battle adjudication.	Automated runtime orchestration of services only.
Consumer	User interactions	Browser-based, much user interaction: planning, terrain maps and layers, and user plan development based upon resources. Services used to compute information needed by user.	Browser-based, minimalist user interfaces.
Integration	Service interoperability; mediation of disparate services; messaging, etc.	Services implement data store from tech stack according to problem space. RESTful APIs for all but messaging API, which is used for update notifications. No proprietary formats.	HLA standard interfaces and DEVS-based with persistent No Structured Query Language (SQL) data store.

SOA RA Layers	Layer Short Description	JTSE	MSaaS
Quality of Service	QoS management of various SOA aspects (e.g., availability, reliability, scalability, and security)	IdAM via SSO. Network security. Configuration Management processes. Stateless services will facilitate future load balancing.	Security not implemented in MSaaS. Scalability through containers and micro-services.
Information	Uniform and consistent representation of the SOA data	Joint Training Tools data model, Joint planning information, relational, graph, and terrain databases utilized.	MSaaS HLA use of the Real-time Platform-level Reference (RPR) Federation Object Model (FOM). MSaaS DEVS use of NoSQL database
Governance	Adherence to guidelines, policies, and standards	Open Geospatial Consortium (OGC) standards, Joint Training Tools Style Guide, JLVC General API Guide, JS Configuration Control Board (CCB), and Cyber Security Risk Management Framework (RMF).	Researching NATO and national policies, guidelines and standards

The MSaaS approach has touched most of the SOA RA layers, with focus on the run-time automated provisioning, discovery and the orchestration of small services using containers.

JTSE uses RESTful APIs to solve Campaign Planning and does not use automated provisioning or discovery. The campaign planning manager calls the services to obtain the answers requested by the user.

Areas where future MSaaS work is required include support for pre-runtime processes automated workflow, security, and automated enforcement of organizational (i.e., NATO) policies and standards.

Areas currently in work or planned for future work for JTSE include automated discovery, automated workflow, visualization, decision, and plan data evaluation processes.

ACHIEVEMENTS

There are already a number of achievements for the previously described EAD objectives for its participation in the MSG-136 MSaaS project. These achievements are listed below for each of those objectives:

- Influence, adopt, and adapt partner developed services that support JS J7 goals in the Joint Force Development mission:
 - EAD participants are extremely influential in MSG-136 subgroups and are key contributors to the development of MSG-136 deliverables.
 - EAD participants are influential and have gained insight on service deployment, invocation, and binding.
 - EAD participants have gained insight on “partner developed services” and SOA and cloud technologies by participating in CWIX and NATO’s Technology for Information, Decision, and Execution (TIDE) Sprint.
- Ensure US interests are considered to enable JTSE interoperability with coalition architectures, services, and systems:
 - EAD participants are concerned that JTSE efforts to satisfy DISA Cyber Security control requirements will make interoperability with coalition architectures, services, and systems problematic.
- Leverage M&S expertise and systems being developed under the MSG-136 charter:
 - EAD participants have reported MSG-136, CWIX, and TIDE Sprint results to the JTSE architecture team with expressed intent of leveraging lessons learned.
- Influence M&S interoperability standards proposed for delivery by the group:

- EAD participants are key contributors to the development of MSG-136 deliverables and some of these will be the basis of standards product development.

LEVERAGING OPPORTUNITIES

- JS J7 seeks more efficient use of M&S for Joint Training. Approaches that might reduce costs and complexity for supporting exercises are needed. The MSaaS approach appears to offer efficiencies that stem from new technologies, cloud computing, consolidated data sharing, and web-enabled services. These have potential to support approaches being explored for the JS J7 JTSE M&S Roadmap.
- NATO's multi-national evolution of cloud solutions, RAs, and M&S standards can significantly contribute to coalition interoperability – a desired objective for the JTSE solution.
- MSG-136 MSaaS explorations of cloud solutions and their actual experimentations could well inform the work being done for the JTSE innovations and perhaps save time and money in advancing similar efforts.

CHALLENGES

- The JTSE is driven by evolving military leadership and is impacted by constant budget changes new operational requirements, and an ever changing complex world. JTSE has to demonstrate a series of easily obtainable and timely releases of software to satisfy Joint Training events that are included in the Combatant Commanders Exercise Engagement program. This is becoming more of a challenge based on the ever increasing Cyber Security and RMF requirements. IdAM solutions cannot simply rely on Common Access Cards (CACs) that are issued to US military personnel, civilians, and contractors because they can be very difficult for coalition partners to obtain. Can future cloud-based simulation solutions meet security requirements and still be effective?
- MSG-136 also is challenged to work through the complicated issues of multinational policy and sharing of services to be developed. Foreign Military Sales (FMS) that utilizes the Export Compliance process has been the solution to allow our coalition partners access to our simulation software, also known as defense articles. Deployment of simulation software has followed traditional methods of delivery: generally shipping a CD to a designated address using standard mail. With CDs becoming obsolete, what will be the mechanism of delivery for stateless services? Cloud-based services and downloading from the internet or work-related networks has become standard practice for software developers attempting to reach consumers on-demand in their homes, offices, and on mobile devices. DoD, NATO, and nations will have to establish a policy together on many levels regarding this practice.

CONCLUSION

JTSE and MSG-136 are addressing the RA from different approaches, but with many similarities. MSG-136 is dealing mostly from the point of view of architecture, discovery, provisioning, and orchestration to include the management and the run-time environment of services (top to bottom approach). JTSE is focusing on the operational functional model simulations, user interaction, and API between services (bottom to top approach). Combining the two efforts offers the potential to meet in the middle and cover all nine layers of the SOA RA. There are many layers involved in potentially new architectures and further testing and exploration is needed of capabilities for development of simulation solutions in a cloud environment. Use of the MSaaS approach offers promising opportunities, yet poses further potential challenges for both JS J7 and NATO that need to be considered.

Both approaches are exploring various aspects and lessons can be learned from both efforts.

REFERENCES

ⁱ CJCSN 3500.01– 2014-2017 Chairman's Joint Training Guidance.

- ii CE2T2 Program Goals & Objectives.
- iii Siegfried, R., & Diehl, A., & Diallo, S., & Bertschik, M., & Herrmann, G., & Rother, M. "Outline of a Service-Based Reference Architecture for Effective and Efficient Use of Modelling and Simulation", NMSG Annual Multi-Workshop 2014, Washington, D.C., USA.
- iv NATO Architecture Framework version 3, NATO.
- v SOA Reference Architecture Technical Standard : Overview of the SOA RA Layers, https://www.opengroup.org/soa/source-book/soa_refarch/layers.htm
- vi Metso Minerals IT Service Architecture (MISA) Generalized Service Template.
- vii IEEE Standard 1730-2010, IEEE Recommended Practice for Distributed Simulation Engineering and Execution Process.
- viii SISO-STD-012-2013 Standard for Federation Engineering Agreements Template (FEAT) Approved 2 Aug 2013.
- ix <https://www.sisostds.org/>
- x https://tide.act.nato.int/cwix/index.php/USA-ATOT_MSG136@CWIX_2016
- xi https://tide.act.nato.int/cwix/index.php/USA-ATOG_MSG136@CWIX_2016
- xii NATO Standardization Agreement (STANAG) 5500 Concept of NATO Message Text Formatting System (CONFORMETS) -ADATP-3.
- xiii RTO Technical Report TR-MSG-048 Coalition Battle Management Language (C-BML) Final Report, Feb 2012.
- xiv Ibid.
- xv RTO Technical Report TR-MSG-085 Standardisation for C2-Simulation Interoperation, Final Report, Nov 2015.
- xvi SISO-STD-007-2008 Standard for Military Scenario Definition Language (MSDL).
- xvii Telecom (23 March 2016) and email exchange (23, 24, 31 March 2016), subject UC ATO/ACO in CBML, Andy Bowers, Adam Brook, Amy Grom.
- xviii <http://ahex.co/json/> Introduction to JSON.