WHITEPAPER

Modernizing Modeling, Simulation and Training (MS&T) Systems

USING DDS TO DELIVER SECURE, MULTI-VENDOR INTEROPERABILITY

OVERVIEW

The modern field training paradigm requires rapidly-deployable, secure simulated environments. Modeling, Simulation, and Training (MS&T) systems need to be assembled and reconfigured in an agile, ad-hoc manner from ready-made, commercial off-the-shelf (COTS) components with response times closely matched to real-world scenarios. High-fidelity simulation data must be sourced across a wide range of public, private and multinational operations sources. This is driving a core requirement to secure that data in order to prevent unauthorized access to both intellectual property and information sources across local and remote operations arenas and up to the cloud-based networks. On top of these challenges, there is a growing pressure for accelerated deployment of new MS&T scenarios to keep warfighters prepared for combat.

Consistent, repetitive exposure to simulated environments is the proven way to train warfighters in order for their reaction time and skills to become muscle memory, reflexive and honed. Effective training requires a system that provides true, high-fidelity simulations with response times closely matched to real-world scenarios. The most realistic training comes from using the same technology that is used in systems deployed in the real world. Yet there are challenges in creating a simulated, real-world scenario with several distributed components, each with its own set of disparate, proprietary technologies.

Simulation standards are one step in solving this challenge, yet the standards alone cannot solve the urgent need for multi-standard, multi-platform integration in decreasing time frames.

This paper describes how a standards-based communications framework can provide the necessary framework for modern warfare training. It uses a multi-level secure (MLS) data architecture to address the challenges of integrating a wide range of MS&T systems, resulting in accelerated creation and delivery of impactful training simulations.

STANDARDS-BASED MS&T PLATFORM INTEROPERABILITY

Today's MS&T environments are built upon traditional and emerging standards. The two leading standards are Distributed Interactive Simulation (DIS)[1] and High-Level Architecture (HLA)[2]. DIS is an IEEE standard for conducting real-time platform-level wargaming across multiple host computers. HLA is an IEEE standard for distributed simulation that was originally driven by the US Department of Defense and is now used globally to build a simulation by federating several simulations. HLA is the recommended standard within NATO operations through the STANAG 4603 standard[3].

Most distributed simulations today integrate simulation exercises using the common wire protocol found in Distributed Interactive Simulation (DIS) or in a particular run-time interface for HLA. To exchange data between the simulation systems, systems integrators need to define and use the Protocol Data Units (PDU) defined in DIS or the run-time interface with the Federation Object Model defined in HLA. Although multiple platforms have used this integration strategy, it does not scale well. It is also more challenging to integrate the actual mission platform technology with newer technologies, such as gaming platforms.

More modern MS&T systems use an open data connectivity framework based on the Object Management Group® (OMG®) Data Distribution Service (DDS) standard[4]. DDS operates using a brokerless, peer-to-peer, publish/subscribe model that includes multi-cast communication, dynamic discovery and proven interoperability. DDS has security capabilities that enable senders to publish data they are authorized to send, and receivers to subscribe to the data they are authorized to receive. The sender and receiver do not need to have knowledge of each other. DDS applications can be coded in different languages and run on different operating systems hosted on virtualized system platforms.

The DDS architecture enables the rapid integration of legacy HLA and DIS simulations while also enabling the integration of other entities such as humans, gaming platforms and hardware-in-the-loop (HIL) systems based upon actual deployed platforms. DDS-based systems enable the rapid scaling of new live, virtual and constructive environments while providing rapid response times for real, augmented and virtual realities in a single lab or across multiple sites connected with dedicated networks and/or cloud platforms.

CREATING AN INTEROPERABLE DDS COMMUNICATIONS FRAMEWORK

In 2018, Real-Time Innovations (RTI) created a pilot project to demonstrate the unique capabilities of DDS for rapidly enabling interoperability between disparate simulation platforms that were built on multiple platforms using different data models and formats.

The goal was to create a cross-vendor, interactive MS&T system that would integrate a HLA-based platform with a DIS-based platform, then integrate those simulation environments with an actual Future Airborne Capability Environment (FACE™) standard avionics platform using avionics hardware and a proven application software stack. The project also sought to integrate a proven gaming platform into the complex environment. The following COTS software programs were selected:

- Harris FliteScene, the FACE-certified conformant, digital moving map software that provides advanced situational awareness
- Microsoft Flight Simulator X, a flight simulation computer game
- National Instruments LabVIEW, a graphical program to visualize aspects of applications, including hardware configuration, measurement data, and debugging
- RTI Connext® DDS, the DDS-based connectivity framework for high-performance distributed systems that includes Services to enable the creation of gateways to legacy protocols, such as DIS and HLA
- Simblocks.io CIGI SDK for Unity, providing a modeling and simulation platform for live, virtual and constructive training
- VT MAK, the modeling and simulation software which also provides a universal translator for distributed simulations

THE INTEGRATION APPROACH

Data Model. Harris FliteScene data model was selected as the data model based on its widespread use in deployed avionics system and its ability to work in cross-platform environments. This model had been successfully deployed in the formal FACE conformance certification for FliteScene.

HLA/DIS with VT MAK. VT MAK provided the HLA/DIS environment, and also supplied their F-18 HLA simulation. VT MAK's VR-Exchange broker for RTI Connext data model topics was used, representing the DIS standard Protocol Data Unit (PDUs) that contain a specific block of information transferred over a network. The Entity State PDU was chosen and was represented as the SimpleBaseEntity topic, which has a position record (x, y, z Cartesian coordinates) and an orientation record in Euler angles. The RTI Routing Service software provided the conversion of coordinates necessary for transforming between the data topics.

Gaming Platform using CIGI – SimBlocks.io. To achieve the goal to integrate the MS&T environment with a popular gaming product, the SimBlocks.io gaming platform was selected, using the SimBlocks.io One World SDK with the Unity Game Engine. The output was linked with the Common Image Generator Interface (CIGI) standard, an on-the-wire data protocol that enables communication between a simulation host and an image generator. The CIGI host subscribed to the DDS FliteScene data model topic and converted this element to a CIGI entity control message. Since there is not an existing data model for the CIGI host, a subscriber was implemented to UPDATEOWNSHIPLOCATION in the CIGI host.

Microsoft Flight Simulator Bridge. A software bridge was created to connect the Microsoft Flight Simulator X (FSX) platform to RTI Connext DDS. This bridge was based on the Microsoft Library example5 using the Microsoft SimConnect SDK. The published data from this platform conformed to the Harris FliteScene data model which enabled a common data communications channel and the rapid integration of the Microsoft FSX system to the demonstration network based upon Connext DDS. The FSX Bridge was designed to publish UPDATEOWNSHIPLOCATION so it could directly drive the CIGI host and the FliteScene map.

Harris FliteScene with FACE Conformant Data Model. With the Harris FliteScene solution stack running on actual embedded hardware, the data of interest was the UPDATEOWNSHIPLOCATION, containing the position data of latitude/longitude in degrees and altitude in feet. It also contained orientation data of heading, pitch and roll in degrees for an aircraft, which in this case was a VK MAK simulated F-18 fighter jet.

Harris FliteScene has multiple input messages including Zoom, Underlay and Overlay, which control the display layout. The FliteScene map is centered based on the current position of the aircraft which is provided through the position update message. There are multiple sources which can be used to provide locations.

National Instruments LabVIEW. To easily control the map features, a simple user interface (UI) was created using National Instrument LabVIEW™ and the RTI DDS Toolkit for LabVIEW. The LabVIEW UI publishes additional topics of the Harris FliteScene data model to control the behavior of the map. This toolkit is based on the Connext DDS connectivity framework, which enabled the distributed network system communication for the integration

DATA MODEL TRANSFORMATION

The next step was to transform the data models: The FliteScene FACE conformant data model, and the DIS PDU representation used by the VR-Exchange broker. The Microsoft Flight Simulator and the CIGI gateway were developed using the same data model. The VR Exchange RTI Connext DDS gateway mapped data from the HLA side to DDS topics (data model elements). The topics were formatted into messages using the DIS PDU definitions.

To connect everything together, the FACE data model needed to be transformed to DIS PDU topics. RTI Routing Service bridged the SimpleBaseEntity topic to the location topic used by FliteScene. Besides the different data types, the two sides also used different measurements. The data coming from the VT MAK F-18 simulation used the HLA standard. The HLA data was in Geocentric coordinates, yet the FliteScene expected data in latitude/longitude coordinate format. RTI Routing Service was used to map the coordinates using a custom transformation library to translate between the different coordinate measurements.

The FACE avionics software stack is an actual avionics hardware platform that interacts with the rest of the simulation demonstration platform as a networked HIL component. Integrating this with Harris FliteScene was a straightforward migration, since FliteScene was already a FACE-certified

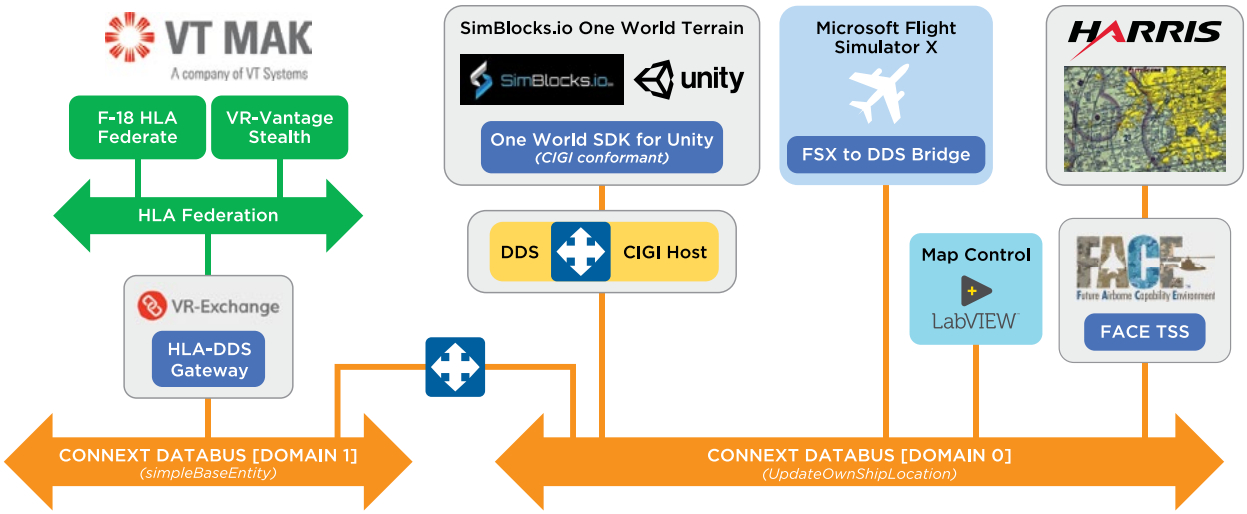

Figure 1: The integration of the different simulation and HIL components in a multi-platform, multiple data format environment

application that uses the FACE Transport Services Segment (TSS) APIs running on a COTS avionics hardware platform. The RTI FACE certified TSS product was linked directly to the FliteScene libraries and the avionics platform integration, validating the FACE approach.

The integration work was completed in 75 engineering hours, proving that creating an open data communications framework using DDS is a viable strategy that drives down integration risk. It also demonstrates that simulation platforms can quickly scale using a wide range of technologies.

However, it was conducted in a closed environment, using known data sources. The challenge lies in enabling and securing a wide range of data sources from global assets.

ACHIEVING MULTI-LEVEL SECURITY

Securing MS&T systems is critical and challenging. As the complexity of Live, Virtual and Constructive (LVC) systems increases, there is a corresponding demand for highly accurate, high-fidelity exercises. The ability to acquire and run mission data in real-time is bounded by the level at which the data can be protected and secure.

Typical approaches for implicitly securing data include user authentication, access control, integrity checks, non-repudiation and confidentiality mechanisms at the domain and link layers, traditionally hosted on very expensive secure hardware platforms. This is now shifting from a hardware-centric approach to software-based security. In order to create high-fidelity MS&T systems, new requirements are emerging to attach security protocols directly to the data itself. Security policies in this case must be targeted and managed at each element of system-identified data. Restrictions must be placed to ensure access to data is shifted from universal access to an as-needed/as-authorized approach.

MS&T systems are typically built around a deployment model based upon very narrow use cases. Security is built to accommodate the specific use case based on assumptions of the deployment and who requires access to the data. The model is only appropriate if the scope, span and use of that system and its data will never change.

For today's MS&T systems, this is a limited and ineffective approach. Next-generation MS&T systems will need to constantly evolve and change with mission demands in order to achieve the required fidelity, utility and scale for modern training, all while running on multiple simulation platforms using a wide range of secured data sources. Traditional platform assumptions can quickly become invalidated for centralized and/or localized storage requirements, user authenticated access, performance requirements, presentation layers of data and more.

Many systems today leverage point-to-point security protocols that provide authentication and access control at a link layer, treating all data on the link equally. However, this point-to-point approach relies on message forwarding, which cannot deliver the necessary scalability and performance requirements for large, deterministic systems.

MULTI-LEVEL SECURITY THROUGH DDS

The challenges described in the previous section can be resolved with the OMG DDS Security[6] specification, which enables fine-grained data-centric security in distributed system environments. It provides DDS implementations with enhanced security mechanisms based on data-centric security policies and controls, resulting in the capability to secure a global data space with:

- Fine-grained control of read and write access and permissions
- Peer-to-peer and serverless authentication capabilities
- Orthogonal data representation, transport, discovery, protocol and security concerns
- Source-specific tagging
- Differentiation of read, write and relay permissions

In general terms, these features allow control over who can access what information and who can control the dissemination of data for each data model topic as opposed to the entire data stream. These capabilities directly map to the standard security concerns within the global data space for MS&T systems:

- Authentication: User and device identities can be checked and validated as part of the process of granting access to a domain. Connection to the DDS databus can be separately managed and specified from connection to the physical layers of the network.
- Access control: Even if connected, users must have specific read and write permissions for a specific topic or an identified set of topics.
- Confidentiality: Discreet data values and related metadata can be encrypted together or separately. Data payloads can be separated and encrypted for confidentiality while routing or implementing last-value historians.
- Integrity: Data samples can include destination-specific signatures or machine access controls (MACs). This can be applied independently or in parallel with confidentiality.
- Non-repudiation: Behaviors and associated quality of service can be specified for each source/sync of data to acknowledge receipt and acceptance of data to the level needed.
- Availability: Behavior management, fault monitoring and failure actions can be designed into the domain on a per-data item basis.

These DDS Security features are integrated into the DDS network protocols and enable the use of a wide range of data sources, which is securely presented to authenticated MS&T users in real-time, increasing fidelity and utility. These features also enable different DDS Security domains and partitions to share communications channels and enable access to simulation topics with proper user and device authentication. DDS Security features enable application developers to configure security features on a topic-by-topic basis, enabling very fine-grained security. The layered security of DDS domains, partitions and individual topics supports defense-in-depth requirements and easily augments other system level security.

DDS Security is more suitable for real-time MS&T environments. It can replace the traditional security approaches that create multi-level communications channels through hard-coded partitioning in operating systems coupled with traditional networking capabilities like sockets. This traditional design is no longer suitable for the agile approaches required for MS&T due to its inflexible design and low application portability, plus high risk and high costs to develop, maintain and certify the systems.

DDS SECURITY IMPACT

Creating new security features in traditional MS&T systems can completely disrupt the design and operation of a platform. Most integrators seek to minimize the security features in order to decrease costs, risk, impact on performance as well as the operational impact of security. Traditional security solutions tend to focus on securing a pipeline for data exchange and using one-to-one communications sessions between systems, a process that limits scalability and adaptability.

Securing DDS applications and data in MS&T environments is different. The OMG DDS Security specification addresses communications security in a one-to-many, data-centric approach. Instead of securing data transmission pipelines, it enables applications to define different security policies based on the nature of the shared data on a per-topic basis. The DDS security plugins are configured via XML to enable security. RTI has an optional SDK for RTI DDS Secure that provides custom plugins, crypto modules and support for custom hardware such as crypto accelerators or TPMs.

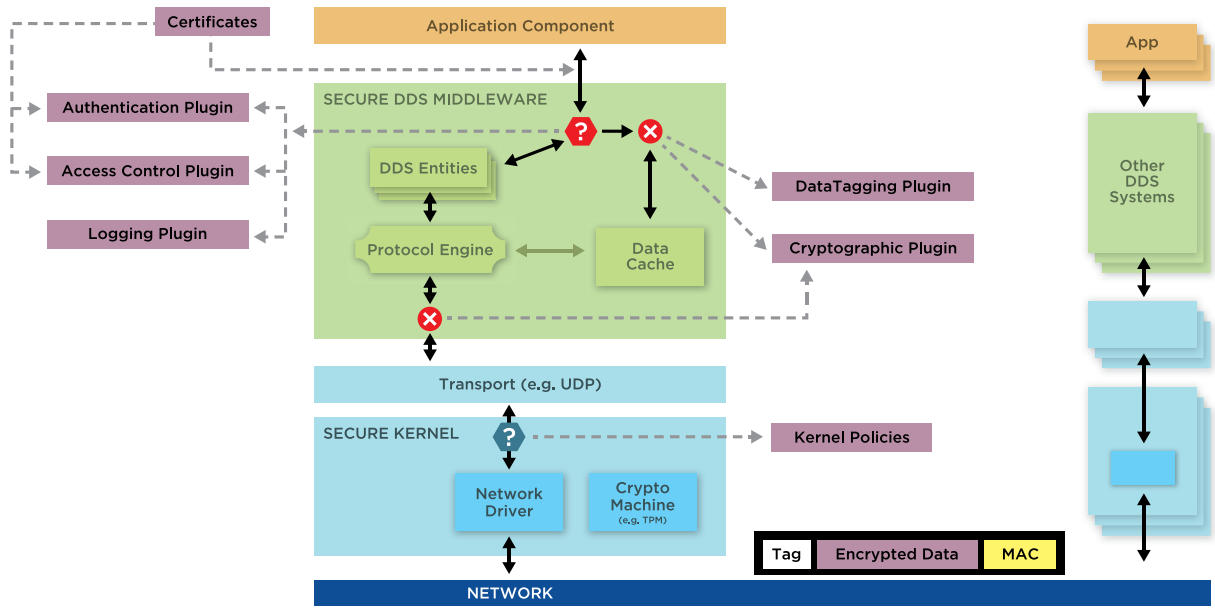

Figure 2: DDS Security Architecture (source: Object Management Group®)

DDS security plug-ins inherently use the existing data architecture and therefore do not require any modification or maintenance of the communications platforms or channels, enabling the immediate use of DDS security capabilities as required. Changes to security components can be dynamically inserted as required, enabling operators and MS&T developers to immediately respond to changes in the security landscape. The DDS security partitions enable the separation of software needed for each MS&T supplier, providing extra security. The DDS security domains easily separate critical software from less critical software and also data associated with different sources and levels of security.

CONCLUSION

Military training scenarios can be rapidly assembled, reconfigured and secured in an agile, ad-hoc manner from ready-made, COTS components and traditional MS&T platforms. This paper proves that systems based upon the DDS standard can integrate a wide range of real-time simulation environments to efficiently deliver Live, Virtual, and Constructive (LVC) training in a secure, interoperable environment. It is now proven and viable to integrate complex, multi-vendor training and simulation systems powered by global public, private and agency data sources through a DDS-based framework. This approach can drive down costs and risk, while providing a secure and interoperable framework for cross-vendor, cross-branch and cross-ally simulation of the ever-evolving battlefield.

[1] https://standards.ieee.org/standard/1278_2-2015.html
[2] https://standards.ieee.org/standard/1516-2010.html
[3] https://www.netn.mscoe.org/standards
[4] https://www.omg.org/spec/DDS/1.4/
[5] https://msdn.microsoft.com/en-us/library/cc730340(v=msdn.10)
[6] https://www.omg.org/spec/DDS-SECURITY

ABOUT RTI

Real-Time Innovations (RTI) is the largest software framework provider for smart machines and real-world systems. The company's RTI Connext® product enables intelligent architecture by sharing information in real time, making large applications work together as one.

With over 1,500 deployments, RTI software runs the largest power plants in North America, connects perception to control in vehicles, coordinates combat management on US Navy ships, drives a new generation of medical robotics, controls hyperloop and flying cars, and provides 24/7 medical intelligence for hospital patients and emergency victims.

RTI is the best in the world at connecting intelligent, distributed systems. These systems improve medical care, make our roads safer, improve energy use, and protect our freedom.

RTI is the leading vendor of products compliant with the Object Management Group® (OMG) Data Distribution Service™ (DDS) standard. RTI is privately held and headquartered in Sunnyvale, California with regional headquarters in Spain and Singapore.

Download a free 30-day trial of the latest, fully-functional Connext DDS software today: https://www.rti.com/downloads.

RTI, Real-Time Innovations and the phrase "Your systems. Working as one," are registered trademarks or trademarks of Real-Time Innovations, Inc. All other trademarks used in this document are the property of their respective owners.
©2020 RTI. All rights reserved. 50041 V1 0820

Your systems. Working as one.

CORPORATE HEADQUARTERS
232 E. Java Drive, Sunnyvale, CA 94089
Telephone: +1 (408) 990-7400
Fax: +1 (408) 990-7402
info@rti.com

rti.com
rti_software
rtisoftware
company/rti
connextpodcast
rti_software