Evolution of NATO standards for federated simulation

Björn Löfstrand
Pitch Technologies
Linköping, Sweden
bjorn.lofstrand@pitchtechnologies.com

Reinhard Herzog
Fraunhofer IOSB
Karlsruhe, Germany
Reinhard.herzog@iosb.fraunhofer.de

Tobias Kuhn
NATO M&S Centre of Excellence
Rome, Italy
mscoe.ms01@smd.difesa.it

Horst Behner
Joint Materiel Office
BAAINBw
Koblenz, Germny
horstbehner@bundeswehr.org

Tom van den Berg
Netherlands Organisation for Applied
Scientific Research (TNO)
The Hague, The Netherlands
tom.vandenberg@tno.nl

Keywords: Federation, Federate, Certification, Simulation, Standard, NATO, NETN

ABSTRACT: *NATO and the Nations regularly use distributed simulation based on the High Level Architecture (HLA) interoperability standard. The current release is IEEE 1516-2010. In the NATO context, several official documents are available to standardize the use of HLA across NATO Nations:*

- *STANAG-4603 describing the HLA standard.*
- *STANREC-4800 describing the NATO Education Training Network (NETN) Federation Object Model and the associated Federation Architecture and FOM Design (FAFD).*

The NATO Modelling and Simulation Group (NMSG) has a close relationship and a Technical Agreement with the Simulation Interoperability Standards Organization (SISO) with respect to Simulation Interoperability Standards and has provided significant input to SISO standards development over the last years. E.g. NMSG Task Groups MSG-068 and MSG-106 provided significant input on the modularization of RPR-FOM v2.0, and other Task Groups have provided significant input on C-BML, MSDL and UCATT SISO standards. NATO is also a user of SISO developed standards including IEEE 1516 (HLA) series of standards which is covered in STANAG 4603.

SISO and NATO standards have successfully been applied in developing Federated Simulations to support Education, Training, Exercise and Evaluation. For example, the Swedish Viking Exercises are based on Federated Simulation using STANAG 4603 and NETN FAFD. Other NMSG Task Groups apply the SISO and NATO standards to support different aspects of M&S, e.g. Task Group MSG-147 is developing NETN FAFD FOM modules for Crisis Management and Disaster Response, MSG-164 is developing the concept of Modeling & Simulation as a Service (MSaaS) to manage Federated Simulation etc.

There is a continued need for NATO to experiment with, update and further evolve NATO Standards for Federated Simulation to meet new and evolving simulation interoperability requirements and to harmonize with new and evolving SISO standards.

The objective of the recently (2018) started Task Group MSG-163 similarly named "Evolution of NATO Standards for Federated Simulation" is to further evolve the NATO standards for Federated Simulation. This includes:

- *An update of the NATO NETN FOM modules and associated Federation Architecture.*
- *An update of the NATO reference documents regarding HLA (STANAG, STANREC and AMSP, etc.).*
- *The definition and implementation of a NATO Certification Service for simulator system interoperability.*
- *The improvement of the NATO HLA Certification Service. This service covers process, organization and a supporting open source tool (Integration, Verification and Certification Tool, IVCT).*

This paper provides an overview of Task Group MSG-163 and presents the preliminary results.

1 Introduction

Modelling and Simulation (M&S) is a key enabler for several activities within NATO, including support to education, training, exercises, and test & evaluation of the alliance’s units and systems. The use of M&S provides the ability to represent complex and challenging environments, large scenarios, and new concepts in distributed and federated systems. National and NATO M&S assets can be provided (as services) to create joint and combined synthetic environments.

Efficient and effective use of NATO and national M&S assets require standards for connecting and integrating M&S components. A strategic view on the development, evolution and implementation of these standards is necessary to exploit the full potential of M&S across the alliance. The NATO M&S Master Plan [1] identifies five (5) high-level objectives:

1. Establish a Common Technical Framework
2. Provide Coordination & Common Services
3. Develop Models & Simulations
4. Employ Simulations
5. Incorporate Technical Advances

The NATO Modelling and Simulation Group (NMSG) is a specific group within the NATO Science & Technology Organization [2] focused on the development and evolution of NATO M&S including the implementation of the NATO M&S Master Plan. Interoperability, Reuse, Affordability and Synergy are the principles that guide the NMSG in its implementation of the master plan objectives.

NMSG is tasked with performing M&S research and to develop NATO standards to promote cooperation among Alliance bodies, NATO member nations, and partner nations to maximize effective utilization of M&S. In 2003, NMSG was officially nominated, as the Delegated Tasking Authority for NATO M&S Standardization and there is a Technical Cooperation Agreement between NMSG and SISO (since 2007 and updated 2019). Over the years, NMSG has provided significant input to SISO standards development, e.g. NATO Task Groups MSG-068 and MSG-106 provided input on the modularization of RPR-FOM v2.0. Other NATO Task Groups provided input on C-BML, MSDL and UCATT SISO standards.

Official M&S publications produced by NMSG are called NATO Allied Modelling and Simulation Publications (AMSP). These can be technical standards, guidance or reference documents. NATO also heavily rely and depend on standards and guidance developed by international Standards Development Organizations (SDOs) such as SISO, IEEE, ISO etc. Promulgation and dissemination of standards in NATO are done by the NATO Standardization Office (NSO) and the documents are labelled as either STANAG (Standard Agreement) or STANREC (Standard Recommendation). The maintenance of these standards is overseen and managed by the NMSG Modelling and Simulation Standards Subgroup (MS3). The MS3 may in turn delegate work to a project (MSG) consisting of national and NATO experts and tasked with delivering updates to a standards document.

One of the fundamental standards related to the Common Technical Framework objective is STANAG 4603, which mandates the use of the IEEE 1516 High-Level Architecture standard for federated distributed simulation. The same STANAG also recommends the use of IEEE 1730 DSEEP and requires alliance members to utilize a NATO Federate Certification Service for testing compliance with the HLA standard. STANAG 4603 is ratified by approximately 20 NATO nations, is supervised by NMSG, and is under the custodianship of the US DoD M&S Coordination Office.

NATO nations and partner nations have successfully applied SISO and NATO standards. The experiences and feedback using these standards are collected by nations and provided either directly to SISO or through NATO MSG activities.

NATO Task Group MSG-163 has been tasked to support MS3 in maintaining and collecting feedback on the use of AMSP-04 NATO Education and Training Network Federation Architecture and FOM Design (NETN FAFD). The NETN FAFD is covered by STANREC 4800 and was published in March 2018. The NETN FAFD originates from MSG-068 established by NATO Allied Command Transformation (ACT) in 2007 to develop standards to support the NETN vision:

“to deliver to NATO and Partners a persistent, distributed and joint training capability able to support training from operational to tactical level across the full spectrum of operations, whilst leveraging existing national expertise and capabilities”

The NETN FAFD is a reference federation agreement document based on the use of STANAG 4603 HLA and the SISO-STD-001 Real-Time Platform Reference FOM. Input from national M&S programs to support Computer Assisted eXercises (CAX) influenced the development of a NETN FOM, which extends the RPR-FOM with additional concepts and patterns for simulation interoperability. Since its first release in 2011 the NETN FOM has evolved based on operational use by NATO and nations to its current version NETN FOM v2.0. MSG-163 is currently updating the NETN FOM, improving existing as well as adding new FOM modules based on feedback from nations. The Task Group expects to deliver a draft NETN FOM v3.0 in 2020, but interim releases of some of the new modules are already available.

NMSG also tasked MSG-163 to evolve the existing HLA Certification Service for verifying compliance against the NETN FOM. The Task Group is expected to deliver a Final Operating Capability (FOC) of the service by the end of 2020. Associated with the certification service is a tool to support Integration, Verification and Certification (IVCT) of individual federates’ compliance with STANAG 4603 HLA and STANREC 4800 NETN FOM.

There is a continued need for NATO to experiment with, update and further evolve NATO Standards for Federated Simulation to meet new and evolving simulation interoperability requirements and to harmonize with new and evolving SISO standards.

The remainder of this paper discusses the NETN FOM, describes the certification concept of operations, and provides an overview of the IVCT. Both the NETN FOM and the IVCT are managed as open source projects on GitHub, enabling the user community to engage the developers and providing early access to releases. Links are provided below.

2 NATO Standards for Federated Simulation

NATO AMSP-01 “The NATO M&S Standards Profile” (NMSSP) identifies STANAG 4603 HLA and STANREC 4800 NETN FAFD as key standards to support federated distributed simulation. NETN FAFD is a modular reference federation agreement that contain a set of HLA FOM Modules that extend and complements the SISO-STD-001 RPR-FOM v2.0.

The NETN FOM modules are recommended for use when implementing NATO AMSP-04 NETN FAFD compliant distributed simulation. These NETN FOM include reference to other standard FOM modules as well as NETN modules developed by NATO Modelling and Simulation Group (NMSG) Modelling and Simulation Standards Subgroup (MS3). The modules have inter-dependencies and have been designed to maximize re-use and interoperability with legacy systems using existing standards, and those having requirements for new patterns of simulation interoperability. The NETN FOM is the complete set of NETN modules and all other modules they depend on (e.g. SISO RPR-FOM modules).

The NETN FOM has evolved since it was first release in 2010 and the current version, NETN FOM v2.0, is currently under revision. Release of a draft NETN FOM v3.0 is expected in 2020 followed by a release by NSO as AMSP-04 Ed B covered by STANREC 4800. A timeline of the NETN FOM is provided in Figure 1.

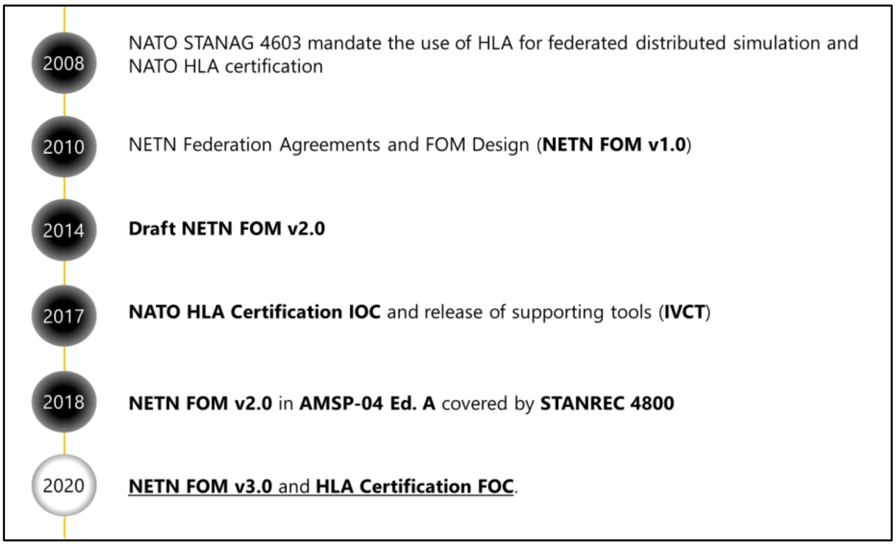

Figure 1: NETN evolution over time.

Input to the revised NETN FOM comes from various national and NATO projects and programs using more or less of the FOM modules to support education, training, exercises and evaluation (ETEE). E.g. the Swedish exercise series Viking, has used several of the current FOM modules in NETN to provide better support for automation of EXCON activities and Simulation-C2 interoperability. In addition, several other NMSG research Task Groups with participants from many NATO and partner nations have supported the development of NETN FOM Modules. The draft NETN FOM v3.0, as it is currently defined, includes 11 FOM modules that complement and/or extend existing RPR-FOM v2.0 modules, see Figure 2.

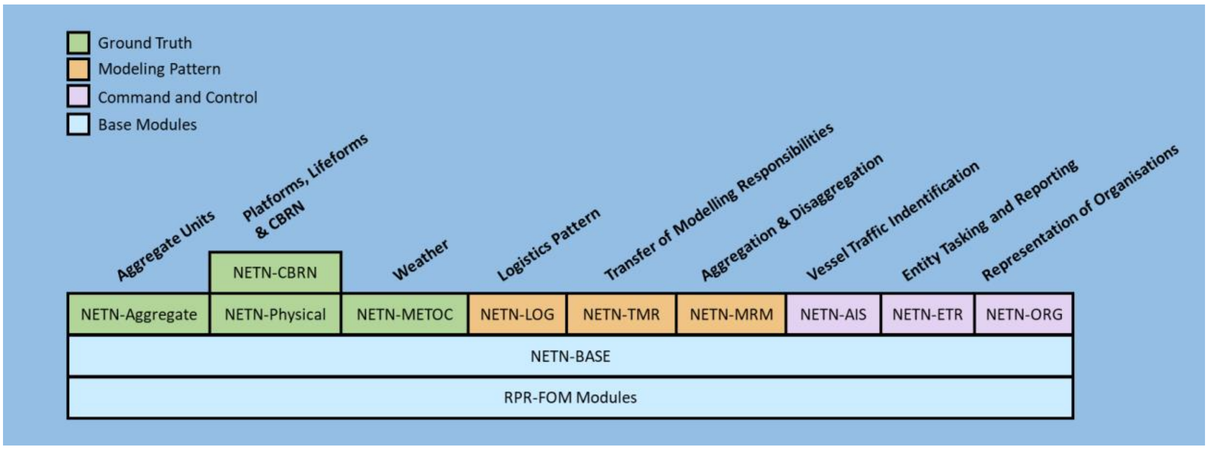

Figure 2: NETN FOM modules.

AMSP-04 Edition A was published in March 2018 covered by a NATO STANREC 4800 and defines the NETN FOM v2.0 FOM modules and associated documentation. The AMSP-04 including the NETN FOM modules are "Not Classified" and are releasable to the public. All NETN FOM modules are published in GitHub and are available to the general public for download and for providing comments/issues. The "development branch" of each FOM module contains the current "under development" version for the module. The version on the development branch can be accessed for early access and engagement. See https://github.com/AMSP-04 [3].

A NETN federation design may extend NETN FOM modules (as new modules), include other FOM modules, and/or select to use only a subset of the NETN modules, all depending on the needs and requirements of the federation. When extending the FOM with additional modules, the naming of classes, data-types and other identifiers must be de-conflicted and the basic FOM Module merging rules as defined in HLA Evolved are applied.

Registered objects and interactions are always discovered/received at the most specific subscribed class level. Extending a FOM Module with additional subclasses provides the possibility to add extra attributes/parameters at the more specific class level. Exchange of information using this more specific level can take place between federates publishing and subscribing to this level. However, to become compatible with and receive information from federates only publishing on the more general level, the receiving federate must subscribe to both class levels. Subscribers of the more general class will receive information from publishers of the more specific class level.

Example: A national extension to the NETN FOM Modules subclasses existing NETN object classes and defines additional attributes. National models aware of this extension can publish and subscribe to the more specific level defined in the national FOM module extensions. Other existing federates not aware of the extension can still discover the object and receive updates, but only on the level they subscribe to. In order for the national federates to discover and receive information from other federates they need to subscribe to the NETN class level as well as the national extension level. Note that the discovered object and attribute updates will be on the NETN level.

2.1 Representation of Organizations

Modelling of an organizational unit in a distributed simulation depends on its intra-organizational relationship with other units, e.g. superior, subordinate, and the relationship between organizations, e.g. friendly or hostile. This organizational information is normally provided to simulation systems as part of initialization based on the scenario.

The NETN Organization FOM Module (NETN-ORG) is a specification of how to represent organizations in a federated distributed simulation and provides a common standard interface for the representation of the state of units including command structure and relationship between organizations. This representation can be used for setting the initial state of simulated entities, capturing subsequent snapshot states and for dynamic change of organizational relationships. An example federation design using MSDL to initialize the simulation and to generate snapshots for viewing or storage is provided in Figure 3.

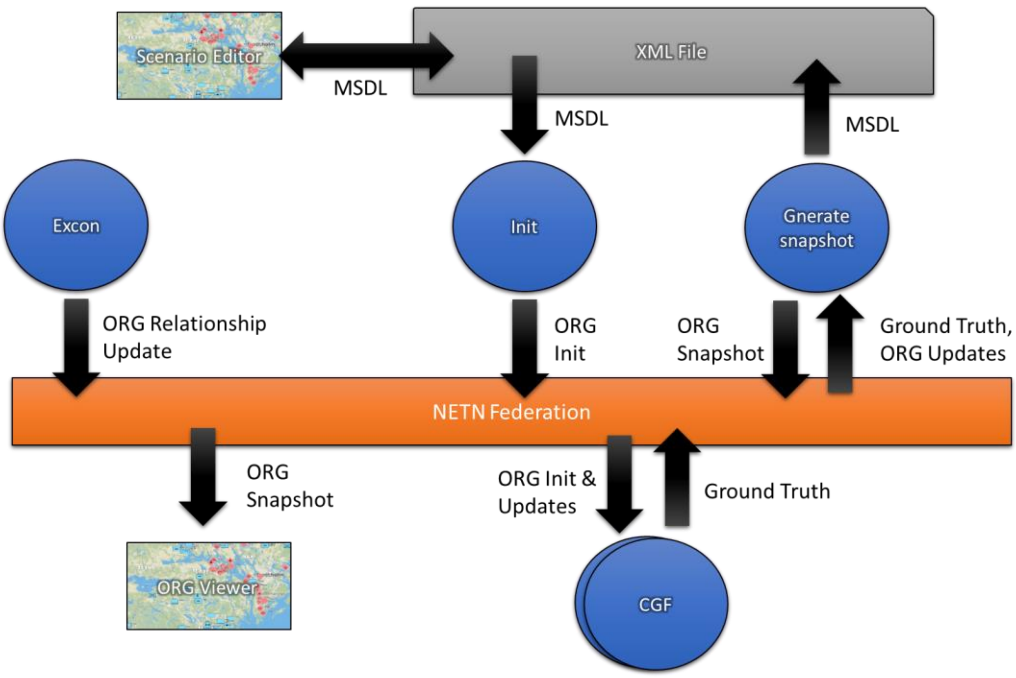

Figure 3: Use of MSDL to initialize the simulation and to generate snapshots for viewing or storage.

The SISO-STD-007-2008 Military Scenario Definition Language (MSDL) is used as the foundation of NETN-ORG and the information modelled in the federation regarding organizations can easily be mapped to the corresponding MSDL representation in XML. This allows for easy generation of snapshots of current state in the federation to XML based

MSDL and for initialization from MSDL files. Some optional extensions to MSDL developed by NATO MSG-106 are also supported including information about the initial allocation of modelling responsibility to federates.

Both MSDL and the NETN-ORG module use a Universally Unique Identifier (UUID) to identify the organizational elements. This provides a way to uniquely identify entities even between federation executions. To take full advantage of the UUID, the NETN FOM defines two FOM modules that extend the RPR-FOM representation of aggregate units and physical entities.

The NETN-Aggregate and NETN-Physical both extend the corresponding RPR-Aggregate and RPR-Physical modules respectively and adds a UUID attribute used to publish the unique identifier during federation execution. This extension allows NETN units and platforms to be represented in multiple executions, e.g. Monte-Carlo simulation, and later correlated for analysis.

2.2 Logistics Modelling & Simulation

Military logistics is the discipline of planning and carrying out the movement and maintenance of military forces including storage, distribution, maintenance and transportation of materiel. The NATO Education and Training Network Logistics Module (NETN LOG) is a specification of how to model logistics services in a federated distributed simulation.

The NETN-LOG FOM Module provides a common standard interface for negotiation, delivery, and acceptance of logistics services between federates modelling different entities involved in the service transaction. E.g. simulation of the transport of a unit modelled in another simulator.

NETN-LOG covers the following services:

- Supply Service offered by a federate capable of simulating the transfer of supplies between consumer and provider.
- Transport Service offered by a federate capable of simulating loading, transport and/or unloading of non-consumable materiel.
- Repair Service offered by a federate capable of simulating repair of consumer provided non-consumable materiel, e.g. platforms.

Examples of use:

- Refuelling of aircraft at an airbase or in the air.
- Transport of supplies between facilities.
- Repair of damaged platforms in a facility or by unit.
- Transport of units, platforms, and humans by train, ship, or aircraft.

All NETN LOG services are based on a Logistics Service Pattern that includes negotiation, delivery, and acceptance of logistics services. Federates participating in the logistics service transaction are either a Service Consumer or a Service Provider.

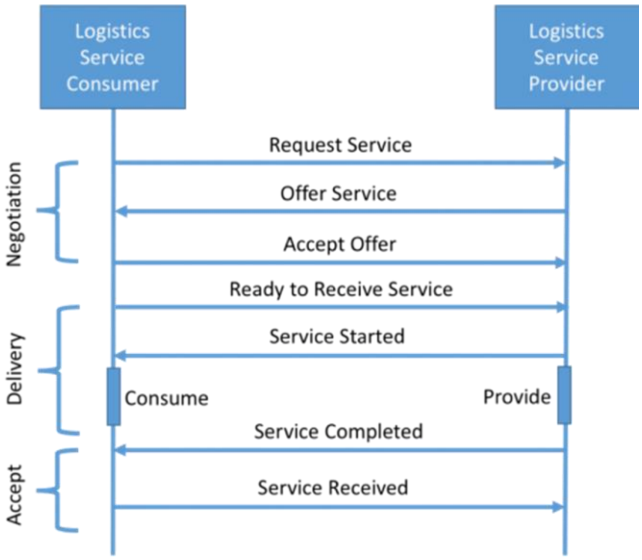

Figure 4: Logistics Service Pattern.

2.3 Transfer of Modelling Responsibilities

In a federated distributed simulation, the participating systems (federates) collectively model the synthetic environment. Allocation of modelling responsibilities are based on individual federate capabilities, federation design agreements, and initial scenario conditions. The responsibility of updating an attribute for a specific simulated entity is allocated to at most one federate. However, during execution, the modelling responsibility may change, and the ownership of attributes can be transferred.

Basic services for the divestiture and acquisition of attribute ownership is provided by HLA. A negotiated and coordinated transfer of modelling responsibilities requires agreements between federates before attribute ownership is transferred.

The NATO Education and Training Network Transfer of Modelling Responsibilities (NETN-TMR) FOM Module is a specification of how to perform a negotiated and coordinated transfer of attribute modelling responsibility between federates in a distributed simulation. It extends the HLA Ownership Management services by providing the means to

1. Negotiate the transfer of ownership.
2. Initiate ownership transfer using a Trigger federate.

A transfer of modelling responsibility is performed during runtime, to dynamically change the responsibility to update specific attributes, to a more suitable federate.

For example:

- Transfer from a Live to a Virtual or Constructive simulation.
- Transfer between Virtual and Constructive simulations.
- Transfer between hi- and low-fidelity models.
- Transfer to allow backup, maintenance or load-balancing.
- Transfer of certain attributes to functional models such as movement, damage assessment etc.

NETN-TMR covers the following cases:

- Negotiated acquisition where a federate request to receive the modelling responsibility.
- Divestiture where a federate request another federate to take modelling responsibility.
- Acquisition without negotiation where a federate receives the modelling responsibility.
- Cancellation of transfer.

A negotiated transfer of modelling responsibility between two federates is shown in Figure 5.

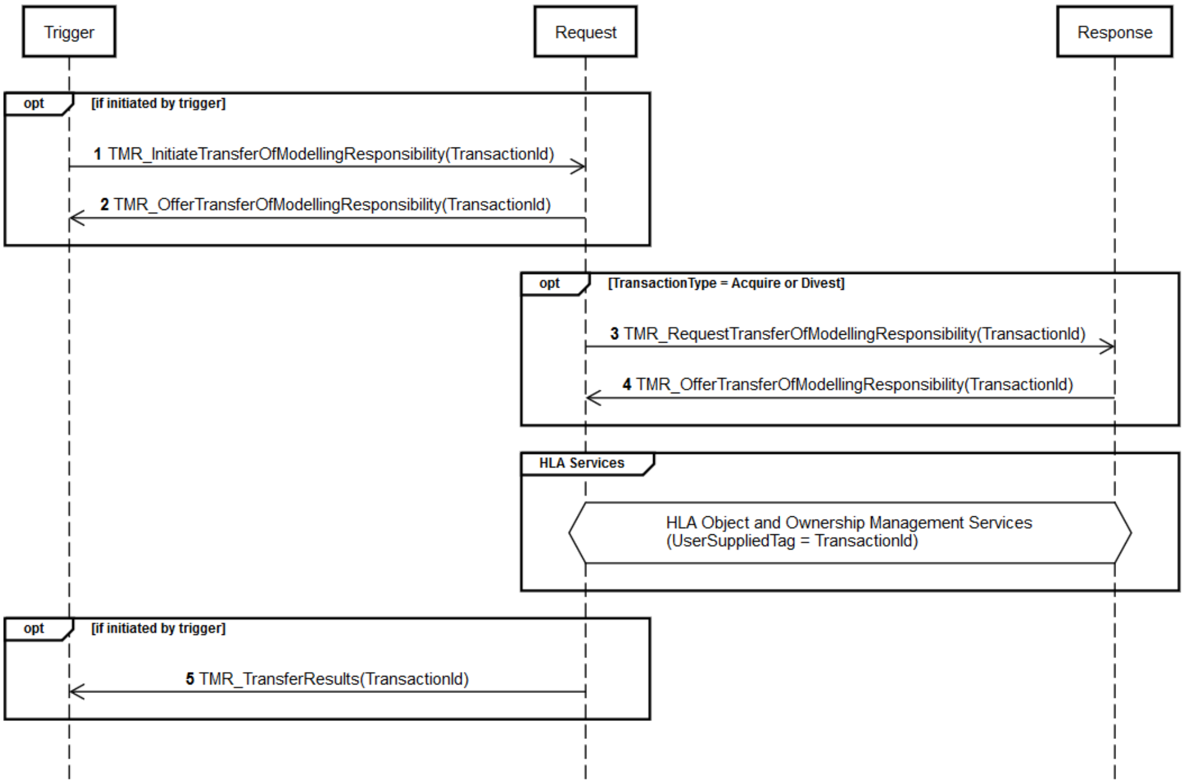

Figure 5: Negotiated Transfer of Modelling Responsibilities between federates.

NETN-TMR uses a combination of HLA interactions and HLA Ownership Management services to negotiate and perform a coordinated transfer of attribute ownership. The pattern includes a triggering interaction (optional) to initiate a transfer, and interactions for requesting, offering, cancelling and sending results of a completed transfer.

2.4 Multi-Resolution Modelling

Models of real-world objects, processes and phenomena are used to create a synthetic representation suitable for simulation. Depending on the purpose and requirements of the simulation, the models can have different levels of resolution and aggregation can be used to create representations of larger combined concepts.

The NATO Education and Training Network Multi-Resolution Modelling (NETN-MRM) FOM Module is a specification of how to perform negotiated and coordinated aggregation and disaggregation of models representing organizational units and individual entities, e.g. platforms, in a federated distributed simulation.

The purpose of NETN-MRM is to support federations where models are represented at multiple levels of resolution and where the level of resolution can change dynamically during a simulation.

For example:

- Disaggregation of a Batallion represented as an Aggregate Entity into Company level Aggregate Entities.
- Disaggregation of a Company to individual platforms such as vehicles and individual soldiers represented at an entity level.
- Aggregation of platforms represented as individual entities to an attribute of an aggregate unit representing e.g. a Platoon.
- Triggering of Aggregation by user command.
- Triggering of Disaggregation based on geo-fencing.

NETN-MRM covers the following cases:

- Disaggregation of AggregateEntity into lower-level AggregateEntities.
- Disaggregation of AggregateEntity into Platforms.
- Aggregation of AggregateEntities into higher-level AggregateEntity.
- Aggregation of Platforms into AggregateEntity.
- Triggering of Disaggregation.
- Triggering of Aggregation.

2.5 Entity Tasking and Reporting

The NETN-ETR module is a specification of how to represent common low-level tasks that can easily be interpreted and executed by simulators that model the behaviour of entities. It also defines a set of reports to provide status information, including the status of the tasks being executed by simulated entities.

The NETN ETR FOM module is simulation oriented and focuses on tasks with a fine granularity:

- It enables the transformation of command and control messages into tasks that can be executed by a simulator.
- It defines status reports that can be used for producing command and control reports needed for decision making.
- It supports the modelling of simulated command and control interactions between federates in a distributed simulation, for example during an MRM disaggregation process.
- It contains a comprehensive set of tasks and reports that can easily be interpreted and executed by simulators.
- It reflects the capabilities commonly found in COTS Computer Generated Forces (CGF) tools, but it is independent of a specific COTS CGF tool, agent framework, or agent modelling paradigm.
- It is independent of any specific doctrine or tactics.

An entity in ETR can be either a physical entity (e.g. platform or lifeform) or an aggregate entity. If a task or report relates to only a physical entity or to only an aggregate entity, then this is specified in the definition of the task. In the definition of each task, it is not specified how an entity (physical or aggregate) will / should perform the task.

The main benefits from using NETN-ETR is the ability to separate applications that provide tasking from the actual simulation of the task by a federate currently having the modelling responsibility of the entity. Sending tasking information to the federation instead to a specific application allows separation of simulation user interfaces from the simulation application and potentially allowing multiple simulation systems to be controlled from a single common simulation GUI, see Figure 6.

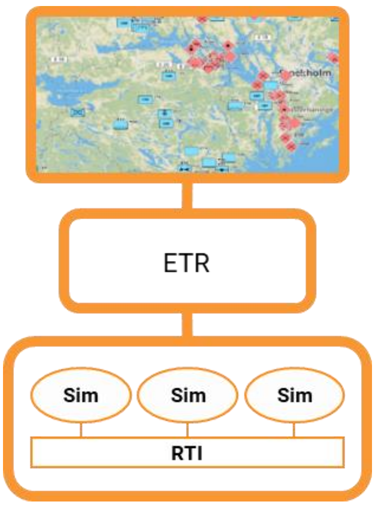

Figure 6: Simulation control via a common entity tasking and reporting.

NETN-ETR was originally developed by FFI, Norway and TNO, The Netherlands and have successfully been used to support exercises such as Viking.

2.6 CBRN Modelling & Simulation

CBRN is Chemical, Biological, Radiological and Nuclear materials that can be delivered intentionally as a weapon using conventional bombs, explosive materials and enhanced blast weapons (e.g., dirty bombs) or unintentionally caused by human error or natural or technological reasons, such as spills, accidental releases or leakages.

The NATO Education and Training Network CBRN Module (NETN-CBRN) is a specification of how to model CBRN related concepts in a federated distributed simulation. NETN-CBRN provides a common standard interface for the representation of CBRN release, detection, effects, and protective measures in a federated distributed simulation. E.g. the exposure effect on individual humans in a CBRN contaminated Hazard area where the human is represented in one simulation and the effect is modelled in another federate simulation.

The NETN-CBRN FOM module covers:
- CBRN Source release modelling.
- CBRN Detector modelling.
- CBRN Effects modelling.
- CBRN Protective measures modelling.
- Hazard area modelling.

Meteorological conditions and CBRN material properties for modelling the dispersion of CBRN material are not explicitly represented in the NETN-CBRN FOM Module. NETN-METOC FOM module can be used to model weather conditions that may impact the dispersion of CBRN materials and cause dynamic change to hazard areas.

2.7 Representation of Weather

The purpose of the NETN METOC module is to provide a standard way to exchange data related to weather conditions and primary effects of weather on terrain, on water surfaces, in the atmosphere and subsurface water conditions. The main objective is to provide a reference model that represents a core common subset of METOC related aspects and to allow extension of the module to incorporate additional detail if required. Therefore, the NETN METOC module shall be viewed as a reference FOM module where extensions are not only allowed but encouraged to fully meet federation specific requirements. However, any extension should also be considered as candidates for improving the NETN METOC module or candidates for new standard NETN modules.

Current weather conditions impact simulations such as platforms and sensors on the ground, on the sea, underwater and in the air. In a federated distributed simulation a correlated representation of these conditions is key to meet interoperability and model requirements. Different simulations require different fidelity of weather conditions concerning data resolution and accuracy.

The NETN METOC focus on the representation of weather conditions related to surfaces and layers. The main difference is that a surface condition does not have a volume and only represents the conditions directly related to the surface of a piece of terrain or water. The layer conditions represent a volume of water or air and are specified with height/depth from surface and layer thickness. Both concepts are also geographically positioned by reference to other concepts shared in the federation such as the position of objects, areal objects or reference to terrain features such as roads etc.

Based on these concepts different levels of fidelity in representing weather conditions can be achieved. Global conditions can be expressed as well as highly detailed conditions e.g. surrounding a specific aircraft.

The aspects and attributes of weather conditions included in the scope of the NETN METOC module are based on input from several sources and are designed to cover the most common levels of representation required by a large set of existing simulators.

- Atmospheric Layer Conditions cover the following aspects: Temperature, Winds, Precipitation, Haze, Humidity, Barometric Pressure, Visibility Range and Clouds.
- Water Layer Conditions cover the following aspects: Temperature, Salinity and Currents.
- Land Surface Conditions cover the following aspects: Temperature, Winds, Precipitation, Haze, Humidity, Barometric Pressure, Visibility Range, Snow Condition, Moisture and Ice Condition.
- Water Surface Conditions cover the following aspects: Temperature, Winds, Precipitation, Haze, Humidity, Barometric Pressure, Visibility Range, Sea State, Salinity, Tide, Ice Conditions, Currents, Waves and Swell.

2.8 Vessel Identification and Data

The Automatic Identification System (AIS) is a world-wide automated tracking system used on vessels and by Vessel Traffic Services for identifying and locating vessels by electronically exchanging messages with other nearby vessels and VTS stations. The purpose of the NETN-AIS FOM module is to represent vessel traffic in a simulation using AIS messages, enable the exchange of AIS in both a real-time and non-real time platform level simulation, and allow HLA federate applications to use regular HLA interaction classes and parameters to represent vessel information rather than using the physical message format in ITU-R M.1371-5 [5]. However, the FOM is aligned well with this specification, enabling relatively easy mapping to/from this specification.

An example of an AIS message transmission is provided in Figure 7, where the CGF simulates the individual vessels and periodically transmits Entity State data, the AIS Transmitter simulates the vessel's AIS transmitter and generates AIS interactions, and where the AIS Base Station simulates a land-side AIS station forwarding AIS information as NMEA-0183 formatted messages to connected C2 systems. Obviously, a CGF may generate AIS interactions also directly, if it supports that. There may also be multiple AIS Base Stations, each covering a certain area in the simulation.

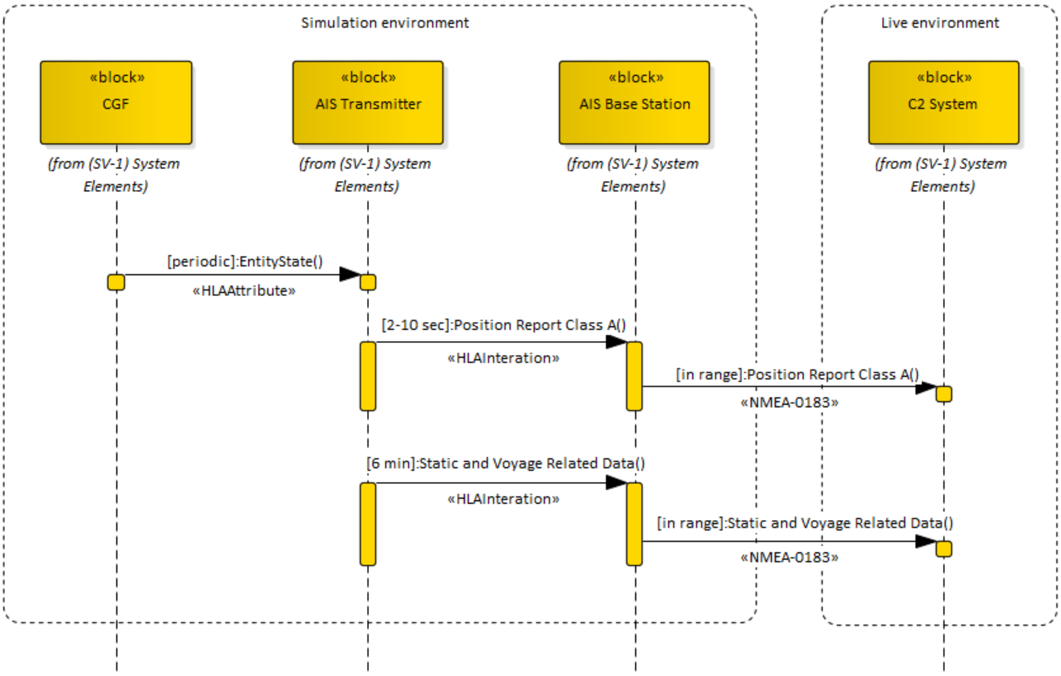

Figure 7: AIS message transmission event trace example.

3 Certification Concept of Operations

Experience shows that setting up a federation for an exercise event can be a time-consuming and frustrating task. Today, with a rising number of different systems and more complexity, this task requires even more effort. Compliance testing and certification before an exercise can greatly reduce this effort. This leads to reduced setup times and thus eventually to allow more exercises, increasing NATO's force readiness.

This chapter describes the certification concept of operations. It begins by giving a broad overview of the certification process and defining key roles and the concept of Capability Badges (CB). The final sections of this chapter explain the two major steps for achieving a NATO interoperability certification. This chapter does not cover details about the IVCT. Those are covered in chapter 4.

3.1 Compliance Testing and Certification Process Overview

The certification process and the IVCT were designed to be as flexible and user-friendly as possible. Therefore, it can be used to test a wide variety of different setups and configurations which includes but is not limited to:

- single commercial off-the-shelf (COTS) products,
- specific configurations or variations,
- federations based on their external interface, or
- federations of federations based on their external interface.

There are also no limitations on who can use the service or the IVCT. That means both system developers as well as military organizations or industry benefit from the compliance testing and certification process.

3.2 Key Roles

There are different actors involved in the certification process to make sure all procedures follow the standards and regulations set by NATO. The key roles and their interactions are summarized in Figure 8.

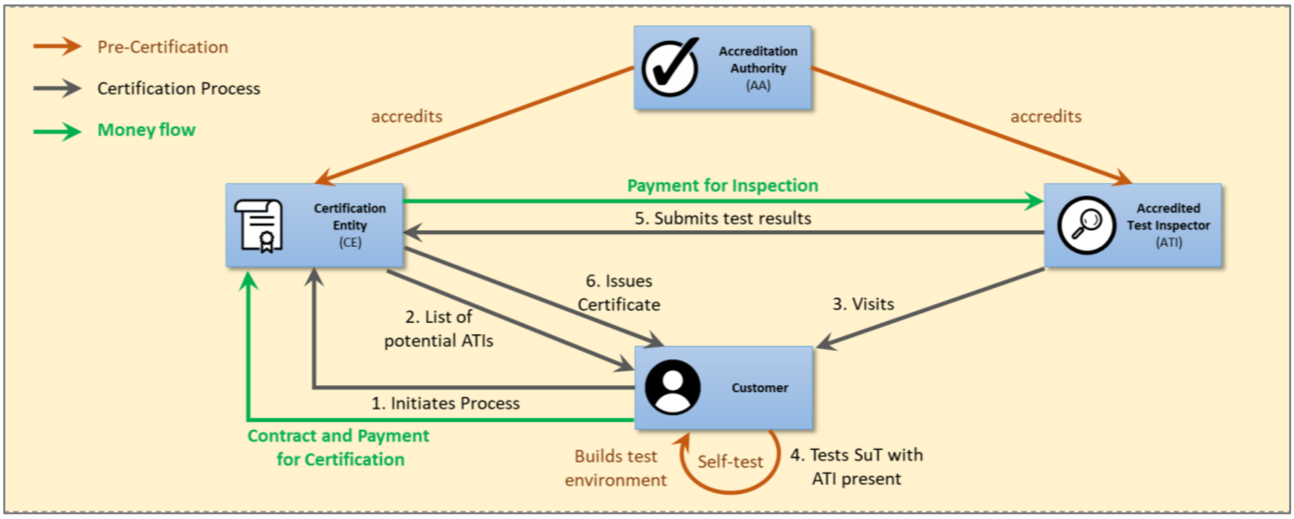

Figure 8: Overview of key roles and interactions.

The Accreditation Authority (AA) is a NATO appointed organization responsible for maintaining the business model and procedures. The AA not only accredits other key roles like the Certification Entity (CE) and the Accredited Test Inspector (ATI), it also accredits the IVCT version and associated test cases that need to be used for the certification. The Modeling and Simulation Standardization Subgroup (MS3), which is a subgroup of NMSG, acts as the AA.

The CE is an organization accredited by the AA and given the authority to issue certificates of compliance to systems that have successfully undergone compliance testing. It connects the Customer to all necessary resources, which involve the accredited version of the IVCT, its associated test cases and manuals as well as the ATIs. It also manages the payment aspects of the process. The Modelling and Simulation Centre of Excellence (M&S COE) acts as the CE.

The ATI, accredited by the AA, is an individual who oversees and inspects the certification test conducted at the Customer's facility. An ATI has knowledge about (NATO) interoperability standards (including NETN), the certification process, and the IVCT. Any individual can become an ATI upon successfully showing his or her skills and being accredited by the AA. However, an ATI cannot inspect tests performed for his or her own company.

Finally, the Customer is the System-under-Test (SuT) owner, who performs the self-test and eventually the certification test at its own facility, the latter overseen by the ATI.

3.3 The Capability Badge

The NATO standards as described in chapter 2 cover a wide range of interoperability features. On the other side stands a multitude of models and simulations with different purposes, each of them implementing only those NATO standards features they need and support. Hence, there cannot be only one 'master' certificate for all available features. For that reason, there is the concept of Capability Badges (CB). An example is provided in Figure 9.

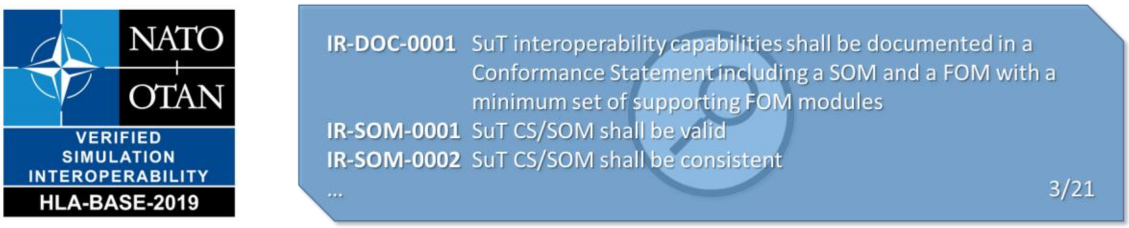

Figure 9: Example of the HLA-Base Capability Badge (CB). A SuT has to pass its 21 Interoperability Requirements (IR) to pass the certification test and receive the HLA-Base CB.

A CB is a selection of Interoperability Requirements (IR) that describe how distributed systems interact and exchange information to collectively meet overall simulation objectives. As an example, a weather model would need to have a different set of IRs compared to a constructive simulation. For one, it would not need to send or receive information about unit positions since they are not needed for weather calculations.

The selection of IR for a particular CB can be based on

- a particular FOM module to test the correct implementation,
- a particular expected behaviour, which can be a combination of different FOM modules, or
- a particular event or exercise to make sure that all federates fulfil the requirements defined in the exercise specifications.

The Customer decides which CBs are tested and all passed CBs are listed on the certificate. The available Capability Badges and Interoperability Requirements are maintained in a "Badge Database", hosted by the CE.

3.4 Step 1: Self-Test

The self-test (see Figure 10) is the first and most important step on the way to a NATO interoperability certificate. Here, the Customer sets up the complete testing environment which includes downloading and installing the accredited version of the IVCT (see also chapter 4). Once this is done, the Customer should run the IVCT to verify that the SuT can successfully pass the next step, the certification test.

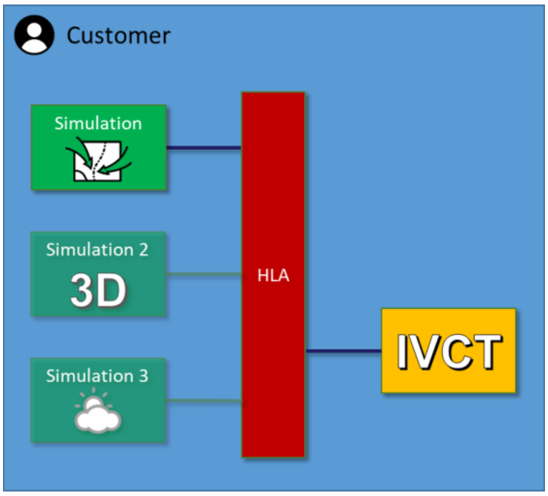

Figure 10: The self-test is the first step in the certification process and performed by the Customer alone.

The Customer performs the self-test alone and without interaction with any of the other key roles. That way the first step can take as much time as needed without any costs, commitments or promises to external stakeholders. Moreover, it builds the confidence that the testing environment is set up correctly and that the SuT will pass the certification test in the next step.

3.5 Step 2: Certification Test

The second and final step is the Certification Test (see Figure 11). This is the first time that the Customer gets in touch with the CE to request a certification. By doing so, the Customer specifies which SuT should be tested against which CB. The CE now uses this information to task a suitable ATI. The ATI inspect the testing environment build by the Customer in the previous step by verifying the correct use of the accredited version of the IVCT and associated test cases. Also, he or she collects the test results from the IVCT and confirms those IRs that cannot be tested by the IVCT.

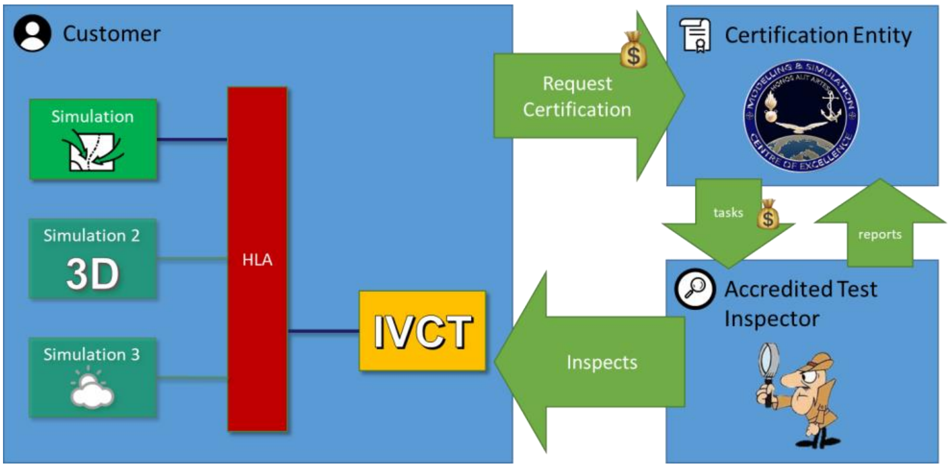

Figure 11: The certification test is the second step where an ATI inspects the test environment and collects test result to report them back to the CE.

The results of the certification test are reported back to the CE. Upon successful testing, the CE then issues a certificate to the customer stating the SuT and all passed capability badges.

In parallel, the CE also manages the payment for the certification services, which has to be made by the Customer directly to the CE. As a non-profit organization, the CE uses this payment to pay the ATI for his or her service as well as for maintaining the certification process and resources.

4 Integration, Verification and Certification Tool

4.1 Design Goals

Interoperability patterns, like the previously presented NATO Standards for federated simulation, are defining guidelines and rules to be respected by the federated systems. The consistent interworking of federates within a federation depends on the compliance of each federate against these rules. Breaking these rules may cause the federation to produce unreliable results. In some cases, this may crash a federate, or even worse, it may cause undetected corruptions to the federation. The primary purpose of the Integration, Verification and Certification Tool (IVCT) is to identify and resolve these issues early before integration.

The IVCT is essentially a software framework with an open architecture for defining interoperability requirements, and to implement and execute test cases to verify the compliance of systems against such requirements. The open architecture enables the simulation community to define and publish their interoperability requirements, and to contribute test cases to support the development and integration of compliant systems.

A further goal for the framework is to use a state-of-the-art technology stack and to leverage the "Modelling and Simulation as a Service" (MSaaS) approach, promoted by NATO Task Group MSG-164. The reasoning behind this goal is to make the software as accessible as possible to users and contributors, and have the flexibility to use the software without relatively too much deployment efforts.

The last high-level design goal to be mentioned here is the easy-to-use requirement. The IVCT shall be used without too much effort by any simulation tool developers providing testing capabilities, and by any simulation integrator to prevent federations becoming invalid by non-compliant federates.

4.2 Interoperability Testing

The IVCT approach to Interoperability Testing includes some key elements, as shown in Figure 12. The federation manager is responsible for setting up a set of federates which are behaving according to the federation agreements. These agreements include "Interoperability Requirements" (1), which are clearly defined rules to be respected by any federate. The Federate Owner must assure that its federate is respecting these rules and will behave accordingly. That guarantee will be expressed by the "Conformance Statement" (2) for the federate. Within that setup, the interoperability test is the task (3) to verify that all interoperability requirements selected by the federation manager, are covered by the conformance statement and fulfilled by the federate. As explained in chapter 3, this can be done during system development as self-testing, or it can be done officially to grant a certificate, proving the interoperability of a product.

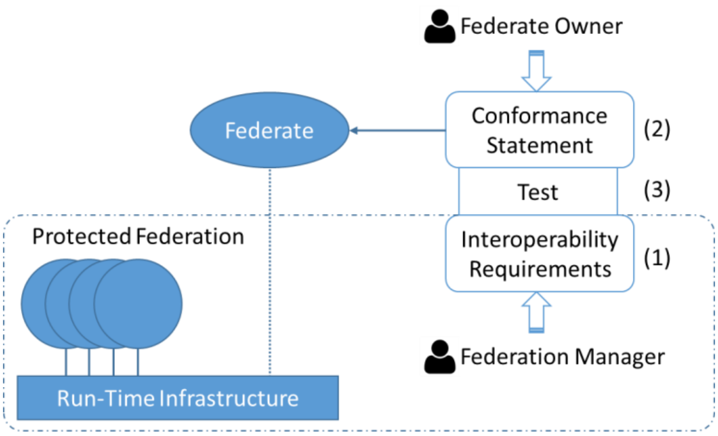

Figure 12: Protecting Federations with Interoperability Requirements.

In all cases the Interoperability rules for HLA-based federated simulations can be very simple, like basic publication patterns. Or they can be very complex, like a behaviour pattern in multi-role scenarios. To test such diverse patterns, the IVCT framework allows test cases to do anything a normal federate would be allowed to do. Figure 13 shows the interfaces and the role of a test case. Primarily, the test cases are just federates, sharing a federation with the System under Test, and optionally other federates required as an environment for the system to be tested. Just like any other federate, the test case is connected to the federation via an HLA interface. The only difference is, that the IVCT is requesting the use of an instrumented interface, in order to document the test case execution.

The connection between the test case and the IVCT framework is realized by the "AbstractTestCase" interface (a Java abstract class). That interface allows the IVCT to control the test case execution, and to collect the results of the test case. The test logic inside the test case is not restricted. It will typically implement some kind of state machines to verify behaviour protocols, and it will follow some timeline to cover different testing phases. A test case is allowed to trigger events into a federation, or it can just observe the system under test while it is interworking with a test environment.

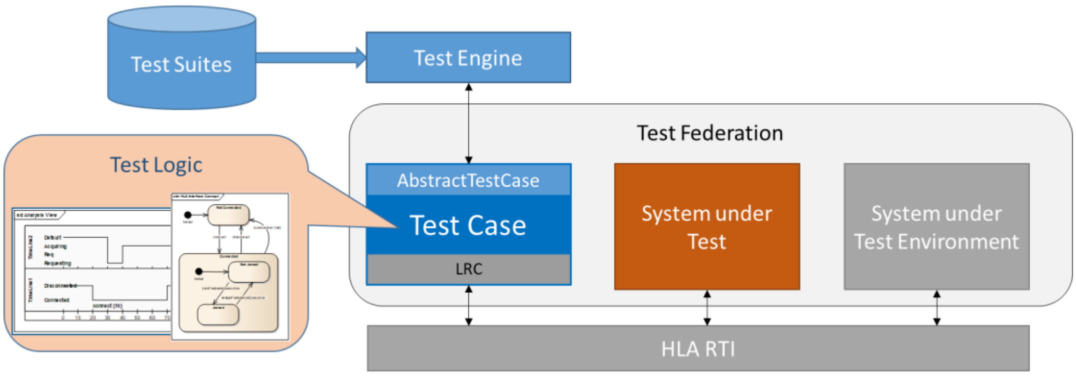

Figure 13: The IVCT Test Case.

4.3 Build and Deployment

Building and deploying a software framework can be quite laborious. Especially if it includes sources from multiple parties, built on proprietary software with diverse license models, and if it needs to communicate within diverse customer networks. Fortunately, the very popular container-based software delivery model helps to keep most of these problems away from the final user.

The IVCT software is maintained as Open Source Software on several GitHub repositories (see [4]). Everybody is allowed to download or clone these repositories and there is a Gradle-based build script to compile and install the software. That approach to building the software is intended to be used by the IVCT developers. For simply using the IVCT, the software is continuously being built by an automated process that generates docker images. These images can be downloaded into a local Docker Engine and are directly useable without any compilation or integration issues.

This approach is called "Continuous Integration", and the IVCT is using the Travis build Engine (see [7]). Figure 14 shows the elements in this build and deployment process. The IVCT developers (*IVCT Dev*) are maintaining the core components and are releasing software versions for the framework. Included into that framework are the test cases, developed and maintained by the Test Case Developers (*TS Dev*). Based on these releases, the Travis CI Engine builds and publishes the containerized and ready-to-use executable software. The final user, which is the operator of the IVCT (*IVCT Operator*), only needs to start-up the system in his local Docker Engine. The Docker Engine is free and also open-source software to run containerized applications, see [6] for details.

The IVCT Operator will normally use the IVCT via a web-based user interface. The connection to the "System under Test" (SuT), which is the federate to be tested, is done by the HLA Run-Time Infrastructure.

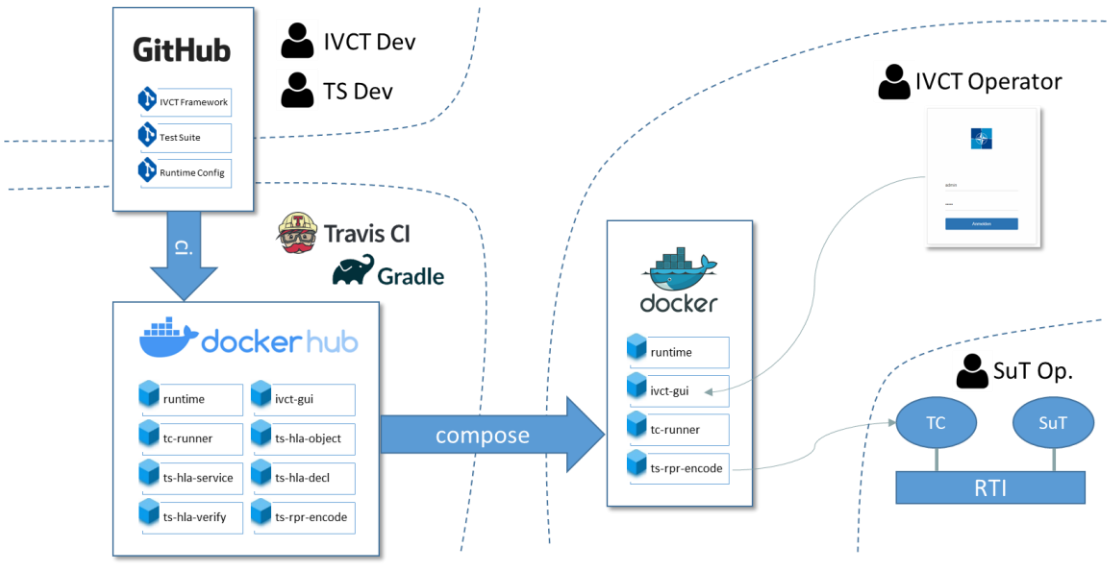

Figure 14: IVCT Build and Deployment.

4.4 IVCT Interface

The IVCT consists of several components which are interworking via an internal message bus, and are controlled by two different types of user interfaces. There is a basic command-line user interface for non-graphical server environments, and there is a web-based graphical user interface, which is probably the standard interface for most users.

Figure 15 shows an overview of the main views of the graphical user interface. The graphical user interface concepts of three different areas. The first area shows the defined “Badges”, the second area is for the installed “Testsuites” providing the available test cases, and the third area contains the configurations for the “System under Test”. A more detailed description of the user interface can be found in the documentation area of the IVCT Operation repository [4].

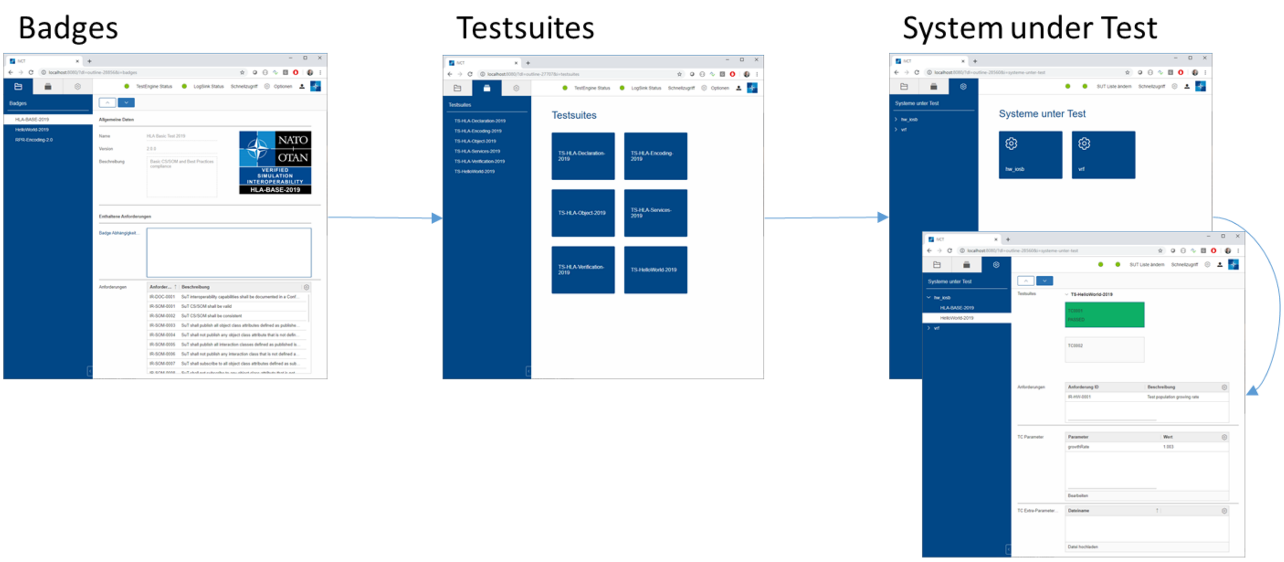

Figure 15: Web-based Interface for the IVCT.

5 Summary and Conclusions

NATO Standards for Federated Simulation are important to NATO in order to successfully connect and integrate multi-national M&S assets. The NATO Education and Training Network Federation Architecture and FOM Design (NETN FAFD) is a NATO M&S interoperability standard (STANREC 4800), based on the use of STANAG 4603 HLA and the SISO-STD-001 Real-Time Platform Reference FOM. This standard was initially released in 2011 and has evolved based on operational use by NATO and nations to its current version NETN FOM v2.0. The NETN FOM modules are recommended for use when implementing a NETN FAFD compliant distributed simulation. Several NETN FOM modules of this standard have been used in exercises such as the Viking series.

There is a continued need for NATO to experiment with, update and further evolve NATO Standards for Federated Simulation to meet new and evolving simulation interoperability requirements and to harmonize with new and evolving SISO standards.

Therefore NMSG tasked NATO Task Group MSG-163 to:

- update NETN FOM v2.0 based on feedback from nations,
- evolve the existing HLA Certification Service for verifying compliance against STANREC 4800 NETN FOM, and
- provide a tool (called IVCT) to support the Integration, Verification and Certification of individual federates' compliance.

Both the NETN FOM and the IVCT are managed as open-source projects on GitHub, enabling the user community to engage the developers and providing early access to releases. A draft release of NETN FOM v3.0 is expected in 2020. Furthermore, a Final Operating Capability (FOC) of the Certification Service, including the IVCT, is expected by the end of 2020.

Future directions for the NETN-FOM and the Certification Service include:

- Incorporate new FOM modules, developed by other NATO Task Groups (for example on the area of crisis management), or provided by SISO (for example Cyber);
- Leverage the new features of HLA-4 and provide design patterns on how to use these i.r.t. the NETN-FOM;
- Develop test cases for the new FOM modules and enhance existing test cases;
- And most importantly, use the IVCT, perform certification and collect lessons learned to improve the service, the tool, and the NETN FOM.

6 Acknowledgement

The authors would like to acknowledge the contributions of the MSG-163 team members for the ideas and results that are included in this paper.

7 References

[1] NATO Modelling and simulation Master Plan – Strategic Plan, 14 September 2012, AC/323/NMSG(2012)-015
[2] NATO Science and Technology Organisation, https://www.sto.nato.int
[3] NATO Distributed Simulation Federation Object Model (NETN FOM), https://github.com/AMSP-04
[4] NATO IVCT, https://github.com/IVCTool
[5] ITU-R M.1371-5, Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band, https://www.itu.int
[6] Docker Container Technology, https://www.docker.com
[7] Travis Continuous Build Service, https://travis-ci.org

8 Author Biographies

BJÖRN LÖFSTRAND is a senior systems architect in the area of modelling and distributed simulation design. Mr. Löfstrand has been engaged in national, international (SISO) and NATO M&S standardization activities for over 20 years participating in the development of standards like High-Level Architecture and engaging in multiple MSG projects addressing NATO standards for federated simulation. Mr. Löfstrand is a NATO Modelling and Simulation Group Member-at-Large and currently Mr. Löfstrand is the NMSG-163 FAFD activities lead. Mr. Löfstrand has a M.Sc. in Computer Science from the University of Linköping (Sweden) and he is the Services and Training Manager at Pitch Technologies.

Lieutenant Colonel TOBIAS KUHN is a German Army officer acting as the Modelling & Simulation Services Branch Chief at the NATO Modelling & Simulation Centre of Excellence (M&S COE) in Rome, Italy. He joined the German Bundeswehr in 1998 as a mechanized infantryman. After finishing his degree in Computer Science at the University of the Federal Armed Forces in Munich, Germany in 2005, he changed into the IT branch of the German Armed Forces. From 2012 to 2014, he studied at the Naval Postgraduate School in Monterey (CA), USA where he finished with two Masters of Science in Operations Research and Applied Mathematics. At the M&S COE he is responsible for wargaming and simulation-based analysis. Moreover, his branch also fulfills the role of the Certification Entity for NATO's HLA interoperability certification.

REINHARD HERZOG is leading the research group "Modelling and System Networking" at the Fraunhofer IOSB. He is responsible for the development of conformance test systems for various communication protocols and the design of communication infrastructures and integration middleware systems. Since 2012 Reinhard Herzog has been member of the NATO Modelling and Simulation Group "Enhanced CAX architecture, design and methodology (MSG-106) and was chairman of the NATO Modelling and Simulation Exploratory Team "Development of HLA Federates Compliance Testing Tool" (MSG-ET-035). Currently he is the NMSG-163 IVCTool activities lead.

HORST BEHNER is Technical Officer at the Bundeswehr Joint Materiel Office (BAAINBw) in Koblenz, Germa-ny. He received his M.Sc. degree in Physics from the University of Karlsruhe, Germany. The first five years he was responsible for the development of the trainer of the German Anti-Aircraft-Tank GEPARD (Cheetah) in Bavaria. Then he participated in the Exchange Program for Engineers and Scientists with the USA and worked as a Lead Engineer for one year with the US Navy at NAVAIR in Orlando, Florida. Back in Germany he became German Speaker and Chairman in several NATO MSGs. From 2005 to 2011, he was the German Liaison Officer for C4ISR at CERDEC in Fort Monmouth, New Jersey, and at the Center of Excellence Team C4ISR in Aberdeen Proving Ground, Maryland. Since fall of 2011, he is again German Speaker with several NATO MSGs and CapTech National Coordinator with the European Defense Agency (EDA).

TOM VAN DEN BERG is a senior scientist in the Modeling, Simulation and Gaming department at TNO, The Netherlands. He holds an M.Sc. degree in Mathematics and Computing Science from Delft Technical University and has over 25 years of experience in distributed operating systems, database systems, and simulation systems. His research area includes simulation systems engineering, distributed simulation architectures, systems of systems, and concept development & experimentation. Tom is a member of several SISO Product Development / Support Groups, participates in several NATO MSG activities, and is co-chair of NATO MSG-164 ("Modelling and Simulation as a Service (MSaaS)).