NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(MSG-134)TP/840

www.sto.nato.int

STO TECHNICAL REPORT **TR-MSG-134-Part-I**

NATO Distributed Simulation Architecture and Design, Compliance Testing and Certification

(Architecture et conception, essais de conformité et certification de la simulation distribuée de l'OTAN)

Final Report of NATO MSG-134.

Published September 2019

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(MSG-134)TP/840

www.sto.nato.int

STO TECHNICAL REPORT **TR-MSG-134-Part-I**

NATO Distributed Simulation Architecture and Design, Compliance Testing and Certification

(Architecture et conception, essais de conformité et certification de la simulation distribuée de l'OTAN)

Final Report of NATO MSG-134.

The NATO Science and Technology Organization

Science & Technology (S&T) in the NATO context is defined as the selective and rigorous generation and application of state-of-the-art, validated knowledge for defence and security purposes. S&T activities embrace scientific research, technology development, transition, application and field-testing, experimentation and a range of related scientific activities that include systems engineering, operational research and analysis, synthesis, integration and validation of knowledge derived through the scientific method.

In NATO, S&T is addressed using different business models, namely a collaborative business model where NATO provides a forum where NATO Nations and partner Nations elect to use their national resources to define, conduct and promote cooperative research and information exchange, and secondly an in-house delivery business model where S&T activities are conducted in a NATO-dedicated executive body, having its own personnel, capabilities and infrastructure.

The mission of the NATO Science & Technology Organization (STO) is to help position the Nations' and NATO's S&T investments as a strategic enabler of the knowledge and technology advantage for the defence and security posture of NATO Nations and partner Nations, by conducting and promoting S&T activities that augment and leverage the capabilities and programmes of the Alliance, of the NATO Nations and the partner Nations, in support of NATO's objectives, and contributing to NATO's ability to enable and influence security and defence related capability development and threat mitigation in NATO Nations and partner Nations, in accordance with NATO policies.

The total spectrum of this collaborative effort is addressed by six Technical Panels who manage a wide range of scientific research activities, a Group specialising in modelling and simulation, plus a Committee dedicated to supporting the information management needs of the organization.

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS System Analysis and Studies Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These Panels and Group are the powerhouse of the collaborative model and are made up of national representatives as well as recognised world-class scientists, engineers and information specialists. In addition to providing critical technical oversight, they also provide a communication link to military users and other NATO bodies.

The scientific and technological work is carried out by Technical Teams, created under one or more of these eight bodies, for specific research activities which have a defined duration. These research activities can take a variety of forms, including Task Groups, Workshops, Symposia, Specialists' Meetings, Lecture Series and Technical Courses.

The content of this publication has been reproduced directly from material supplied by STO or the authors.

Published September 2019

ISBN 978-92-837-2167-3

Table of Contents

List of Figures

List of Tables

List of Acronyms

AA	Accreditation Authority
AAR	After Action Review
AIMS	Architectures, Interoperability and Management of Simulation
AMSP	Allied Modelling and Simulation Publication
ATC	Abstract Test Case
ATL	Accredited Test Laboratory
ATS	Abstract Test Suit
AuxF	Auxiliary Federate
AuxS	Auxiliary Service
BGR	Bulgaria (NATO Country Code)
CA	Certification Agent
CAN	Canada (NATO Country Code)
CAX	Computer Assisted eXercise
CB	Capability Badge
CE	Certification Entity
CeAG	Certification Advisory Group
CFI	Connected Forces Initiative
CIGI	Common Image Generator Interface
CIS	Communication and Information System
COE	Centre of Excellence
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
CS	Conformance Statement
CSO	STO Collaboration Support Office
CWIX	Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise
CZE	Czech Republic (NATO Country Code)
DEU	Germany (NATO Country Code)
DIS	Distributed Interactive Simulation
DSA	Distributed Simulation Agreement
DSEEP	Distributed Simulation Engineering and Execution Process
DSTL	Defence Science and Technology Laboratory
DVCS	Distributed Version Control System
ET	Exploratory Team
ETC	Executable Test Case
EXCON	EXercise CONtrol
ESC	Exercise Specification Conference
FA	Focus Area
FAFD	Federation Architecture and FOM Design
FCC	Final Coordination Conference
FCTS	Federate Compliance Test System
FCTT	Federate Compliance Test Tool
FMN	Federated Mission Networking
FOM	Federation Object Model

FRA	France (NATO Country Code)
FTMS	Federate Test Management System
GBR	United Kingdom (NATO Country Code)
GMF	German Maritime FOM
GNU	GNU not unix
GOTS	Government Off-the-Shelf
GPL	GNU General Public License
GUI	Graphical User Interface
HLA	High Level Architecture
IED	Improvised Explosive Device
IEEE	Institute of Electrical and Electronics Engineers
I/ITSEC	Interservice / Industry Training, Simulation and Education Conference
IOC	Initial Operating Capability
IPC	Initial Planning Conference
IR	Interoperability Requirement
ISBN	International Standard Book Number
ITA	Italy (NATO Country Code)
ITEC	International Training and Education Conference
IVCT	Integration, Verification, and Certification Tool
JFTC	Joint Force Training Center
JMS	Java Message Service
JSON	JavaScript Object Notation
JWC	Joint Warfare Center
LAMP	Linux, Apache, MySQL, PHP
LCIM	Levels of Conceptual Interoperability Model
LGPL	GNU Lesser General Public License
MC	Military Committee
MEL	Master Event List
METOC	Meteorological and Oceanographic
MIL	Master Incident List
MOT	Means of Testing
MPC	Main Planning Conference
MPL	Mozilla Public License
MSCO	Modelling and Simulation Coordination Office
MSDL	Military Scenario Definition Language
MSG	Modelling and Simulation Group
MS3	Modelling and Simulation Standards Subgroup
M&S	Modelling and Simulation
NAC	North Atlantic Council
NATO	North Atlantic Treaty Organization
NC3B	NATO Consultation, Command and Control Board
NETN	NATO Education and Training Network
NMSG	NATO Modelling and Simulation Group
NRF	NATO Response Force
NSO	NATO Standardization Office
OMT	Object Model Template
OSS	Open Source Software

POL	Poland (NATO Country Code)
RPR	Real-Time Platform Reference
RTG	Research Task Group
RTI	Runtime Infrastructure
SISO	Simulation Interoperability Standards Organization
SIW	Simulation Innovation Workshop
SME	Subject Matter Expert
SOM	Simulation Object Model
STANAG	Standard NATO Agreement
STANREC	Standard NATO Recommendation
STO	NATO Science and Technology Organization
SuT	System under Test
SuTE	System under Test Environment
SuTO	System under Test Operator
SWE	Sweden (NATO Country Code)
SQL	Structured Query Language
TAP	Technical Activity Proposal
TC	Technical Column
TE	Test Engine
TL	Test Laboratory
URL	Uniform Resource Locator
USA	United States (NATO Country Code)
WAN	Wide Area Network

Glossary

Abstract Test Case	ISO/IEC 9646-1: A complete and independent specification of the actions required to achieve a specific test purpose (or a specified combination of test purposes), defined at the level of abstraction of a particular Abstract Test Method, starting in a stable state for testing and ending in a stable state for testing. This specification may involve one or more consecutive or concurrent connections.
Abstract Test Method	ISO/IEC 9646-1: The description of how an IUT is to be tested, given an appropriate level of abstraction to make the description independent of any particular realization of a Means of Testing, but with enough detail to enable tests to be implemented for this test method.
Abstract Test Suite	ISO/IEC 9646-1: A test suite composed of abstract test cases.
Accreditation	DoD M&S Glossary: The official certification that a model, simulation, or federation of models and simulations and its associated data are acceptable for use for a specific purpose.
Accreditation Authority (AA)	DoD M&S Glossary: The organization or individual responsible to approve the use of models, simulations, and their associated data for a particular application.
Accredited Test Laboratory	A Test Laboratory which has been accredited by an Accreditation Authority to perform Compliance Testing.
Capability Badge	A token of achievement in terms of passing a test related to Interoperability Requirements.
Certification Agent	An entity or person that has been approved by the Accreditation Authority to perform Compliance Testing.
Certification Artefact	IEEE-24765-2010: The tangible results from a certification process.
Certification Criteria	IEEE-24765-2010: A set of standards, rules, or properties to which an asset must conform in order to be certified to a certain level.
Certification Process	IEEE-24765-2010: The process of assessing whether an asset conforms to predetermined certification criteria appropriate for that class of asset.
Certification Property	IEEE-24765-2010: A statement about some feature or characteristic of an asset that may be assessed as being true or false during a certification process.
Certification Test	Test done during the Certification Process.
Certification	IEEE-24765-2010: The process of confirming that a system or component complies with its specified requirements and is acceptable for operational use.
Compliance	The statement that an asset fulfils the required behaviour rules of a given standard.

Compliance Certificate	Adapted from IEEE-24765-2010: A written guarantee that a system or component complies with its specified requirements and is acceptable for operational use.
Compliance Testing	The process of testing the behaviour of an asset against a given standard conducted by the test tool.
Concept of Operations	IEEE 1362-1998: A ConOps is a user-oriented document that describes system characteristics for a proposed system from the users' viewpoint. The ConOps document is used to communicate the overall quantitative and qualitative system characteristics to the user, buyer, developer and other organizational elements (e.g., training, facilities, staffing and maintenance). It is used to describe the user organization(s), mission(s) and organizational objectives from an integrated systems point of view.
Conformance	In this document, conformance is considered to be a synonym to Compliance.
Conformance Statement	A written statement that confirms the conformance of a SuT (System under Test) to a given standard.
Customer	An entity (or a person) who has sufficient legal rights to submit a given federate to compliance testing and to allow the CA to publically announce the compliance of the SuT (System under Test).
Federate	IEEE-1516-2010: An application that may be or is currently coupled with other software applications under a Federation Object Model (FOM) Document Data (FDD) and a runtime infrastructure (RTI).
Federate Owner	An entity (or a person) who has legal ownership rights to a given federate.
Federation	IEEE-1516-2010: A named set of federate applications and a common Federation Object Model (FOM) that are used as a whole to achieve some specific objective.
Integration, Verification, and Certification Tool (IVCT)	Software framework to support integration and verification task for simulation federates and to perform the certification tests for a SuT (System under Test).
Means of Testing	ISO/IEC 9646-1: The combination of equipment and procedures that can perform the derivation, selection, parameterization and execution of test cases, in conformance with a reference standardized ATS, and can produce a conformance log.
Science Connect	Collaborative Workspace provided by NATO CSO.
System under Test (SuT) (SuT)	The System which is the target of Compliance Testing. An SuT is an instance of an asset.
Test	IEEE-829-2008: The activity of executing a Test Procedure/Test Case.
Test Case	IEEE-829-2008: A set of test inputs, execution conditions, and expected results developed for a particular objective, such as to exercise a particular program path or to verify compliance with a specific requirement.
Test Case Developer	Individuals / organizations responsible for the design, implementation and maintenance of the test cases.

Test Class	IEEE-829-2008: A designated grouping of test cases.
Test Federate	A member application that is part of the IVCT and that tests whether the SuT (System under Test) complies with (a subset of) the federation agreements.
Test Laboratory	An entity which has the technical capabilities to perform the tests specified for a SuT (System under Test), but has not been accredited (see ATL).
Test Procedure	IEEE-829-2008: Detailed instructions for the set-up, execution, and evaluation of results for a given test case.
Test Tool Developer	Individuals / organizations responsible for design, implementation and maintenance of the certification tool.
WebEx	Web-based teleconferencing system provided by NATO CSO.

MSG-134 Membership List

CO-CHAIRS

Mr. Horst BEHNER*
Bundeswehr
GERMANY
Email: horstbehner@bundeswehr.org

ICT José RUIZ*
French MoD
FRANCE
Email: jose.ruiz@intradef.gouv.fr

MEMBERS

Dr. Martin ADELANTADO
ONERA
FRANCE
Email: Martin.Adelantado@onera.fr

LTC Raniero CASTROGIOVANNI (OF4)
NATO M&S CoE
ITALY
Email: mscoe.cd02@smd.difesa.it

MAJ. Lubomir CHYLIK
JCBRN Defence COE
CZECH REPUBLIC
Email: chylikl@jcbrncoe.cz

Major Mario DE LA FUENTE
ES MoD/INTA
SPAIN
Email: mariodlf@et.mde.es

Dr. (Col Rtd) Yuri FEDULOV
United Institute of Informatics Problems
BELARUS
Email: fynhome@hotmail.com

Mr. Allan GILLIS*
DRDC – Atlantic Research Centre
CANADA
Email: allan.gillis2@forces.gc.ca

Mr. Maurizio GLADIORO
SELEX ES
ITALY
Email: maurizio.gladioro@selex-es.com

Mr. Reinhard HERZOG*
Fraunhofer IOSB
GERMANY
Email: Reinhard.Herzog@iosb.fraunhofer.de

LTC. Jan HODICKY*
University of Defence
CZECH REPUBLIC
Email: Jan.Hodicky@seznam.cz

Mr. Antony HUBERVIC
Masa Group
FRANCE
Email: antony.hubervic@masagroup.net

Mr. Magnus KARPERYD
FMV
SWEDEN
Email: magnus.karperyd@fmv.se

Mr. Bjorn LOFSTRAND*
Pitch Technologies AB
SWEDEN
Email: bjorn.lofstrand@pitch.se

Mr. Régis MAUGET*
Capgemini Technology Services
FRANCE
Email: regis.mauget@capgemini.com

LTC Jan MAZAL
NATO M&S CoE
ITALY
Email:mscoe.det01@smd.difesa.it

* Contributing Author.

Capt(N) Vincenzo MILANO
STATO MAGGIORE DIFESA
ITALY
Email: sesto.mes@smd.difesa.it

Mr. Johannes MULDER
Fraunhofer IOSB
GERMANY
Email: Johannes.Mulder@iosb.fraunhofer.de

Col. Orlin NIKOLOV
NATO CMDR CoE
BULGARIA
Email: orlin.nikolov@cmdrcoe.org

Mr. Lennart OLSSON
Pitch Technologies AB
SWEDEN
Email: lennart.olsson@pitch.se

Lt. Juan Jose PEREZ CONSUEGRA
ITM/INTA
SPAIN
Email: jpercon@oc.mde.es

Mr. Marco PICOLLO*
Finmecanica
ITALY
Email: marco.picollo@finmeccanica.com

Mr. Nils SMEDBERG
FMV
SWEDEN
Email: nils.smedberg@fmv.se

Mr. Stefan VRIELER*
Technical Center for Weapons and
Ammunition (WTD 91)
GERMANY
Email: stefanvrieler@bundeswehr.org

ADDITIONAL CONTRIBUTING AUTHORS

Mr. Adam BROOK
QinetiQ
UNITED KINGDOM
Email: rabrook@qinetiq.com

* Contributing Author.

NATO Distributed Simulation Architecture and Design, Compliance Testing and Certification

(STO-TR-MSG-134-Part-I)

Executive Summary

Integration of distributed simulations and tools into interoperable federations of systems is a complex and time-consuming task, requiring extensive testing of individual components, interfaces, and an integrated solution. To support this task NATO relies on standards and agreements as well as their consistent application. Improving the interoperability, reuse, and cost effectiveness of Modelling and Simulation (M&S) when integrating solutions to support NATO and national simulation and training, is a long-term goal with several challenges. An incremental and iterative approach for harmonizing distributed simulation federation agreements is required to cope with issues related to legacy systems, multiple architectures, new advances in Information Technology (IT) and software technologies, industry adoption of standards, new business models, and the process of developing open standards.

Standards, federation agreements, compliance testing, and certification are important tools that reduce integration time, diminish risks, increase reuse of existing systems, and support procurement of new interoperable simulation components. New and updated standards for simulation interoperability, such as High Level Architecture (HLA), require the NATO simulation certification service to be continuously maintained and updated to manage more complex test cases using the latest versions of applicable standards. Certification of simulation components requires additional testing beyond the core HLA services interface, and should also include testing of compliance with federation agreements.

Within the M&S community, it is generally recognized that the technical interoperability between systems is no longer a fundamental problem. High-level interoperability, however, is still considered a major challenge in establishing reliable and trusted federations of distributed simulations. The required degree of interoperability not only depends on the purpose and objectives of the simulation system, but also on the federation design and interoperability capabilities of specific system components. Early identification of interoperability issues reduces risk, and the costs associated less interoperable system components. A high degree of interoperability allows more flexible federation designs, and composability of simulation systems, without significantly increasing the risk and costs associated with test and integration.

Depending on the degree of interoperability between participating simulation components, the integration of federates into complex federations can be a time-consuming and ambitious task. Tools, processes, and services to support early detection of interoperability issues will significantly reduce integration time and cost. Verification of compliance with standards and interfaces is not only relevant to support certification, but can also be valuable for system integrators, and simulation system developers.

Compliance testing of system components to interoperability standards and agreements is the basis for the verification of interoperability. Testing and verification of simulation components' interoperability capabilities is fundamental for enabling rapid design and integration of heterogeneous distributed simulation systems. Readily available, up-to-date, and trusted tools are keys to supporting compliance testing.

A certification service can provide unbiased compliance testing of a System under Test (SuT) against a set of Interoperability Requirements (IR) based on conformance statements. Certificates are provided by authorized Certification Entities (CE) and are tokens of achieved compliance with interoperability requirements. Simulation components are required to have, or obtain, certificates to be candidates for procurement or for acceptance testing as specified in STANAG 4603.

MSG-134 was tasked with establishing a NATO Simulation Interoperability Test and Certification Service, based on existing standards and experiences from using previous tools and certification processes. The focus and priority of the MSG-134 project was to provide tools for certification services based on HLA and the NATO Education and Training Network (NETN) Federation Architecture and FOM Design (FAFD). This Service is composed of tools, processes, and organizations that manage and provide testing, verification, and certification of simulation components to enable efficient integration.

In 2016, the MSG-134 established the Certification Service and it was used during the CWIX 2017 experimentation for the first time, where it proved its functional capability.

Architecture et conception, essais de conformité et certification de la simulation distribuée de l'OTAN

(STO-TR-MSG-134-Part-I)

Synthèse

L'intégration des simulations distribuées et des outils en fédérations interopérables de systèmes est une tâche complexe et chronophage, qui requiert une solution intégrée et l'essai complet de chaque composant et interface. Dans ce but, l'OTAN s'appuie sur des normes et des accords, ainsi que sur leur application cohérente. Lorsque des solutions sont intégrées pour soutenir la simulation et l'entraînement de l'OTAN et des pays, il est souhaitable d'améliorer l'interopérabilité, la réutilisation et la rentabilité de la modélisation et simulation (M&S). Il s'agit d'un objectif à long terme et les défis ne manquent pas. Une démarche progressive et itérative d'harmonisation des accords fédérant la simulation répartie est nécessaire pour traiter les problèmes liés aux systèmes hérités, aux architectures multiples, aux nouveaux progrès des technologies de l'information (TI) et des logiciels, à l'adoption de normes par le secteur, aux nouveaux modèles économiques et au processus d'élaboration de normes ouvertes.

Les normes, les accords de fédération, les essais de conformité et la certification sont des outils importants qui réduisent les délais d'intégration et les risques, accroissent la réutilisation des systèmes existants et soutiennent l'approvisionnement en nouveaux composants de simulation interopérables. Les normes d'interopérabilité de la simulation, nouvelles et actualisées, telles que l'architecture de haut niveau (HLA), imposent le maintien et la mise à jour continue du service de certification de la simulation de l'OTAN pour gérer les cas d'essai plus complexes à l'aide des dernières versions des normes en vigueur. La certification des composants de la simulation exige des essais supplémentaires, au-delà de l'interface centrale des services HLA, et devrait également inclure des tests de conformité aux accords de fédération.

Au sein de la communauté de M&S, il est généralement admis que l'interopérabilité technique entre systèmes n'est plus un problème fondamental. En revanche, l'interopérabilité de haut niveau est toujours considérée comme un défi de taille dans l'établissement de fédérations fiables et validées de simulations distribuées. Le degré d'interopérabilité nécessaire dépend non seulement de la finalité et des objectifs du système de simulation, mais également de la conception de la fédération et des capacités d'interopérabilité de certains composants du système. L'identification précoce des problèmes d'interopérabilité réduit le risque et les coûts associés à des composants de système moins interopérables. Un haut niveau d'interopérabilité permet des modèles de fédération plus souples et la composabilité des systèmes de simulation, sans augmenter significativement le risque ni les coûts associés aux essais et à l'intégration.

En fonction du degré d'interopérabilité entre les composants participant à la simulation, l'intégration de fédérés dans des fédérations complexes peut être une tâche ambitieuse et chronophage. Les outils, processus et services facilitant la détection précoce des problèmes d'interopérabilité réduiront sensiblement le délai et le coût de l'intégration. La vérification de la conformité aux normes et interfaces est non seulement pertinente pour soutenir la certification, mais peut s'avérer précieuse pour les intégrateurs de systèmes et les développeurs de systèmes de simulation.
Les essais contrôlant la conformité des composants de système aux normes et accords d'interopérabilité forment la base de la vérification de l'interopérabilité. Les tests et la vérification des capacités

d'interopérabilité des composants de simulation sont fondamentaux pour la conception et l'intégration rapides de systèmes hétérogènes de simulation répartie. La disponibilité immédiate, la mise à jour et la validation des outils sont essentielles au soutien des tests de conformité.

Un service de certification peut réaliser des essais de conformité non biaisés d'un système à tester par rapport à un ensemble de besoins d'interopérabilité basés sur les déclarations de conformité. Les certificats sont fournis par les organismes de certification homologués et indiquent la conformité aux besoins d'interopérabilité. Les composants de simulation doivent avoir, ou obtenir, un certificat pour pouvoir être achetés ou passer les essais d'acceptation selon les spécifications du STANAG 4603.

Le MSG-134 était chargé d'établir un service OTAN d'essai et de certification de l'interopérabilité de la simulation, à partir des normes existantes et de l'expérience d'utilisation des précédents outils et processus de certification. La priorité du MSG-134 était de fournir des outils servant à la certification, fondés sur la HLA et sur l'architecture de fédération et la conception des modèles d'objets fédérés (FAFD) du Réseau OTAN de formation et d'entraînement (NETN). Ce service se compose d'outils, de processus et d'organismes qui gèrent et fournissent des essais, une vérification et la certification des composants de simulation pour permettre une intégration efficace.

En 2016, le MSG-134 a mis en place le service de certification, qui a été utilisé pour la première fois pendant l'expérimentation CWIX 2017, où il a démontré sa capacité fonctionnelle.

Chapter 1 – INTRODUCTION

1.1 BACKGROUND AND JUSTIFICATION

The integration of distributed simulations and tools into interoperable federations is a complex and time-consuming task requiring extensive testing of individual components, interfaces, and the integrated solution. To support this task, NATO relies on standards and agreements on their use. The Allied Modelling and Simulation Publication AMSP-01, NATO M&S Standards Profile, provides a list of recommended M&S related standards. The NETN Federation Architecture and FOM Design Document (NETN FAFD) developed by MSG-068 and MSG-106 provides additional agreements on the use of standards to support distributed simulation.

STANAG 4603 is identified as one of the core standards for distributed simulation. It states that participating nations agree to utilize the HLA Compliance Certification Process established by the NATO Modelling and Simulation Group (NMSG). The current software used, the HLA Federation Compliance Test Tool (FCTT), was developed by the USA and released to NATO in 2004. Since that time, the USA has made updates to the FCTT but has been unable to release the updated FCTT due to export restrictions. MSG-ET-035 investigated the feasibility of developing an open source version of the FCTT that would be available to all NATO and partner nations, but it was determined that the FCTT cannot be used as the foundation for a future certification tool. MSG-ET-035 also concluded that the compliance testing of HLA needs to be extended beyond the HLA interface and data exchange testing to address more complex federation agreements and requirements.

Standards, federation agreements, compliance testing, and certification are important tools that will reduce integration risks, increase reuse of existing systems, and support procurement of new interoperable simulation components. MSG-134 researches and delivers:

1) Maintenance and update of the NETN FAFD; and
2) The procedures and the Integration Verification and Certification Tool (IVCT) to support compliance testing and certification of NETN FAFD compliant simulation components, including certification against STANAG 4603.

1.2 OBJECTIVES

The objectives of the MSG-134 were the following:

- Coordination with other MSG task groups to promote use of FAFD and incorporation of MSG task group results;
- Maintenance of NETN FAFD including update and release of new versions of the technical specification;
- Dissemination of NETN FAFD through presentations, papers and standardization activities within NMSG, SISO, and other venues;
- Development of test, verification, and certification procedures;
- Design and implementation of IVCT to support certification, integration, and verification of federates in specific federations; and
- Development of IVCT tests to support NETN FAFD test, verification, and certification.

1.3 TOPICS COVERED

The topics covered by the MSG-134 were the following:

- Update and maintain NETN FAFD based on user feedback;
- Develop NETN FAFD compliance testing procedure and test cases;
- Design IVCT based on available Use Cases and Requirements;
- IVCT implementation in three one-year phases:
  - 1st year: Implement the first prototype able to test Conformance statement;
  - 2nd year: Implement test cases for Integration and Verification purposes;
  - 3rd year: Implement the whole IVCT infrastructure; and
- Set up data flow among all entities in IVCT processes.

Chapter 2 – PROGRAM OF WORK

2.1 DELIVERABLES

MSG-134 is not only focused on producing research papers, presentations and technical reports; a main deliverable is a software package to support integration, verification, and testing of simulation interoperability (see Table 2-1). A supporting database for maintaining information about interoperability requirements and capability badges used in certification is also delivered.

Table 2-1: Deliverables of MSG-134.

Deliverable	Format
NATO Simulation Interoperability Test and Certification Service – Concept of Operations (CONOPS)	Document
IVCT software and documentation	Open source – GitHub
NETN FAFD published as AMSP-04 covered by STANREC 4800	Document
Papers, presentations, publications and marketing material	Papers and presentations
Technical Report	Document

2.2 PLANNING

MSG-134 was initiated in December 2014 and ran for three years, from 2015 to 2017. During this period, the activities of the group were focused on two domains:

- The definition of the certification process (CONOPS), the development of a software suite to support the certification activity, and the initial trial of these tools during an exercise (i.e., CWIX 2017); and
- The support of the NATO process for setting the NETN FOM as a standard recommendation (STANREC).

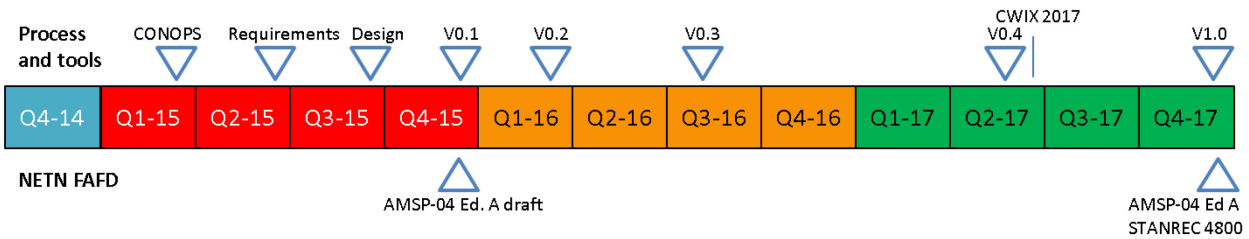

Figure 2-1: Planning of MSG-134.

The software suite (main core IVCT, executable test cases, and capability badge database) was developed in a collaborative process among the MSG-134 members and provided to NATO as an Initial Operational Capability (IOC) for HLA certification. The status of the work was continuously disseminated during multiple M&S events (ITEC, I/ITSEC, SISO SIW, CAX Forum), as is indicated in Figure 2-2, below.

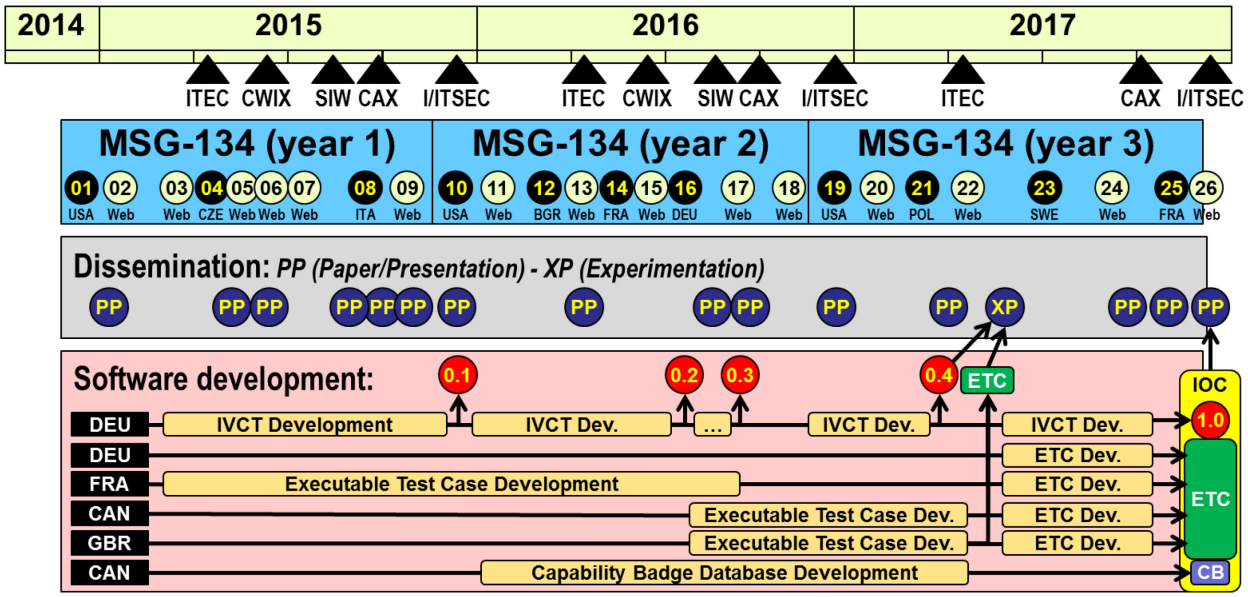

Figure 2-2: Planning of Software Development and Results Dissemination.

During MSG-134, a total of twenty-six meetings were held (fifteen by using WebEx support and eleven in face-to-face). In addition to this, a number of technical WebEx sessions were conducted.

2.3 ACTIVITIES

The work in MSG-134 was organized by activities and categorized as Organizational, IVCT-related, FAFD-related or Management-related. No subgroups were formed, and all members of MSG-134 participated in each activity. See Table 2-2, below.

Table 2-2: Activities of MSG-134.

Activity	Main Deliverable
Concept of Operations Development	NATO Simulation Interoperability Test and Certification Service – Concept of Operations (CONOPS)
NETN FAFD Maintenance	AMSP-04 (STANREC 4800)
IVCT Development	IVCT software and documentation
Capability Badges Database	Database structure and initial content
Experimentation during CWIX 2017	Feedback on IVCT and CONOPS
Dissemination	Final Report, papers and presentations

2.3.1 CONOPS Development

MSG-134 has defined roles and responsibilities, key concepts and components, as well as the business model for a NATO Simulation Interoperability Test and Certification Service. The CONOPS deliverable [1] is available with detailed information about the certification service. See Figure 2-3, below.

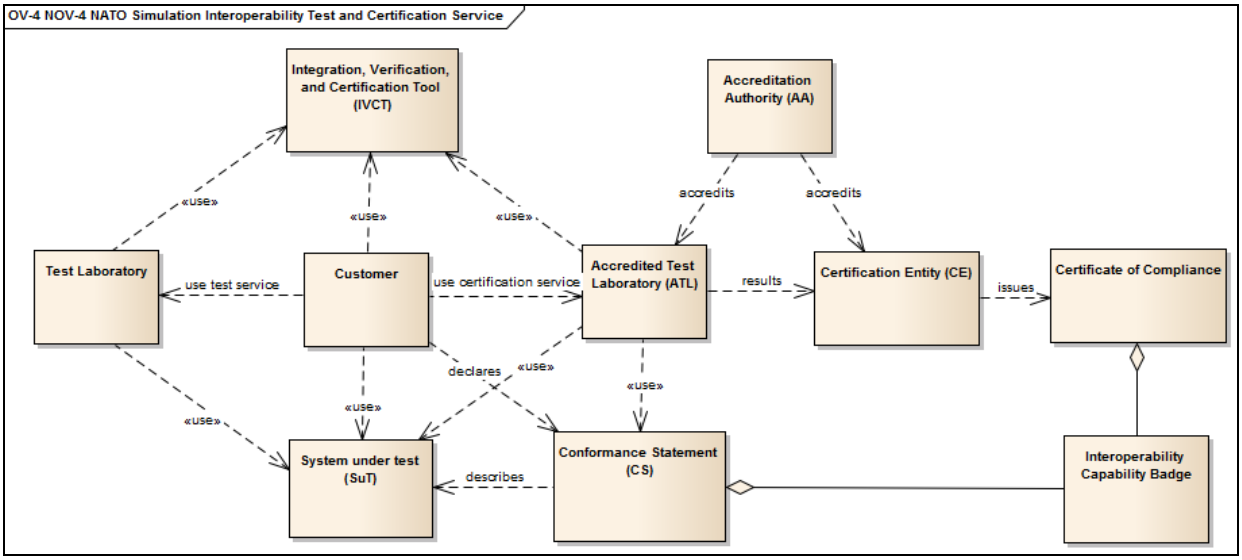

Figure 2-3: Summary of CONOPS Key Aspects.

2.3.1.1 Key Roles and Responsibilities

- The **Accreditation Authority** (AA) is a NATO-appointed organization responsible for maintaining the business model and procedures used by Accredited Test Laboratories (ATL) and Certification Entities (CE).
- The **Certification Entity** (CE) is an organization with the authority to issue certificates of compliance to systems that have successfully passed testing of Interoperability Requirements (IR). The CE is responsible for the management aspects of certification and is the initial point of contact for customers that want to certify their system with the right to refuse the certification. The CE also maintains the official version of the Integration, Verification and Certification Tool (IVCT) and delivers it, along with the executable test cases, to accredited test laboratories.
- An **Accredited Test Laboratory** (ATL) is a test laboratory given the official authority by the CE to perform certification tests of interoperability requirements and whose test results are recognized by the CE as being valid for issuing certificates of compliance.

2.3.1.2 Key Concepts and Components

- A simulation **Interoperability Requirement** (IR) is related to how distributed systems interact and exchange information in order to collectively meet overall simulation objectives. IRs are specified to ensure that a system component can be easily combined and interoperate with other system components. The ability of a system to interoperate can be described as the set of fulfilled IR requirements.
- An Interoperability **Capability Badge** (CB) is defined as a token of achievement in terms of passing testing related to interoperability requirements (IR) associated with the CB. Successful compliance testing, verification, and certification of a system's compliance with sets of IRs can be expressed as a set of CBs representing this achievement.
- An **Abstract Test Case** (ATC) is a complete, implementation-independent specification of the actions required to verify a specific test purpose expressed as a set of interoperability requirements (IR) associated with the ATC.
- An **Executable Test Case** (ETC) is a script or compiled program that can execute as part of IVCT to implement the ATC procedure for verifying the associated IRs.

- **The Integration, Verification and Certification Tool** (IVCT) is a core technical framework provided by the Certification Entity (CE) and used to support test and verification of simulation interoperability requirements.
- A **Conformance Statement** (CS) is a written statement declaring a system's compliance with identified interoperability requirements. A CS is provided by the owner of the System under Test (SuT) to identify which standard sets of IRs the SuT should be certified against. In the CS, the sets of IRs are referenced as Capability Badges (CB).
- A **System under Test** (SuT) is the simulation system, which is the target of compliance testing.

Figure 2-4, below, shows the relationships between the requirements, the abstract and executable test, the IVCT, and the SuT. The System under Test (SuT) is certified against a Conformance Statement (CS), expressed as a set of interoperability Capability Badges (CB) identifying the SuT Interoperability Requirements (IRs). Abstract Test Cases (ATCs) describe how the IRs are tested, and these are implemented in Executable Test Cases (ETCs). The Integration Verification and Certification Tool (IVCT) uses ETCs to execute tests and to verify SuT compliance with IRs. An SuT that successfully completes verification can receive a certificate and CBs as tokens of interoperability compliance.

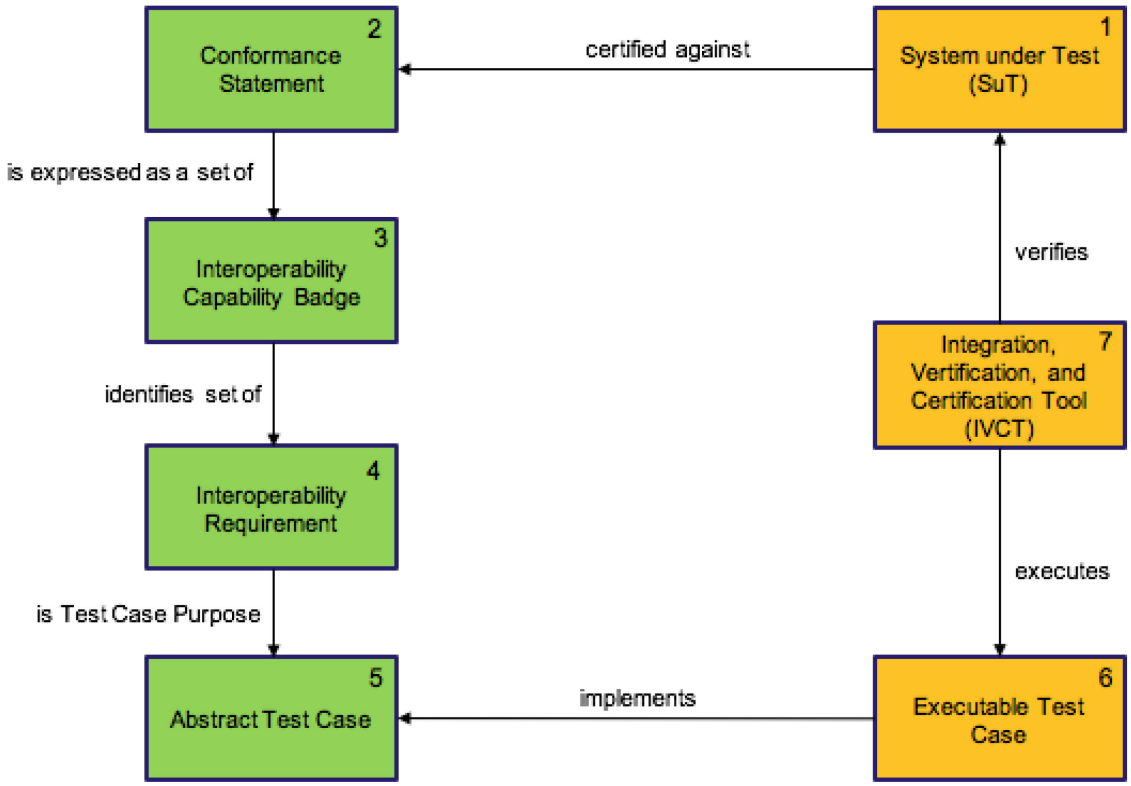

Figure 2-4: Overview of Certification Process.

2.3.1.3 Business Model

Business of Certification Activity

Nations participating in MSG-134 have designed and developed IVCT version 1.0. The NMSG delivered this version to the CE, which is responsible for maintenance of the IVCT.

ATLs will provide feedback on IVCT to the CE. The CE maintains the list of IVCT requirements and gets approval from the AA for IVCT updates. The CE may conduct updates itself or participate in collaborative efforts initiated by the AA.

MSG-134 has developed the first set of Abstract Test Cases and corresponding Executable Test Cases. The AA is responsible for managing all Capability Badge definitions and prioritization. The CE is responsible for abstract and executable test case development. The AA supports the CE by providing SME contacts to help define abstract test cases for particular badge/interoperability requirements.

The primary customers of certification services and use of the IVCT have been identified as:

- NATO organizations and NATO partner nations' government organizations providing certification services;
- Procurement agencies and supporting organizations for acquisition of distributed simulation systems;
- Simulation System Integrators (10-50 NATO-wide); and
- Simulation System Developers (50-100 COTS/GOTS vendors willing to certify their systems).

It is hard to estimate the exact size of the market for the proposed system. The market for the IVCT is substantially larger than the certification service since it can be used by any simulation system developer and integrator in many contexts.

The 28 NATO nations and 42 partner nations are the primary stakeholders of the certification service. The number of systems used and integrated in these nations to support activities (e.g., training and exercises) will define the level of utilization of the certification service. Based on existing certification services provided, we estimate that a fully functional and operational service will conduct 10-20 certifications per year. Initial Operating Capability (IOC) is estimated to conduct 5-10 certifications per year.

IOC is expected to include a single ATL, with 5-10 customers, conducting interoperability tests and verification for an average of 7 Capability Badges per customer.

MSG-134 proposes one option for a business model to fund development and maintenance of the Certification Service Process and Tools: A customer-funded business model with income streams to cover the cost of the certification process.

Customer-Funded Business Model

Early Development (2015-2017): MSG-134 developed a first business model and the nations participating in MSG-134 funded the development of the IVCT, resulting in version 1.0 of the IVCT, as well as developing some ETCs.

Initial Operational Capability (2018-2020): During this period, MSG-134 suggests continuing the previous business model of having participating nations of the MSG-134 follow-on activity fund the continued development of the IVCT and ETCs.

The follow-on of MSG-134 will act as the ATL, and the NATO M&S COE will act as the CE during this period.

Certification for the customer will be free of charge during this period.

Fully Operational Capability (2021 and Beyond): During this period, ATLs will be established, and the NATO M&S COE continues to act as the CE.

IVCT maintenance and ETC development will be funded by:

- A yearly fee defined by the AA, paid by the ATLs to the CE for the maintenance of the IVCT; and
- Fees paid by the customer to the ATLs on the basis of the specific CB requested. Part of this fee will be transferred to the CE for further development of the IVCT and for development of new ETC as needed and agreed by the AA.

The AA together with the CE defines the fee for Badge Certificates paid by ATLs to CE.

ATLs will be responsible for establishing the cost of certification testing for their customers.

2.3.1.4 Key Findings

The Business model should be exercised to gain more knowledge, experience and lessons learned, and to adjust this business model.

2.3.2 NETN FAFD Maintenance

The NETN FAFD maintenance had two main activities: receiving, processing and managing comments, questions and feedback on the NETN FAFD, and publishing the NETN FAFD as AMSP-04 by the NATO Standardization Office (NSO). The NETN FAFD Maintenance also included receiving and evaluating proposals for new simulation and modelling areas that could be added to the NETN FOM.

Tasks:

- Created support email (msg@cso.nato.int) for AMSP-04 feedback;
- Investigated possibilities for quick FAFD publication (as delivered by MSG-106) to get feedback as soon as possible; and
- Post-FAFD on CSO Web (Science Connect), including instructions on how to provide feedback.

The process for submitting and reviewing changes to FOMs and new FOMs was managed by MSG-134 and involved exchange of information made by experts in the field.

The following proposals for updating and extending the NETN FAFD have been received (see Table 2-3):

Table 2-3: Main Proposals for Updating and Extending the NETN FAFD.

Module	Description of Change Proposal
Update of NETN-Physical	A specialization of object class RPR-Physical_v2 BaseEntity.PhysicalEntity.Munition is needed to match the NETN object class style: • NETN_Munition.
Update of NETN-LBML	There is a need for more tasks that can be assigned to entities, following tasks have been identified: Patrol; Establish Checkpoint; Operate Checkpoint; Magic Move; Stop at Side of the Road Set Sensor Mode; Set Area of Interest; Fixed Wing Takeoff; Fixed Wing Land; Orbit; Inert IED.

Module	Description of Change Proposal
FOM Module for MSDL	To publish the MSDL ORBAT in a NETN federation, a FOM module describing the information is needed. This implies that an application will get the ORBAT either by reading the MSDL file or by subscribing to the information.
FOM Module for Synthetic Environment	The synthetic environment needs to be extended in NETN. The following object class that inherits from RPR object classes is suggested: • CheckPoint (inherits from RPR-SE_v2 EnvironmentObject.PointObject.OtherPointObject).
FOM Module for MEL/MIL	The use of Master Event List (MEL) / Master Incident List (MIL) applications is common in CAX to support the EXCON and gaming cells, which guide the exercise toward the training objectives. Key information related to scripted events, incidents, and injects can be related to simulation control actions, simulated events, and state changes. In order to better support After Action Review (AAR), there is a need to create these relationships in the data produced by the simulation environment. The proposed FOM module is intended to allow publication of MEL/MIL-related data in an HLA federation with key information regarding the units involved, the geographical area, and other information needed by simulations to determine if and when to include references to the MEL/MIL when publishing simulation data. The FOM also includes specification of operators and simulation instructions.

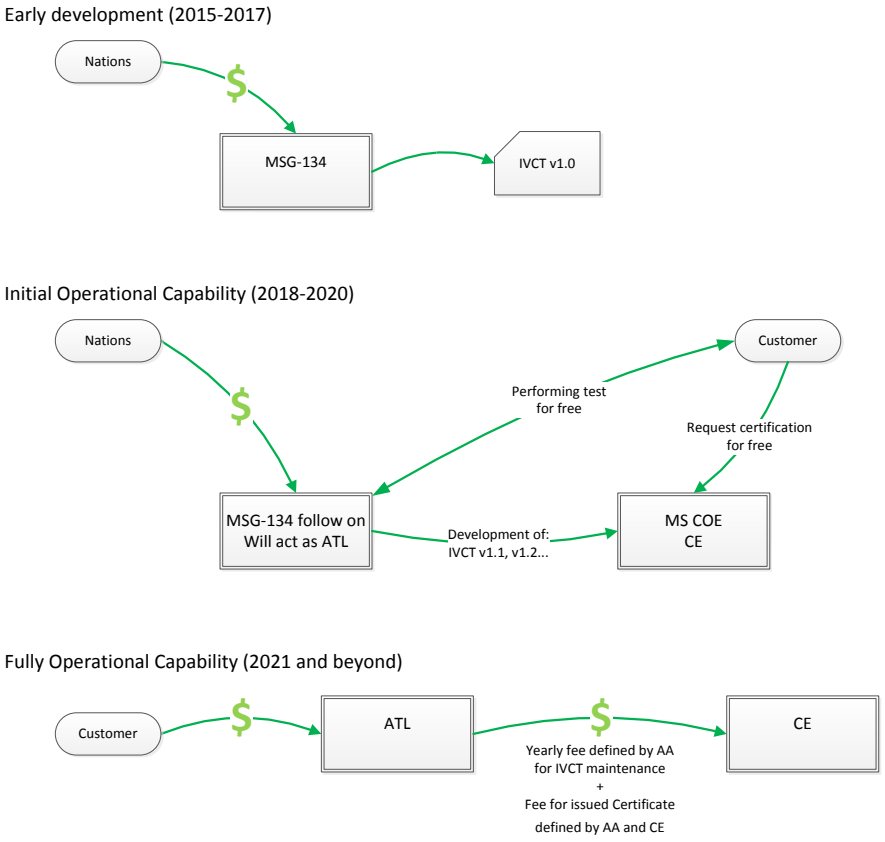

Figure 2-5: Funding of IVCT and Certification Service.

Other simulation and modelling areas that were identified for possible inclusion in future versions of the NETN FAFD are shown in Table 2-4:

Table 2-4: Additional Proposals for Updating and Extending the NETN FAFD.

Module	Description of Change Proposal
METOC Module	Identified in MSG-106 as a key module in GMF with potential to be included in future versions of NETN FAFD. A METOC Module for representation of meteorology and oceanology related environmental properties and events at different levels of fidelity are required in order to ensure fair-fight conditions and accurate analysis results among distributed simulation models. A METOC module may include space, atmosphere/weather, surface and sub-surface conditions that affect simulation models, including signal-propagation, line-of-sight, and platform/munition-dynamics. Already existing standards that should be taken into consideration and will influence design of METOC module include the CIGI standard.
Dynamic Terrain	An interoperability issue that MSG-086 identified is the difficulty in keeping different synthetic environments synchronized within a simulation exercise during the execution. Each simulation component typically determines the consequences of events that influence the environment, locally, therefore, the different representations of the synthetic environments might diverge over time. A service that processes changes to the synthetic environment centrally would be a solution to ensure these changes happen consistently across different systems. These systems would need to request information from this central service. Data could be distributed to subscribers when there are changes in the synthetic environment. These kinds of interactions would be captured during FOM design, interaction classes could be created in an SDS Module (Synthetic Dynamic Service).
Crisis Management and Disaster Response	MSG-146 has identified the need to extend NETN FAFD with additional chapters and new and/or updated FOM modules to support simulation of aspects related to crisis management and disaster response. These may include the following areas of interest: • Geophysical: Earthquake, Mass Movement, Volcanic activity; • Hydrological: Flood, Landslide, Wave Action; • Meteorological: Storm, Extreme temperature, Fog; • Climatological: Drought, Glacial lake outburst, Wildfire; • Biological: Animal accident, Epidemic, Insect infestation; and • Extra-terrestrial: Impact, Space Weather.

The STANAG publication activity involved the following actions:

- A presentation to MS3 meeting at the Fall 2014 NMSG Business Meeting on a proposal for making NETN FAFD as AMSP-04;
- Investigated the procedure for NSO publication;
- Identified required templates and preparatory work required before submitting to NSO;

- A draft for the standardization proposal was made;
- A draft for the standardization task was made;
- Submitted the standardization proposal and standardization task to NMSG via MSCO and MS3;
- The NETN FAFD was reviewed and feedback was recorded in an issue-tracking document;
- Updated NETN FAFDv2.0 using the correct template;
- The AMSP-04 draft was sent to MSCO:
  - MSCO made an admin revision;
  - MSCO circulated it in MS3 for endorsement and NMSG approval.

The consecutive versions of the AMSP-04 are the following (see Table 2-5):

Table 2-5: Consecutive Versions of the AMSP-04.

Version	Date	Description
NETN FAFD v2.0 Draft 4	3 October 2014	Final Version as developed by MSG-106.
AMSP 04 (A) Draft 1	17 August 2015	Version submitted to MSG-106 and NMSG for final review.
AMSP 04 (A) Draft 2	21 September 2015	Version submitted to MS3 for approval.
AMSP 04 (A) Draft 3	January 2016	Version submitted to NMSG for approval.
AMSP 04 (A) Final Draft	October 2017	Final version to be approved by NMSG and published by CSO.

The AMSP-04 has been approved by NMSG and will be covered by STANREC.

2.3.2.1 Key Findings

The AMSP-04 has been applied and successfully used during exercises, such as VIKING series.

Multiple commercial and non-commercial software packages have been adapted for AMSP-04.

2.3.2.2 Recommendations

Update existing NETN-Physical and NETN-LBML FOM modules and add FOM modules for MSDL, Synthetic Environment and MEL/MIL in NETN.

Continued issue tracking will be done using Science Connect dedicated area for AMSP-04 maintenance.

2.3.3 IVCT Development

2.3.3.1 Requirements Specifications

In the first year of the MSG-134 work, the group concentrated on the evaluation of the requirements for a testing and certification tool. An initial study of requirements was done by the exploratory team MSG-ET-035. These requirements have been used as input for the IVCT requirement analysis. The use case descriptions have

been refined and extended and are used to describe the operational scenarios within the CONOPS deliverable (see CONOPS Annex A: Operating Procedures).

The functional and non-functional requirements have been updated and extended and are documented in the IVCT deliverables. These requirements have been used to guide the architecture design and the software development for the IVCT.

Because of the limited time and resources available to the MSG-134 group, not all requirements could be realized during the development.

2.3.3.2 Licensing

The IVCT software shall foster interoperability between simulation systems. To further that purpose, the software needs to be available to simulation-solution providers, integrators, and users without any restrictions. Furthermore, the interoperability requirements implemented in the software shall be freely accessible to all interested stakeholders.

The concept of Open Source Software (OSS) is the most appropriate answer to these requirements. The members of the MSG-134 group analysed several OOS license models (see Annex A: Open Source Software Licensing Strategy) and decided to use the Apache 2.0 license. This is a very business-friendly license, and it supports a cooperative development process.

2.3.3.3 Framework Development

The central focus of the software development is the IVCT framework. The framework provides all test case independent components required for the execution of test cases. The figure below gives an overview of the IVCT architecture. It shows two main areas, one is the IVCT and the other is the SuT Environment (SuTE), which are connected by the (HLA) Run Time Infrastructure (RTI). Within the IVCT, there is a Test Engine (TE) executing the test cases and producing the test results, the configuration and reporting component, and the Graphical User Interface (GUI) with the federation execution control components. Inside the SuTE, there is the System under Test (SuT) and, potentially, additional components required for the operation of the SuT, such as auxiliary federates or services (see Figure 2-6).

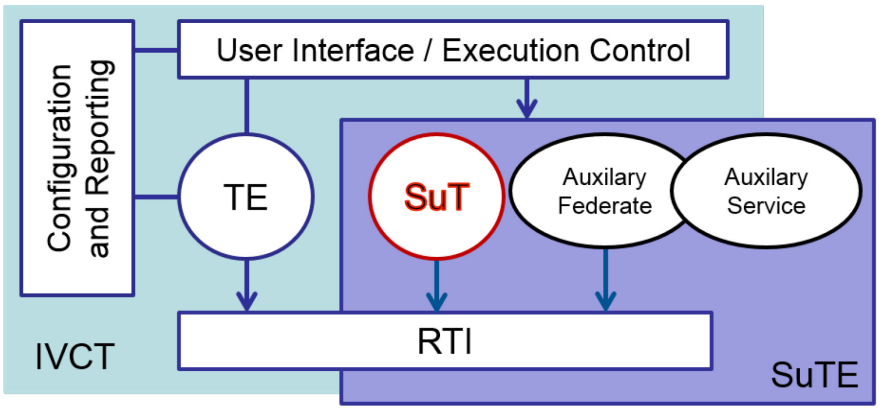

Figure 2-6: IVCT Architecture Overview.

The IVCT framework components use a Message-Oriented Middleware (MOM) for internal communications. To be implementation independent, the Java Message Service (JMS) interface is used to provide a product independent interface. Currently, the Apache Foundation's ActiveMQ software has been chosen as the MOM implementation.

The development of the IVCT framework followed the implementation plan below:

- **Version 0.1** (26 Dec 2015):
  - Java Messaging Service adapter for the IVCT-internal communication module;
  - Collector module for the command module and the test case protocol information;
  - Test case execution module.
- **Version 0.2** (21 Jul 2016):
  - Command-and-control interface to the IVCT components. Execution control of individual test cases and test schedules;
  - Command line interface to the IVCT commander;
  - Draft version for the definition of test schedules in version 0.2;
  - Library for test case development.
- **Version 0.3** (18 Aug 2016):
  - Test case verdict file writer.
- **Version 0.4** (10 Jun 2017): used for CWIX 2017:
  - Graphical user interface to the IVCT commander.
- **Version 1.0** (End 2017): final release:
  - Final implementation of interoperability badge-based schedules in version 1.0.

The communication and synchronization module between the IVCT operator, test case, and the SuT operator has not been implemented within the working period of the MSG-134.

In the final release of the IVCT, the graphical user interface will be the main interface to the system. The interface is based on a Web application, as shown in Figure 2-7:

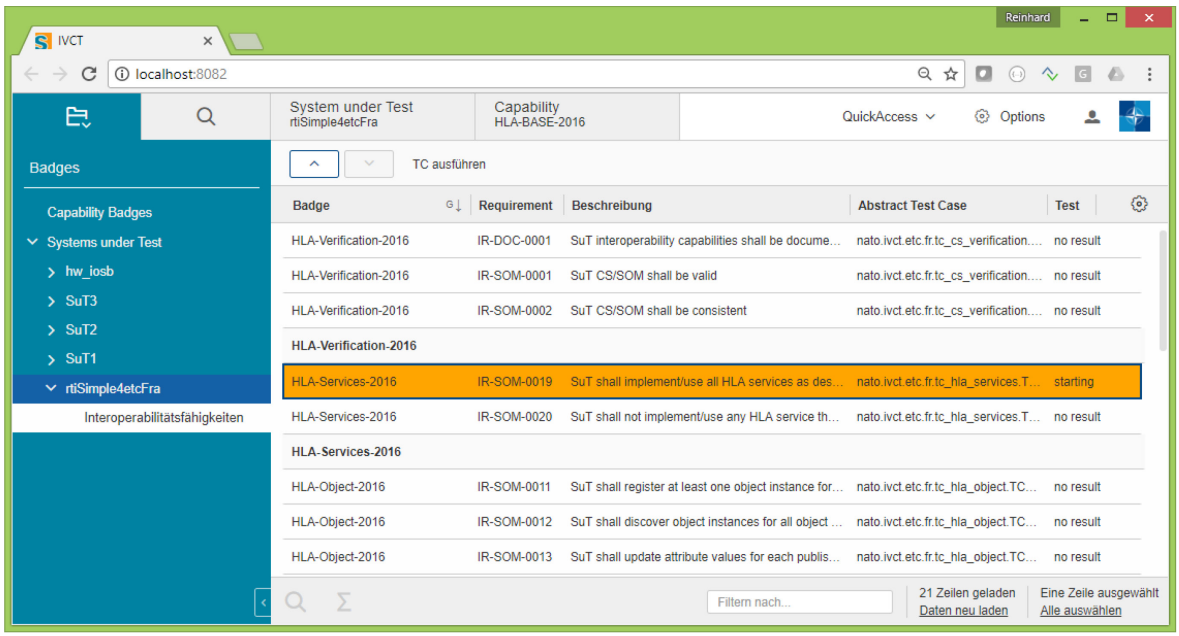

Figure 2-7: Screenshot of the Graphical User Interface for the IVCT System.

The implementation language is Java, and all components are released under the Apache 2.0 open source license. All external libraries are also Java-based and provided as open source under the same license.

2.3.3.4 Test Suites Development

To support the development of test suites, a HelloWorld test suite has been created. This example shows the proposed software and component structure for a typical test suite. It is documented in the GitHub wiki and serves as a tutorial for test suite developers who are implementing Executable Test Cases (ETC).

The first operational test suite for the IVCT is HLA-BASE-2016. It contains four specific test suites: verification, object management, service verification, and HLA best practices. These test cases cover the FCTT_NG configuration verification tests, as well as tests to verify the published and subscribed objects, interactions, along with their attributes and parameters, according to the SuT's SOM. Included are several tests for basic Conformance Statement (CS), SOM and best practices compliance rules.

A second test suite is dedicated to the RPR2 specifications. It is focused on the validity of attributes for the EntityType of class PhysicalEntity, and the validating of the WeaponFire interaction. It includes two simple federates for confirming the correct operation of the tests.

2.3.3.5 GitHub Environment

The development of the IVCT framework and the test suites is done by the participating nations in distributed way. For such development setups, a *Distributed Version Control Systems* (DVCS) is the most appropriate support tool. A popular DVCS is *git*, which is supported by the hosting facility, *GitHub*. GitHub is one of the largest code hosts in the world with more than 52 million projects. It is free of charge for open source projects, and it supports a wiki-based documentation and a simple issue-tracking system. It has been chosen as the hosting platform for the IVCT framework and test suite development.

At the entry page to the MSG-134 repositories (the URL is https://github.com/MSG134) (See Figure 2-8), all repositories are located on a so-called Organization. An organization is container element to organize user groups and access rights to the contained repositories. The main repositories in the MSG134 container are:

- **IVCT_Framework**: This is the source code for the core components of the IVCT system. These components are required to start the tool and to develop test cases.
- **TS_HelloWorld**: This is a tutorial test suite repository to illustrate and explain the structure of a typical test suite.
- **IVCT_Runtime**: This repository shows the typical set-up of the IVCT run-time environment to be used for the execution of test cases.

Within the MSG-134 GitHub organization page, there are other repositories for the test suite implementations, along with common test case libraries. The contributors are assigned to user groups, according to their role in the development. Each repository GitHub supports an issue-tracking system to report software bugs and feature requests, or to answer questions.

2.3.3.6 Capability Badges Database

The capability badges database was created soon after the concept of capability badges was accepted by MSG-134. The database provides a central repository of information regarding interoperability requirements, the badges defined by these requirements, and the test cases that allow IVCT to determine if federates meet these requirements. The database has a web interface allowing the public to browse the database, and a restricted access editor's interface that allows for updates to the database.

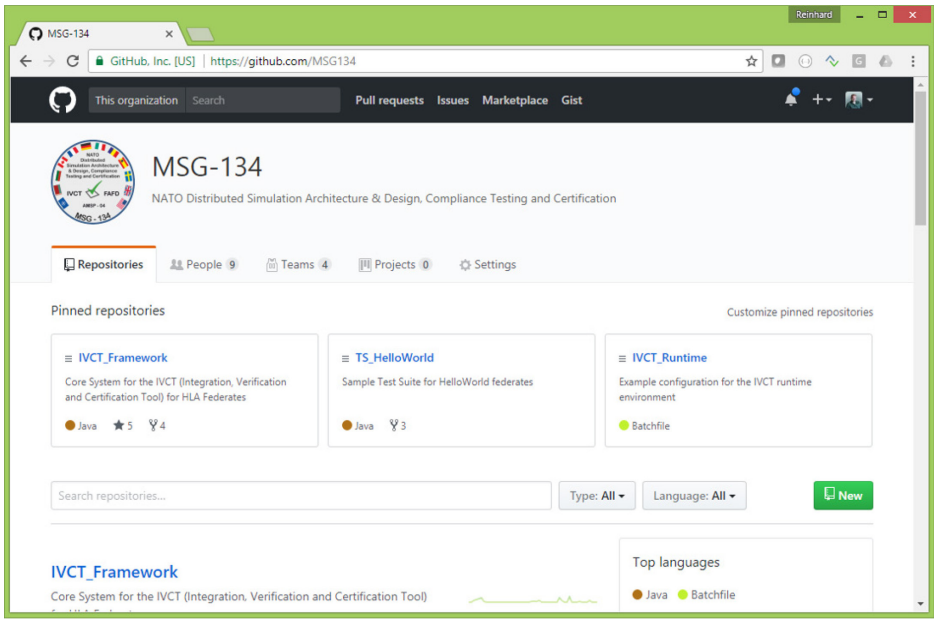

Figure 2-8: MSG-134 Source Code Repository on GitHub.

Definition and Browsing of Interoperability Requirements

Interoperability requirements are the most basic information needed to define badges and test cases for the IVCT. The database contains a single table of requirements. Anyone can view the requirements (which are also grouped together in broad categories) and editors are able to create, modify, and delete interoperability requirement records. Each requirement record has an identifier that is used to refer to it, as well as a description of the requirement. For example, IR-NETN-0063 "SuT shall define BaseEntity.AggregateEntity.NETN_Aggregate or a subclass and/or a NETN subclass of BaseEntity.PhysicalEntity as published and/or subscribed in CS/SOM."

Definition and Browsing of Capability Badges

A capability badge represents a collection of individual requirements which, together, define a particular capability. For example, the capability badge "HLA-BASE-2016" has a total of twenty eight (28) individual requirements that cover technical requirements and best practices for using HLA services. Requirements for a badge may also include dependency on other badges, for example, the "RPR-ENTITY-2016" badge has a dependency on HLA-BASE-2016 and an additional eleven (11) interoperability requirements.

Anyone may browse through or search capability badges, while registered users may also create, edit, and delete them.

Abstract Test Cases and Executable Test Cases

In order to test that a federate complies with an interoperability requirement, both abstract and executable test cases are required. The abstract test case provides information about the requirement to be tested and the methodology that will be used for the test. This information is in the form of a human readable document and can be thought of as the design document a developer will use to create an executable test. Every testable interoperability requirement must have an abstract test case associated with it. An executable test case is actual code written to work with the IVCT framework to verify that a SuT complies with a requirement. Executable test cases are grouped together as test suites within the IVCT to create tests that provide complete coverage for a capability badge.

Currently the database supports abstract test cases, with a reference to the applicable interoperability requirement and a document detailing the ATC. These records may be viewed by anyone and can be created, edited, and deleted by registered users. Executable test cases have not been implemented within the database, but this has been identified for future work.

Operation and Maintenance

The database is based on a standard Linux-Apache-MySQL-PHP (LAMP) platform, packaged as a VMWare virtual machine. In particular, it is a Turn-Key Linux LAMP [2] stack virtual appliance. This platform was chosen to maximize the potential pool of developers available to provide updates in the future.

While the database has a public interface, editing access is controlled. The database includes a "users" table that holds user accounts for editors. Anyone can request an editor account, but an existing editor must approve the application before the account becomes active.

The editors also have access to a function that allows them to obtain a complete snap-shot of the database contents as a standard SQL file. This can be used to migrate the database to another system, update offline copies of the virtual machine, and to perform periodic back-ups.

Future work

The addition of an executable test case table will allow for the generation of IVCT configuration files directly from the database. CAN and DEU intend to add executable test cases to the database and to set up a function to export JSON files for the IVCT.

The web interface to the database is functional but could benefit from improvements to the look-and-feel. Improved views of the data (reports) would also help users and administrators. Some thought should also be given to the control and review of editor accounts.

2.3.3.7 Key Findings and Recommendations

The key findings are:

- The use of "git" as the version control system has been proven to be very useful when dealing with distributed development teams working with offline repositories. The support for offline repositories is especially important when working in experimentation networks, which are not always connected to the public Internet. While this is true for the git-based version control functions, the GitHub documentation and the issue tracking system is only available with an online connection.
- The IVCT framework supports the independent development of test suites by many developers. The current test suites were developed by three different teams without any interaction between them. This is an indication that the current libraries are well defined.
- Deployment of the individual IVCT components in the current system is not yet fully automated.
- The participation of IVCT developers in experiments like CWIX was very helpful to gain first-hand experience and feedback about the usability of the tool in environments outside their developer spaces. This is also a very effective way to test new software releases under realistic working conditions, such as limited time for installation and experimentation, or interpretation of test results.
- The configuration of new SuTs can be complex, depending on the required configuration of the supported badges.
- The use of the JMS interface to communicate between internal components, as well as to interface with external components has proven to be useful.

- The standard “Simple Logging Facade” (SLF) interface enabled a common logging concept for all IVCT components, including the external frameworks (ActiveMQ, Apache Tomcat, LOGBack).

The recommendations are:

- Continue the use of GitHub for future development of the IVCT framework, as well as for test suite development.
- Adopt the reference architecture of the NMSG-136 MSaaS to improve the deployment of IVCT components in cloud-based environments.
- Improve the installation process for the IVCT user by simplifying the required steps and by providing appropriate documentation.
- Provide the online documentation within GitHub for offline usage.
- The configuration of new SuT candidates should be supported by a configuration wizard. Ideally, this should be an interactive process, based on test suite templates, that guide the user through the set-up of the test case parameters.
- The IVCT user interface should provide feedback on the progress of the test case execution.
- It is recommended to continue participation in large scale events to gain first-hand user experience. Participation of the IVCT framework and test case developers is also recommended.
- Not all requirements have been implemented during the MSG-134 working period. It is recommended to finish the missing ones in a follow-on activity.
- Other standards than HLA should also be supported, such as DIS.
- The capability badges database should be integrated in the IVCT suite of tools.

2.3.4 Experimentation during CWIX

Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise (CWIX) is a computer information systems event that brings together the Alliance and Partner Nations to solve interoperability challenges by federating people, processes, and technology. CWIX is endorsed by the North Atlantic Council (NAC) and directed by the Military Committee. In 2014 the Modelling and Simulation (M&S) Focus Area was created to test interoperability between the numerous existing simulation systems present in CWIX to facilitate Communication and Information Systems (CIS) testing events.

In 2015 MSG-134 evaluated the possibility of participating in the M&S Focus Area with IVCT, and representatives attended the CWIX 2016 conferences. The goal was to understand the CWIX process, requirements, and effort needed, and to promote the work done by the group. In 2016, MSG-134 decided not to participate in the execution phase because IVCT was not mature enough, postponing this activity to CWIX 2017. Attending the CWIX conferences was also very useful from IVCT development point of view, since the group was able to get initial feedback from potential partners and better understand their needs, doubts, and expectations for an integration, validation, and certification tool.

In 2017 MSG-134 produced a version of the IVCT suitable for performing basic test cases as part of CWIX. At least one member participated in each CWIX conference to coordinate and prepare, and to give feedback about which test cases were most desirable to potential partners. Under the umbrella and sponsorship of NATO M&S Centre of Excellence (M&S CoE), IVCT participated in the CWIX Execution phase in June 2017. NATO M&S CoE handled the administrative, security and accreditation procedures, allocating hardware and human resources, and presenting IVCT as one of its own capabilities. Executable test cases were developed by France and Canada. Germany enhanced the graphical user interface and actively supported the M&S CoE during the execution of the test cases.

A brief summary of CWIX 2017 activities performed by IVCT follows.

IVCT performed a total of seven test runs.

Each test run included the execution of two ETCs, in order to reduce the effort in administrating test cases and focus on the tests themselves.

ETCs were grouped as follows:

- HLA_Verification and HLA_Declaration
- HLA_Objects and HLA_Services

Testing days:

- 20th – 23rd, 26th, and 27th of June 2017.

Total of four testing partners:

- NATO-MSCOE-SGA
- NATO-MSCOE-LVC-GTW
- NATO-JFTC-JCATS
- NATO-JWC-VBS3

Other participants were interested but unavailable to test during the event.

2.3.4.1 Key Findings

- The CWIX M&S Focus Area lead had collected information about federate conformance requirements, but not in a format that could be used for testing. IVCT ETCs required each SuT to provide its SOM but usually capabilities cannot provide it.

2.3.4.2 Recommendations

- Provide a guideline to create special purpose interoperability badges for exercises like the CWIX (i.e., create interoperability requirements with abstract test cases and organize them in badges). SuT interested in having tests with IVCT should provide their SOM prior to the tests.

2.3.5 Dissemination

The dissemination activities of MSG-134 included papers, presentations, marketing materiel, and general collaboration with other MSGs and related national and NATO projects.

A complete list of papers and presentations is given in Table 2-6.

Table 2-6: Dissemination Activities of MSG-134.

Reference	Description
Herzog 2015	Reinhard Herzog. Zertifizierung – der Weg zur verlässlichen föderierten Simulation. https://www.dwt-sgw.de/veranstaltungen/veranstaltungen-der-sgw/veranstaltungen-2015/

Reference	Description
DiBella 2015	LTC Paolo Di Bella. NATO Distributed Simulation Architecture and Design Compliance Testing and Certification. Presentation for ACT CD&E. May 2015.
Löfstrand and Hodicky 2015	Björn Löfstrand, Jan Hodicky. NATO Distributed Simulation Architecture and Design, Compliance Testing and Certification – MSG-134. September 2015. 10th NATO CAX Forum 2015.
Herzog *et al.* 2015	Reinhard Herzog, Johannes Mulder, Horst Behner, Björn Löfstrand. A Safe Way to Reliable Federations. STO-MP-MSG-133-021. NMSG Symposium on M&S Support to Operational Tasks including War Gaming, Logistics, Cyber Defence. October 2015. Munich, Germany (Presentation).
Behner and Ruiz 2016	Horst Behner. ITEC 2016. MSG-134_ITEC2016Presentation_V1.ppt. London, May 2016. GBR.
Löfstrand and Behner 2016	Björn Löfstrand and Horst Behner. MSG-134 CONOPS, Business Model and Recommendations. Modelling and Simulation Standards Subgroup (MS3) meeting at NMSG 37th Business Meeting. June 2016. Rome, Italy.
Ruiz, *et al.* 2016	Towards a New NATO Certification Capability for HLA Interoperability. (Paper, Presentation, SISO Award).
Hodicky and Vrieler 2017	Jan Hodicky, Stefan Vrieler. Establishment of HLA Compliance Certification Within NATO. SISO Seminar at ITEC 2017. May 2017. Rotterdam, Netherlands.
Behner and Löfstrand 2017a	Horst Behner and Björn Löfstrand. The New HLA Certification Process in NATO**.** Paper 19. MSG-149 Symposium on M&S Technologies and Standards for Enabling Alliance Interoperability and Pervasive M&S Applications. October 2017. Lisbon
Löfstrand 2017	Björn Löfstrand. NATO Education and Training Network Federation Architecture and FOM Design (NETN FAFD**)**. 12th CAX Forum. September 2017. Florence.
Behner and Löfstrand 2017b	Horst Behner and Björn Löfstrand. Establishing an HLA Certification Process in NATO. Paper 17058. November 2017. I/ITSEC (Interservice/ Industry Training, Simulation and Education Conference).

Chapter 3 – SUMMARY

3.1 KEY FINDINGS

A business model should be exercised to gain more knowledge, experience and lessons learned, and to adjust this business model.

The AMSP-04 has been applied and successfully used during exercises, such as VIKING series.

Multiple commercial and non-commercial software packages have been adapted for AMSP-04.

The use of "git" as the version control system has been proven to be very useful when dealing with distributed development teams working with offline repositories. The support for offline repositories is especially important when working in experimentation networks, which are not always connected to the public Internet. While this is true for the git based version control functions, the GitHub documentation and the issue tracking system is only available with an online connection.

The IVCT framework supports the independent development of test suites by many developers. The current test suites were developed by three different teams without any interaction between them. This is an indication that the current libraries are well defined.

The participation of IVCT developers in experiments like CWIX was very helpful to gain first-hand experience and feedback about the usability of the tool in environments outside their developer spaces. This is also a very effective way to test new software releases under realistic working conditions, such as limited time for installation and experimentation, or interpretation of test results.

The CWIX M&S Focus Area lead had collected information about federate conformance requirements, but not in a format that could be used for testing. IVCT ETCs required each SuT to provide its SOM but usually capabilities cannot provide it.

3.2 RECOMMENDATIONS

A follow-on activity of MSG-134 would contribute to the following objectives:

- Collaborating with SISO to contribute actively to the new version of the standard "HLA 4" in aim to evaluate impacts to the certification process and tools;
- Improving the NATO HLA data products (Federation Object Model, Federation Architecture and FOM Design, etc.); and
- Improving the NATO certification process and tool (final operational capability).

Chapter 4 – REFERENCES

[1] NATO Simulation Certification Service CONOPS. Annex A of MSG-134 Technical Report.

[2] TurnKeyLinux: Website, https://www.turnkeylinux.org/lampstack, accessed 29 August 2017.

[3] NATO09: Strategy for the Use of Open Source Software in NATO Systems. NATO Document AC/322-D(2009)0015, 16 March 2009.

[4] NATO15: NATO Software Management Policy. NATO Document AC/322-N(2014)0119, 2 February 2015.

[5] GPL2: Gnu Public License v2.0, website, https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html, accessed 30 August 2017.

Annex A – OPEN SOURCE LICENSING STRATEGY FOR IVCT

The IVCT software shall foster the interoperability between simulation systems. To further that purpose, the software needs to be available to simulation solution providers, integrators, and users, without any restrictions. Furthermore, the interoperability tests implemented in the software shall be freely accessible to all interested stakeholders. The concept of Open Source Software (OSS) is the most appropriate answer to these requirements.

A.1 BACKGROUND

On 24 April 2009, under the silence procedure, the NC3 Board approved the Strategy for the use of Open Source Software (OSS) in NATO systems as outlined in Enclosure 1 of the main document, and agreed to invite the Information Services Sub-Committee (SC/5) to inform the NC3B about results and experience gained from the application of the strategy and the use of OSS in NATO and Nations. For detailed background information see the Strategy for the use of Open Source Software in NATO Systems [3].

This study addressed several key areas to be considered for selection of OSS. Many of them apply to the IVCT software, such as:

- Architectures and standards;
- Migration and integration; and
- Management, support, and maintenance.

There is an ongoing activity to lay out the policies for the management of NATO Software, which also mentioned the use of OSS. Section 8 of the NATO Software Management Policy [4] described the usage of OSS. The bottom line of these policies is that NATO favours the use of OSS where appropriate, in order to reduce license costs, to avoid dependencies on single vendors, and, most importantly, to improve interoperability of systems through the use of open standards.

A.2 RESTRICTIONS ON COPYLEFT

The IVCT software supports the core functionality for integration, verification, and certification tasks. The software shall include all the necessary functionality to allow unified and NATO-wide to test interoperability. The IVCT core software will never be able to cover every possible requirement of each nation or company. For that reason, the selected license must not prevent the extension of the IVCT software with added-value functionality, by copyright protected software.

OSS-related business models which are compliant with the NATO expectations are:

- Selling of optional proprietary extensions;
- Selling professional services; and
- Partnership with funding organizations (most likely the NATO itself).

A.3 OWNERSHIP

Like every other product OSS has an owner. The difference is that OSS software owners don't control possession and use of the software, only the copyright. It is the owner who assigns the license and grants copyright permissions. The OSS model is that the software developer (possibly his or her employer) owns

copyright permissions. The OSS model is that the software developer (possibly his or her employer) owns the copyright to this software. Changing the license gets complicated when many developers are contributing to a single product and therefore own different pieces of the product. Like the Linux kernel, which is licensed under the Gnu Public License version 2 (GPL2) [5] with many copyright holders, there is no intention to ever change the license.

For this reason, some OSS projects require that contributors assign copyright to a single legal entity. The contributors, like everybody else, have the right to use it according to the license agreement, but they do not own the copyright on their work anymore. Oracle is doing this with the Java technology.

Copyright assignment can simply be done by getting an informal statement from a contributor. Typically, a statement like:

> *"I hereby assign copyright in this code to the project, to be licensed under the same terms as the rest of the code."*

Some organizations do have a more formal process in place, including signatures, and paperwork. The result of a more formal assignment process should be the same but may be more reliable if disagreements arise.

A.4 FINAL DECISION OF MSG-134 FOR THE IVCT LICENSE

MSG-134 analyzed the following software license models:

- The GNU General Public License (GPL): https://www.gnu.org/licenses/gpl-3.0
- The GNU Library or "Lesser" General Public Licence (LGPL): https://www.gnu.org/licenses/lgpl-3.0
- The Apache 2.0 license: http://www.apache.org/licenses
- The Mozilla Public Licence (MPL): https://www.mozilla.org/en-US/MPL

The LGPL is only an extension to the GPL license. If code is modified inside an LGPL code base, the GPL license applies for that code. This will make everything in the added code GPL+LGPL. If an application is built on top of anything GPL based, which is not an LGPL library, then it will all become GPL. Many companies do not allow building on top of GPL licensed code, since they will lose their trade secrets. The LGPL only works where there can be a clear separation of the LGPL part, such as libraries or subroutines, and the rest of the software components. It focuses on how a completed library can be packaged and redistributed.

Software components which are covered by the Mozilla Public License (MPL) have to remain under that license, but commercial extensions can be created. If the implementation of the core tool is based on existing libraries or frameworks, then its license may influence the IVCT license decision. In addition, the MPL is incompatible with any GPL or LGPL-licensed component.

The group found that further development and maximum reuse are facilitated with the Apache 2.0 license. Under this license a user may use, modify, and distribute software freely in any environment. When the software is distributed, the user must include a statement that the software was used under the Apache license and that it originates from the licensor. Changes to the source code of the software under the Apache license do not have to be returned to the licensor. The Apache 2.0 version is compatible with Version 3 of the LGPL, but not with any other previous version.

Annex B – IVCT REQUIREMENTS SPECIFICATION

B.1 OVERVIEW

This annex describes the requirements for the IVCT design. The requirements are divided into two groups, one for all functional aspects of the software and another for all non-functional aspects. The non-functional requirements of the IVCT are stated in terms of availability, implementation constraints, performance, reliability, security, supportability, and usability. All requirements are explained to a level of detail sufficient to enable software developers to design a system to satisfy those requirements, and the tests needed to demonstrate that it does.

At the end of this annex, a table shows the mapping of requirements to software components. In some cases, requirements are not yet implemented; in these cases, the mapping will be empty.

B.2 UNIQUE IDENTIFICATION SCHEMA

Each requirement is defined by a unique name and a text description. The unique name is constructed with a tag and a short title:

```
<requirement name> ::= <tag> '-' <group label> '-' <number> SPACE <title>
<tag> :: 'REQ'
<group label> ::= 'FUNC' | 'DOC' | 'IMPL' | 'PERF' | 'RELY' | 'SECURE' | 'SUPP' | 'USE'
<number> ::= <digit><digit><digit>
<digit> ::= 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
<title> ::= STRING
```

B.3 FUNCTIONAL REQUIREMENTS

Table B-1: Functional Requirements of IVCT.

Title	Description
REQ-FUNC-001 Certification	The IVCT shall support the certification test of a federate. This is the primary purpose of the IVCT.
REQ-FUNC-002 Integration	The IVCT shall support the integration of individual federates into one federation. This is the secondary purpose of the IVCT.
REQ-FUNC-003 Verification	The IVCT shall support the verification of a federate in a given federation. This is an optional purpose for the IVCT.
REQ-FUNC-006 Verdict summary	A verdict for each test case must clearly be shown, as well as the total number of test cases runs, and a breakdown into categories (failed, inconclusive or passed).
REQ-FUNC-007 Repeatability	Characteristic of a test case, such that repeated executions on the same SuT under the same conditions lead to the same test verdict. By extension this is also a characteristic of a test suite.

Title	Description
REQ-FUNC-009 Certification Coverage	The IVCT shall be able to test the SuT's use of HLA services. Not all HLA services need to be implemented by a Federate to be certifiable (depending on the conformance statement and badges). The certificate shall report these certified/implemented HLA services.
REQ-FUNC-011 After Action Review	The IVCT shall provide test results to an external issue tracking system.
REQ-FUNC-012 Test Case Traceability	A version number is needed to trace changes to the test cases. The IVCT shall write this number in the log files and summary reports.
REQ-FUNC-013 Test Case Selection	The selection of test cases to be performed for a given SuT shall be done based on the conformance statement.
REQ-FUNC-014 Test Case Library	The IVCT shall provide a library of convenience functions that help the test case developer reduce repetitive code in the test cases.
REQ-FUNC-015 Test Case Extensibility	The IVCT shall have clearly defined interfaces to allow the straightforward addition of new test cases and new test suites.
REQ-FUNC-016 Certification Workflow Support	The IVCT shall implement support for the certification process workflow. This requirement needs to be expanded during the design phase to include all functional requirements for workflow support.
REQ-FUNC-020 SOM Consistency	IVCT should validate SOM consistency according to the HLA OMT specification.
REQ-FUNC-021 SOM-FOM Consistency	Check the consistency between SOM and FOM.
REQ-FUNC-023 Conformance Statement Consistency	Check the consistency of the SuT conformance statements.
REQ-FUNC-024 SOM Conformance Statement Consistency	Check if the SOM is consistent with the SuT conformance statement.
REQ-FUNC-040 Remote Operating mode	The IVCT should allow testing of a SuT connected over WAN (remote site).
REQ-FUNC-041 Local Operating mode	The IVCT should allow testing of a SuT connected in a LAN (locally).
REQ-FUNC-042 Remote UI for Instructions	The IVCT shall include a text-messaging function.
REQ-FUNC-043 Remote UI for TC Synchronization	The IVCT shall support remote operator control of test case execution.

Title	Description
REQ-FUNC-100 Test based on Federation Agreement	The IVCT shall test interoperability based on federation agreement definitions.
REQ-FUNC-101 Test based on Test Cases	The IVCT shall test SuT based on test cases.
REQ-FUNC-102 Active/Passive Testing	The IVCT shall support test cases for monitoring and/or interacting with SuT.
REQ-FUNC-103 Test for Invalid Behaviour	The IVCT shall identify invalid SuT behaviour.
REQ-FUNC-104 Test for Invalid Data	The IVCT shall identify invalid SuT data.
REQ-FUNC-105 Test Result Analysis	The IVCT shall propose possible cause of SuT failing a test case.
REQ-FUNC-300 Test Case Execution Control	It shall be possible to start and abort a test case/schedule.
REQ-FUNC-310 Adjustable Level of Execution Documentation	The level of documentation generated during test case execution shall be adjustable by changing the logging level.
REQ-FUNC-320 Unique Identification for Test	The test clients (SuT) and the test session shall be identified in a unique manner by the IVCT software.
REQ-FUNC-330 Modelling of Basic Test Case Components	The basic components of the test case are coded in the test environment.
REQ-FUNC-340 Execution of Test Case Sequence	The test environment shall be able to execute test cases (sequences of basic components). The test environment shall be defined independently from the test cases.

B.4 NON-FUNCTIONAL REQUIREMENTS

B.4.1 Documentation

Table B-2: Non-Functional Requirements of IVCT – Documentation.

Title	Description
REQ-DOC-100 User Manual	A user manual shall be created as a technical communication document to give assistance to the IVCT operators.
REQ-DOC-110 Test Case Developer Guide	A “Test Case Developer Guide” document shall be created, to explain the concepts behind the test case development and the technical details to implementation within the IVCT.

Title	Description
REQ-DOC-120 Required Hardware	The minimum hardware requirements for execution of the IVCT shall be documented.
REQ-DOC-200 Test Result Logging	The results of a test case execution shall be documented within log files. This includes tests performed for certification as well as tests for integration and validation purposes. The individual steps and events of a test case execution shall be documented. The test results shall be provided in a self-explanatory way, listing the succeeded, inconclusive and failed tests. The test results should have a certain format, which shall be explained in the user manual.
REQ-DOC-210 Test Case Documentation	Each test step of a test case shall be illustrated and explained with test case documentation.
REQ-DOC-220 Test Sequence Documentation	Test case sequences shall be clearly defined and documented. The documentation shall be related to the definition of the associated interoperability badge definition.
REQ-DOC-300 Documentation Language	All documentation shall be delivered in the English language. In case of any other language requirements, these will be done at the national level and are out-of-scope for this project.

B.4.2 Implementation Constraints

Table B-3: Non-Functional Requirements of IVCT – Implementation Constraints.

Title	Description
REQ-IMPL-001 Support for HLA 1.3	IVCT shall support the HLA 1.3 standard.
REQ-IMPL-002 Support for HLA 1516-2000	IVCT shall support the IEEE 1516-2000 standard.
REQ-IMPL-003 Support for HLA 1516-2010	IVCT shall support the IEEE 1516-2010 standard.
REQ-IMPL-010 Support for HLA Java API	The IVCT software shall be able to test federates using the HLA Java API interface.
REQ-IMPL-011 Support for HLA C++ API	The IVCT software shall be able to test federates using the HLA C++ API interface.
REQ-IMPL-052 Operating Systems	The IVCT shall be based on mainstream operating systems. The actual requirements must be defined during the detailed implementation planning.

Title	Description
REQ-IMPL-100 Generalizability	IVCT shall be designed for easy adoption to other simulation interoperability standards than HLA.
REQ-IMPL-101 IVCT Core Generalizability	IVCT core shall be designed independent of interoperability standard used.
REQ-IMPL-110 System Result Interface	IVCT should have an interface for publication of certification test results.
REQ-IMPL-111 System Module Interfaces	IVCT shall have clearly defined interfaces between internal modules.
REQ-IMPL-200 Open Source Software	The IVCT software shall be available as Open Source Software (OSS) to everybody, without vendor-lock-ins. Any modifications shall be done under the control of some "IVCT-authority" and shall always be available to every user and developer.
REQ-IMPL-201 Third party proprietary components	The IVCT shall not rely on proprietary interfaces of 3rd party components.
REQ-IMPL-202 Third party standard components	Any use of 3rd party components must use standard interfaces where the interface is independent of a specific vendor implementation.
REQ-IMPL-203 Commercial Extension	It shall be possible to create commercial software on top of IVCT. Such software will use IVCT as a library or as service, and it may contain patents or Intellectual Property Rights (IPR), and it may have different ownership, and it may not be open source. Any modification in the core IVCT tool must be available without limitations to every user. No IPR protection or trade secrets, shall limit this. The IVCT shall maintain a clear separation between the core IVCT library/service elements and any add-ons.

B.4.3 Performance

Table B-4: Non-Functional Requirements of IVCT – Performance.

Title	Description
REQ-PERF-032 Execution Environment Restriction	The IVCT shall not show any performance-related deficiencies if minimum hardware requirements are fulfilled. This includes for example the network latency, CPU speed, main memory, and file system access.
REQ-PERF-036 Hardware Requirements	The IVCT shall be able to install and run on a standard PC, laptop or desktop computer.

B.4.4 Reliability

Table B-5: Non-Functional Requirements of IVCT – Reliability.

Title	Description
REQ-RELY-030 Certified RTIs	Certification tests can only be performed by using certified RTIs.
REQ-RELY-031 Reliable Test Cases	The test cases shall provide good coverage and the test case implementation must be reliable.

B.4.5 Supportability

Table B-6: Non-Functional Requirements of IVCT – Supportability.

Title	Description
REQ-SUPP-043 Ease of Installation	The installation of the IVCT shall be controlled by an installation program. The installation program shall require only a limited number of configuration interactions and shall otherwise operate in an automated manner.
REQ-SUPP-044 Planned Maintenance	As far as security procedures allow it, the IVCT shall implement a built-in check for updates. In order to control and identify these updates, a source code versioning system shall be used e.g., subversion. For each update, release notes shall be provided, and these should also be kept within the source-control system.
REQ-SUPP-046 Built-in Testing for Robustness	The IVCT shall provide basic self-test features with built-in diagnosis for invalid behaviour.

B.4.6 Usability

Table B-7: Non-functional requirements of IVCT – Usability.

Title	Description
REQ-USE-018 User Ability	The IVCT shall be designed to be used by operators with a basic knowledge of RTIs and the handling of federations. The user shall have a good knowledge of SOMs and FOMs, and of HLA rules and messages, objects, and interactions. This is important in order to share information about test procedures with the certification entity as a whole.
REQ-USE-022 Remote Testing	The IVCT shall be able to perform remote testing.

B.5 IMPLEMENTATION STATUS

The table below shows the implementation status at the time of writing. All requirements explained earlier are listed with a short explanation of the status and the release with the first implementation. As status indications, the following keywords are used:

- **Implemented:** The requirement is fully implemented, and the feature is available in the referred release.
- **Basic support:** The requirement is partly implemented as proof of concept and may need further improvement.
- **Not implemented:** The requirement is not yet implemented.

Table B-8: Implementation Status of IVCT.

Title	Status
REQ-DOC-100 User Manual	Implemented, v0.3.0 – online in GitHub wiki
REQ-DOC-110 Test Case Developer Guide	Implemented, v0.3.0 – TS_HelloWorld tutorial as example with wiki documentation
REQ-DOC-120 Required Hardware	Not implemented, performance benchmarks required
REQ-DOC-200 Test Result Logging	Implemented, v0.2.0
REQ-DOC-210 Test Case Documentation	Basic support, see test suite development
REQ-DOC-220 Test Sequence Documentation	Not implemented, test case sequences are not used
REQ-DOC-300 Documentation Language	Implemented
REQ-FUNC-001 Certification	Implemented, v0.1.0
REQ-FUNC-002 Integration	Basic support, v0.1.0
REQ-FUNC-003 Verification	Basic support, v0.1.0
REQ-FUNC-006 Verdict summary	Implemented, v0.3.0
REQ-FUNC-007 Repeatability	Implemented, v0.1.0
REQ-FUNC-009 Certification Coverage	Implemented, HLA-BASE-2017
REQ-FUNC-011 After Action Review	Basic support, v0.1.0 – results are provided as JMS messages
REQ-FUNC-012 Test Case Traceability	Implemented, v0.1.0
REQ-FUNC-013 Test Case Selection	Implemented, v0.4.0
REQ-FUNC-014 Test Case Library	Implemented, v0.1.0

Title	Status
REQ-FUNC-015 Test Case Extensibility	Implemented, v0.1.0
REQ-FUNC-016 Certification Workflow Support	Basic support, v1.0.0
REQ-FUNC-020 SOM Consistency	Implemented, HLA-BASE-2017
REQ-FUNC-021 SOM-FOM Consistency	Implemented, HLA-BASE-2017
REQ-FUNC-023 Conformance Statement Consistency	Implemented, HLA-BASE-2017
REQ-FUNC-024 SOM Conformance Statement Consistency	Implemented, HLA-BASE-2017
REQ-FUNC-040 Remote Operating mode	Not implemented, external communication to SuT operator is required
REQ-FUNC-041 Local Operating mode	Implemented, v0.1.0
REQ-FUNC-042 Remote UI for Instructions	Not implemented
REQ-FUNC-043 Remote UI for TC Synchronization	Not implemented
REQ-FUNC-100 Test based on Federation Agreement	Implemented, v0.4.0
REQ-FUNC-101 Test based on Test Cases	Implemented, v0.1.0
REQ-FUNC-102 Active/Passive Testing	Implemented, v0.1.0
REQ-FUNC-103 Test for Invalid Behaviour	Implemented, see test suite implementation
REQ-FUNC-104 Test for Invalid Data	Implemented, see test suite implementation
REQ-FUNC-105 Test Result Analysis	Implemented, see test suite development
REQ-FUNC-300 Test Case Execution Control	Implemented, v0.3.0
REQ-FUNC-310 Adjustable Level of Execution Documentation	Implemented, v0.4.0
REQ-FUNC-320 Unique Identification for Test	Basic support, v0.4.0 identification based on unique name (digital signatures are potential improvement)

Title	Status
REQ-FUNC-330 Modelling of basic Test Case Components	Implemented, v0.1.0
REQ-FUNC-340 Execution of Test Case Sequence	Implemented, v0.1.0
REQ-IMPL-001 Support for HLA 1.3	Not implemented
REQ-IMPL-002 Support for HLA 1516-2000	Not implemented
REQ-IMPL-003 Support for HLA 1516-2010	Implemented, v0.1.0
REQ-IMPL-010 Support for HLA Java API	Implemented, v0.1.0
REQ-IMPL-011 Support for HLA C++ API	Not implemented
REQ-IMPL-052 Operating Systems	Implemented, v0.1.0 – all implementations done in Java which is available for all major operating systems
REQ-IMPL-100 Generalizability	Implemented, v0.1.0 provides JMS based activation of test cases
REQ-IMPL-101 IVCT Core Generalizability	Implemented, v0.1.0 only test case engine is standard dependent
REQ-IMPL-110 System Result Interface	Not implemented
REQ-IMPL-111 System Module Interfaces	Implemented, v0.1.0 uses JMS messages to communicate between modules
REQ-IMPL-200 Open Source Software	Implemented, v0.1.0 uses Apache 2.0 license
REQ-IMPL-201 Third party proprietary components	Implemented, v1.0.0 only open and standardized interfaces are used
REQ-IMPL-202 Third party standard components	Implemented, v1.0.0 uses only open and standard interfaces
REQ-IMPL-203 Commercial Extension	Implemented, v1.0.0 uses Apache 2.0 license
REQ-PERF-032 Execution Environment Restriction	Not implemented, minimal hardware requirements are not specified
REQ-PERF-036 Hardware Requirements	Implemented, v1.0.0
REQ-RELY-030 Certified RTIs	Not implemented, IVCT does not check RTI for certificate

Title	Status
REQ-RELY-031 Reliable Test Cases	Not implemented, see test suite development
REQ-SUPP-043 Ease of Installation	Not implemented
REQ-SUPP-044 Planned Maintenance	Not implemented
REQ-SUPP-046 Built-in Testing for Robustness	Basic support, v1.0.0 invalid behaviour is reported by error and warning logging messages
REQ-USE-018 User Ability	Implemented, v1.0.0
REQ-USE-022 Remote Testing	Basic support, v1.0.0 requires only RTI connectivity to SuT. Additional SuT operator (SuTO) communication will be required

B.6 SUMMARY

This document contains the initial collection of requirements for the IVCT software. These requirements have been assigned to different releases of the IVCT. The collected requirements reflect the current assessment of the participating nations within the MSG-134. It may be the case that these requirements will be adjusted in the future. If that happens, this document shall be updated along with the software design document.

Annex C – CWIX EXPERIMENTATION

The Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX), is an event that is North Atlantic Council (NAC)-endorsed, Military Committee (MC) directed and NATO C3 Board (NC3B) guided.

NATO commands and agencies, member nations and partner nations sponsor Communication and Information Systems (CIS) capabilities with specific interoperability testing objectives. These objectives prepare NATO and partner nation CIS for current and future alliance led operations, including the NATO Response Force (NRF). During the CWIX execution event, interoperability tests will improve interoperability between CIS systems.

The "X" in CWIX stands for eXploration, eXperimentation, eXamination, and eXercise:

- *eXploration*. CWIX uses a robust operational architecture based on Federated Mission Networking (FMN) principles to explore emerging concepts and their impact on future networked and federated CIS;
- *eXperimentation*. CWIX allows participants to 'push the boundaries' by testing CIS to their limit. Interoperability experiments between emerging and fielded systems will identify challenges and opportunities for fielding new CIS capabilities;
- *eXamination*. CWIX support a spiral approach to capability development by allowing engineers to test the interoperability of emerging systems to capture and refine requirements that will lead to future spirals of CIS capabilities; and
- *eXercise*. CWIX uses a Joint Warfare Centre (JWC) scenario that uses the same data and vignettes as the NRF CIS validation and certification exercise (Steadfast Cobalt and Trident exercises). The scenario allows participants from different nations to test the interoperability of fielded capabilities for operational preparation and readiness.

In 2014, the Modelling and Simulation (M&S) Focus Area was created to test interoperability between numerous existing simulation systems present in CWIX, to facilitate CIS testing events. Within NATO, the Connected Forces Initiative (CFI) discusses the better use of technology, which includes utilizing simulation to enhance NATO Readiness for 2020 and beyond. The ability to federate and connect M&S systems in the future will allow a more distributed, but connected, exercise and training environment through a common picture. CWIX provides a unique environment to test and explore different federations without the risk of

losing valuable training time. In addition, it allows for multi-tiered federation of M&S systems and the possibility to test with current CIS capabilities to ensure that the proper information and data is provided.

In this context and for these reasons CWIX has been selected as a perfect venue to test, verify and spread knowledge about the IVCT software releases. Starting from 2015, the NATO M&S Centre of Excellence based in Rome (ITA) leads this Focus Area, pursuing the most challenging objectives using state of the art of technology to support the Connected Forces Initiative (CFI). After a first attempt in 2016, taking advantage of the participation of NATO M&S CoE, MSG-134 produced a version of IVCT, together with a set of Executable Test Cases that CoE could bring to CWIX Execution as one of its own capabilities. This allowed IVCT to be tested, for the first time, with M&S NATO systems.

C.1 CWIX 2016

In 2015, during the MSG-134 meeting held in conjunction with the NATO CAX Forum 2015 in Vicenza (Italy) from Sep 29th to October 2nd, NATO M&S CoE presented the activities in CWIX and suggested it as a potential venue for IVCT experimentation and dissemination. It reported about HLA interoperability issues recorded during the past CWIX executions and how the IVCT could help in support of the M&S Focus Area activities.

It was then decided to investigate this possibility and some of MSG-134 members participated to CWIX 2016 conferences. A participation form was also created for IVCT, but it was decided the tool was not mature enough to participate and IVCT was withdrawn. MSG-134 decided to postpone its participation to the next CWIX in 2017.

A roadmap and a description of the activities of MSG-134 during CWIX 2016 preparation follows.

C.1.1 Roadmap

- CWIX 2016 IPC – 3rd to 6th November 2015 – Porvoo (Finland)
- CWIX 2016 MPC – 26th to 29th January 2016 – Potsdam (Germany)
- CWIX 2016 FCC – 8th to 11th March 2016 – Bydgoszcz (Poland)
- CWIX 2016 Exercise – 13th to 30th June 2016 – Bydgoszcz (Poland)

C.1.2 Activities

In order to start promoting IVCT and MSG-134 activities among CWIX participants, NATO M&S CoE, in the role of M&S Focus Area leader, suggested as a first objective for the Focus Area:

- Federate different types of simulation systems and record test results also for contributions to NATO STO MSG-134

This was accepted and allowed MSG-134 to have presentations during the conferences and to start gathering feedback and first impressions from the community. This was a very good result, because getting doubts and objections from the attendees was very useful. It helped the MSG-134 team better understand how to clarify and explain MSG-134 activity, and the benefits of the certification process, as well as the usefulness of the IVCT software.

Germany led the activities related to participation of IVCT in the execution phase, creating the capability number #106 in the CWIX database, named "*DEU-IVCT 01@CWIX 2016"* and pushing it through all the phases of the CWIX process. At the CWIX process deadline in April, after the final coordination conference,

where the accreditation of the capability and final confirmation of its participation is required, MSG-134 decided to withdraw IVCT because it was not ready to perform properly during the execution.

In any case, all the activities done up to that time allowed the group to acquire the required knowledge of CWIX process and procedures, from technical to administrative and security aspects, in order to be better prepared for participating to CWIX 2017.

C.2 CWIX 2017

Under the sponsorship of NATO M&S CoE, M&S Focus Area had, as a first objective for CWIX 2017, the following one:

- Federate different types of networked simulation systems building a complex federation facilitated by NATO MSG-134's Integration, Verification and Certification Tool and associated Process and promoting the participation and added value of IVCT.

C.2.1 Roadmap

- Exercise Specification Conference – 13th to 15th September 2016 – Beatenberg (Switzerland)
- Initial Planning Conference – 8th to 11th November 2016 – Garmisch (Germany)
- Main Planning Conference – 24th to 27th January 2017 – Slagelse (Denmark)
- Final Coordination Conference – 21th to 24th March 2017 – Bydgoszcz (Poland)
- Exercise Execution – 12th to 29th June 2017 – Bydgoszcz (Poland)

C.2.2 Preparation of the IVCT capability

IVCT participated as capability number #177 named "NATO-MSCOE-IVCT MSG134@CWIX 2017CWIX".

The CWIX Participation Form workflow represented in (Figure C-1) gives a rough idea of the process IVCT went through in order to participate to CWIX execution.

C.2.3 Preparation of the IVCT test cases

During the preparation conferences an analysis was performed in order to identify the best trade-off between CWIX ETCs development effort and the interests and the most common elements of the capabilities participating to the M&S Focus Area. A set of three potential badges were created mainly covering aspects regarding Entity, Warfare interactions and Dead-Reckoning.

C.2.3.1 CWIX Badges Proposal

Given the interoperability issues recorded in the M&S Focus Area during the CWIX executions since 2014, even very simple capability badges could bring in added value if tested by the IVCT during CWIX 2017.

Considering the recorded issues and the data fields involved in a limited analysis of PhysicalEntity objects and Warfare interactions, these would be a useful participation of the IVCT from a technical point of view, given that there could be enough time to develop the code for these test cases. Starting from the current definition of badges in terms of requirements and test procedures (HLA-BASE-2016, RPR-ENTITY-2016 and RPR-WARFARE-2016) a proposal for the definition and development of two specific CWIX badges follow.

They apply to RPR-FOM v2.0 or RPR-FOM modules of NETN.

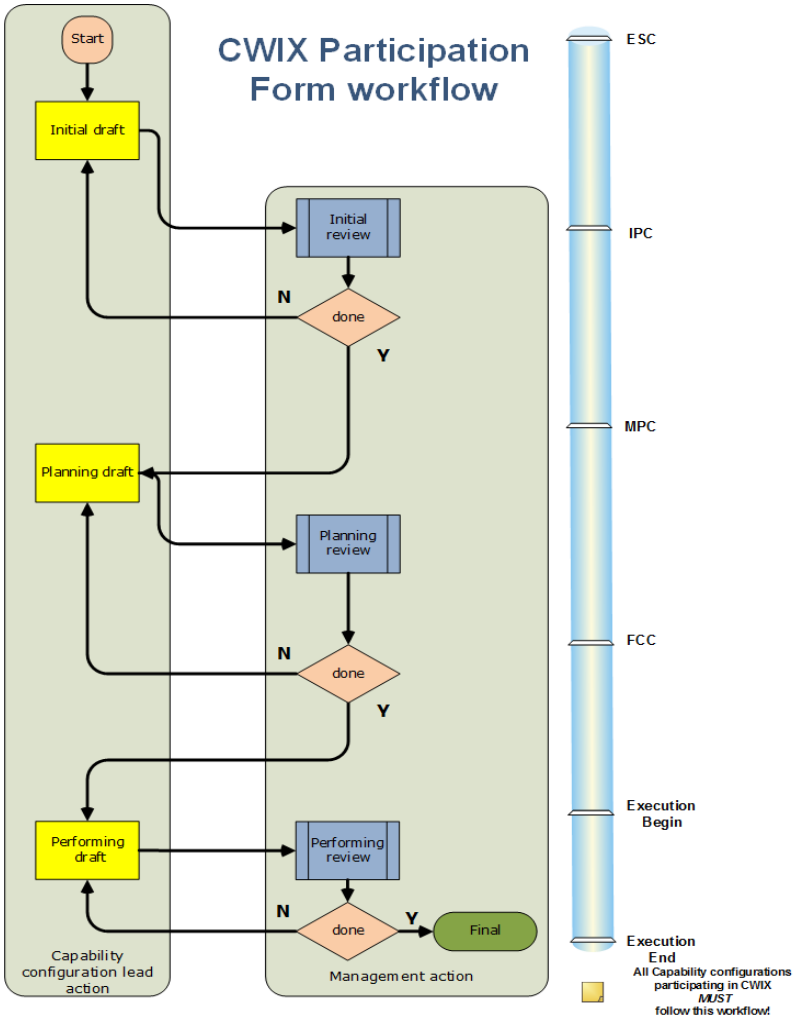

Figure C-1: CWIX Participation Form Workflow.

C.2.3.2 CWIX-ENTITY-2017

This test case is the main and most important one as a basis for all the others.

1) PREREQUISITE FOR SuT: Configure SuT with parameters defined in the Distributed Simulation Agreement (DSA): Federation Name, Federate Name, RTI network parameters, FOM Modules and configure DSA enumerations for EntityType
2) Configure IVCT with time-limits for tests
3) Configure IVCT with list of expected/acceptable Entity Type Enumerations (as defined in the DSA) through an external file
4) Start IVCT and connect to the RTI
5) Start the SuT and connect to the RTI
6) IVCT checks that the SuT properly joined the federation
7) IVCT subscribes to HLAfederate object class
8) IVCT requests AttributeValue updates of FederateName and FederateType of discovered HLAfederate object instances

9) IVCT verifies that the SuT FederateName and FederateType equals configured values
10) IVCT verifies that FOM modules loaded by the SuT matches the CS
11) IVCT subscribes to the DSA-specified published object class attributes
12) IVCT: check at least one object instance for each published object class was registered (HLA Object discovery service call)
13) IVCT requestAttributeValue updates of published object class attributes
14) IVCT verifies that attribute updates are reflected for discovered instances
15) IVCT VALIDATES that SuT-published values for EntityType attribute are compliant with the agreed list of enumerations
16) IVCT VALIDATES that SuT-published values for Spatial attribute are compliant with the agreed values
17) IVCT VALIDATES that for all the specified attributes in DSA, SuT-published values are compliant with the agreed list of values (e.g., EntityIdentifiers)
18) The SuT removes all the published instances
19) IVCT verifies the instances have been removed properly
20) The SuT resign from the federation
21) IVCT checks that the SuT properly resigned from the federation

C.2.3.3 CWIX-WARFARE-2017 (Depends on CWIX-ENTITY-2017)

REQUISITE for this test is for the SuT to have passed successfully the CWIX-ENTITY-2017 test case.

1) PREREQUISITE FOR the SuT: Configure the SuT with parameters defined in the Distributed Simulation Agreement (DSA): Federation Name, Federate Name, RTI network parameters, FOM Modules and configure DSA enumerations for MunitionType
2) Configure IVCT with time-limits for tests
3) Configure IVCT with list of expected/acceptable Munition Type Enumerations (as defined in the DSA) through an external file
4) Start IVCT and connect to the RTI
5) Start the SuT and connect to the RTI
6) IVCT checks that the SuT properly joined the federation
7) IVCT subscribe to HLAfederate object class
8) IVCT requestAttributeValue updates of FederateName and FederateType of discovered HLAfederate object instances
9) IVCT verifies that the SuT FederateName and FederateType equals configured values
10) IVCT verifies that FOM modules loaded by the SuT matches the CS
11) IVCT subscribes to in DSA-specified published object class attributes
12) IVCT subscribes to DSA-specified published interaction class and parameters
13) The SuT publishes WeaponFire
14) IVCT receives WeaponFire interaction and parameters

15) IVCT check required parameters for the WeaponFire interaction: EventIdentifier, FiringLocation, FiringObjectIdentifier, FuseType, InitialVelocityVector, MunitionType, WarheadType
16) When a tracked munitions is used (e.g., torpedoes, missiles, etc.): the SuT publishes BaseEntity.PhysicalEntity.Munition
17) When a tracked munitions is used (e.g., torpedoes, missiles, etc.): IVCT checks if the WeaponFire parameter MunitionObjectIdentifier is provided by the SuT
18) The SuT publish MunitionDetonation
19) IVCT receives MunitionDetonation interaction and parameters
20) IVCT check required parameters for the MunitionDetonation interaction: DetonationResult, DetonationLocation, EventIdentifier, FuseType, MunitionType, WarheadType
21) When a tracked munition is used, IVCT checks if the MunitionDetonation parameter MunitionObjectIdentifier is provided by the SuT (coherent with step 19)
22) When a tracked munition is used, IVCT checks if the SuT provides a value for EventIdentifier parameter that refers to a previous WeaponFire interaction
23) When a tracked munition is used, IVCT checks the state/removal of the SuT-published munition
24) The SuT removes all the published instances
25) IVCT verifies the instances have been removed properly
26) The SuT resign from the federation
27) IVCT checks that the SuT properly resigned from the federation

C.2.3.4 CWIX-DEADRECKON-2017 (Depends From CWIX-ENTITY-2017)

This could be another interesting badge to test, validating the dead-reckoning capability of a SuT; but not part of the 2017 tests.

C.2.3.5 TEST CASE TEMPLATE

A general-purpose Test Case Template was created in CWIX database in order to facilitate interested capabilities in writing appropriate test cases with IVCT. It is found in the CWIX Test Case Templates database as "*MS – HLA IVCT"* (#1296).

Purpose

Test Objective: The PRODUCER will join an HLA Federation together with the Integration Verification Certification Tool (IVCT) as a CONSUMER and the PRODUCER will have its HLA interface verified by the IVCT tool concerning the main aspects about RTI service calls and FOM management and entity data exchange.

Precondition

The following preconditions must be checked before running the test:

- Systems properly connected over the network;
- Time synchronization;

- Configure Producer and CONSUMER: Federation Name, Federate Name, RTI network parameters, FOM Modules and configuration data; and
- Start IVCT and it connects to RTI.

Validation Criteria

- **Success**: IVCT produce a report (log) about the PRODUCER activities that captures the PRODUCER behaviour during all the steps of the verification process;
- **Limited Success**: some steps in the verification process cannot be performed or verified; and
- **Interoperability Issue**: whenever a step is not performed or verified due to an unattended reason.

Verification Process

Following test cases rules, a 4-step verification process has been identified and described.

Table C-1: Verification Process of IVCT Test Case Template.

Number	Description	Expected Result
1	PROVIDER joins the federation.	IVCT reports the PROVIDER's activity in the IVCT log file. IVCT verifies that PROVIDER's FederateName and FederateType equals configured values.
2	PROVIDER declares its publish/subscribe modules.	IVCT verifies that FOM modules declared by PROVIDER correspond to the expected ones and reports the results in its log file.
3	PROVIDER publishes and updates entity data.	IVCT checks and validates the data published by the PROVIDER and reports the results in its log file.
4	PROVIDER removes all the published instances and resigns from the federation.	IVCT reports the PROVIDER's activity in resigning from the federation in the IVCT log file.

C.2.4 IVCT partners

Potential partners for test cases were identified during the conferences, but at the end of the execution it was possible to test only with some of them.

Table C-2: IVCT Partners.

Partner Name	Final interaction with IVCT
CAN-MSAAS 0.1@CWIX 2017	Not tested due to different RTIs used
HUN-KRONOS@CWIX 2017	Not tested, it was deployed on another network
HUN-MARCUS@CWIX 2017	Not tested, it was deployed on another network

Partner Name	Final interaction with IVCT
NATO-JFTC-JCATS@CWIX 2017	TESTED
NATO-JFTC-JLOD@CWIX 2017	Tested together with the one above
NATO-JFTC-VBS3@CWIX 2017	Not Tested
NATO-JWC-VBS3 (Collector)@CWIX 2017	TESTED
NATO-MSCOE-LVC GTW@CWIX 2017	TESTED
NATO-MSCOE-SGA@CWIX 2017	TESTED
POL-AFCCS TOPAZ@CWIX 2017	Not tested, it did not participate in an HLA Federation
SVN-JCATS@CWIX 2017	Not tested, this capability was withdrawn

C.2.5 Conduct of the IVCT Test Cases During CWIX Execution (12th to 29th June 2017)

Of the identified badges for CWIX, a set of basic ETCs were developed by France, covering HLA Verification, Declaration, Services and Objects (the only ones tested in CWIX). Canada produced ETCs covering HLA Entity and HLA Warfare (not tested due to configuration problems after the adoption of a new version of the framework with the graphical interface). The UK provided ETCs covering dead-reckoning (not tested because it was not possible to have them delivered in time due to delays in release approval). The tests did not focus on the badges' definition but on the specific ETCs involved. This was done in order to optimize the development effort in order to have ETCs already aligned with the final badges' definitions, not specifically for CWIX.

C.2.3.5.1 IVCT Installation, New GUI and Storyline

- 12th to 13th June: HW and capabilities check-in.
- 14th to 15th June: Set-up and Configuration of IVCT Virtual Machine inside CWIX Network.
- 16th June: no activities on IVCT, Focus Area HLA-tests postponed.
- 19th June: Issues in rebuilding the ETCs (IVCT dev-environment is user-dependent).
- 20th June:
- Installation of the new version and of the new GUI;
- FRA ETCs inserted into the new framework; and
- First tests with NATO-MSCOE-SGA (SOM required but no one had it).
- 21st June:
    - IVCT presentation to the Focus Area: useful for CWIX but it cannot be a requirement;
    - IVCT tests with NATO-MSCOE-SGA and NATO-JWC-VBS3.
- 22nd June: IVCT tests with NATO-JFTC-JCATS. Tests with CAN-MSAAS were scheduled as well but

it couldn't be tested as it required a different MAK RTI version than the one used by all the others in the Focus Area.

- 23rd June: IVCT tests with NATO-MSCOE-LVC GTW (Failed to load CAN ETC inside GUI).
- 26th June: IVCT tests with NATO-JFTC-JCATS (CAN ETC loaded but launch from GUI failed).
- 27th June: IVCT tests with NATO-MSCOE-LVC GTW (Issue reported due to continuous calls to HLAreportServiceInvocation).

C.2.6 IVCT CWIX Final Report Statements

The final statements summarizing IVCT participation to CWIX in its final report, taken from CWIX database, are reported in the following.

C.2.6.1 Interoperability Achievements

The first version of IVCT, even if yet a prototype, was able to connect and interoperate successfully with other partners' systems, and it was able to produce reports about conformance to HLA-BASE-2016 Capability Badge as defined by the NATO MSG 134. HLA Verification, HLA Declaration, HLA Services and HLA Objects executables were run and tested within the new graphical user interface of the tool. An important achievement for the capability was the interest it raised among the participants of the Focus Area and the feedback received by the partners.

C.2.6.2 Interoperability Challenges

The main challenges concerned the different configuration changes needed to test with different capabilities and the fact that some pre-requisites, such as the SOM, were not available from the partners, and a default SOM file had to be used.

C.2.6.3 Improvements from Previous CWIXs

This is the first year in CWIX for IVCT.

C.2.7 IVCT Hot Topics

Testing IVCT in CWIX was a very useful activity in order to identify which aspects of the tools need improvements, from both the developer and the user point of view, from installation, to configuration, to running tests.

The main topics identified are as follows:

- **IVCT development environment**: is user-dependent (since dependencies are downloaded in the user-profile folder), and first installation requires an Internet connection. A full offline installation, independent from the user account, should be available given that, like in CWIX, Internet cannot be expected to be available in the laboratory.
- **IVCT GUI**: still needs improvements and an easier configuration process, but it gives a good user-friendly tool to perform tests, avoiding annoying and complex shell scripting.
- **SOM:** this is a problem for IVCT since few SuT owners are able to provide its SOM. Using a default SOM covering all the services and publishing/subscribing to everything causes the SuT to fail certification testing every time, even if it is useful for checking the SuT HLA characteristics. Useful for integration and verification but useless for certification.

- **RTI versions and configurations:** unfortunately, the MAK RTI was not tested due to conflicts over the network between different versions with the same configuration that couldn't be changed due to tests scheduling. The Pitch RTI was only one present as a single version, so all the tests were performed using Pitch RTI version 5.0.1.0. The MAK RTI problem caused IVCT to be unable to test CAN-MSAAS 0.1 capability. After many attempts we gave up since it was not possible to change configurations.
- Unfortunately, the **CAN ETCs** were not tested. It was properly installed and compiled but, due to time limitations at CWIX we were unable to configure it under the new IVCT GUI.
- HLA_Services ETC behaved strangely with NATO-MSCOE-LVC GTW: IVCT was recording and logging a continuous call to **HLAreportServiceInvocation.** Even though this was probably the SuT's fault, it caused the generation of 100+ Mb logfiles, decrease in performance, and a log that was hard to manage or analyse. There could be some check to avoid strange behaviours or "infinite loops" in the log.
- "IVCT message" in CWIX and other experimentation venues have to be tailored to the context where certification is not the focus; in fact, many SuT owners in this context do not want their systems certified. Integration and validation are applications are more appealing to this audience, and the benefits they have in reducing configuration and integration efforts is much more appreciated.

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TR-MSG-134-Part-I AC/323(MSG-134)TP/840	ISBN 978-92-837-2167-3	PUBLIC RELEASE

5. Originator

Science and Technology Organization
North Atlantic Treaty Organization
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

6. Title

NATO Distributed Simulation Architecture and Design, Compliance Testing and Certification

7. Presented at/Sponsored by

Final Report of NATO MSG-134.

8. Author(s)/Editor(s)	9. Date
Multiple	September 2019
10. Author's/Editor's Address	**11. Pages**
Multiple	72

12. Distribution Statement

There are no restrictions on the distribution of this document. Information about the availability of this and other STO unclassified publications is given on the back cover.

13. Keywords/Descriptors

Capability badge
Certification
Federation of simulations
Integration
Interoperability
High Level Architecture
Verification

14. Abstract

NATO relies on standards and agreements, especially for distributed simulation (AMSP-01, STANAG 4603, etc.). Prior to 2004, the USA provided the High Level Architecture (HLA) certification tool suite, but since then, updates have not been made available. In conjunction with the development of a new certification tool suite, there is a need to maintain and update the NATO Education and Training Network (NETN) Federation Architecture and FOM Design (FAFD), as well. The NATO Modelling & Simulation Group 134 (MSG-134) began its work in October 2015 and will deliver the Integration, Verification and Certification Tool (IVCT), the associated Concept of Operations, and the updated NETN FAFD in October 2017. This open-source tool suite was tested during CWIX 2017 at JFTC, in June 2017.

The expectation is that IVCT will be generally used by NATO, and at the national level during the procurement process of simulators, as an acceptance test tool, and by industry during the development of simulators. Testing and certifying of systems will result in an overall improved interoperability of simulators in distributed networked simulation systems. Capability Badges, issued to federate that pass-certification testing provides an easy way for stakeholders to recognize the interoperability capabilities of a federate.

NORTH ATLANTIC TREATY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DIFFUSION DES PUBLICATIONS
STO NON CLASSIFIEES

Les publications de l'AGARD, de la RTO et de la STO peuvent parfois être obtenues auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la STO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus soit à titre personnel, soit au nom de votre organisation, sur la liste d'envoi.

Les publications de la STO, de la RTO et de l'AGARD sont également en vente auprès des agences de vente indiquées ci-dessous.

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivi du numéro de série. Des informations analogues, telles que le titre est la date de publication sont souhaitables.

Si vous souhaitez recevoir une notification électronique de la disponibilité des rapports de la STO au fur et à mesure de leur publication, vous pouvez consulter notre site Web (http://www.sto.nato.int/) et vous abonner à ce service.

CENTRES DE DIFFUSION NATIONAUX

ALLEMAGNE
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7, D-53229 Bonn

BELGIQUE
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research
for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30, 1000 Bruxelles

BULGARIE
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DGSIST 2
Recherche et développement pour la défense Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

DANEMARK
Danish Acquisition and Logistics Organization
(DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESPAGNE
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

ESTONIE
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

ETATS-UNIS
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72
92322 Châtillon Cedex

GRECE (Correspondant)
Defence Industry & Research General
Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HONGRIE
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALIE
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

LUXEMBOURG
Voir Belgique

NORVEGE
Norwegian Defence Research
Establishment
Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

PAYS-BAS
Royal Netherlands Military
Academy Library
P.O. Box 90.002
4800 PA Breda

POLOGNE
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

REPUBLIQUE TCHEQUE
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

ROUMANIE
Romanian National Distribution
Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

ROYAUME-UNI
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down
Salisbury SP4 0JQ

SLOVAQUIE
Akadémia ozbrojených síl gen.
M.R. Štefánika, Distribučné a
informačné stredisko STO
Demänová 393
031 01 Liptovský Mikuláš 1

SLOVENIE
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

TURQUIE
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi
Başkanlığı
06650 Bakanliklar – Ankara

AGENCES DE VENTE

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
ROYAUME-UNI

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications STO, RTO et AGARD figurent dans le « NTIS Publications Database » (http://www.ntis.gov).

NORTH ATLANTIC TREATY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DISTRIBUTION OF UNCLASSIFIED STO PUBLICATIONS

AGARD, RTO & STO publications are sometimes available from the National Distribution Centres listed below. If you wish to receive all STO reports, or just those relating to one or more specific STO Panels, they may be willing to include you (or your Organisation) in their distribution.

STO, RTO and AGARD reports may also be purchased from the Sales Agencies listed below.

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number. Collateral information such as title and publication date is desirable.

If you wish to receive electronic notification of STO reports as they are published, please visit our website (http://www.sto.nato.int/) from where you can register for this service.

NATIONAL DISTRIBUTION CENTRES

BELGIUM
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30
1000 Brussels

BULGARIA
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DSTKIM 2
Defence Research and Development Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

CZECH REPUBLIC
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

DENMARK
Danish Acquisition and Logistics Organization (DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESTONIA
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc – BP 72
92322 Châtillon Cedex

GERMANY
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7
D-53229 Bonn

GREECE (Point of Contact)
Defence Industry & Research General Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HUNGARY
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALY
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

LUXEMBOURG
See Belgium

NETHERLANDS
Royal Netherlands Military Academy Library
P.O. Box 90.002
4800 PA Breda

NORWAY
Norwegian Defence Research Establishment, Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

POLAND
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

ROMANIA
Romanian National Distribution Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

SLOVAKIA
Akadémia ozbrojených síl gen M.R. Štefánika, Distribučné a informačné stredisko STO
Demänová 393
031 01 Liptovský Mikuláš 1

SLOVENIA
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

SPAIN
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

TURKEY
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanliklar – Ankara

UNITED KINGDOM
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down, Salisbury SP4 0JQ

UNITED STATES
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

SALES AGENCIES

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
UNITED KINGDOM

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of STO, RTO and AGARD publications are given in "NTIS Publications Database" (http://www.ntis.gov).

ISBN 978-92-837-2167-3