



STO TECHNICAL REPORT

TR-MSG-134-Part-II

NATO Simulation Interoperability Test and Certification Service – Concept of Operations (CONOPS)

(Service de l'OTAN de certification et de test d'interopérabilité
dans le domaine de la simulation)

Version 1.0 D7. Developed by NATO MSG-134.



Published September 2019





STO TECHNICAL REPORT

TR-MSG-134-Part-II

NATO Simulation Interoperability Test and Certification Service – Concept of Operations (CONOPS)

(Service de l'OTAN de certification et de test d'interopérabilité
dans le domaine de la simulation)

Version 1.0 D7. Developed by 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 power-house 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

Copyright © STO/NATO 2019
All Rights Reserved

ISBN 978-92-837-2168-0

Single copies of this publication or of a part of it may be made for individual use only by those organisations or individuals in NATO Nations defined by the limitation notice printed on the front cover. The approval of the STO Information Management Systems Branch is required for more than one copy to be made or an extract included in another publication. Requests to do so should be sent to the address on the back cover.

Table of Contents

	Page
List of Figures	vi
List of Tables	vii
List of Acronyms	viii
Glossary	xi
MSG-134 Membership List	xiv
Executive Summary and Synthèse	ES-1
Chapter 1 – Overview	1-1
1.1 Identification	1-1
1.2 Revision History	1-1
1.3 Document Overview	1-2
1.4 System Overview	1-2
Chapter 2 – Current System Situation	2-1
2.1 Background, Objectives, and Scope	2-1
2.2 Operational Constraints	2-1
2.3 Description of the Current System	2-1
2.4 User Profiles	2-1
2.5 Support Environment	2-2
Chapter 3 – Justification and Nature of the Changes	3-1
3.1 Justification for Changes	3-1
3.2 Description of the Desired Changes	3-2
3.3 Priorities	3-3
3.4 Changes Considered, but Not Included	3-3
3.5 Assumptions and Constraints	3-3
Chapter 4 – Concept of the Proposed System	4-1
4.1 Background, Objectives and Scope	4-1
4.2 Key Roles	4-1
4.2.1 Accreditation Authority	4-2
4.2.2 Certification Entity	4-2
4.2.3 Accreditation Test Laboratory	4-2
4.3 Key Components	4-2
4.3.1 Interoperability Requirements	4-3
4.3.2 Abstract Test Case	4-4

4.3.3	Interoperability Capability Badges	4-5
4.3.4	Conformance Statement	4-7
4.3.5	Integration, Verification, and Certification Tool (IVCT)	4-7
4.3.6	Information Available to the Public <i>via</i> the CE website	4-9

Chapter 5 – Operational Scenarios **5-1**

5.1	Accreditation and Certifications	5-1
5.2	Accreditation Process of a Candidate for the ATL Role	5-2
5.3	Accreditation Process of a Candidate for the CE Role	5-2
5.4	Development and Maintenance	5-2

Chapter 6 – Summary of Impacts **6-1**

Chapter 7 – Analysis of the Proposed System **7-1**

Chapter 8 – Business Model **8-1**

8.1	Business of Certification Activity	8-1
8.2	Customer-Funded Business Model	8-1
8.2.1	Early Development (2015-2017)	8-2
8.2.2	Initial Operational Capability (2018-2020)	8-2
8.2.3	Fully Operational Capability (2021 And Beyond)	8-2
8.3	Proposed Organization	8-2
8.4	Strategy for Initial Operational Capability	8-2
8.5	Business Model for the Transition Period From IOC to FOC	8-4
8.6	Ownership of the IVCT, Abstract Test Cases, and Executable Test Cases	8-4

Chapter 9 – References **9-1**

Annex A – Operating Procedures **A-1**

A.1	Roles and Responsibilities	A-1
A.1.1	Accreditation Authority	A-1
A.1.1.1	Initial Operational Requirements	A-1
A.1.1.2	Operational Use Cases	A-2
A.1.2	Certification Entity	A-3
A.1.2.1	Operational Requirements	A-3
A.1.2.2	Operational Use Cases	A-3
A.1.3	Accredited Test Laboratory	A-5
A.1.3.1	Operational Requirements	A-6
A.1.3.2	Operational Use Cases	A-6
A.1.4	Customer	A-7
A.1.4.1	Operational Requirements	A-8
A.1.4.2	Operational Use Cases	A-8
A.2	Policies and Constraints	A-8
A.3	Use Cases and Scenarios	A-10

A.3.1	Accreditation and Certification	A-10
A.3.2	Accreditation Process of a Candidate for the ATL Role	A-12
A.3.3	Accreditation Process of a Candidate for the CE Role	A-12
A.3.4	Perform Certification Test	A-12
A.3.5	Definition of Certification Workflow	A-13
A.3.6	Development and Maintenance	A-14
A.3.6.1	Test Tool Development	A-15
A.3.6.2	Test Case Implementation	A-17

Annex B – Capability Badges, Interoperability Requirements and Abstract Test Cases **B-1**

B.1	Interoperability Capability Badges	B-1
B.2	Interoperability Requirements	B-5
B.3	Abstract Test Cases	B-16

Annex C – Conformance Statement **C-1**

Annex D – Integration, Verification and Certification Tool **C-2**

List of Figures

Figure		Page
Figure 1-1	NOV-1 NATO Simulation Interoperability Test and Certification Service	1-3
Figure 3-1	Increase Interoperability, Reuse, and Cost Effectiveness	3-3
Figure 4-1	New Scope of Interoperability Certification	4-1
Figure 4-2	NOV-4 Organizational Relationships and Key Roles	4-2
Figure 4-3	Key Concept Used in Certification Service	4-3
Figure 4-4	Relationships Between the Concepts of a CB, its Associated IRs, and the System under Test	4-6
Figure 4-5	Major IVCT Modules	4-8
Figure 4-6	Using IVCT	4-9
Figure 5-1	Use Case of Certification Service	5-1
Figure 5-2	Use Case of Development	5-3
Figure 5-3	Definition of Certification Workflow Use Case Diagram	5-4
Figure 8-1	Funding of IVCT and Certification Service	8-3
Figure 8-2	Proposed Organizational Structure	8-4
Figure A-1	NOV-2 User Roles	A-1
Figure A-2	Use Case of Certification Service	A-11
Figure A-3	Use Case of Perform Certification Test	A-12
Figure A-4	Use Case of Definition Certification Workflow	A-13
Figure A-5	Use Case of Development	A-14
Figure A-6	Use Case of Test Tool Development	A-16
Figure A-7	Use Case of Test Case Implementation	A-17
Figure B-1	Key Elements of the Certification Process	B-1
Figure B-2	Relationships Between a CB, Its Associated IRs and the System under Test (SuT)	B-2
Figure D-1	Major IVCT Modules	D-1
Figure D-2	Using IVCT	D-2

List of Tables

Table		Page
Table 4-1	Categories of Interoperability Requirements	4-4
Table 4-2	First Set of Abstract Test Cases	4-4
Table 4-3	Initial Set of Capability Badges	4-6
Table 5-1	Use Cases Related to Certification Service	5-2
Table 5-2	Use Cases Related to Development	5-3
Table 5-3	Use Cases of Verification Workflow	5-5
Table 7-1	Analysis Results of Certification Service	7-1
Table A-1	Initial Operational Requirements of Accreditation Authority	A-2
Table A-2	Use Cases Related to Accreditation Authority	A-2
Table A-3	Operational Requirements of Certification Entity	A-3
Table A-4	Use Cases Related to Certification Entity	A-4
Table A-5	Operational Requirements of Accredited Test Laboratory	A-6
Table A-6	Use Cases Related to Accredited Test Laboratory	A-6
Table A-7	Operational Requirements of Customer	A-8
Table A-8	Use Cases Related to Customer	A-8
Table A-9	Operational Requirements for Operational Policies and Constraints	A-8
Table A-10	Use Cases Related to Certification Service	A-11
Table A-11	Use Cases Related to Perform Certification Test	A-13
Table A-12	Use Cases Related to Definition Certification Workflow	A-14
Table A-13	Use Cases Related to Development	A-15
Table A-14	Use Cases Related to Test Tool Development	A-16
Table A-15	Use Cases Related to Test Case Implementation	A-17
Table B-1	Interoperability Capability Badges	B-2
Table B-2	Categories of Interoperability Requirement	B-5
Table B-3	Initial Set of Interoperability Requirements	B-6
Table B-4	Set of Abstract Test Cases	B-16

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
FOC	Final Operational Capability

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
NSRL	NATO Simulation Resources Library

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
SQL	Structured Query Language
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)
SWOT	Strengths, Weaknesses, Opportunities, and Threats
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

<i>Abstract Test Case</i>	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.
<i>Abstract Test Method</i>	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.
<i>Abstract Test Suite</i>	ISO/IEC 9646-1: A test suite composed of abstract test cases.
<i>Accreditation</i>	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.
<i>Accreditation Authority (AA)</i>	DoD M&S Glossary: The organization or individual responsible to approve the use of models, simulations, and their associated data for a particular application.
<i>Accredited Test Laboratory</i>	A Test Laboratory which has been accredited by an Accreditation Authority to perform Compliance Testing.
<i>Capability Badge</i>	A token of achievement in terms of passing a test related to Interoperability Requirements.
<i>Certification Agent</i>	An entity or person that has been approved by the Accreditation Authority to perform Compliance Testing.
<i>Certification Artefact</i>	IEEE-24765-2010: The tangible results from a certification process.
<i>Certification Criteria</i>	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.
<i>Certification Process</i>	IEEE-24765-2010: The process of assessing whether an asset conforms to predetermined certification criteria appropriate for that class of asset.
<i>Certification Property</i>	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.
<i>Certification Test</i>	Test done during the Certification Process.
<i>Certification</i>	IEEE-24765-2010: The process of confirming that a system or component complies with its specified requirements and is acceptable for operational use.
<i>Compliance</i>	The statement that an asset fulfils the required behaviour rules of a given standard.

<i>Compliance Certificate</i>	Adapted from IEEE-24765-2010: A written guarantee that a system or component complies with its specified requirements and is acceptable for operational use.
<i>Compliance Testing</i>	The process of testing the behaviour of an asset against a given standard conducted by the test tool.
<i>Concept of Operations</i>	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.
<i>Conformance</i>	In this document, conformance is considered to be a synonym to Compliance.
<i>Conformance Statement</i>	A written statement that confirms the conformance of a SuT (System under Test) to a given standard.
<i>Customer</i>	An entity (or a person) who has sufficient legal rights to submit a given federate to compliance testing and to allow the CA to publicly announce the compliance of the SuT (System under Test).
<i>Federate</i>	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).
<i>Federate Owner</i>	An entity (or a person) who has legal ownership rights to a given federate.
<i>Federation</i>	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.
<i>Integration, Verification, and Certification Tool (IVCT)</i>	Software framework to support integration and verification task for simulation federates and to perform the certification tests for a SuT (System under Test).
<i>Means of Testing</i>	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.
<i>Science Connect</i>	Collaborative Workspace provided by NATO CSO.
<i>System under Test (SuT)</i>	The System which is the target of Compliance Testing. An SuT is an instance of an asset.
<i>System under Test Environment (SuTE)</i>	Environment required for the SuT to function correctly for certification tests.
<i>Test</i>	IEEE-829-2008: The activity of executing a Test Procedure/Test Case.
<i>Test Case</i>	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.

<i>Test Case Developer</i>	Individuals organizations responsible for the design, implementation and maintenance of the test cases.
<i>Test Class</i>	IEEE-829-2008: A designated grouping of test cases.
<i>Test Federate</i>	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.
<i>Test Laboratory</i>	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).
<i>Test Procedure</i>	IEEE-829-2008: Detailed instructions for the set-up, execution, and evaluation of results for a given test case.
<i>Test Tool Developer</i>	Individuals/organizations responsible for design, implementation and maintenance of the certification tool.
<i>WebEx</i>	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

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

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

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

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

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

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

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

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

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

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

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

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

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

* Contributing Author.

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

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

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

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

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

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

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

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-II)

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 with 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.

Service de l'OTAN de certification et de test d'interopérabilité dans le domaine de la simulation

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

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 – OVERVIEW

1.1 IDENTIFICATION

The system described in this Concept of Operations (CONOPS) covers the organization, process and tools to support NATO certification of simulation components' interoperability capability and is referred to as the **NATO Simulation Interoperability Test and Certification Service**. See Table 1-1 below. This includes, but is not limited to, simulation interoperability agreements as specified in the NETN Federation Agreement and FOM Document [1], capability badges, and interoperability requirements.

Table 1-1: Identification.

Title	NATO Simulation Interoperability Test and Certification Service – Concept of Operations (CONOPS).
Activity Reference	MSG-134: NATO Distributed Simulation Architecture and Design, Compliance Testing and Certification.
Originator's Reference	STO-xx-MSG-134, etc.
ISBN Reference	ISBN xxxx
Security Classification	PUBLIC RELEASE
Originator	NATO Science and Technology Organization
Published	xxx 2018
Distribution Statement	This document is distributed in accordance with NATO Security Regulations and STO policies.

1.2 REVISION HISTORY

Table 1-2 indicates the revision history associated with the report writing for this activity.

Table 1-2: Revision History.

Date	Version	Description	Sign
2015-09-21	v1.0 D1	Initial Draft.	BL
2015-12-07	v1.0 D2	Updates based on comments from 8th Meeting (MSG-134). Major clean-up between Req. spec and CONOPS.	BL
2016-02-18	v1.0 D3	Updates based on the IITSEC meeting and received comments until 2-18-2016.	JH

Date	Version	Description	Sign
2016-07-14	v1.0 D4	Major update based on comments and actions. Harmonization of definitions, inclusion of annexes with detailed information.	BL
2017-10-05	V1.0 D5	Updates based on comments from 25th Meeting (MSG-134).	JR
2017-10-18	V1.0 D6	Update of customer funded business model.	JR
2018-02-26	V1.0 D17	Update of remaining comments.	JR

1.3 DOCUMENT OVERVIEW

The primary audience of this document is the members of the MSG-134 Research Task Group (RTG) and other research groups in the NATO Modelling and Simulation Group (NMSG).

The main purpose of this document is to communicate and build consensus on:

- The needs of users and the proposed system expectations
- The proposed business model, processes, and roles
- The scope of work for MSG-134 activities in the realization of the system
- The system developer's understanding of user needs and how the system will meet those needs

Furthermore, the CONOPS is a deliverable of MSG-134 and a summary of the CONOPS will be included in the MSG-134 final technical report, in papers and presentations, and in other marketing and information material.

Chapter 1 provides an overview of the NATO Simulation Interoperability Test and Certification Service.

Chapter 2 provides references to background material and related documentation.

Chapter 3 describes the current state of the system and issues.

Chapter 4 describes the rationale and justification for the proposed service.

Chapter 5 describes the main concepts and constructs of the proposed service.

Chapter 6 describes in more detail the different operational scenarios.

Chapter 7 provides a summary of the impacts of the proposed service.

Chapter 8 provides a Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis of the proposed service.

Chapter 9 describes the service business model.

1.4 SYSTEM OVERVIEW

MSG-134 delivers a system for certification, including processes and tools, to enable cost-effective and reliable Plug and Play of multinational simulations for the warfighter.

The purpose of the system is to implement a capability for NATO certification of simulation components' interoperability. The system consists of organizations, roles, processes and tools. See Figure 1-1 below. The system is used to verify individual simulation component compliance with NATO interoperability standards for modelling and simulation, and to provide certificates of compliance for simulation components that successfully complete the certification process.



Figure 1-1: NOV-1 NATO Simulation Interoperability Test and Certification Service.

The Integration, Verification, and Certification Tool (IVCT) is defined as a software package supporting test and verification in the certification process. However, the IVCT is also expected to be available for other test and integration activities in other processes.



Chapter 2 – CURRENT SYSTEM SITUATION

2.1 BACKGROUND, OBJECTIVES, AND SCOPE

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 identifies standards and common agreements and relies on partners to comply with these standards. The NATO M&S Standards Profile [2], provides a list of recommended M&S related standards. The NATO Education and Training Network Federation Architecture and Federation Object Model (FOM) Design Document (NETN FAFD) [1] developed by MSG-068 and MSG-106 provides additional agreements on the use of standards to support distributed simulation. High Level Architecture (HLA) [3] is identified as one of the core standards for distributed simulation. It states that participating nations agree to use the HLA Compliance Certification Process established by the NATO Modelling and Simulation Group (NMSG).

The Federate Compliance Test System (FCTS) software tool manages and performs the compliance verification processes for interoperable High Level Architecture (HLA) based federates built in compliance with the HLA 1.3 and IEEE 1516-2000 standards for modelling and simulation. It consists of the Federate Compliance Test Tool (FCTT) and the Federate Test Management System (FTMS). These tools were developed by the USA and released to NATO in 2004. The NATO Certification Advisory Group (CeAG) was established as a subgroup to NMSG to create a community of NATO nations willing to provide certification services using FCTS. NATO certification services were established and are, or have, been operational in France, the USA, and Sweden. This document supersedes the HLA Certification Testing Capability procedures produced by the HLA Working Group – MSG-050.

2.2 OPERATIONAL CONSTRAINTS

The FCTT developed by the USA has undergone several updates based on feedback from the user community. However, due to export restrictions, new versions of FCTT have not been released to NATO. The NATO version of FCTT is currently limited to testing of compliance with HLA 1.3 and HLA IEEE 1516-2000 interfaces and cannot be used to test the latest version of HLA [4].

2.3 DESCRIPTION OF THE CURRENT SYSTEM

The FTMS is a web-based management system that supports the certification process. Requests for certification and all artefacts required for submitting and performing certification testing are provided through the FTMS. The FCTT is the actual software that performs federate testing. It checks the System under Test (SuT) for compliance with a Conformance Statement (CS) provided by the owner of the SuT. The tests include the federates' use of HLA services, and Object Model Template (OMT) / Simulation Object Model (SOM) consistency and conformance.

2.4 USER PROFILES

Testing is performed by a nationally designated Certification Agent and certificates are issued by a national Certification Entity.

2.5 SUPPORT ENVIRONMENT

The existing FCTS software is no longer maintained by the USA although a version has been made available as Open Source under GNU General Public License version 3.0 (GPLv3). No active contributions to the Source Forge project, where the source code is hosted, have been noticed.

Chapter 3 – JUSTIFICATION AND NATURE OF THE CHANGES

3.1 JUSTIFICATION FOR CHANGES

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. Updated and new standards for simulation interoperability 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 HLA services interface to also include testing of compliance with federation agreements.

Due to the lack of support for the latest version of the HLA standard (IEEE 1516-2010) [4] and the general need for additional types of testing, NATO has conducted research (ET-35 and MSG-134) on ways to move forward and provide an enhanced capability for simulation interoperability certification.

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 concluded that the FCTT cannot be used as a foundation for a future certification tool. MSG ET-035 also concluded that HLA compliance tests needs to be extended beyond the HLA interface and data exchange testing to address more complex federation agreements and requirements.

MSG-134 researched and delivered:

- 1) Maintenance and update of the NETN FAFD; and
- 2) Procedures and reference implementations of Integration Verification and Certification Tools (IVCT) modules.

This work is to support compliance testing and certification of NETN FAFD compliant simulation components, including certification of STANAG 4603.

Within the M&S community, it is generally recognized that the technical interoperability between systems is no longer a fundamental problem. However, high-level interoperability 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 selected system components. Early identification of interoperability issues reduces the risk and cost associated with less interoperable system components. A high degree of interoperability allows more flexible federation design and composability of simulation systems without significantly increasing the complexity and costs associated with test and integration [5].

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 it can also be valuable for the system integrator and simulation system developer.

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

JUSTIFICATION AND NATURE OF THE CHANGES

A certification service provides unbiased compliance testing against predefined sets of interoperability requirements based on the conformance statement provided by the SuT owner. Certificates are provided by authorized certification entities and are tokens of achieved compliance with interoperability requirements as specified in conformance statements. Simulation components are required to have, or obtain, certificates in order to be candidates for procurement, or as acceptance test requirements as specified in STANAG 4603 [3].

The following value propositions are recognized:

- **Improving Federate Tool Quality:** by using the IVCT in the development phase of a simulation component, the federate developer is provided with a high quality and well-recognized testing tool to support development and quality assurance. In such a setting, the IVCT can be used in privately hosted test laboratories.
- **Proving Federate Compliance:** by certifying a federate against a conformance statement, the federate developer improves the value of the federate by being able to provide proof of interoperability. Certification must be done by an independent and trusted certification service.
- **Compliance Label:** a compliance label provides the user of a federate with a solid statement about its quality. Such a label reduces the risk of faulty software and incompatible federates. This concept is further developed as the concept of interoperability capability badges.
- **Federate Integration Assistance:** by using the monitoring and testing capabilities of the IVCT, a federation integrator has better control, diagnostic and documentation functions. Essentially it will be easier to identify federates behaving outside their conformance statements. It will also facilitate the integration of a certified federate into a new federation.
- **Federate Verification Assistance:** by using the test cases definition and execution framework of the IVCT, federate users can verify application behaviour. For simple tests, this can be done using standard use cases. For more complex tests, the generic test case development framework can be used to create test cases for validation of specific application logic.

The following effects are anticipated by composing synthetic environments based on pre-tested and verified simulation components with certified interoperability capabilities (see Figure 3-1, below):

- Reduced Cost of Distributed Simulation Integration;
- Reduced Risk in Distributed Simulation Integration;
- Reduced Integration Time; and
- Increased Level of Interoperability in Distributed Simulation.

3.2 DESCRIPTION OF THE DESIRED CHANGES

Following from the discussion of Section 4.1, the following is a list of desired outcomes:

- A formalized process and procedures for compliance testing and certification;
- Accreditation of test laboratories and certification entities;
- Tools to support Federation Agreement testing;
- Tools to support HLA IEEE 1516-2010 testing;
- Tools availability to support development, test and integration; and
- Open source core for tools extendable by COTS vendors.

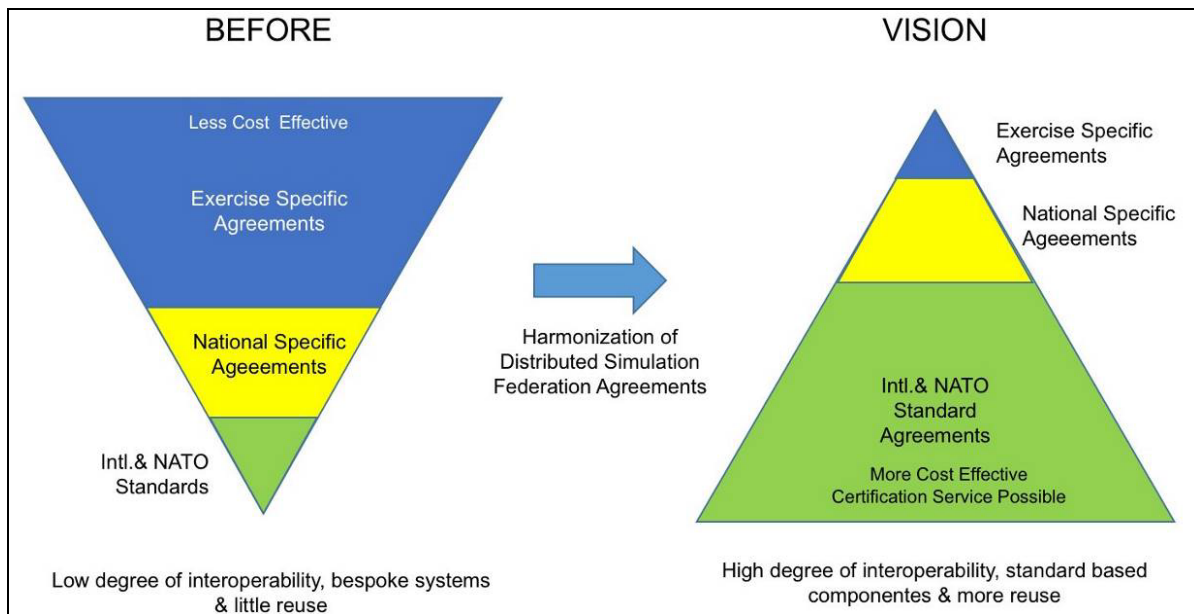


Figure 3-1: Increase Interoperability, Reuse, and Cost Effectiveness.

3.3 PRIORITIES

Tools developed as part of MSG-134 will focus on the core testing engine and not user interface experience. The following areas of interoperability have been identified as priorities:

- STANAG 4603 (HLA Evolved) – HLA Compliance.
- NETN Physical – a federate’s ability to produce and/or consume entity-state information to/from other federates in a federation.
- NETN Warfare – a federate’s ability to produce and/or consume events related to weapon firing, munition detonations and resulting effects on simulated models.
- NETN TMR – a federate’s ability to transfer and/or receive modelling responsibilities from other federates in the federation.
- NETN MRM – a federate’s ability to participate in a controlled aggregation and/or de-aggregation of simulated models.

3.4 CHANGES CONSIDERED, BUT NOT INCLUDED

The following areas of interoperability have been considered but are only partially addressed in the scope of work for MSG-134:

- Time Management-Related interoperability requirements – synchronization of time, time-stamping, time-stamp-ordered data delivery, etc.
- Fault and Performance-Related interoperability requirements – Managing Federate and Federation lost call backs gracefully; survivability in large federations (robustness).

3.5 ASSUMPTIONS AND CONSTRAINTS

The current focus is HLA and specifically IEEE 1516-2010 and the assumption is that HLA will not be replaced in the near future.

JUSTIFICATION AND NATURE OF THE CHANGES

Customers need to see the receipt of a compliance label for their products as a necessity. It might be assured in two ways; the first is to request at the NATO/National level to have a compliance label before any component is used for any training event, exercise, or experimentation effort. The second is to use a marketing strategy to challenge companies to get the highest available compliance label for their products.

Chapter 4 – CONCEPT OF THE PROPOSED SYSTEM

4.1 BACKGROUND, OBJECTIVES AND SCOPE

The NATO Simulation Interoperability Test and Certification Service is composed of tools and organizations that manage and deliver services for testing, verification, and certification of simulation components to enable efficient integration. These services must be self-sustaining, meaning there must be a business case with clear definitions of roles and responsibilities of the organizations involved. To be viable the proposed services must provide a benefit for customers. The main added value is the common understanding and description of NATO defined interoperability compliance.

The scope of interoperability certification provided by the system is wider than previous systems, limited to HLA certification of primarily technical interoperability (see Figure 4-1).

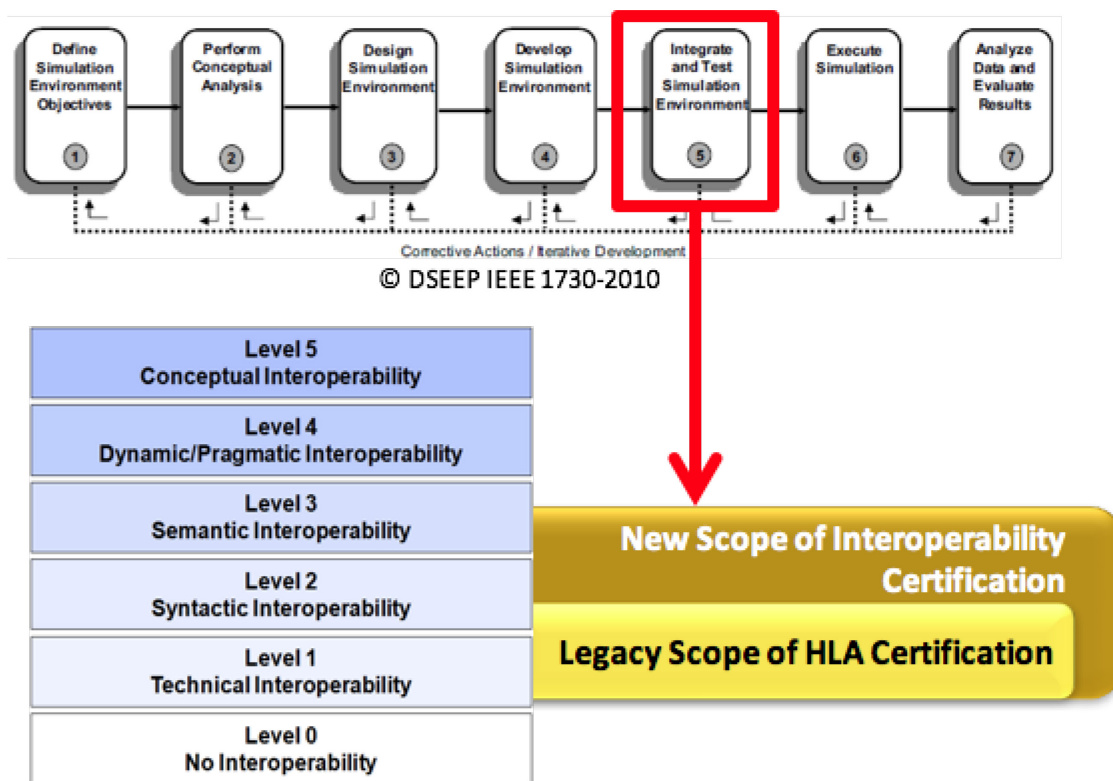


Figure 4-1: New Scope of Interoperability Certification.

4.2 KEY ROLES

Annex A: Operating Procedures defines all identified roles and responsibilities in more detail.

All the following roles' responsibilities are defined for the FOC. The IOC responsibilities are the same but supported by an MSG-134 follow-on activity (see Figure 4-2).

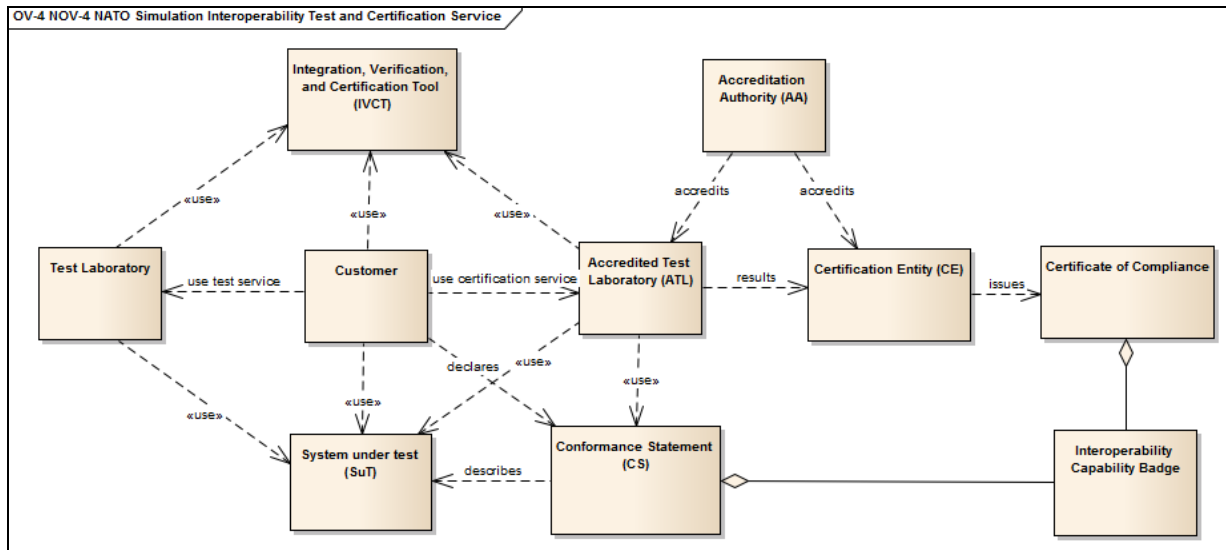


Figure 4-2: NOV-4 Organizational Relationships and Key Roles.

4.2.1 Accreditation Authority

The **Accreditation Authority (AA)** is a NATO-appointed organization responsible for maintaining the business model and procedures used by Accredited Test Laboratories (ATLs) and Certification Entities (CEs).

4.2.2 Certification Entity

The **Certification Entity (CE)** is an organization accredited by the Accreditation Authority (AA) and given the authority to issue certificates of compliance to systems that have successfully undergone 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 with the Executable Test Cases (ETCs) to ATLs.

4.2.3 Accreditation Test Laboratory

An **Accredited Test Laboratory (ATL)** is a Test Laboratory accredited by the Accreditation Authority (AA) and given the official authority to perform certification tests of Interoperability Requirements (IR) where the test results are recognized by the Certification Entity (CE) as valid for issuing certificates of compliance. The role of an ATL is to, upon request from a Customer, conduct certification tests on a System under Test (SuT) on behalf of a CE according to the business model defined by the AA. ATLs use the Integration, Verification and Certification Tool (IVCT) and Executable Test Cases (ETCs) provided by the CE to verify IRs associated with Capability Badges (CBs) defined in the SuT Conformance Statement (CS). The CS is submitted by the Customer along with the SuT. The ATL delivers test results to the CE in a secure manner for official certification. ATLs continuously provide feedback on IVCT use to the CE and propose improvements to the test system and procedures. ATLs support the CE in maintenance tasks according to the business model set by the AA. ATLs collect IRs and proposed them to the AA for inclusion in the test suite.

4.3 KEY COMPONENTS

The NATO Simulation Interoperability Test and Certification Service, as shown below in Figure 4-3, consists of tools, organization and associated processes to deliver functional services related to test, verification, integration, and certification of interoperability capabilities, of simulation systems and components.

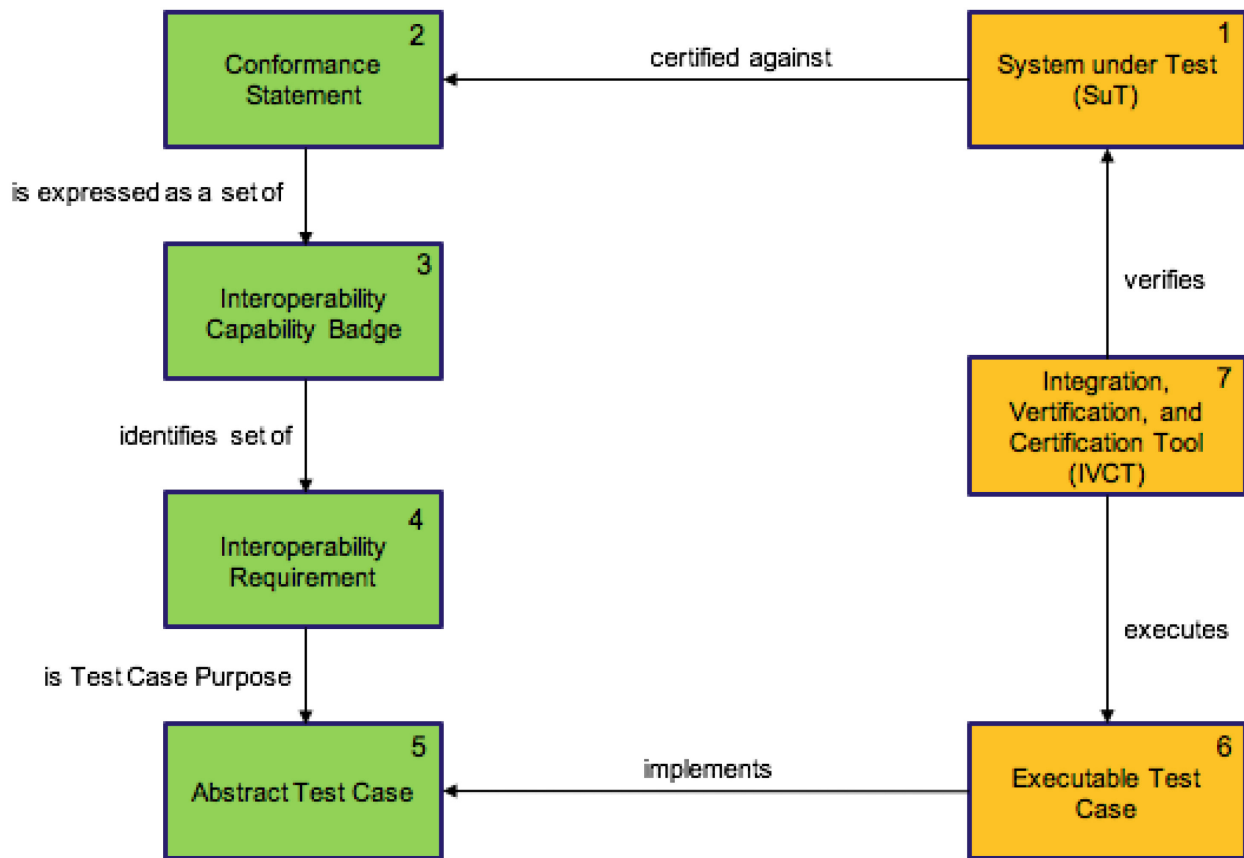


Figure 4-3: Key Concept Used in Certification Service.

The System under Test (SuT) is certified against a Conformance Statement (CS) expressed as a set of interoperability Capability Badges (CBs) which identify 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 capability badges as tokens of interoperability compliance.

4.3.1 Interoperability Requirements

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. See Table 4-1 below.

Sets of related IRs can be defined and grouped to form interoperability Capability Badges (CBs) used to express a system’s capability to interoperate on a higher level than individual IRs.

IRs can also be grouped and associated with Abstract Test Cases (ATCs) as the implicit purpose of an ATC is to verify all associated IRs.

IRs can be grouped into categories (see Table 4-1).

Table 4-1: Categories of Interoperability Requirements.

ID	Name	Description
BP	Best Practice Conformance	Requirements related to best practices for distributed simulation.
DOC	Documentation Conformance	Requirements for documenting interoperability capabilities.
NETN	NETN Requirements	Requirements related to NETN FAFD, AMSP-04 Ed A, STANREC 4800.
RPR2	RPR2 Requirements	Requirements related to RPR-FOM v2.0.
SOM	Simulation Object Model Conformance	Requirements related to the Conformance of a SuT to the SOM provided in a CS.

Annex B: Capability Badges, Interoperability Requirements and Abstract Test Cases, defines the initial set of interoperability requirements in more detail.

4.3.2 Abstract Test Case

An IVCT **Abstract Test Case (ATC)** is a complete, and implementation independent, specification of the actions required to verify a specific set of Interoperability Requirements (IR) associated with the ATC. This implies that the purpose of the ATC is to test all associated IRs.

The Certification Entity (CE) is responsible for defining the test case purposes (associating IRs with the ATC), and based on the purpose, specifying the test steps, actions, and valid responses and outcomes. Validation of an ATC against its test purpose is done by a CE.

A Test Case Developer (TCD) is contracted by a CE to implement Executable Test Cases (ETCs) based on ATCs. These are scripts or compiled programs that can execute as part of IVCT. ETCs are verified by a CE and delivered to Accredited Test Laboratories (ATL) for use with the Integration, Verification and Certification Tool (IVCT).

MSG-134 has developed the first set of ATCs. See Table 4-2 below.

Table 4-2: First Set of Abstract Test Cases.

ID	Name	Description
CS-VERIFY	CS Verification	Verify Conformance Statement (CS) completeness and format.
FOM-DECODE	FOM Data Decoding Verification	Verify attribute and parameter value decoding conformance with the SOM specified in the CS.
FOM-ENCODE	FOM Data Encoding Verification	Verify attribute and parameter value encoding conformance with the SOM in the CS.
HLA-BEST	HLA-Best Practices Verification	Verify use of HLA services and callbacks according to best practices.

ID	Name	Description
HLA-DECLARE	HLA Declaration Management	Verify HLA declaration management services are used according to the CS.
HLA-OBJECT	HLA Object Management	Verify HLA object management services are used according to the CS.
HLA-SERVICES	HLA Services Verification	Verify use of HLA services and callbacks.
ATC-TMR-REQUEST-2016	NETN TMR Request Test	Verify SuT compliant with NETN TMR Request Requirements.
ATC-TMR-RESPOND-2016	NETN TMR Respond Test	Verify the SuT complies with SuT requirements for responding to TMR.
ATC-TMR-TRIGGER-2016	NETN TMR Trigger Test	Verify the SuT is compliant with NETN TMR Trigger Requirements.
RPR-PLATFORM	RPR Platform Testing	Verify the CS and GRIM requirements on RPR-Physical FOM Module attributes for platform and lifeform entities.

Annex B: Capability Badges, Interoperability Requirements and Abstract Test Cases, defines the initial set of ATCs in more detail.

4.3.3 Interoperability Capability Badges

An interoperability Capability Badge (CB) is defined as a token of achievement for passing testing related to Interoperability Requirements (IR) associated with the CB. Successful compliance testing, verification, and certification of individual systems' compliance with sets of IRs can be labelled using a CB representing this achievement.

The concept of using badges to indicate achievements is nothing new. It can be found in many domains from the scouts to the military. In online gaming, badges are frequently used to display an individual gamer's skill, accomplishments, and level of play. The semantics associated with badges and how they are used vary between different domains. Even within a single domain you can find different types of badges showing skill, quantitative and qualitative achievements, specific mission badges, and badges showing general maturity or level. Applying the badges concept to interoperability capabilities has been explored in research activities in the United Kingdom (UK) [6] and [7].

Achievement Graphs¹ are used to specify dependencies between different CBs and to visualise roadmaps for increased simulation component interoperability, e.g., achieving RPR-ENTITY-2017 also requires achieving the HLA-BASE-2016 CB requirements. By using achievement graphs combinations/aggregations of CB, associated IRs can be expressed. See Figure 4-4 below.

MSG-134 recommends the use of CBs as tokens for passing testing related to interoperability and as the basis for certificates of compliance. CBs are also used in the Conformance Statements (CSs) provided by the SuT owners as the basis for certification.

¹ An achievement graph is used to express implicit requirements for achieving a specific CB that includes requirements related to other badges.

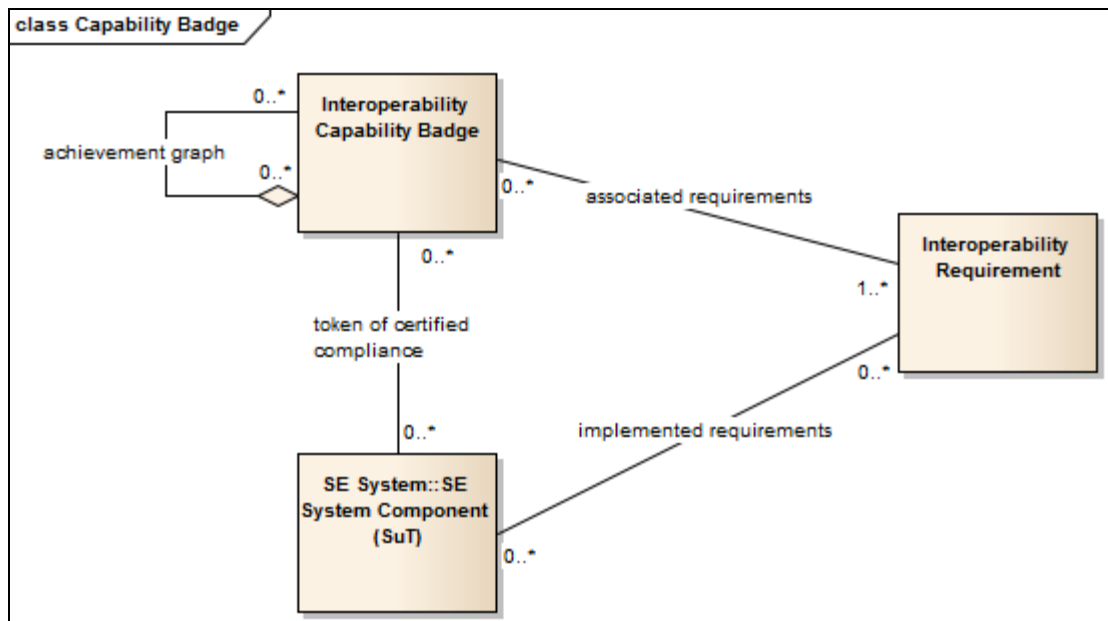


Figure 4-4: Relationships Between the Concepts of a CB, its Associated IRs, and the System under Test.

A CB is identified by name, type and year. It has a short description and a graphical representation (“the badge”). The CB is defined by the set of associated IRs including references to Abstract Test Cases (ATCs) describing how the IRs are verified.

The definition of CBs used in the NATO Simulation Interoperability Test and Certification Service is the responsibility of the Accreditation Authority (AA).

An initial set of CBs, based on NATO Simulation Interoperability Test and Certification Service priorities, has been defined (as shown in Table 4-3 below).

Table 4-3: Initial Set of Capability Badges.

ID	Dependency	Description
CWIX-DR-2017	CWIX-ENTITY-2017	Simulation Interoperability Compliance Badge for CWIX 2017.
CWIX-ENTITY-2017	–	Simulation Interoperability Compliance Badge for CWIX 2017.
CWIX-WARFARE-2017	CWIX-ENTITY-2017	Simulation Interoperability Compliance Badge for CWIX 2017.
HLA-BASE-2017	–	Basic CS/SOM and Best Practices compliance.
NETN-AGG-2017	RPR-AGG-2017	NETN-FOM v2.0 Aggregate FOM Module.
NETN-ENTITY-2017	RPR-ENTITY-2017	NETN-FOM v2.0 Physical FOM Module.
NETN-LBML-INTREP-2017	NETN-AGG-2017, NETN-ENTITY-2017	NETN-FOM v2.0 LBML FOM Module.

ID	Dependency	Description
NETN-LBML-OWNSITREP-2017	NETN-AGG-2017, NETN-ENTITY-2017	NETN-FOM v2.0 LBML FOM Module.
NETN-LBML-TASK-2017	NETN-AGG-2017, NETN-ENTITY-2017	NETN-FOM v2.0 LBML FOM Module.
NETN-MRM-2017	NETN-TMR-2017	NETN-FOM v2.0 MRM FOM Module.
NETN-TMR-2017	HLA-BASE-2017	Basic support for NETN TMR pattern (AMSP-04 Ed A). SuT is able to respond to TMR requests.
RPR-AGG-2017	HLA-BASE-2017	RPR-FOM v2.0 Aggregate FOM Module.
RPR-ENTITY-2017	HLA-BASE-2017	RPR-FOM v2.0 Physical FOM Module support. GRIM compliance wrt. Platforms, Lifeforms, etc. representation of required attributes.
RPR-WARFARE-2017	HLA-BASE-2017 RPR-ENTITY-2017	RPR-Warfare v2.0 FOM Module support.

Annex B: Capability Badges, Interoperability Requirements, and Abstract Test Cases, defines the initial proposed set of interoperability capability badges in more detail.

4.3.4 Conformance Statement

A **Conformance Statement** (CS) is a written statement declaring a systems' compliance with identified Interoperability Requirements (IRs). A CS is provided by the owner of a 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 (CBs).

A CS shall include the following information:

- Metadata including SuT identification, date and POC information
- A Simulation Object Model (CS/SOM) (if SuT creates multiple federates, each needs to be described in separate CSs and are tested individually)
 - The SOM must contain the complete list of HLA services used
- A Federation Object Model (CS/FOM)
- Identified set of CBs to test against
 - Additional CS information and parameters as required by CB

Annex C: Conformance Statement, defines the CS template in more detail.

4.3.5 Integration, Verification, and Certification Tool (IVCT)

The NATO Simulation Interoperability Test and Certification Service **Integration, Verification and Certification Tool** (IVCT) is a core technical framework provided by Certification Entity (CE) and used to support test and verification of simulation interoperability requirements. The IVCT is used to for testing of individual simulation components interoperability capabilities and to support integration of distributed simulations. Accredited Test Laboratories (ATLs) use the IVCT to perform certification testing.

CONCEPT OF THE PROPOSED SYSTEM

The IVCT is a component-based software package with modules supporting scheduling, execution and reporting of results from running Executable Test Cases (ETCs) (see Figure 4-5).

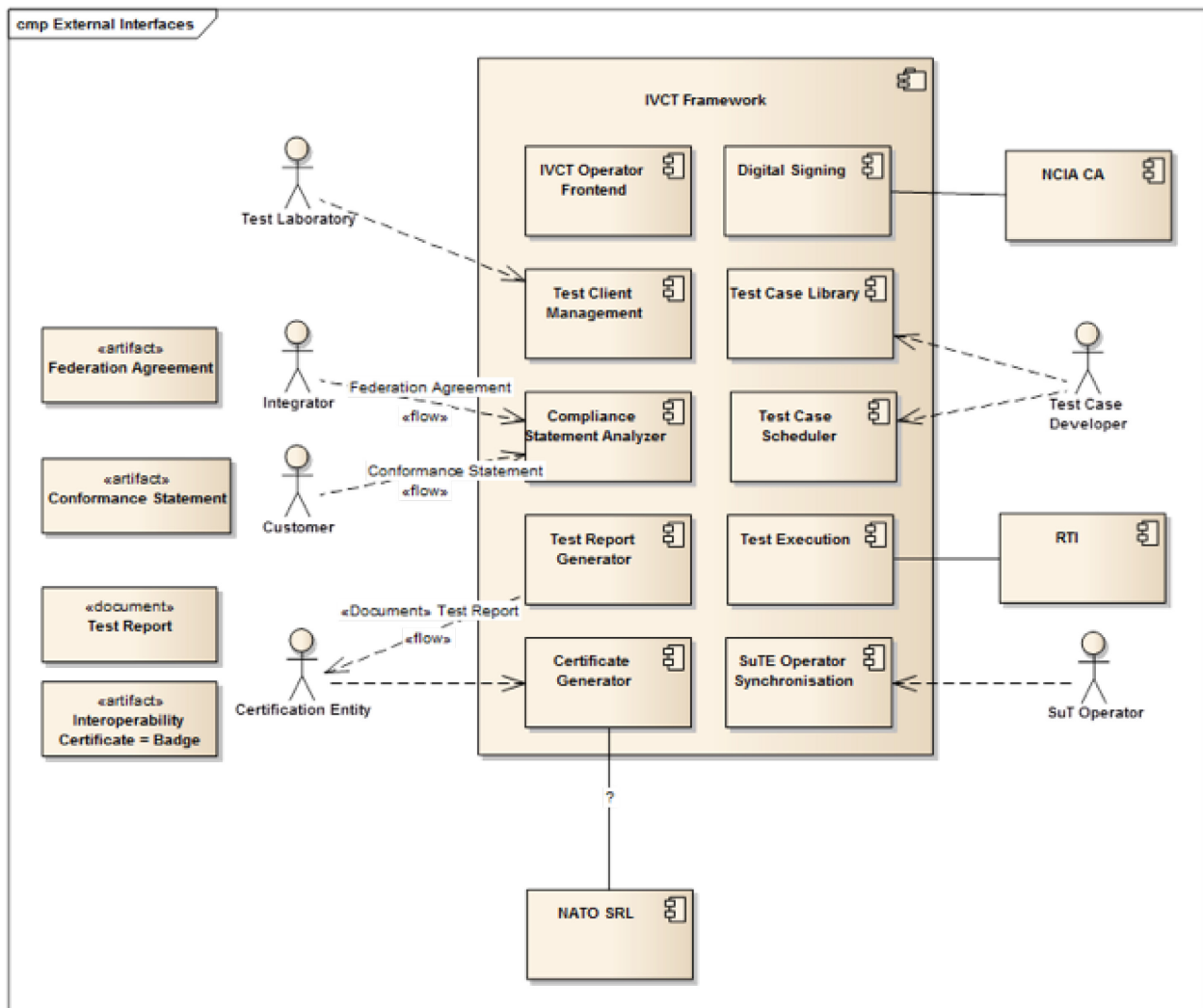


Figure 4-5: Major IVCT Modules.

ETCs are implementations of Abstract Test Cases (ATCs) developed to verify defined sets of Interoperability Requirements (IRs).

The IVCT executes in an HLA federation together with the System under Test Environment (SuTE) consisting of the System under Test (SuT) and other auxiliary federates and systems. The IVCT Test Engine (TE) runs ETCs to stimulate and to check responses from the SuT. See Figure 4-6 below. Results are reported by the IVCT as successful or unsuccessful verification of IRs.

MSG-134 has implemented a first version of IVCT including core TE and supporting modules. The IVCT is implemented and provided as Open Source and is maintained by CE.

Annex D: Integration, Verification and Certification Tool, defines the IVCT operational requirements in more detail.

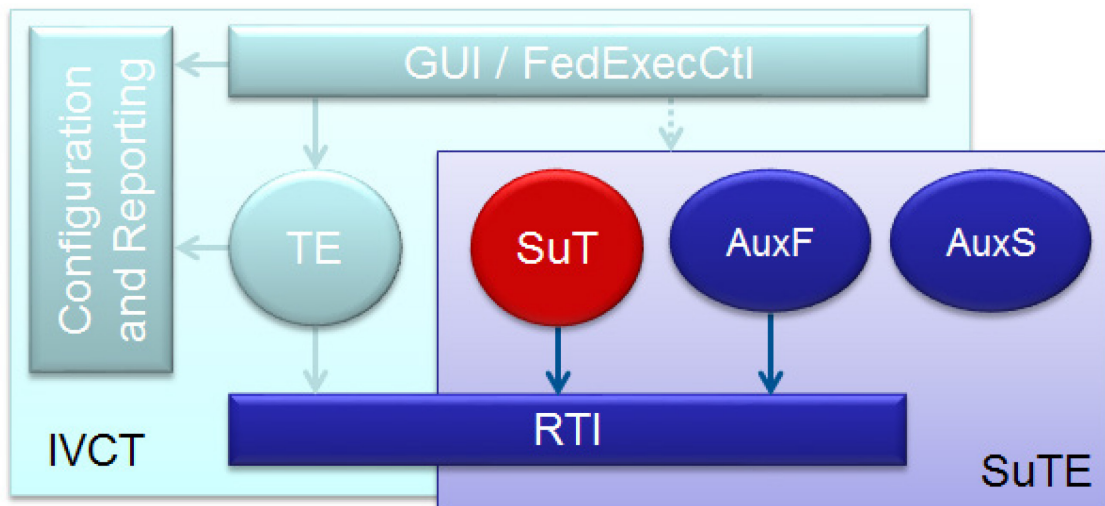


Figure 4-6: Using IVCT.

4.3.6 Information Available to the Public *via* the CE Website

Procedures and processes about the flow of the certification will be displayed in a specific page of the CE Portal as well as the advantage of having tools NATO certified.

There will be a login form for starting the accreditation procedures and detailed explanation on fee amount.

Once the Customers are appropriately registered on the CE Portal, it will be ensured the possibility to download the latest IVCT version (which will be released for free), as well as the needed ETC through a dedicated download area.

CE will maintain a dedicated page on which issued certificates will be published, with the permission of the SuT owner.

Indications on H/W, S/W and network requirements will be provided in the CE Portal.



Chapter 5 – OPERATIONAL SCENARIOS

Operational Scenarios and Use Cases define the operational procedures of all identified roles that are needed to fulfil their respective responsibilities and to comply with operational policies and constraints.

More detailed descriptions of operational scenarios and use cases can be found in Annex A: Operating Procedures.

5.1 ACCREDITATION AND CERTIFICATIONS

The following diagram shows the details of the Certification Service as a Use Case (UC) (Figure 5-1). There are basically two loops in this service. The first (on the right side of the diagram) is the accreditation phase, where the Certification Entity and the Test Laboratory must be accredited by the Accreditation Authority. The second loop (on the left side of the diagram) is the certification process for a System under Test. Table 5-1 lists the use cases related to certification service.

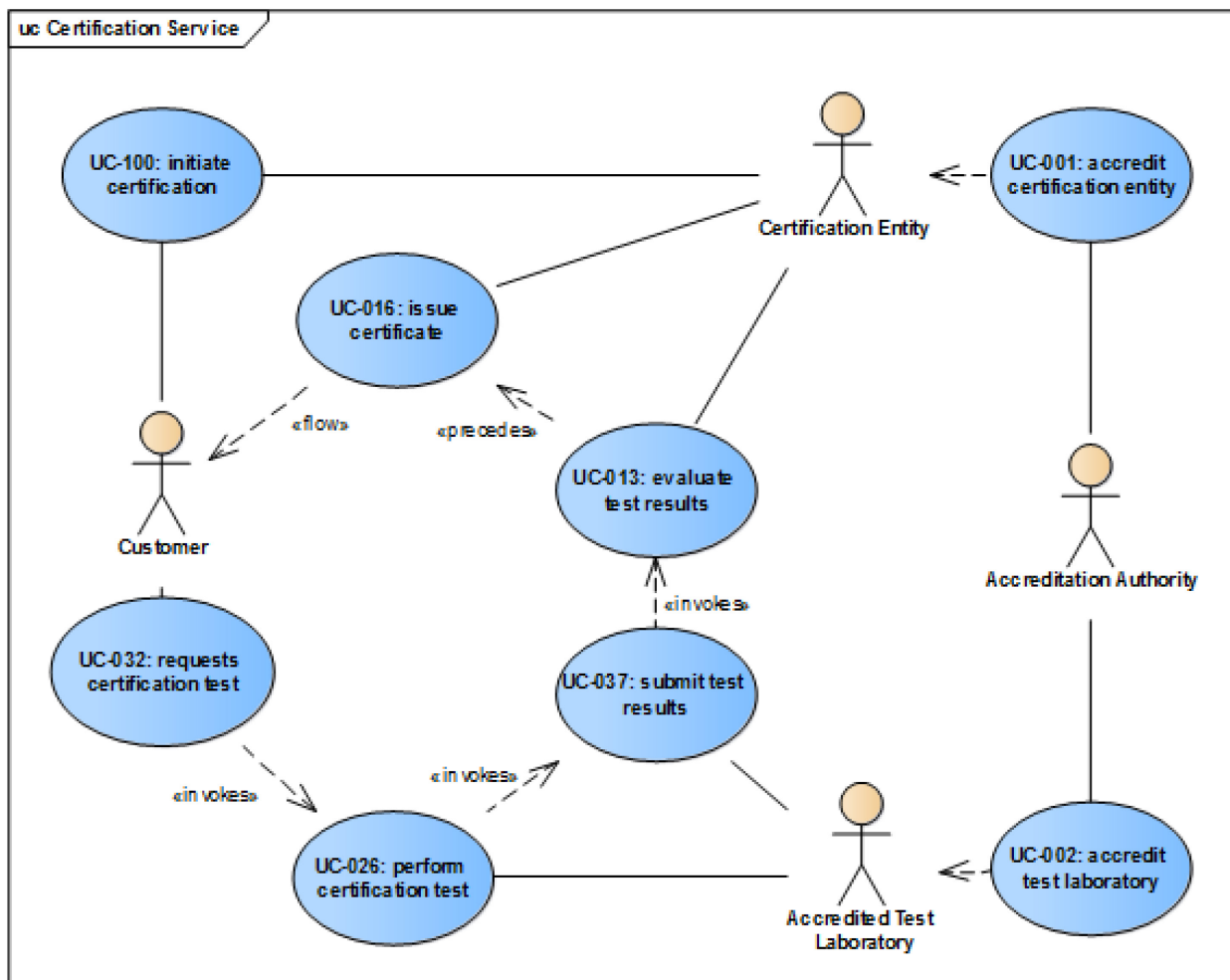


Figure 5-1: Use Case of Certification Service.

Table 5-1: Use Cases Related to Certification Service.

Title	Description
UC-001 Accredited Certification Entity	The AA receives a CE accreditation request from a CE candidate organization. The AA checks whether the CE candidate meets defined CE requirements, including organizational and security standards. If the CE candidate complies with all CE requirements the AA will accredit the CE candidate. Otherwise the reasons for non-compliance will be provided to the CE candidate.
UC-002 Accredited Test Laboratory	The AA receives an accreditation request from an ATL candidate to conduct certification testing. The AA checks whether the ATL candidate meets defined ATL requirements including organizational, technical, and security. If the ATL candidate complies with all ATL requirements the AA will accredit the ATL candidate. Otherwise the reasons for non-compliance will be provided to the ATL candidate.
UC-013 Evaluate Test Results	A Certification Entity will evaluate the results according a predefined procedure to determine whether the System under Test has met the requirements needed to merit a Conformance certificate.
UC-016 Issue Certificate	The Certification Entity, upon successful evaluation of the test results, will issue a certificate to the Customer.
UC-026 Perform Certification Test	The ATL analyses the SuT CS, and based on the requested CBs, selects and configures appropriate ETCs and sets-up the IVCT. The ATL runs the IVCT test system using the configuration derived from the SuT CS.
UC-032 Requests Certification Test	The Customer contacts an ATL to arrange for certification testing. The Customer negotiates the conditions for the SuT certification test with the ATL. The Customer submits the SuT, SuTE and CS to the ATL.
UC-037 Submit Test Results	The Accredited Test Laboratory will submit the results of a certification test via a secure transport mechanism to the Certification Entity.
UC-100: Initiate Certification	The Customer initiates the certification process by contacting a CE and providing a request for certifying the SuT against a CS. The CE informs the Customer which ATLs are able to perform the tests required by the CS.

5.2 ACCREDITATION PROCESS OF A CANDIDATE FOR THE ATL ROLE

Not defined by MSG-134 for IOC.

5.3 ACCREDITATION PROCESS OF A CANDIDATE FOR THE CE ROLE

The candidate for the CE Role must be an organization, NATO accredited, that needs to show its capability in performing the related roles detailed in Annex A and will be evaluated by a dedicated team issued by the Accreditation Authority.

5.4 DEVELOPMENT AND MAINTENANCE

The following diagram (Figure 5-2) shows the various developer roles involved in implementing the test tool software. This includes the implementation of the test tool, the test cases, and the management system, as well as their maintenance and documentation. Table 5-2 lists the use cases related to development.

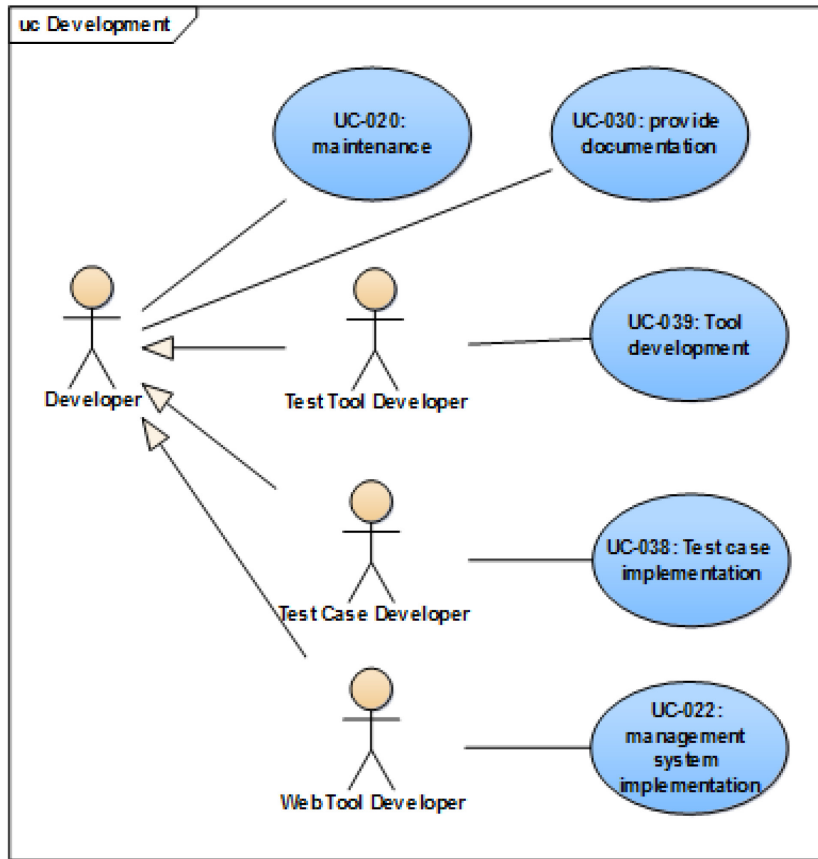


Figure 5-2: Use Case of Development.

The following diagram (Figure 5-3) shows the various roles involved in the certification and verification workflow of use cases. This includes issue handling, definition of certification, application of certification, and maintenance of the certification processes. Table 5-3 lists the use cases related to verification workflow.

Table 5-2: Use Cases Related to Development.

Title	Description
UC-020 Maintenance	The test tool requires maintenance due to issues with the tool or test cases, operating system changes, enhancements, as well as changes in the pattern specifications, or interpretation of the pattern specifications.
UC-022 Management System Implementation	The Management System will manage the documents and data files related to a certification test. These files will be stored in an online database such as NSRL. This system must guarantee the files are transferred and stored in a secure manner to prevent tampering with, or unauthorized disclosure of, the contents. The files will be accessed via Web Services.
UC-030 Provide Documentation	A Developer must provide documentation for the development, maintenance and enhancement of the test tool. Since even a minor change can cause incompatibilities, it is necessary to know exactly the tool behaviour in each version.

Title	Description
UC-038 Test Case Implementation	The Certification Entity is responsible for defining the test case purposes. The abstract test cases (specifying the test steps and allowable reactions) are created by the Certification Entity, based on the test purposes. The validation of the abstract test cases against the test purposes is also done by the Certification Entity. Test purposes are specified by implementation pattern protocol experts and these are implemented by Test Case Developers into executable test cases. Usually executable test cases will use a test case library to handle bundled events or other support functions. The log files can be examined and checked against the test purposes to prove the valid implementation of the test cases. The Test Case Developer implements the executable test cases from the abstract test cases. The executable test cases are compiled programs using the IVCT Application Programming Interface (API). The work done by the Test Case Developer also includes the verification of the executable test cases against the abstract test cases as well as the long-term maintenance of the test cases.
UC-039 Tool Development	Test Tool development will take place only after a design specification is created. Several test tool developers may work on various well-designed independent modules. When the test tool has reached a significant level of quality and maturity and has been employed in certification test and accepted by the CE, it will be considered to be in the maintenance phase.

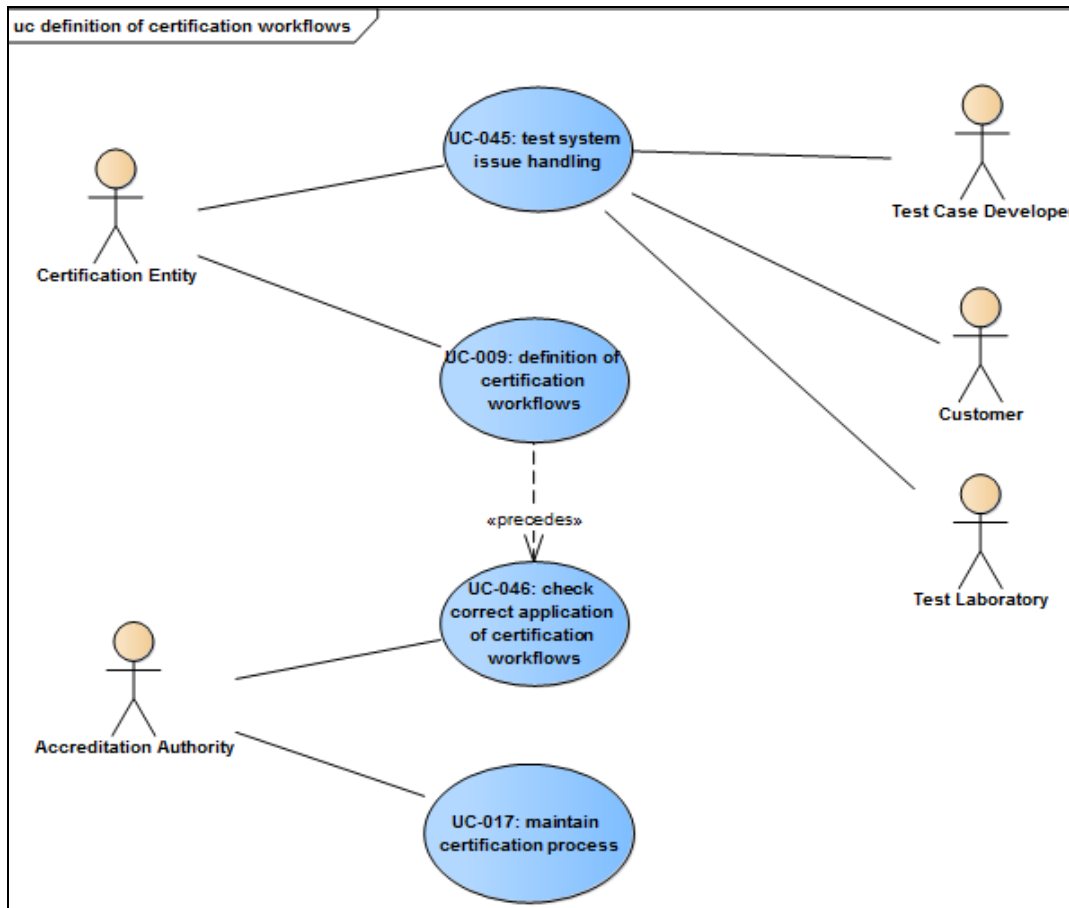


Figure 5-3: Definition of Certification Workflow Use Case Diagram.

Table 5-3: Use Cases of Verification Workflow.

Title	Description
UC-009 Definition of Certification Workflows	The Certification Entity will define procedures for all the roles in the Certification Workflow. The workflow must include the practical needs of a certification test as well as the security needs for secure report management and Customer confidentiality. The Customer must be informed of his role when contacting a CE. All other roles must be defined and known for a Test Laboratory to be accredited.
UC-017 Maintain Certification Process	The AA updates and maintains a documented certification process including CE and ATL operational requirements and criteria for accreditation.
UC-045 Test System Issue Handling	An issue handling system is an important part of any Test System, since when a change is made it may invalidate previous results. All issues, and any changes or rejections, of these issues must be recorded. Through use of an issue tracking system the status of the test system and test case interpretations at any point in time is known. The quality of the test system is improved when issues are properly tracked and resolved.
UC-046 Certification Workflow Compliance Review	The AA evaluates the conformance of CEs and ATLs with certification processes and operational requirements on a regular basis. The AA provides CEs with updated ATL status and contact information.



Chapter 6 – SUMMARY OF IMPACTS

NATO and Partners certification of simulation components' interoperability capability will have a major impact on how interoperability requirements are expressed and tested for new simulation components, and for the integration of federated distributed simulations.

The way systems are procured, integrated and tested will change when:

- Simulation components are required to conform with NATO standards;
- NATO simulation interoperability certification services must be used as part of the delivery process; and
- NATO certificates of simulation interoperability compliance are in place for existing systems.

To include the use of NATO services for certification:

- Acquisition organizations and authorities will need to understand the benefits of using NATO certified simulation components; and
- Procurement processes may have to be adapted to include the use of NATO services for certification.

In order for a simulation component to be accepted as part of a federated distributed simulation system:

- Simulation interoperability requirements should be specified in accordance with NATO standards; and
- Vendors should be required to undergo certification or provide proof of compliance.

The availability of common tests, and free tools, for interoperability test and verification will also have a major impact by allowing COTS, GOTS, and other system developers to pre-test their systems and to perform self-certification to some extent. This will reduce the risks and costs associated with solving interoperability issues during integration.



Chapter 7 – ANALYSIS OF THE PROPOSED SYSTEM

An analysis of the proposed system has been made to identify and make visible any strengths, weaknesses, opportunities and threats (see Table 7-1).

Table 7-1: Analysis Results of Certification Service.

Helpful		Harmful
Internal	<p>Strengths:</p> <ul style="list-style-type: none"> • Definition of standard procedures • Initial experience and knowledge of earlier certification tools (FCTT) • Good representation of stakeholders in group 	<p>Weaknesses:</p> <ul style="list-style-type: none"> • No clear/aligned budget • Unbalanced contribution • Limited focus/restricted to HLA certification • Unclear business process
External	<p>Opportunities:</p> <ul style="list-style-type: none"> • Integration cost reduction • Integration risk reduction • Reduction integration time • Increased market for interoperable simulation components • Aligned parallel activities (reuse) • Enforce use of STANAG 4603 	<p>Threats:</p> <ul style="list-style-type: none"> • Market might be too small to sustain maintenance • Market moves in another direction • Resistance to adoption • Non-aligned parallel activities (redundancy)



Chapter 8 – BUSINESS MODEL

8.1 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 seven 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.

8.2 CUSTOMER-FUNDED BUSINESS MODEL

8.2.1 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.

8.2.2 Initial Operational Capability (2018-2020)

In this time frame, MSG-134 suggests to continue using the current business model while having the participating nations in a follow-on activity of MSG-134 to fund the continued development of the IVCT and ETCs.

A follow-on activity (e.g., a separate working group or as part of a bigger group) of MSG-134 will be acting as the ATL and the NATO M&S COE will be acting as the CE.

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

8.2.3 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 (see Figure 8-1).

8.3 PROPOSED ORGANIZATION

The Initial Operating Capability (IOC) organization to support NATO Simulation Interoperability Testing and Certification can be limited in size, with few resources manning the organization. Initially a single ATL is envisioned with a limited number of certifications. However, the proposed organizational structure has been designed to support a growing market and demand for test and certification services in a scalable manner (see Figure 8-2).

The following IOC allocation of responsibilities is recommended:

- The AA is NMSG; a candidate is MS3, if the group includes the M&S NATO entities (JFTC, JWC, M&S COE).
- The CE is the NATO M&S CoE.
- Initial ATL activity could be supported by the members of the MSG-134 Follow-on group.

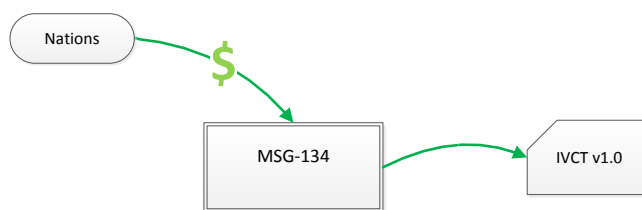
8.4 STRATEGY FOR INITIAL OPERATIONAL CAPABILITY

The IOC will create the conditions for establishing the processes and procedures and gaining broad audience acceptance:

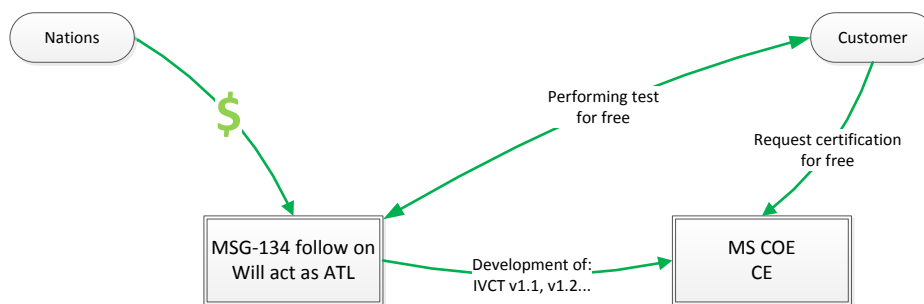
- MSG-134 has created the initial IVCT, certification processes and procedures, and the first set of abstract and executable test cases.
- MSG-134 has created marketing material and will continue an information campaign to create demand for certification services, and to make government, and procurement agencies aware of these capabilities. Activities include:

- CWIX 2016, 2017 participation; and
- Marketing at CD&E Conference, CAX Forum, ITEC, I/ITSEC, etc.
- MSG-134 will promote use of tools and services and establish IOC, with NMSG acting as the AA and the NATO M&S CoE acting as the CE.
- MSG-134 will identify and engage the initial ATL.
- The NATO M&S CoE (CE) will assume responsibility for IVCT maintenance.
- Acting as the AA, MSG -134 will evaluate and continue to promote capability.
- Final Operational Capability (FOC) is planned for 2020.

Early development (2015-2017)



Initial Operational Capability (2018-2020)



Fully Operational Capability (2021 and beyond)

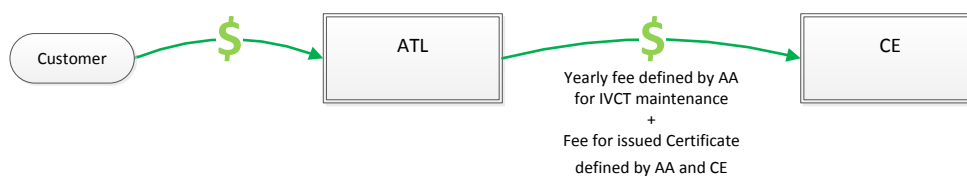


Figure 8-1: Funding of IVCT and Certification Service.

8.5 BUSINESS MODEL FOR THE TRANSITION PERIOD FROM IOC TO FOC

- The follow-on activity will support the following entities: ATL, the NATO M&S CoE as the CE, and MS3 as the AA.
- The yearly fee charged to the ATL is zero, but the ATL is expected to participate to the follow-up activity by contributing to the development and maintenance of the IVCT and test cases.

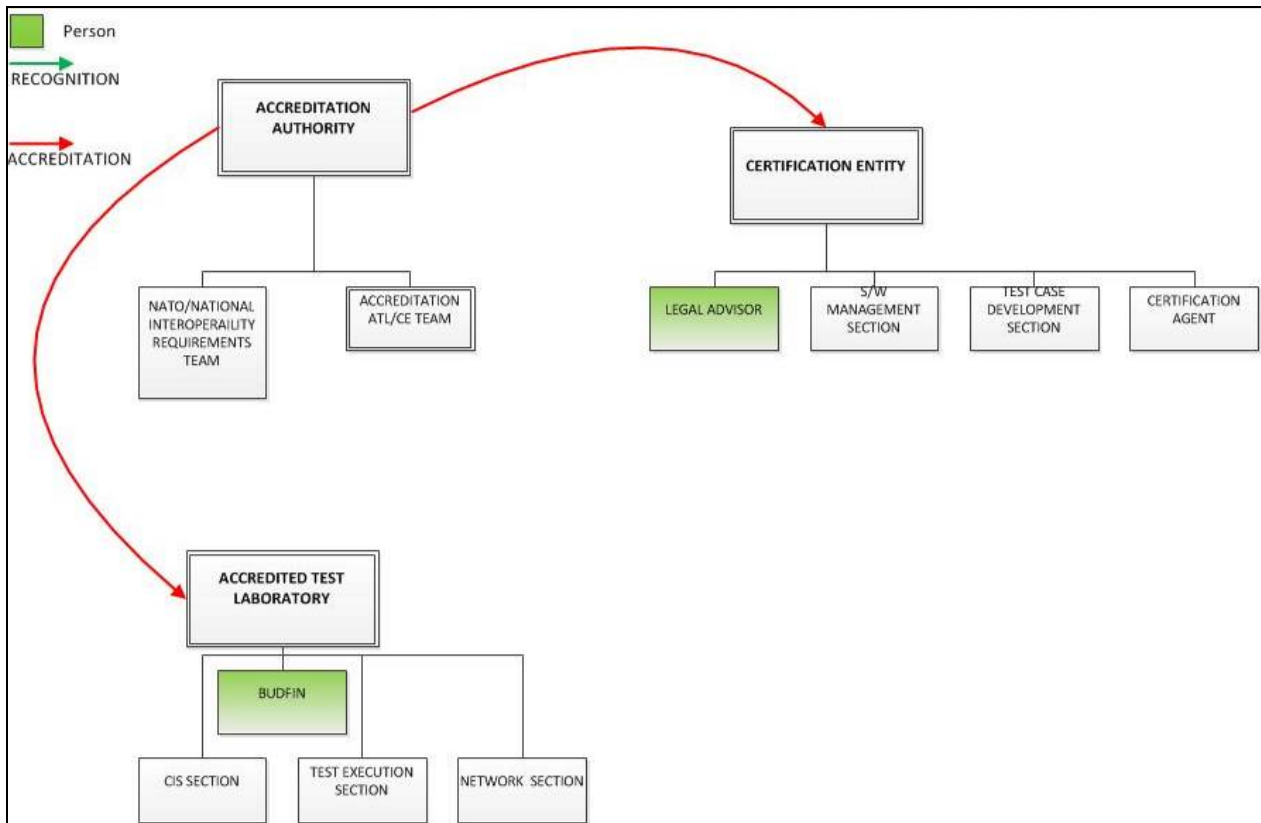


Figure 8-2: Proposed Organizational Structure.

8.6 OWNERSHIP OF THE IVCT, ABSTRACT TEST CASES, AND EXECUTABLE TEST CASE

IVCT is an open source product initially developed by the MSG 134 and owned by the AA. It will be available to the ATLS and other test laboratories through the CE website once the stable version is delivered to the CE; no later than the end of the MSG 134 mandate.

Abstract test cases and executable test cases verified by the CE and approved by the AA will be shared with ATLS. Sharing of non-approved test cases is the responsibility of the owner.

The AA defines and prioritizes the development of ATCs and ETCs based on the IRs.

Chapter 9 – REFERENCES

- [1] AMSP-04, NATO Education and Training Network (NETN) Federation Agreements and FOM Design (FAFD), Edition A, Version 1 (Draft) March 2018.
- [2] AMSP-01, NATO Modelling and Simulation Standards Profile, Edition C, Version March 2015.
- [3] STANAG 4603, Modelling and Simulation Architecture Standards for Technical Interoperability: High Level Architecture (HLA), Ed. 2 (2015) NSO(AC/323)0234 (2015) NMSG/4603.
- [4] IEEE 1516-2010, IEEE Standard for Modelling and Simulation (M&S) High Level Architecture (HLA) – a.k.a HLA Evolved, August 2018.
- [5] Tolk, A., and Muguira, J.A. (2003). The Levels of Conceptual Interoperability Model (LCIM). Proceedings, IEEE Fall Simulation Interoperability Workshop, IEEE CS Press.
- [6] Löfstrand, B., Sandberg, S. (2013). Capability Classification and Automated Test Procedures, Final Report, DSTLX10000079012. CDE30665.
- [7] Löfstrand, B., Falkenjak, Å. (2015). Visualisation and Discovery of Systems' Interoperability Capability using 'Capability Badges' and 'Achievement Trees', Final Report SE Tower TC1 AIMS Task 3 Novel Approaches.

REFERENCES



Annex A – OPERATING PROCEDURES

A.1 ROLES AND RESPONSIBILITIES

The main operational roles in the NATO Simulation Interoperability Test and Certification Service are the Accreditation Authority, the Certification Entity, Accredited Test Laboratories, and the Customer. The responsibilities of these roles are defined by operation requirements. Procedures and activities associated with each role are defined by operational Use Cases. Figure A-1 provides a diagram of the user roles.

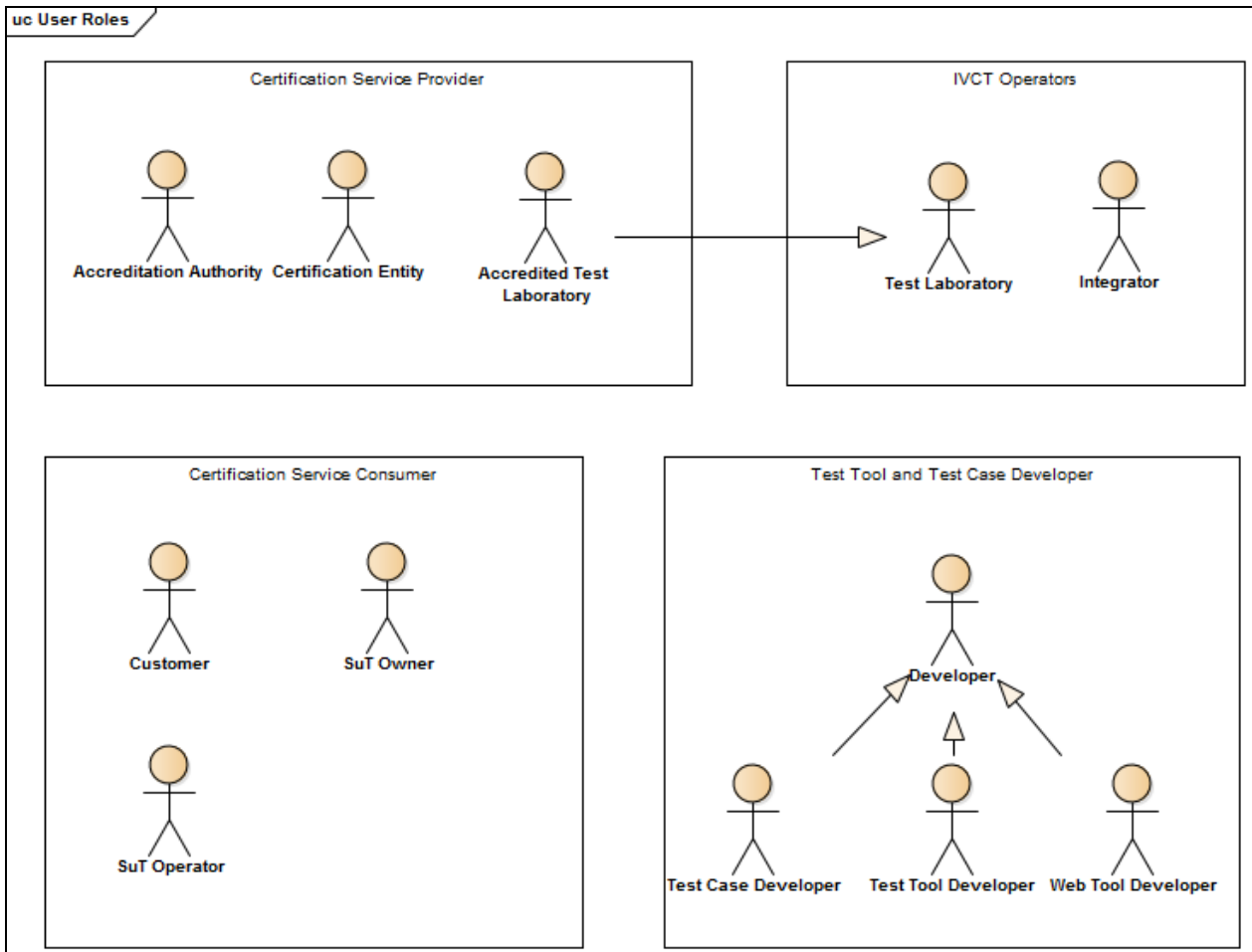


Figure A-1: NOV-2 User Roles.

A.1.1 Accreditation Authority

The **Accreditation Authority (AA)** is a NATO appointed organization responsible for maintaining the business model and procedures used by Accredited Test Laboratories (ATLs) and Certification Entities (CEs).

A.1.1.1 Initial Operational Requirements

Table A-1 lists the initial operational requirements of the Accreditation Authority.

Table A-1: Initial Operational Requirements of Accreditation Authority.

ID	Description
OR-AA-0001	The AA shall maintain procedures for accreditation of CEs and ATLs including the maximum time period to be accredited.
OR-AA-0002	The AA shall perform accreditation of CEs within the time period specified in the accreditation procedure.
OR-AA-0003	The AA shall perform accreditation of Test Laboratories within the time period specified in the accreditation procedure.
OR-AA-0004	The AA shall collect IRs from CEs and set priorities according to the NATO certification strategy.
OR-AA-0005	The AA shall define the list of approved NATO Capability Badges, in relation of prioritized IRs.
OR-AA-0006	The AA shall provide contact information of experts to the CE to assist with the definition, development, and implementation of abstract test cases.
OR-AA-0007	AA shall maintain the IVCT requirement specifications.

A.1.1.2 Operational Use Cases

Table A-2 lists Use Cases related to the Accreditation Authority.

Table A-2: Use Cases Related to Accreditation Authority.

Title	Description
UC-001 Accredite Certification Entity	The AA receives CE accreditation requests from CE candidate organizations. The AA determines if the CE candidate meets defined CE requirements, including organizational and security standards. If the CE candidate complies with all CE requirements the AA will accredit the CE candidate, otherwise the reasons for withholding accreditation will be provided to the candidate.
UC-002 Accredite Test Laboratory	The AA receives an accreditation request from an ATL candidate to conduct certification testing. The AA checks whether the ATL candidate meets defined ATL requirements including organizational, technical and security aspects. If the ATL candidate complies with all ATL requirements the AA will accredit the ATL candidate, otherwise the reasons for non-compliance will be provided to the ATL candidate.
UC-017 Maintain Certification Process	The AA updates and maintains the documented certification process including CE and ATL operational requirements, and criteria for accreditation.
UC-046 Certification Workflow Compliance Review	The AA evaluates the conformance of CEs and ATLs with the certification process and operational requirements on a regular basis. The AA provides CEs with updated ATL status and contact information.

A.1.2 Certification Entity

The **Certification Entity** (CE) is an organization accredited by the Accreditation Authority (AA) and given the authority to issue certificates of compliance to systems that have successfully undergone certification testing against Interoperability Requirements (IRs). 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 (customers have the right to refuse the certification). The CE also maintains the official version of the Integration, Verification, and Certification Tool (IVCT) and delivers it and executable test cases to ATLS.

A.1.2.1 Operational Requirements

Table A-3 lists the operational requirements of the Certification Entity.

Table A-3: Operational Requirements of Certification Entity.

ID	Description
OR-CE-0001	The CE shall confirm ATL submission of certification test results within one week.
OR-CE-0002	The CE shall process certification test results and deliver certification result within time specified by contract.
OR-CE-0003	The CE shall store certification test results in a secure environment.
OR-CE-0004	The CE shall provide a central point of contact for all certification services.
OR-CE-0005	The CE shall provide a Web-based information system for certification service users.
OR-CE-0006	The CE shall provide an IVCT and ETC issue tracking system.
OR-CE-0007	The CE shall provide IVCT configuration management and up-to-date software status information to ATLS.
OR-CE-0008	The CE shall evaluate and correct irregular IVCT and ETC software behaviour as soon as possible.
OR-CE-0009	The CE shall define a procedure for releasing new versions of the IVCT software.
OR-CE-0010	The CE shall provide a test environment for verifying the IVCT software before release.
OR-CE-0011	The CE shall manage all IVCT software contributions.
OR-CE-0012	The CE shall, with SuT owner permission, publish certificates.
OR-CE-0013	The CE shall provide IVCT software on request to SuT owners and test laboratories.

A.1.2.2 Operational Use Cases

Table A-4 lists Use Cases related to the Certification Entity.

Table A-4: Use Cases Related to Certification Entity.

Title	Description
UC-003 Archive and Remove Test Results	Once the Test Results have been sent to the Certification Entity, they should be archived in a dedicated repository and deleted from the storage where they were generated. The Test Results are the most important information for determining if a certificate should be awarded and care should be taken against any manipulation of these results. The test results should not be made viewable by any customer other than the one that provided the SuT. The test results should be stored in a secure location with access by authorized personnel only.
UC-006 Define Abstract Test Case	Once the test purposes have been defined, it is possible to define the steps required to achieve these purposes in the form of abstract test cases. Abstract Test Cases are the sequences of requests and expected responses independent of a programming language.
UC-007 Define Test Purpose	When a pattern protocol is defined, it is a good idea to define Test Purposes which will constitute a comprehensive test of the functionalities and variations of these functionalities. As far as possible the Test Purposes should also cover error handling invalid behaviour.
UC-009 Definition of Certification Workflows	The CE will define the procedures for the roles of all participants of the certification workflow. The workflow must include the practical needs of a certification test as well as the security needs of secure report management and customer confidentiality. The customer must be informed of his role when contacting the CE. All other roles must be defined and known for a test laboratory to be accredited.
UC-013 Evaluate Test Results	A Certification Entity will evaluate the results according a predefined procedure to determine whether the SuT has shown sufficient capabilities to merit a conformance certificate.
UC-016 Issue Certificate	The Certification Entity, upon successful evaluation of the test results, will issue a certificate to the customer.
UC-018 Maintain Test Cases	During the course of testing implementations, various issues may occur that require changes to test cases. This maintenance activity should be done in a disciplined manner, since even small changes could invalidate previous test certificates. After a change to any test cases, the test cases should be run against SuT from two different SuT developers to test for side effects. All changes must be documented in respect to an issue and its solution.
UC-019 Maintain Test System	<p>Whenever the IVCT is used an issue may occur that requires a modification or extension to the system. A change to any test cases may invalidate test results and should be handled very carefully. Each issue should be well-documented, and the software should be checked in to a source control system after each modification.</p> <p>The Certification Entity must review the changes before authorizing a new Test Tool release.</p>

Title	Description
UC-020 Maintenance	The IVCT requires maintenance due to issues with the tool or test cases, operating system changes, enhancements, as well as changes in the pattern specifications or interpretation of the pattern specifications.
UC-021 Manage Test Case Results	The results of the execution of the ETCs are saved in a safe manner, sent to the CE and to the Customer. Results are logging files for the executed tests and a summary with the ETC verdicts.
UC-031 Publish Certification Result	After receiving permission from the federate owner, the CE will publish the certification test result.
UC-037 Submit Test Results	An ATL will submit the results of a certification test via a secure transport mechanism to the Certification Entity.
UC-040 Validate Test Case	Once an abstract test case is created, it should be checked to confirm it is a valid interpretation of the test purposes. The CE should make sure this is completed before executable test cases are created.
UC-045 Test System Issue Handling	An issue handling system is an important part of any test system, since when a change is made it may invalidate previous results. All issues and any changes or rejections of these issues must be recorded so that the status of the test system and test case interpretations at any point in time is known. The quality of the test system is improved when issues are properly resolved.
UC-046 Certification Workflow Compliance Review	The AA evaluates the conformance of CEs and ATLs with the certification process and operational requirements on a regular basis. The AA provides CEs with updated lists providing ATL status and contact information.
UC-050 Secure Access and Archive	The Test Results should not be made viewable to any other Customers than the Customer who provides the SuT. The Test Results should be stored in a secure location with access by authorized personnel only.
UC-051 Secure Transportation Mode	A CE will receive test results from an ATL via a secure transportation mode.

A.1.3 Accredited Test Laboratory

An **Accredited Test Laboratory** (ATL) is a test laboratory accredited by the Accreditation Authority (AA) and given the official authority to perform certification tests of Interoperability Requirements (IRs) and whose test results are recognized by Certification Entities (CEs) as valid for issuing certificates of compliance. The role of an ATL is to conduct certification tests at the request of a customer on the customer's System under Test (SuT) on behalf of a CE according to the business model defined by the AA. ATLs use the Integration, Verification and Certification Tool (IVCT) provided by CEs and run Executable Test Cases (ETCs) (also provided by CEs) to verify IRs associated with Capability Badges (CBs) defined in the SuT Conformance Statement (CS) submitted by the Customer. An ATL delivers test results to a CE in a secure manner for official certification. ATLs continuously provide feedback on IVCT use to the CE and propose improvements to the test system and procedure. ATLs supports the CE in maintenance tasks according to the business model set by the AA. ATLs collect IRs and propose them to the AA for inclusion in new CBs.

A.1.3.1 Operational Requirements

Table A-5 lists the operational requirements of an Accredited Test Laboratory.

Table A-5: Operational Requirements of Accredited Test Laboratory.

ID	Description
OR-ATL-0001	Each ATL shall define its terms and conditions for providing the certification test service.
OR-ATL-0002b	The ATL certification service may be performed at customer site.
OR-ATL-0003	An ATL shall comply with agreed Customer security requirements.
OR-ATL-0004	An ATL shall safely transfer certification test results to the CE, using the security protocol established by the CE.
OR-ATL-0005	An ATL shall provide a capability to backup test results.
OR-ATL-0006	An ATL shall store certification test results in a secure manner.
OR-ATL-0007	An ATL shall only allow access to certification test results by authorized personnel.
OR-ATL-0008	An ATL shall ensure that certification test results cannot be manipulated after certification test has finished.
OR-ATL-0009	An ATL shall report irregular IVCT software behaviour to the CE.
OR-ATL-0010	An ATL shall only use the latest released ETC versions, provided by the CE, for certification testing.
OR-ATL-0011	An ATL shall ensure that only SuTE components are connected to IVCT during testing.
OR-ATL-0012	An ATL should allow customers to choose to submit, or not, their SuT test results for certification.

A.1.3.2 Operational Use Cases

Table A-6 lists Use Cases related to an Accredited Test Laboratory.

Table A-6: Use Cases Related to Accredited Test Laboratory.

Title	Description
UC-004 Configure Network Infrastructure	In the case of a LAN, the network addresses have to be configured and the ports have to be opened. In case of a WAN, further routing and forwarding may have to be configured. This task requires knowledge of networking by both the ATL and the customer.
UC-011 Evaluate CS	The ATL will evaluate the CS pertaining to the SuT and select the relevant ETCs to be executed.

Title	Description
UC-014 Execute Test Cases	The selected Test Cases are run against the SuT and the results of the test are recorded.
UC-019 Maintain Test System	Whenever the Test Tool is used an issue may occur that requires a modification or extension to the system. A change to any test case may invalidate test results and should be handled very carefully. Each issue should be well-documented and the software should be checked in to a source control system after each modification. The CE must review the changes before authorizing a new test tool release.
UC-021 Manage Test Case Results	The results of the execution of ETCs are saved in a secure manner and sent to the CE and the customer. Results are log files for the test execution and a summary with the ETC verdicts.
UC-026 Perform Certification Test	The ATL analyses the SuT CS and, based on requested CBs, selects and configures appropriate ETCs and sets-up the IVCT. The ATL runs the IVCT test system using the SuT CS.
UC-028 Perform Test	Run the IVCT test System using the conformance statement of the SuT to select the appropriate test cases. The IVCT operator may select the mode (integration, verification or certification) in which the test system should operate. These modes are realized by specific test cases designed for the mode.
UC-029 Perform Verification Test	The ATL will run the verification test against the SuT using the procedures defined. The SuT may require a specific environment (SuTE) for its operation.
UC-032 Requests Certification Test	A customer contacts an ATL to arrange for certification testing. The customer negotiates the conditions of the certification test with the ATL. The customer submits SuT, SuTE, and CS to the ATL.
UC-037 Submit Test Results	The ATL will submit the results of a certification test via a secure transport mechanism to the CE.
UC-045 Test System Issue Handling	An issue handling system is an important part of any test system, since when a change is made it may invalidate previous results. All issues and any changes or rejections of these issues must be recorded so that the status of the test system and test case interpretations at any point in time is known. The quality of the test system is improved when issues are properly resolved.
UC-047 Operate IVCT	The IVCT operator uses the IVCT test system to test a SuT. The operator needs to have sufficient knowledge to configure, start, operate, and stop the test system.

A.1.4 Customer

A **Customer** of the NATO Simulation Interoperability Test and Certification Service is either a system owner or has obtained the rights from the system owner to initiate certification testing of the system. The customer initiates the certification process by contacting the Certification Entity (CE) and by providing a request for certifying the System under Test (SuT) against a Conformance Statement (CS).

ANNEX A – OPERATING PROCEDURES

A.1.4.1 Operational Requirements

Table A-7 lists the operational requirements of the customer.

Table A-7: Operational Requirements of Customer.

ID	Description
OR-CUSTOMER-0001	The customer shall provide the System under Test Environment (SuTE) to the ATL if required by the SuT to correctly operate during testing.
OR-CUSTOMER-0002	The customer shall identify the SuT Owner when initiating certification.

A.1.4.2 Operational Use Cases

Table A-8 contains Use Cases related to the customer.

Table A-8: Use Cases Related to Customer.

Title	Description
UC-032 Requests Certification Test	The customer contacts an ATL to arrange for certification testing. The customer negotiates the conditions for the SuT certification test with the ATL.
UC-033 Self-Testing	A customer can use the IVCT at any time to aid in developing their SuT, and as a final check before submitting it for certification testing.
UC-034 Submit CS	The customer submits a Conformance Statement (CS) with basic info about the SuT and the Capability Badges (CBs) to be certified against. The CS provides the basis for test case selection.
UC-035 Submit SuT	The Customer provides the SuT as an executable according to ATL requirement.
UC-100: Initiate Certification	Customer initiates the certification process by contacting CE and by providing a request for certifying the SuT against a CS. CE informs the Customer which ATLs are able to perform the tests required by the CS.

A.2 POLICIES AND CONSTRAINTS

Operational Policies and **Constraints** are expressed as Operational Requirements (OR) associated with identified Roles (see Table A-9).

Table A-9: Operational Requirements for Operational Policies and Constraints.

ID	Description
OR-AA-0001	The AA shall maintain procedures for accreditation of CEs and ATLs including the maximum time required for the accreditation process.
OR-AA-0002	The AA shall perform accreditation of a CE within the time period specified in the accreditation procedure.

ID	Description
OR-AA-0003	The AA shall perform accreditation of test laboratories within the time period specified in the accreditation procedure.
OR-AA-0004	The AA shall collect IRs from CEs and set priorities for inclusion in badges and test cases according to the NATO certification strategy.
OR-AA-0005	The AA shall define and maintain the list of approved NATO capability badges, in accordance with the prioritized IRs.
OR-AA-0006	The AA shall provide contact information of subject matter experts to the CE to assist with the definition, development, and implementation of abstract and executable test cases.
OR-AA-0007	The AA shall maintain the IVCT requirement specifications.
OR-ATL-0001	Each ATL shall define their terms and conditions for providing the certification test service.
OR-ATL-0002b	The ATL Certification Service may be performed at a customer site.
OR-ATL-0003	The ATL shall comply with agreed customer security requirements.
OR-ATL-0004	The ATL shall safely transfer certification test results to the CE, using the security solution established by the CE.
OR-ATL-0005	The ATL shall provide a capability to backup test results.
OR-ATL-0006	The ATL shall store certification test results in a secure manner.
OR-ATL-0007	The ATL shall only allow access to certification test results by authorized personnel.
OR-ATL-0008	The ATL shall ensure that certification test results cannot be manipulated after a certification test has finished.
OR-ATL-0009	The ATL shall report irregular IVCT software behaviour to the CE.
OR-ATL-0010	The ATL shall only use the latest released ETC versions, provided by the CE, for certification testing.
OR-ATL-0011	The ATL shall ensure that only SuTE components are connected to the IVCT during testing.
OR-ATL-0012	The ATL should allow a customer to choose to submit, or not, the results of testing a SuT for certification.
OR-CE-0001	The CE shall confirm ATL submission of certification test results within one week.
OR-CE-0002	The CE shall process certification test results and deliver a certification result within the time specified by contract.
OR-CE-0003	The CE shall store certification test results in a secure environment.

ID	Description
OR-CE-0004	The CE shall provide a central point of contact for all certification services.
OR-CE-0005	The CE shall provide a Web-based information system for certification service users.
OR-CE-0006	The CE shall provide an IVCT and ETC issue tracking system.
OR-CE-0007	The CE shall provide IVCT configuration management and up-to-date software status information.
OR-CE-0008	The CE shall evaluate and correct irregular IVCT and ETC software behaviour as soon as possible.
OR-CE-0009	The CE shall define procedure for how to release a new version of the IVCT software.
OR-CE-0010	The CE shall provide a test environment for verifying the IVCT software before release.
OR-CE-0011	The CE shall manage all IVCT software contributions.
OR-CE-0012	The CE shall, with SuT owner permission, publish certificates.
OR-CE-0013	The CE shall provide IVCT software on request to SuT owners and/or test laboratories.
OR-CUSTOMER-0001	The customer shall provide System under Test Environment (SuTE) to the ATL if required for the SuT to function correctly during testing.
OR-CUSTOMER-0002	The customer shall identify the SuT owner when initiating certification.

A.3 USE CASES AND SCENARIOS

Operational Scenarios and **Use Cases** define the operational procedures for all identified roles that are needed to fulfil their respective responsibilities and to comply with operational policies and constraints.

A.3.1 Accreditation and Certification

Figure A-2 shows the details of the Certification Service as a Use Case (UC). There are basically two loops in this service. The first (on the right side of the diagram) is the accreditation phase, where the CE and the test laboratory must be accredited by the Accreditation Authority. The second loop (on the left side of the diagram) is the certification process for a System under Test. Table A-10 contains Use Cases related to Certification Service.

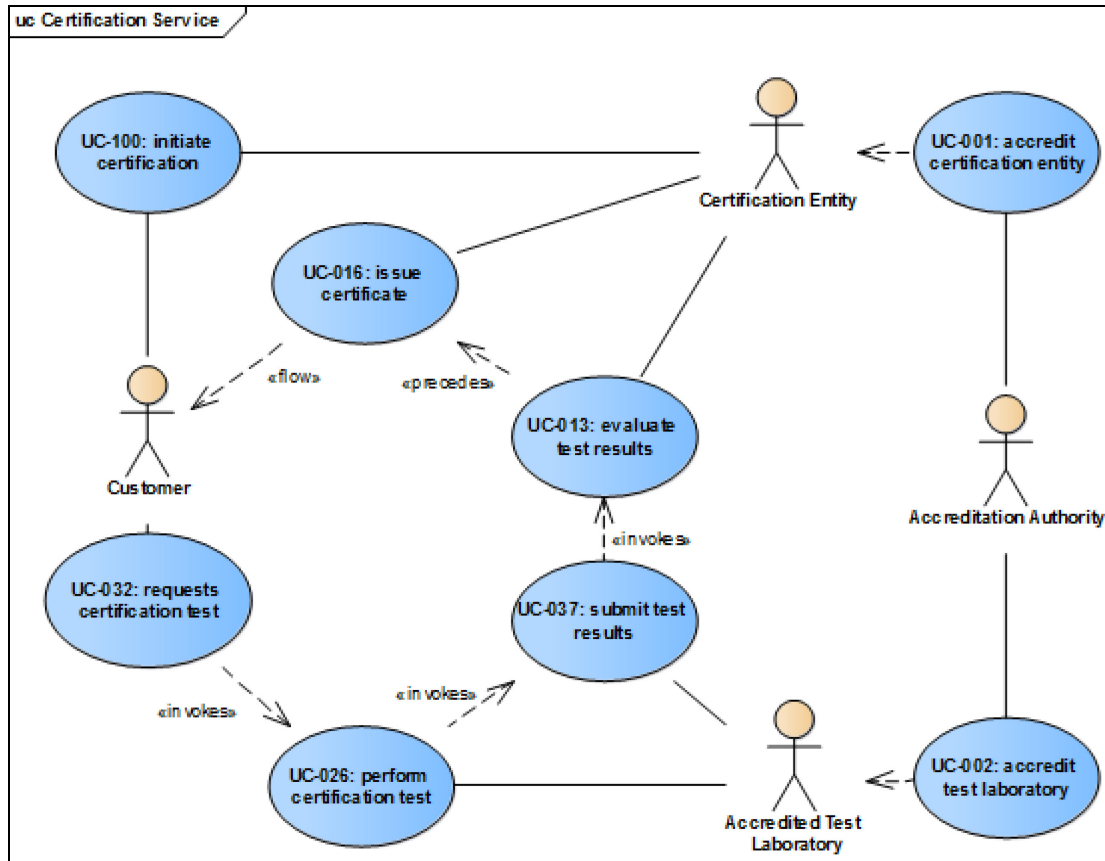


Figure A-2: Use Case of Certification Service.

Table A-10: Use Cases Related to Certification Service.

Title	Description
UC-001 Accredited Certification Entity	The AA receives a CE accreditation request from a CE candidate organization. The AA determines whether the CE candidate meets the CE requirements, including organizational and security standards. If the CE candidate complies with all CE requirements the AA will accredit the CE candidate, otherwise the reasons for non-compliance will be provided to the candidate.
UC-002 Accredited Test Laboratory	The AA receives an accreditation request from an ATL candidate. The AA checks whether the ATL candidate meets the ATL requirements including organizational, technical and security standards. If the ATL candidate complies with all ATL requirements the AA will accredit the ATL candidate, otherwise the reasons for non-compliance will be provided to the candidate.
UC-013 Evaluate Test Results	A CE will evaluate the results according to a predefined procedure to determine whether the SuT has passed certification testing and merits a conformance certificate.
UC-016 Issue Certificate	The CE will issue a certificate to the customer upon determination that the SuT has successfully passed.

Title	Description
UC-026 Perform Certification Test	The ATL analyses the SuT CS and, based on requested CBs, selects and configures appropriate ETC and sets up the IVCT. The ATL runs the IVCT test system using the SuT CS.
UC-032 Requests Certification Test	The customer contacts an ATL to arrange for certification testing. The customer negotiates the conditions for testing the SuT with the ATL. The customer submits the SuT, the SuTE, and the CS to the ATL.
UC-037 Submit Test Results	The ATL will submit the results of the certification test via a secure transport mechanism to the CE.
UC-100: Initiate Certification	The customer initiates the certification process by contacting the CE and providing a request for certifying the SuT against a CS. The CE informs the customer which ATLs are able to perform the tests required by the CS.

A.3.2 Accreditation Process of a Candidate for the ATL Role

Not defined for IOC.

A.3.3 Accreditation Process of a Candidate for the CE Role

Not defined for IOC.

A.3.4 Perform Certification Test

The ATL analyses the SuT CS and based on requested CB selects and configures appropriate ETC and sets up the IVCT. ATL runs the IVCT test system using the SuT CS (see Figure A-3). Table A-11 lists the Use Cases related to perform the certification test.

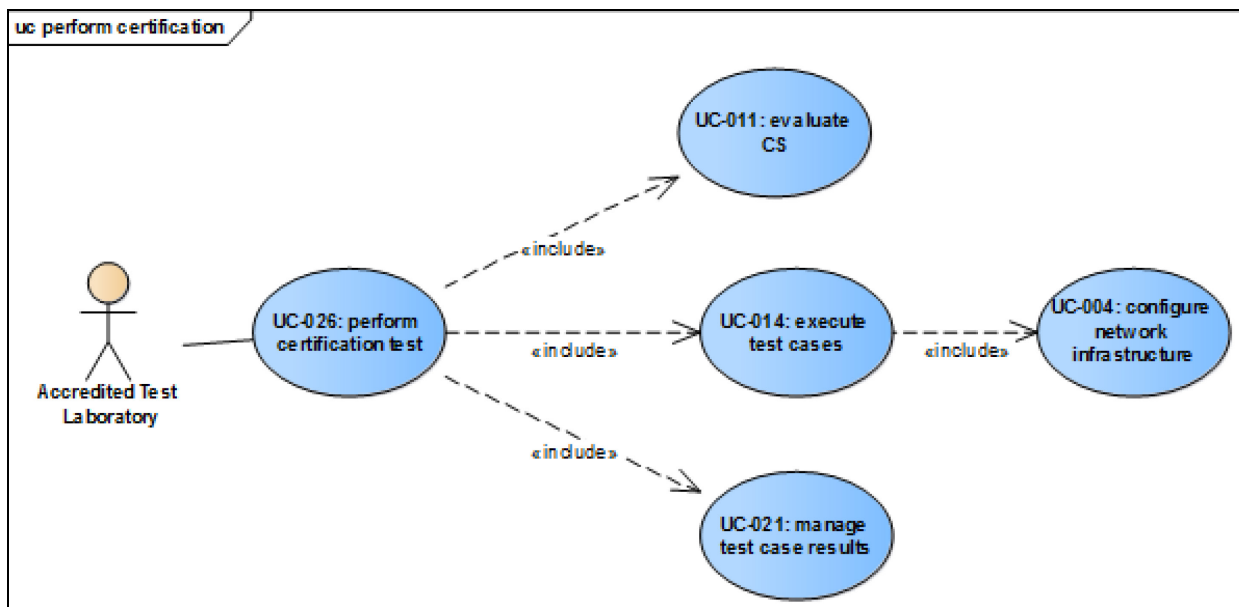


Figure A-3: Use Case of Perform Certification Test.

Table A-11: Use Cases Related to Perform Certification Test.

Title	Description
UC-004 Configure Network Infrastructure	In the case of a LAN, the network addresses have to be configured and the ports have to be opened. In case of a WAN, further routing and forwarding may have to be configured. This task requires knowledge of networking by both the ATL and the customer.
UC-011 Evaluate CS	The ATL will evaluate the CS pertaining to the SuT and select the relevant ETCs required.
UC-014 Execute Test Cases	The selected test cases are run against the SuT and the results of the test are recorded.
UC-021 Manage Test Case Results	The results of the execution of the ETCs are saved in a secure manner, sent to the CE and the customer. The results are log files for the test execution and a summary with the ETC verdicts.

A.3.5 Definition of Certification Workflow

The diagram in Figure A-4 shows the Use Case of definition certification workflow. Table A-12 lists the Use Cases related to definition certification workflow.

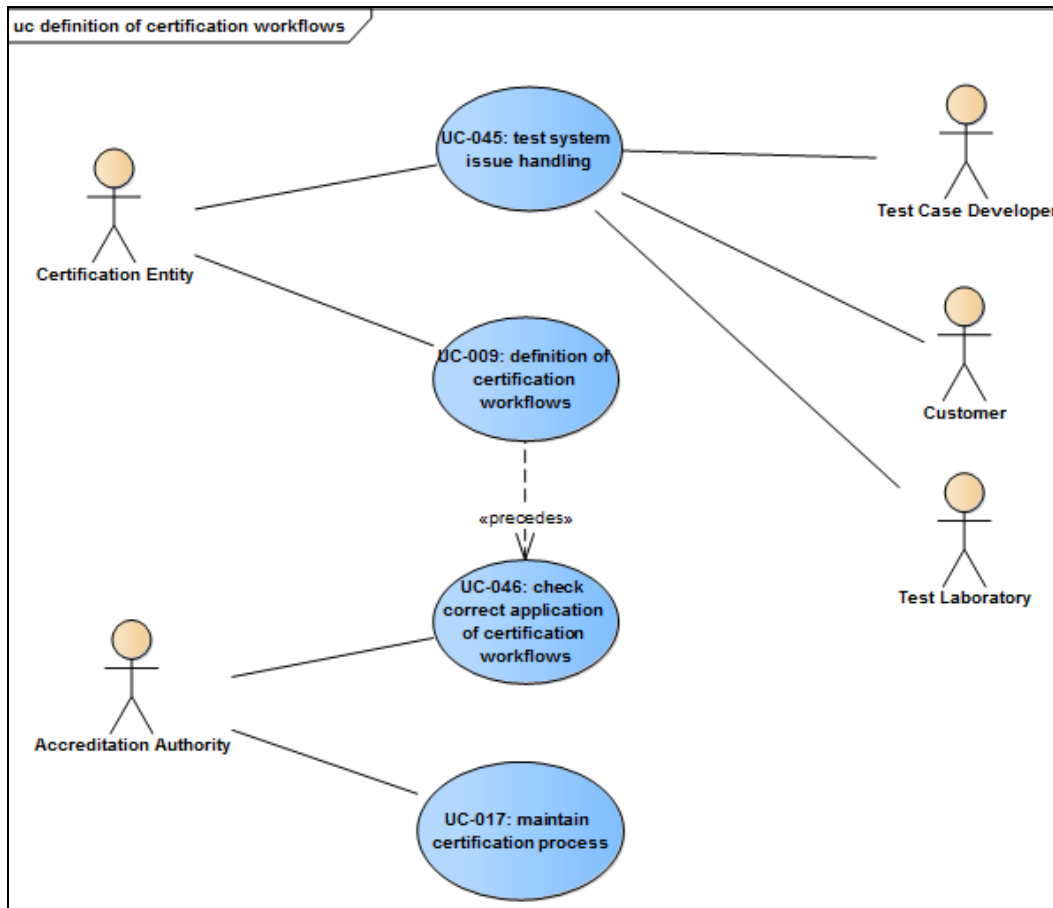


Figure A-4: Use Case of Definition Certification Workflow.

Table A-12: Use Cases Related to Definition Certification Workflow.

Title	Description
UC-009 Definition of Certification Workflows	The CE will define the procedures all participants in the certification workflow. The workflow must include the practical needs of a certification test as well as the security needs related to report management and confidentiality of customer data. The customer must be informed of his role when contacting the CE. All other roles must be defined and known for a test laboratory to be accredited.
UC-017 Maintain Certification Process	The AA updates and maintains documented certification process including the CE and ATL operational requirements and criteria for accreditation.
UC-045 Test System Issue Handling	An issue handling system is an important part of any test system, since when a change is made it may invalidate previous results. All issues and any changes or rejections of these issues must be recorded so that the status of the test system and test case interpretations at any point in time is known. The quality of the test system is improved when issues are properly resolved.
UC-046 Certification Workflow Compliance Review	The AA evaluates the conformance of CEs and ATLs with the certification process and operational requirements on a regular basis. The AA provides the CEs with updated ATL status and contact information.

A.3.6 Development and Maintenance

Figure A-5 shows the various developer roles involved in implementing the test tool software. This includes the implementation of the test tool, test cases, and the management system, as well as the maintenance and documentation. Table A-13 lists Use Cases related to development.

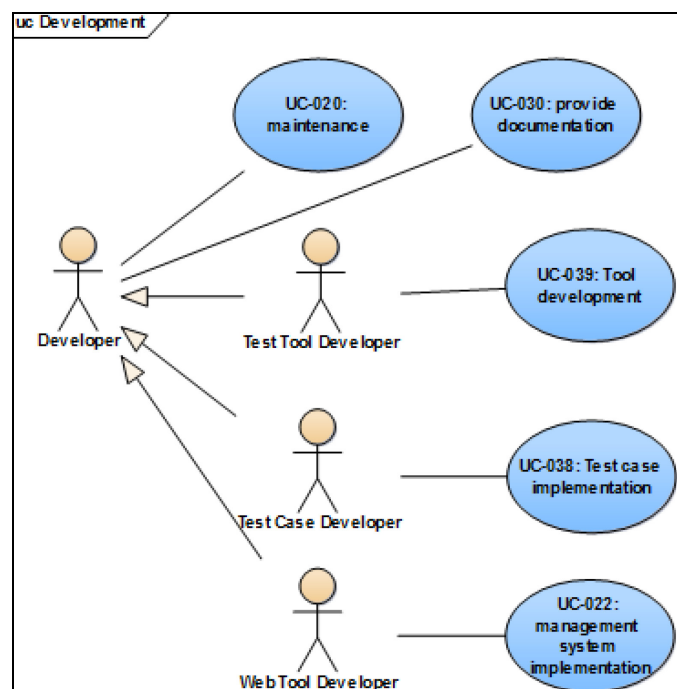


Figure A-5: Use Case of Development.

Table A-13: Use Cases Related to Development.

Title	Description
UC-020 Maintenance	The test tool requires maintenance to address issues with the tool, test cases, operating system changes, and enhancements, as well as changes in the pattern specifications or interpretation of the pattern specifications.
UC-022 Management System Implementation	The management system will manage the documents and data files related to certification tests. These files will be stored in an online database such as NATO Simulation Resources Library (NSRL). This System must guarantee that the files are transferred and stored in a secure manner to prevent tampering with the contents. The files will be accessed via web services.
UC-030 Provide Documentation	A Developer must provide documentation for the development, maintenance, and enhancement of the test tool. Since even a minor change can cause incompatibilities, it is necessary to know the tool behaviour in each version.
UC-038 Test Case Implementation	The CE is responsible for defining the test case purposes. The abstract test cases (specifying the test steps and allowable reactions) are created by the CE, based on the test purposes. The validation of the abstract test cases against the test purposes is also done by the CE. Test purposes are specified by implementation pattern protocol experts and these are implemented by test case developers as executable test cases. Executable test cases are expected to use a test case library to handle bundled events or other support functions. To prove the valid implementation of the test cases, the log files can be examined and checked against the test purposes. The test case developer implements the executable test cases based on the abstract test cases. The executable test cases are scripts or compiled programs which can be run by the IVCT. The work done by the test case developer also includes the verification of the executable test cases against the abstract test cases and the long-term maintenance of the test cases.
UC-039 Tool Development	Test tool development will take place after working out the design specification. Several test tool developers may work on various independent modules. When the test tool has reached a significant level of maturity and has been employed in certification testing and accepted by the CE, it will be considered to be in the maintenance phase.

A.3.6.1 Test Tool Development

The test tool development will take place after working out the design specification. Several test tool developers may work on various well-designed independent modules. When the test tool has reached a significant level of quality and maturity and has been employed in certification testing and been accepted by the CE, it will be considered to be in the maintenance phase. Figure A-6 contains a diagram of a Use Case of test tool development. Table A-14 lists Use Cases related to test tool development.

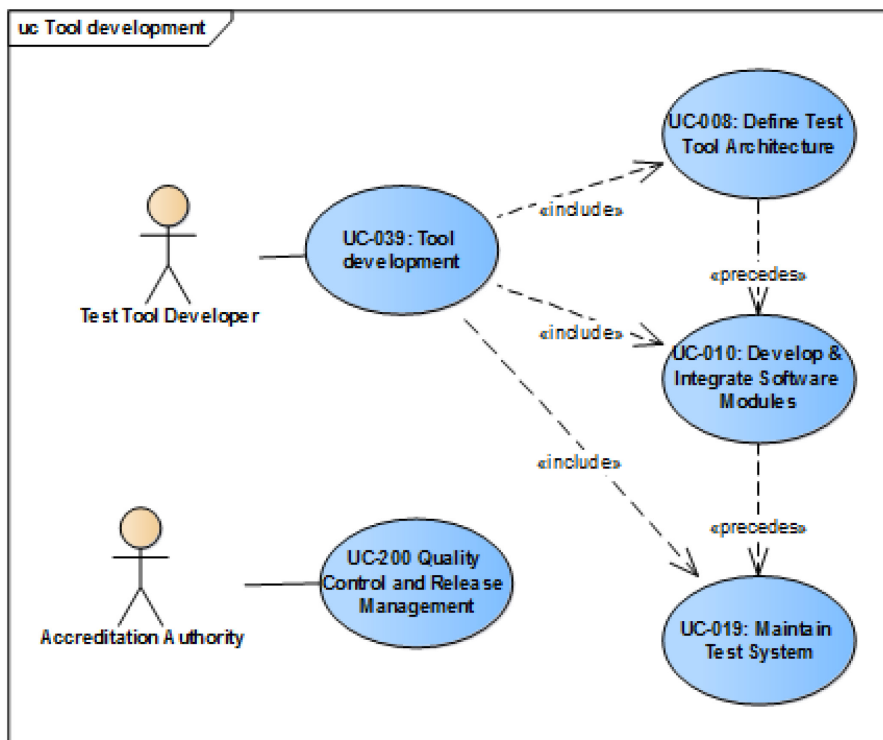


Figure A-6: Use Case of Test Tool Development.

Table A-14: Use Cases Related to Test Tool Development.

Title	Description
UC-008 Define Test Tool Architecture	The test tool provides a platform for executing test cases. The test tool can also read in conformance statement files, select test cases, and provides a logging mechanism to generate test case log and summary report files. The basic architecture can be sketched roughly in advance, but exact details of the interfaces have to be agreed upon with the test case developer.
UC-010 Develop and Integrate Software Modules	According to the test tool architecture, define the functionality and interfaces of all modules for the test tool. The individual modules can be given to different developers for implementation. For each module a test concept should be defined to test the module before attempting integration (unit testing). In Java, JUnit is ideal for this purpose and should be used after every change to detect side effects of those changes. JUnit can also be used to help integrate modules and the JUnit tests should be defined well in advance. The final integration of all modules should be done at one location with a predefined checklist of functionalities to be tested - a federate should be available to exercise the test cases or integrations tests.
UC-019 Maintain Test System	Whenever the test tool is used an issue may occur that requires a modification or extension to the system. A change to any test cases may invalidate test results and should be handled very carefully. Each issue should be well documented and the software should be checked in to a source control system after each modification. The CE must review the changes before authorizing a new test tool release.

A.3.6.2 Test Case Implementation

The Certification Entity is responsible for defining the test case purposes. Figure A-7 contains a diagram of a Use Case of Test Case implementation. The abstract test cases (specifying the test steps and allowable reactions) are created by the CE, based on the test purposes. The validation of the abstract test cases against the test purposes is also done by the CE. Test purposes are specified by implementation pattern protocol experts and these are implemented by test case developers into executable test cases. Executable test cases will use a test case library to handle bundled events or other support functions. To prove the valid implementation of the test cases, the log files can be examined and checked against the test purposes. The test case developer implements the executable test cases from the abstract test cases. The executable test cases are scripts or compiled programs which can be started by the IVCT. The work done by the test case developer also includes the verification of the executable test cases against the abstract test cases, and the maintenance of the test cases. Table A-15 lists Use Cases related to test case implementation.

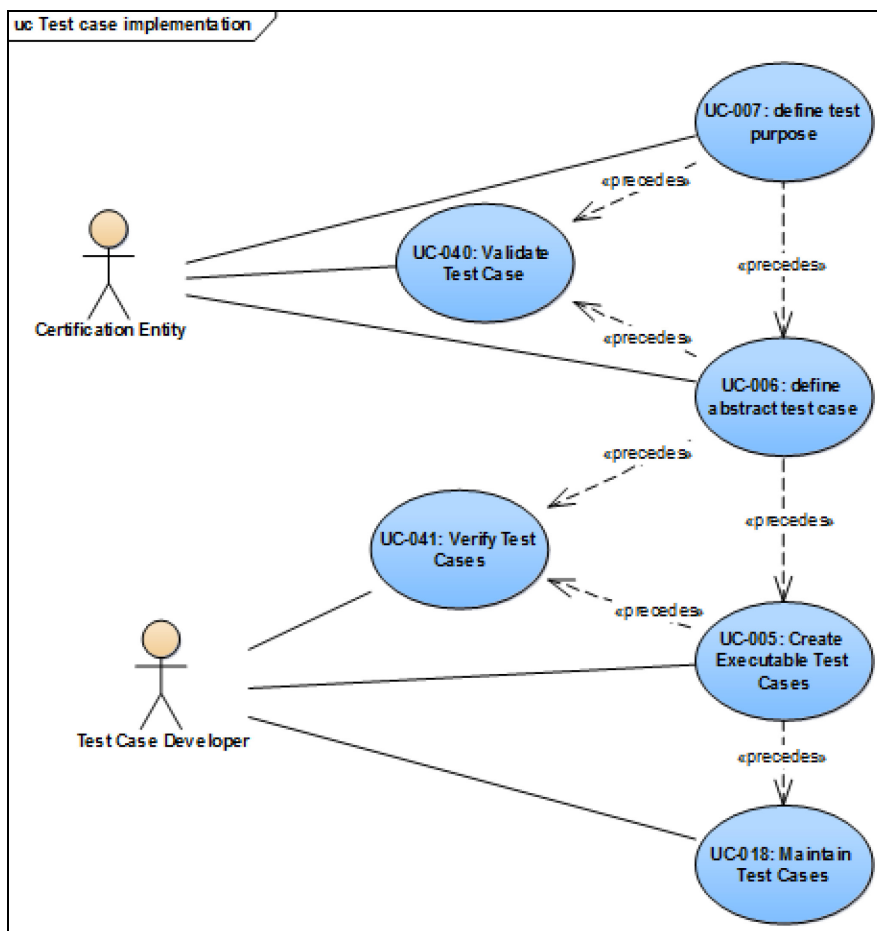


Figure A-7: Use Case of Test Case Implementation.

Table A-15: Use Cases Related to Test Case Implementation.

Title	Description
UC-005 Create Executable Test Cases	Once the abstract test cases have been validated, a test case developer can start with the implementation of the executable test cases and the supporting library functions in a specific programming language.

Title	Description
UC-006 Define Abstract Test Case	Once the test purposes have been defined, it is possible to define the test steps required to achieve these purposes in the form of abstract test cases. The abstract test cases are the sequences of requests and expected responses independent of a programming language.
UC-007 Define Test Purpose	When a pattern protocol is defined, it is a good idea to define test purposes which will constitute a comprehensive test of the functionality and variations of this functionality. The test purposes should also cover error handling and reactions to invalid behaviour.
UC-018 Maintain Test Cases	During the course of testing the implemented executable test cases, various issues may occur that require changes to them. This maintenance activity should be done in a disciplined manner, since even small changes could invalidate previous certificates. After a change to any executable test case, it should be run against SuTs from two different owners to test for side effects. All changes must be documented in respect to an issue and its solution.
UC-040 Validate Test Case	Once abstract test cases are created, they should be checked to ensure are a valid interpretation of the test purposes. The CE should make sure this is completed before executable test cases are created.
UC-041 Verify Test Cases	Once executable test cases are created, they should be checked to ensure they are a valid interpretation of the abstract test cases. The test case developer should make sure this is completed before they are used for certification testing.

Annex B – CAPABILITY BADGES, INTEROPERABILITY REQUIREMENTS AND ABSTRACT TEST CASES

B.1 INTEROPERABILITY CAPABILITY BADGES

An interoperability **Capability Badge** (CB) is defined as a token of achievement in terms of passing testing related to Interoperability Requirements (IRs) associated with the CB. Successful compliance testing, verification, and certification of individual systems' compliance with sets of IRs can be labelled using a CB representing this achievement. Figure B-1 represents the key elements of the Certification Process.

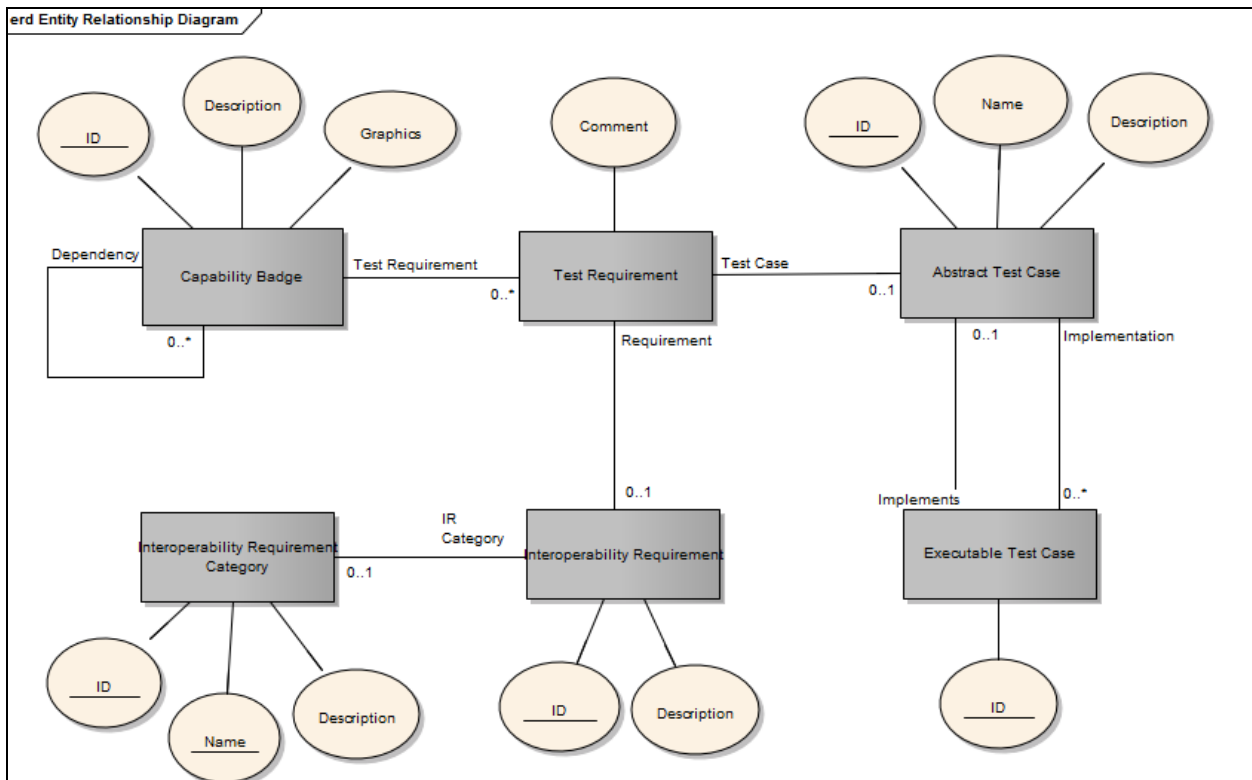


Figure B-1: Key Elements of the Certification Process.

The concept of using badges to indicate achievements is nothing new. It can be found in many domains from the scouts to the military. In online gaming, badges are frequently used to display an individual gamer's skill, accomplishments, and level of play. The semantics associated with badges and how they are used vary between different domains, and even within a single domain you can find different types of badges showing skill, quantitative and qualitative achievements, accomplishment of a specific mission, and badges showing general maturity or level. Applying the badges concept to interoperability capabilities has been explored in research activities in the UK [6] and [7]. Figure B-2 represents relationships between a CB, its associated IRs and the System under Test (SuT).

Achievement graphs are used to specify dependencies between different CBs and to visualise road-maps for increased simulation component interoperability. An achievement graph is used to express implicit requirements for achieving a specific CB that includes requirements related to other badges, e.g., Achieving RPR-ENTITY-2016 also requires achieving the HLA-BASE-2016 CB requirements. By using achievement graphs, combinations/aggregations of CB associated IRs can be expressed.

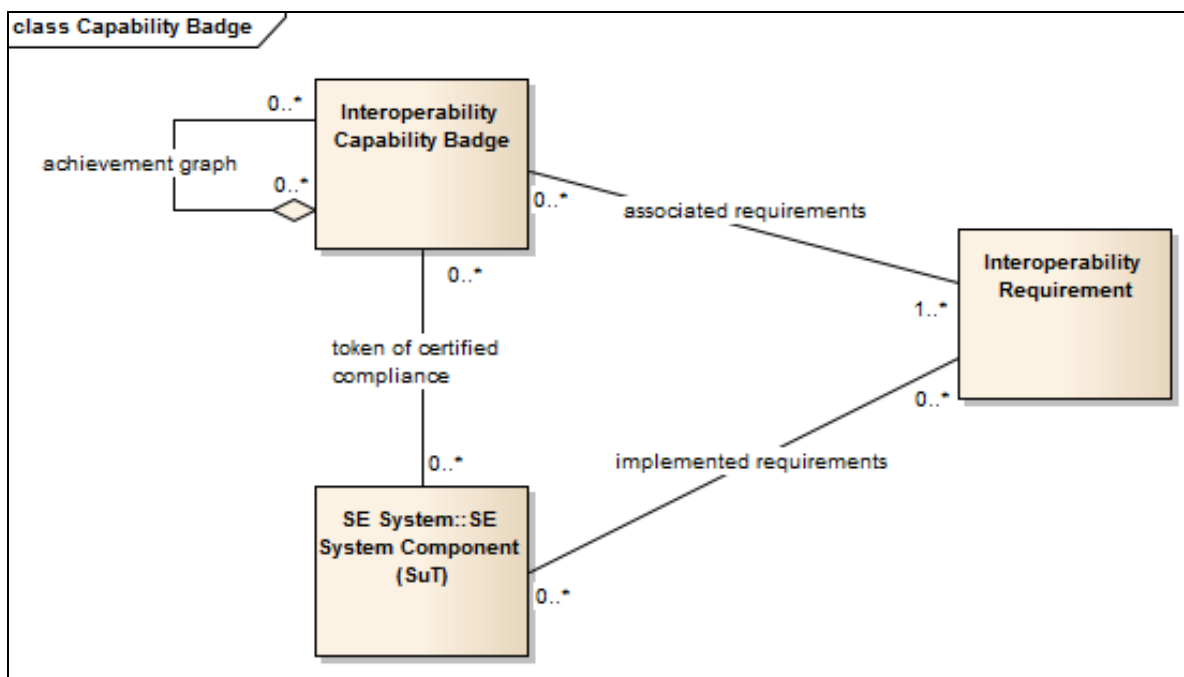


Figure B-2: Relationships Between a CB, Its Associated IRs and the System under Test (SuT).


MSG-134 recommends the use of CBs as tokens for passing testing related to interoperability, and as the basis for certificates of compliance. CBs are also used in the Conformance Statements (CSs) provided by the SuT owners as the basis for certification.

A CB is identified by name, type and year. It has a short description and a graphical representation (“the badge”). The CB is defined by the set of associated IRs including references to Abstract Test Cases (ATCs) describing how the IRs are verified.

The definition of CBs used in the NATO Simulation Interoperability Test and Certification Service is the responsibility of the Accreditation Authority (AA).

An initial set of CBs based on NATO Simulation Interoperability Test and Certification Service priorities have been defined. Table B-1 lists the Interoperability Capability Badges.




Table B-1: Interoperability Capability Badges.

ID	Dependency	Description	Graphics
CWIX-DR-2017	CWIX-ENTITY-2017	Simulation Interoperability Compliance Badge for CWIX 2017.	

ID	Dependency	Description	Graphics
CWIX-ENTITY-2017		Simulation interoperability compliance badge for CWIX 2017.	
CWIX-WARFARE-2017	CWIX-ENTITY-2017	Simulation interoperability compliance badge for CWIX 2017.	
HLA-BASE-2017		Basic CS/SOM and best practices compliance.	
NETN-AGG-2017	RPR-AGG-2017	NETN-FOM v2.0 aggregate FOM module.	
NETN-ENTITY-2017	RPR-ENTITY-2017	NETN-FOM v2.0 physical FOM module.	

ANNEX B – CAPABILITY BADGES, INTEROPERABILITY REQUIREMENTS AND ABSTRACT TEST CASES

ID	Dependency	Description	Graphics
NETN-LBML-INTREP-2017	NETN-AGG-2017, NETN-ENTITY-2017	NETN-FOM v2.0 LBML FOM module.	
NETN-LBML-OWNSITREP-2017	NETN-AGG-2017, NETN-ENTITY-2017	NETN-FOM v2.0 LBML FOM module.	
NETN-LBML-TASK-2017	NETN-AGG-2017, NETN-ENTITY-2017	NETN-FOM v2.0 LBML FOM module.	
NETN-MRM-2017	NETN-TMR-2017	NETN-FOM v2.0 MRM FOM module.	
NETN-TMR-2017	HLA-BASE-2017	Basic support for NETN TMR pattern (AMSP-04 Ed A). SuT is able to respond to TMR requests.	

ID	Dependency	Description	Graphics
RPR-AGG-2017	HLA-BASE-2017	RPR-FOM v2.0 aggregate FOM Module.	
RPR-ENTITY-2017	HLA-BASE-2017	RPR-FOM v2.0 physical FOM Module support. GRIM compliance wrt. Platforms, Lifeforms, etc. representation of required attributes.	
RPR-WARFARE-2017	HLA-BASE-2017 RPR-ENTITY-2017	RPR-Warfare v2.0 FOM module support.	

B.2 INTEROPERABILITY REQUIREMENTS

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.

Sets of related IRs can be defined and grouped to form interoperability Capability Badges (CBs) used to express a systems capability to interoperate on a higher level than individual IRs.

IRs can also be grouped and associated with Abstract Test Cases (ATCs) as the implicit purpose of ATCs is to verify all associated IRs. IRs can be grouped into categories (Table B-2).

Table B-2: Categories of Interoperability Requirement.

ID	Name	Description
BP	Best Practice Conformance	Requirements related to best practices for distributed simulation.
DOC	Documentation Conformance	Requirements for documenting interoperability capabilities.

ID	Name	Description
NETN	NETN Requirements	Requirements related to NETN FAFD, AMSP-04 Ed A, STANREC 4800.
RPR2	RPR2 Requirements	Requirements related to RPR-FOM v2.0.
SOM	Simulation Object Model Conformance	Requirements related to the conformance of a SuT to the SOM provided in a CS.

Table B-3 lists the initial set of interoperability requirements as identified by MSG-134.

Table B-3: Initial Set of Interoperability Requirements.

ID	Category	Description
IR-BP-0001	BP	The SuT shall provide attribute value updates for requested attributes owned by the SuT.
IR-BP-0002	BP	The SuT shall create a federation execution before joining, if it does not already exist.
IR-BP-0003	BP	The SuT shall create or join a federation execution with only those FOM modules that are specified in its CS.
IR-BP-0004	BP	The SuT shall be configurable for the following parameters: <i>FederateType</i> , <i>FederateName</i> , <i>FederationName</i> .
IR-BP-0005	SOM	The SuT shall remove at least one object instance if RemoveObjectInstance HLA service is described as used in CS/SOM.
IR-BP-0006	SOM	The SuT shall resign federation if ResignFederation HLA service is described as used in CS/SOM.
IR-BP-0007	SOM	The SuT shall only update values, for attributes with the Enumerated Datatype, compliant with the Distributed Simulation Agreement.
IR-DOC-0001	DOC	The SuT interoperability capabilities shall be documented in a conformance statement including a SOM and a FOM with a minimum set of supporting FOM modules.
IR-NETN-0001	NETN	The SuT shall comply with STANREC 4800, AMSP-04 NETN FAFD Ed A, October 2017.
IR-NETN-0002	NETN	The SuT shall define BaseEntity.AggregateEntity.NETN_Aggregate as published and/or subscribed in its CS/SOM.
IR-NETN-0003	NETN	The SuT shall update the following required attributes for NETN_Aggregate object instances registered by SuT: <i>UniqueID</i> , <i>Callsign</i> , <i>Status</i> , <i>Echelon</i> , <i>HigherHeadquarters</i> , <i>AggregateState</i> , <i>Dimensions</i> , <i>EntityIdentifier</i> , <i>EntityType</i> , <i>Spatial</i> .
IR-NETN-0004	NETN	The SuT updates of NETN_Aggregate instance attributes shall be valid according to STANREC 4800.

ID	Category	Description
IR-NETN-0005	NETN	The SuT shall assume default values for optional attributes on instances of NETN_Aggregate object class.
IR-NETN-0006	NETN	The SuT shall not rely on updates of optional attributes on instances of NETN_Aggregate object class.
IR-NETN-0007	NETN	The SuT shall use predefined IDs to generate the same UniqueID for an NETN_Aggregate instance in different Federation Executions.
IR-NETN-0008	NETN	The SuT shall document in its CS if it acts as a NETN TMR trigger, requesting and/or responding federate.
IR-NETN-0009	NETN	The SuT triggering TMR shall define TMR_InitiateTransferModellingResponsibility as published in its CS/SOM.
IR-NETN-0010	NETN	The SuT triggering TMR shall define TMR_OfferTransferModellingResponsibility as subscribed in its CS/SOM.
IR-NETN-0011	NETN	The SuT triggering TMR shall define TMR_TransferResult as subscribed in its CS/SOM.
IR-NETN-0012	NETN	The SuT requesting TMR shall define TMR_InitiateTransferModellingResponsibility as subscribed in its CS/SOM.
IR-NETN-0013	NETN	The SuT requesting TMR shall define TMR_OfferTransferModellingResponsibility as published and subscribed in its CS/SOM.
IR-NETN-0014	NETN	The SuT requesting TMR shall define TMR_TransferResult as published in its CS/SOM.
IR-NETN-0015	NETN	The SuT requesting TMR shall define TMR_RequestTransferModellingResponsibility as published in the CS/SOM.
IR-NETN-0016	NETN	The SuT requesting TMR shall define TMR_CancelRequest as published in CS/SOM.
IR-NETN-0017	NETN	The SuT responding to TMR shall define TMR_RequestTransferModellingResponsibility as subscribed in the CS/SOM.
IR-NETN-0018	NETN	The SuT responding to TMR shall define TMR_OfferTransferModellingResponsibility as published in the CS/SOM.
IR-NETN-0019	NETN	The SuT responding to TMR shall define TMR_CancelRequest as subscribed in CS/SOM.
IR-NETN-0020	NETN	The SuT triggering TMR shall comply with TMR design pattern for a TMR Triggering federate as documented in NETN FAFD, STANREC 4800.
IR-NETN-0021	NETN	The SuT requesting TMR shall comply with TMR design pattern for a TMR Requesting federate as documented in NETN FAFD, STANREC 4800.

ID	Category	Description
IR-NETN-0022	NETN	The SuT responding to TMR shall comply with TMR design pattern for TMR Responding federate as documented in NETN FAFD, STANREC 4800.
IR-NETN-0023	NETN	The SuT shall respond to a TMR_InitiateTransferModellingResponsibility directed to the SuT with a negative TMR_OfferTransferModellingResponsibility if it is not possible to initiate a transfer of modelling responsibility.
IR-NETN-0024	NETN	The SuT shall respond to a TMR_InitiateTransferModellingResponsibility directed to the SuT with a positive TMR_OfferTransferModellingResponsibility if it is possible to initiate a transfer of modelling responsibility.
IR-NETN-0025	NETN	The SuT shall respond to a TMR_InitiateTransferModellingResponsibility directed to the SuT with a TMR_TransferResult.
IR-NETN-0026	NETN	The SuT shall not respond to a TMR_InitiateTransferModellingResponsibility if it is not directed to the SuT.
IR-NETN-0027	NETN	The SuT shall respond to a TMR_RequestTransferModellingResponsibility directed to the SuT with a negative TMR_OfferTransferModellingResponsibility if it is not possible to perform a transfer of modelling responsibility.
IR-NETN-0028	NETN	The SuT shall respond to a TMR_RequestTransferModellingResponsibility directed to the SuT with a positive TMR_OfferTransferModellingResponsibility if it is possible to perform a transfer of modelling responsibility.
IR-NETN-0029	NETN	The SuT shall not respond to a TMR_RequestTransferModellingResponsibility if it is not directed to the SuT.
IR-NETN-0030	NETN	The SuT shall, if SuT responds positive to a TMR_RequestTransferModellingResponsibility, use HLA services to perform TMR according to pattern defined in NETN FAFD, STANREC 4800.
IR-NETN-0031	NETN	The SuT shall cancel or not perform TMR as a response to a TMR_CancelRequest directed to the SuT.
IR-NETN-0032	NETN	The SuT shall document time-out condition for receiving a TMR_OfferTransferModellingResponsibility corresponding to a TMR_RequestTransferModellingResponsibility sent by the SuT.
IR-NETN-0033	NETN	The SuT shall send TMR_CancelRequest after TMR_RequestTransferModellingResponsibility sent by SuT has timed-out.
IR-NETN-0034	NETN	The SuT acting as an MRM Service Provider shall define interaction class MRM_AggregationRequest as published in its CS/SOM.
IR-NETN-0035	NETN	The SuT acting as an MRM Service Provider shall define interaction class MRM_AggregationResponse as subscribed in its CS/SOM.

ID	Category	Description
IR-NETN-0036	NETN	The SuT acting as a MRM Service Provider shall define interaction class MRM_ActionComplete as published in its CS/SOM.
IR-NETN-0037	NETN	The SuT MRM Service Provider shall respond to interaction MRM_Trigger with interaction MRM_TriggerResponse.
IR-NETN-0038	NETN	The SuT MRM Service Provider shall send interaction MRM_ActionComplete, positive result when MRM actions are completed.
IR-NETN-0040	NETN	The SuT MRM Aggregate Federate shall comply with MRM design pattern for an MRM Service Provider federate as documented in NETN FAFD, STANREC 4800.
IR-NETN-0041	NETN	The SuT acting as an Aggregate Federate shall define object class NETN_Aggregate as published and subscribed in its CS/SOM.
IR-NETN-0042	NETN	The SuT acting as an Aggregate Federate shall define interaction class MRM_DisaggregationRequest as subscribed in its CS/SOM.
IR-NETN-0043	NETN	The SuT acting as an Aggregate Federate shall define interaction class MRM_DisaggregationResponse as published in its CS/SOM.
IR-NETN-0044	NETN	The SuT acting as an Aggregate Federate shall define interaction class MRM_AggregationRequest as subscribed in its CS/SOM.
IR-NETN-0045	NETN	The SuT acting as an Aggregate Federate shall define interaction class MRM_AggregationResponse as published in its CS/SOM.
IR-NETN-0046	NETN	The SuT acting as an Aggregate Federate shall define interaction class MRM_ActionComplete as subscribed in its CS/SOM.
IR-NETN-0047	NETN	The SuT Aggregate Federate shall respond to interaction MRM_DisaggregationRequest with interaction MRM_DisaggregationResponse.
IR-NETN-0048	NETN	The SuT Aggregate Federate shall respond to interaction MRM_AggregationRequest with interaction MRM_AggregationResponse.
IR-NETN-0049	NETN	The SuT MRM Higher Resolution Federate shall comply with MRM design pattern for an MRM Service Provider federate as documented in NETN FAFD, STANREC 4800.
IR-NETN-0050	NETN	The SuT acting as a Higher Resolution Federate shall define the NETN-Physical leaf object classes as published and subscribed in its CS/SOM.
IR-NETN-0051	NETN	The SuT acting as a Higher Resolution Federate shall define interaction class MRM_DisaggregationRequest as subscribed in its CS/SOM.
IR-NETN-0052	NETN	The SuT acting as a Higher Resolution Federate shall define interaction class MRM_DisaggregationResponse as published in its CS/SOM.
IR-NETN-0053	NETN	The SuT acting as a Higher Resolution Federate shall define interaction class MRM_AggregationRequest as subscribed in its CS/SOM.

ID	Category	Description
IR-NETN-0054	NETN	The SuT acting as a Higher Resolution Federate shall define interaction class MRM_AggregationResponse as published in its CS/SOM.
IR-NETN-0055	NETN	The SuT acting as a Higher Resolution Federate shall define interaction class MRM_ActionComplete as subscribed in its CS/SOM.
IR-NETN-0056	NETN	The SuT Higher Resolution Federate shall respond to interaction MRM_DisaggregationRequest with interaction MRM_DisaggregationResponse.
IR-NETN-0057	NETN	The SuT Higher Resolution Federate shall respond to interaction MRM_AggregationRequest with interaction MRM_AggregationResponse.
IR-NETN-0058	NETN	The SuT MRM Service Provider shall, if SuT receives positive MRM_DisaggregationResponse, use HLA services and TMR interactions to perform MRM disaggregation according to pattern defined in NETN FAFD, STANREC 4800.
IR-NETN-0059	NETN	The SuT MRM Service Provider shall, if SuT receives positive MRM_AggregationResponse, use HLA services and TMR interactions to perform MRM aggregation according to pattern defined in NETN FAFD, STANREC 4800.
IR-NETN-0060	NETN	The SuT Aggregate or Higher Resolution Federate shall, if SuT responds positive to a MRM_DisaggregationRequest, use HLA services and TMR interactions to perform MRM disaggregation according to pattern defined in NETN FAFD, STANREC 4800.
IR-NETN-0061	NETN	The SuT Aggregate or Higher Resolution Federate shall, if SuT responds positive to a MRM_AggregationRequest, use HLA services and TMR interactions to perform MRM aggregation according to pattern defined in NETN FAFD, STANREC 4800.
IR-NETN-0062	NETN	The SuT Aggregate or Higher Resolution Federate shall, if SuT responds positive to a MRM_AggregationRequest, use HLA services and TMR interactions to perform MRM aggregation according to pattern defined in NETN FAFD, STANREC 4800.
IR-NETN-0063	NETN	The 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.
IR-NETN-0064	NETN	The SuT defined as producer in CS/SOM shall for LBMLMessage.LBMLTask leaf interactions provide the following required parameters for the LBMLMessage.LBMLTask leaf classes: Task, Taskee, Tasker, TaskType.
IR-NETN-0065	NETN	The SuT defined as producer in its CS/SOM shall for LBMLMessage.LBMLTask leaf interactions provide all required parameters defined in the LBMLMessage.LBMLTask leaf interaction class.

ID	Category	Description
IR-NETN-0066	NETN	The SuT shall define NETN LBMLMessage.LBMLTask.MoveToLocation and LBMLMessage.LBMLTask.MoveToUnit as published and/or subscribed in CS/SOM.
IR-NETN-0067	NETN	The SuT shall define at least one leaf interaction class of NETN LBMLMessage.LBMLTaskManagement (CancelAllTasks, CancelSpecifiedTasks) as published and/or subscribed in its CS/SOM.
IR-NETN-0068	NETN	The SuT shall define NETN LBMLReport.StatusReport.TaskStatusReport as subscribed in its CS/SOM if SuT has defined leaf classes of LBMLTask as published in CS/SOM.
IR-NETN-0069	NETN	The SuT shall define NETN LBMLReport.StatusReport.TaskStatusReport as published in its CS/SOM if SuT has defined leaf classes of LBMLTask as subscribed in its CS/SOM.
IR-NETN-0070	NETN	The SuT shall define NETN LBMLMessage.LBMLTask.FireAtLocation and LBMLMessage.LBMLTask.FireAtUnit or subclasses of these as published and/or subscribed in its CS/SOM.
IR-NETN-0071	NETN	The SuT defined as consumer in its CS/SOM shall for NETN LBMLMessage.LBMLTask.FireAtLocation and LBMLMessage.LBMLTask.FireIndirectWM fire at the specified location.
IR-NETN-0072	NETN	The SuT defined as consumer in its CS/SOM shall for NETN LBMLMessage.LBMLTask.FireAtUnit and LBMLMessage.LBMLTask.FireDirectWM fire at the specified unit.
IR-NETN-0073	NETN	The SuT defined as a consumer in its CS/SOM shall clear all tasks at the entity when an LBMLMessage.LBMLTaskManagement.CancelAllTasks is received.
IR-NETN-0074	NETN	The SuT defined as a consumer in its CS/SOM shall clear the tasks at the entity that is specified in the LBMLMessage.LBMLTaskManagement.CancelSpecifiedTasks when it is received.
IR-NETN-0075	NETN	The SuT defined as consumer in its CS/SOM shall for NETN LBMLMessage.LBMLTask.MoveToLocation and LBMLMessage.LBMLTask.MoveToUnit move the specified unit to the specified location and if the route is specified use it.
IR-NETN-0076	NETN	The SuT defined as a producer of NETN LBMLReport.StatusReport.TaskStatusReport in its CS/SOM shall respond to a leaf class of LBMLMessage.LBMLTask with a status report of the task (Accepted/Refused).
IR-NETN-0077	NETN	The SuT defined as a producer of NETN LBMLReport.StatusReport.TaskStatusReport in its CS/SOM shall update the status of the task (Aborted/Completed) when the status change.
IR-NETN-0078	NETN	The SuT shall define LBMLReport.SpotReport.ActivitySpotReport.CurrentActivitySpotReport as published and/or subscribed in its CS/SOM.

ID	Category	Description
IR-NETN-0079	NETN	The SuT defined as a provider in its CS/SOM shall define BaseEntity.AggregateEntity.NETN_Aggregate or a subclass and/or a NETN subclass of BaseEntity.PhysicalEntity as subscribed in its CS/SOM.
IR-NETN-0080	NETN	The SuT defined as a provider in SOM/CS shall send LBMLReport.SpotReport.ActivitySpotReport.CurrentActivitySpotReport about spotted enemies, neutral, or unknown units (in relation to the observer) when these are able to observe (determined by the SuT observing model).
IR-NETN-0081	NETN	The SuT shall define LBMLReport.StatusReport.ActivityStatusReport.CurrentActivityStatusReport as published and/or subscribed in its CS/SOM.
IR-NETN-0082	NETN	The SuT defined as a provider in its CS/SOM shall define BaseEntity.AggregateEntity.NETN_Aggregate or a subclass and/or a NETN subclass of BaseEntity.PhysicalEntity as published in its CS/SOM.
IR-NETN-0083	NETN	The SuT defined as a provider in its SOM/CS shall send LBMLReport.StatusReport.ActivityStatusReport.CurrentActivityStatusReport from friendly units about their own (perceived) state.
IR-NETN-0084	NETN	The SuT defined as a consumer in its SOM/CS shall receive LBMLReport.StatusReport.ActivityStatusReport.CurrentActivityStatusReport for friendly units about their (perceived) state and base its low-level BML tasks on this perceived truth data of blue units instead of RPR ground truth data.
IR-NETN-0085	NETN	The SuT defined as a consumer in its SOM/CS shall receive LBMLReport.SpotReport.ActivitySpotReport.CurrentActivitySpotReport for spotted enemy, neutral, or unknown unit and base its low-level BML tasks on this perceived truth data on non-friendly / unknown units instead of RPR ground truth data.
IR-RPR2-0001	RPR2	The SuT shall comply with SISO-STD-001-2015, Standard for Guidance, Rationale, and Interoperability Modalities for the Real-time Platform Reference Federation Object Model, Version 2.0, 10 August 2015.
IR-RPR2-0002	RPR2	The SuT shall define BaseEntity.AggregateEntity as published or define a subclass of BaseEntity.AggregateEntity as published and/or define BaseEntity.AggregateEntity as subscribed in its CS/SOM.
IR-RPR2-0003	RPR2	The SuT shall update the following required attributes for AggregateEntity object instances registered by SuT: AggregateState, Dimensions, EntityIdentifier, EntityType, Spatial.
IR-RPR2-0004	RPR2	The SuT updates of AggregateEntity instance attributes shall be valid according to SISO-STD-001-2015 and SISO-STD-001.1-2015.
IR-RPR2-0005	RPR2	The SuT shall assume default values for optional attributes on instances of AggregateEntity object class.

ID	Category	Description
IR-RPR2-0006	RPR2	The SuT shall not rely on updates of optional attributes on instances of AggregateEntity object class.
IR-RPR2-0007	RPR2	The SuT shall be configurable for the following parameters: SiteID, ApplicationID.
IR-RPR2-0008	RPR2	The SuT shall define at least one leaf object class of BaseEntity.PhysicalEntity as published and/or subscribed in its CS/SOM.
IR-RPR2-0009	RPR2	The SuT shall in CS specify the use of Articulated Parts for all published and subscribed BaseEntity.PhysicalEntity and subclasses.
IR-RPR2-0010	RPR2	The SuT shall, in its, CS specify the use of Dead-Reckoning algorithms for all published and subscribed BaseEntity.PhysicalEntity and subclasses.
IR-RPR2-0011	RPR2	The SuT shall update the following required attributes for PhysicalEntity subclass object instances registered by SuT: <i>EntityIdentifier</i> , <i>EntityType</i> , <i>Spatial</i> .
IR-RPR2-0012	RPR2	The SuT shall not update non-applicable PhysicalEntity Attributes as specified in Domain Appropriateness table in SISO-STD-001-2015.
IR-RPR2-0013	RPR2	The SuT updates of instance attributes shall, for BaseEntity.PhysicalEntity and subclasses, be valid according to SISO-STD-001-2015 and SISO-STD-001.1-2015.
IR-RPR2-0014	RPR2	The SuT updates of instance attribute Spatial shall, for BaseEntity.PhysicalEntity and subclasses, include valid Dead-Reckoning parameters for supported algorithms as specified in its CS.
IR-RPR2-0015	RPR2	The SuT shall assume default values for optional attributes on instances of BaseEntity.PhysicalEntity and subclasses according to SISO-STD-001-2015.
IR-RPR2-0016	RPR2	The SuT shall not rely on updates of optional attributes on instances of BaseEntity.PhysicalEntity and subclasses.
IR-RPR2-0017	RPR2	The SuT shall define BaseEntity.PhysicalEntity.Munition or at least one leaf object class as published or subscribed in CS/FOM when tracked munitions is used (e.g., torpedoes, missiles, etc.).
IR-RPR2-0018	RPR2	The SuT shall define interaction class WeaponFire or at least one leaf class as published and/or subscribed in CS/SOM.
IR-RPR2-0019	RPR2	The SuT shall provide the following required parameters for the WeaponFire interaction: EventIdentifier, FiringLocation, FiringObjectIdentifier, FuseType, InitialVelocityVector, MunitionType, WarheadType.
IR-RPR2-0020	RPR2	The SuT shall when tracked munition is used provide the WeaponFire parameter MunitionObjectIdentifier.
IR-RPR2-0021	RPR2	The SuT shall provide parameters for sent interactions of WeaponFire and subclasses according to SISO-STD-001-2015 and SISO-STD-001.1-2015.

ID	Category	Description
IR-RPR2-0022	RPR2	The SuT shall assume default values for optional parameters at interactions of WeaponFire and subclasses according to SISO-STD-001-2015.
IR-RPR2-0023	RPR2	The SuT shall not rely on receiving optional parameters on interactions of WeaponFire and subclasses.
IR-RPR2-0024	RPR2	The SuT shall define interaction class MmunitionDetonation or at least one leaf class as published and/or subscribed in its CS/SOM.
IR-RPR2-0025	RPR2	The SuT shall provide the following required parameters for the MmunitionDetonation interaction: DetonationLocation, EventIdentifier, FuseType, MmunitionType, WarheadType.
IR-RPR2-0026	RPR2	The SuT shall when munition type is not a mine provide the following required parameters for the MmunitionDetonation interaction: FiringObjectIdentifier, FinalVelocityVector.
IR-RPR2-0027	RPR2	The SuT shall when tracked munition is used provide the MmunitionDetonation parameter MmunitionObjectIdentifier.
IR-RPR2-0028	RPR2	The SuT shall when the parameter TargetObjectIdentifier at MmunitionDetonation is provided, provide the parameter RelativeDetonationLocation.
IR-RPR2-0029	RPR2	The SuT shall provide parameters for sent interactions of MmunitionDetonation and subclasses according to SISO-STD-001-2015 and SISO-STD-001.1-2015.
IR-RPR2-0030	RPR2	The SuT shall assume default values for optional parameters on interactions of MmunitionDetonation and subclasses according to SISO-STD-001-2015.
IR-RPR2-0031	RPR2	The SuT shall not rely on receiving optional parameters on interactions of MmunitionDetonation and subclasses.
IR-RPR2-0032	RPR2	The SuT shall provide the parameter EventIdentifier of a MmunitionDetonation interaction that follows a corresponding WeaponFire interaction with the same value in both the interactions.
IR-RPR2-0033	RPR2	The SuT shall when receiving a MmunitionDetonation interaction with a specified target (Direct Fire) and SuT has the modelling responsibility for the damage assessment at that entity, update the BaseEntity.PhysicalEntity attribute DamageState with an appropriate value.
IR-RPR2-0034	RPR2	The SuT shall when receiving a MmunitionDetonation without a specified target (Indirect Fire), but the same location as an entity and SuT has the modelling responsibility for the damage assessment at that entity, update the BaseEntity.PhysicalEntity attribute DamageState with an appropriate value.
IR-RPR2-0035	RPR2	The SuT shall only update values for EntityType attribute compliant with Distributed Simulation Agreement.
IR-RPR2-0036	RPR2	The SuT shall only update values for Spatial attribute compliant with Distributed Simulation Agreement.

ID	Category	Description
IR-RPR2-0037	RPR2	The SuT shall remove or update damage state of Munition object instances for tracked munitions when detonated.
IR-RPR2-0038	RPR2	The SuT shall provide the following parameters for the MunitionDetonation interaction: DetonationResult.
IR-SOM-0001	SOM	The SuT's CS/SOM shall be valid.
IR-SOM-0002	SOM	The SuT's CS/SOM shall be consistent.
IR-SOM-0003	SOM	The SuT shall publish all object class attributes defined as published in its CS/SOM.
IR-SOM-0004	SOM	The SuT shall not publish any object class attribute that is not defined as published in its CS/SOM.
IR-SOM-0005	SOM	The SuT shall publish all interaction classes defined as published in its CS/SOM.
IR-SOM-0006	SOM	The SuT shall not publish any interaction class that is not defined as published in its CS/SOM.
IR-SOM-0007	SOM	The SuT shall subscribe to all object class attributes defined as subscribed in its CS/SOM.
IR-SOM-0008	SOM	The SuT shall not subscribe to any object class attribute that is not defined as subscribed in its CS/SOM.
IR-SOM-0009	SOM	The SuT shall subscribe to all interaction classes defined as subscribed in its CS/SOM.
IR-SOM-0010	SOM	The SuT shall not subscribe to any interaction class that is not defined as subscribed in its CS/SOM.
IR-SOM-0011	SOM	The SuT shall register at least one object instance for each published object class.
IR-SOM-0012	SOM	The SuT shall discover object instances for all object classes with attributes defined as subscribed in its CS/SOM.
IR-SOM-0013	SOM	The SuT shall update attribute values for each published object class attribute.
IR-SOM-0014	SOM	The SuT shall reflect attribute values for each subscribed object class attribute.
IR-SOM-0015	SOM	The SuT shall send at least one interaction for each published interaction class.
IR-SOM-0016	SOM	The SuT shall receive interactions for each subscribed interaction class.
IR-SOM-0017	SOM	The SuT shall encode all updated attribute values according to its CS/SOM.
IR-SOM-0018	SOM	The SuT shall encode all sent interaction class parameters according to its CS/SOM.

ID	Category	Description
IR-SOM-0019	SOM	The SuT shall implement/use all HLA services as described as implemented/used in its CS/SOM.
IR-SOM-0020	SOM	The SuT shall not implement/use any HLA service that is not described as implemented/used in its CS/SOM.
IR-SOM-0027	SOM	The SuT shall be able to decode attribute value updates of all object class attributes defined as subscribed in its CS/SOM.
IR-SOM-0028	SOM	The SuT shall be able to decode interaction class parameters for all interaction classes defined as subscribed in its CS/SOM.

B.3 ABSTRACT TEST CASES

An IVCT **Abstract Test Case** (ATC) is a complete, and implementation independent, specification of the actions required to verify a specific test purpose expressed as a set of Interoperability Requirements (IRs) associated with the ATC. This implies that the purpose of the ATC is to test all associated IRs.

The Certification Entity (CE) is responsible for defining the test case purposes (associating IRs with the ATC) and specifying the test steps, actions, and valid responses and outcomes. Validation of an ATC against its test purpose is done by a CE.

A Test Case Developer (TCD) is contracted by a CE to implement an Executable Test Case (ETC) based on an ATC. An ETC is a script or compiled program that can execute as part of IVCT. ETCs are verified by a CE and delivered to the Accredited Test Laboratories (ATL) for use with the Integration, Verification and Certification Tool (IVCT).

<p>Format for documenting ATC</p> <p>Metadata: Unique <i>ID</i>, <i>Name</i>, Short <i>Description</i> of overall test purpose</p> <p>Test Purpose: List of associated IRs</p> <p>Abstract Test Case Description: Sequence of actions and expected responses</p>
--

MSG-134 has developed the first set of ATCs (Table B-4).

Table B-4: Set of Abstract Test Cases.

ID	Name	Description
CS-VERIFY	CS Verification	Verify the Conformance Statement's (CS) completeness and format.
FOM-DECODE	FOM Data Decoding Verification	Verify the attribute and parameter value decoding conformance of the SOM in the CS.

ID	Name	Description
FOM-ENCODE	FOM Data Encoding Verification	Verify the attribute and parameter value encoding conformance of the SOM in the CS.
HLA-BEST	HLA-Best Practices Verification	Verify the use of HLA services and callbacks according to best practices.
HLA-DECLARE	HLA Declaration Management	Verify that HLA declaration management services are used according to the CS.
HLA-OBJECT	HLA Object Management	Verify that HLA object management services are used according to the CS.
HLA-SERVICES	HLA Services Verification	Verify the use of HLA services and callbacks.
ATC-TMR-REQUEST-2016	NETN TMR Request Test	Verify that the SuT is compliant with NETN TMR Request Requirements.
ATC-TMR-RESPOND-2016	NETN TMR Respond Test	Verify that the SuT is compliant with SuT requirements for responding to TMR.
ATC-TMR-TRIGGER-2016	NETN TMR Trigger Test	Verify that the SuT is compliant with NETN TMR Trigger Requirements.
RPR-PLATFORM	RPR Platform Testing	Verify the CS and GRIM requirements for RPR-Physical FOM Module attributes at platform and lifefrom entities.



Annex C – CONFORMANCE STATEMENT

A **Conformance Statement** (CS) is a written statement declaring a system’s compliance with identified Interoperability Requirements (IRs). A CS is provided by the owner of a 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 (CBs).

A CS shall include the following information:

- Metadata including SuT identification, date and POC information;
- A Simulation Object Model (CS/SOM) (if SuT creates multiple federates each needs to be described in a separate CS and they are tested individually);
 - the SOM must contain the complete list of HLA services used.
- A Federation Object Model (CS/FOM); and
- A set of CBs to test against:
 - Additional CS information and parameters as required by the CBs.

Simple CS Example

System Name	MyFederate
Date	2016-07-12
ID	MyFederateCS-v1.0
POC	John Doe, ACME, +1 555 111 222
SOM	MyFederateSOM.xml
FOM	MyTestFederationFOM.xml
Badge Name	Additional Information
HLA-BASE-2017	
NETN-TMR-2017	NETN TMR Requesting, NETN TMR Responding, TMR_OfferTimeOut=5s

Conformance statement definition supersedes the previous one stated in the documents produced by MSG 025, MSG 050 and CeAG.



Annex D – INTEGRATION, VERIFICATION AND CERTIFICATION TOOL

The NATO Simulation Interoperability Test and Certification Service’s **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. The IVCT is used for testing of individual simulation components interoperability, and to support integration of distributed simulations. Accredited Test Laboratories (ATLs) use the IVCT to perform certification testing.

As shown in Figure D-1, the IVCT is a component-based software package with modules supporting scheduling, execution and reporting of results from running Executable Test Cases (ETCs).

ETCs are implementations of Abstract Test Cases (ATCs) developed to verify defined sets of Interoperability Requirements (IRs).

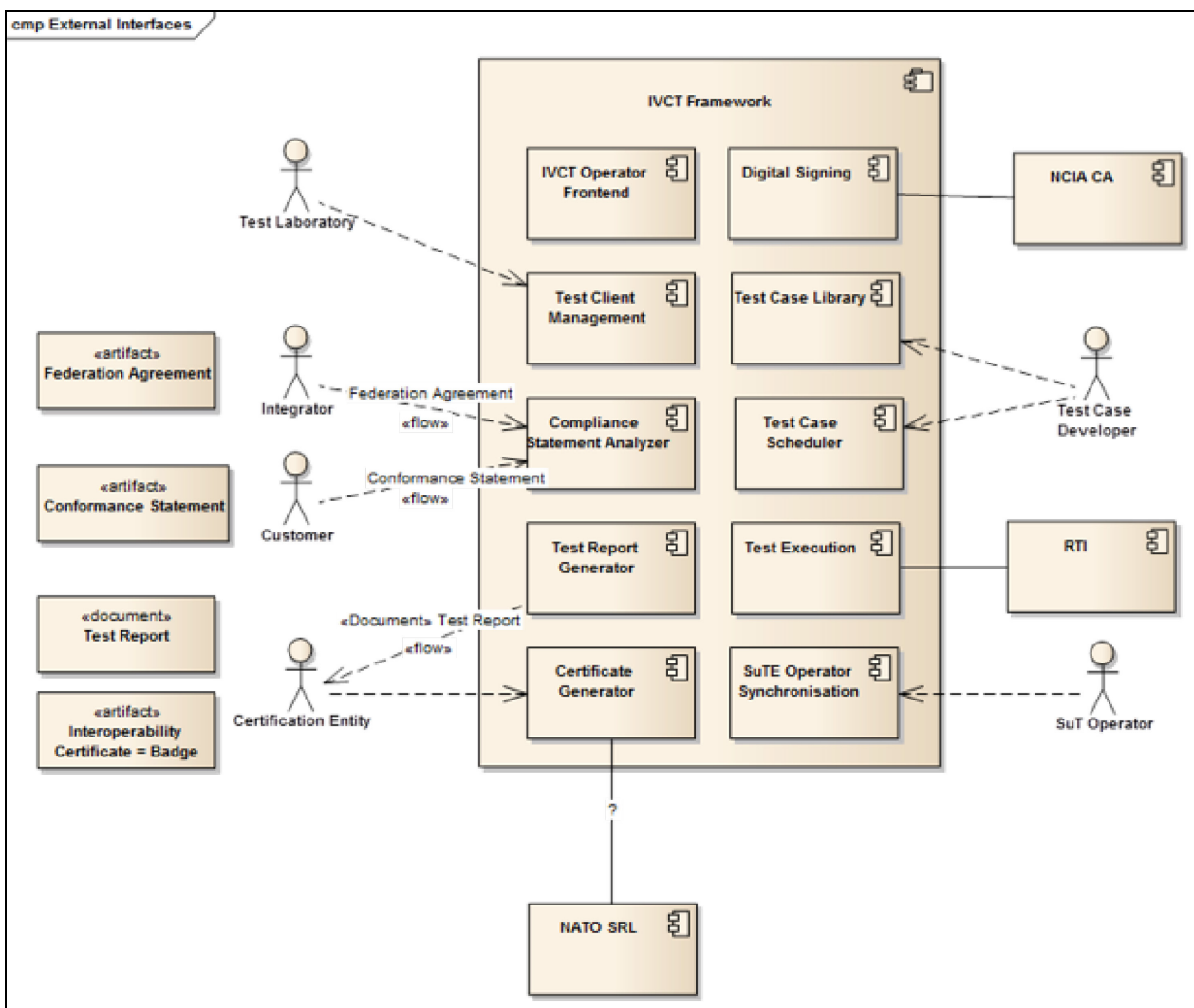


Figure D-1: Major IVCT Modules.

The IVCT is an HLA federation combined with the System under Test Environment (SuTE). The SuTE consists of the System under Test (SuT) and other auxiliary federates and systems (Figure D-2). The IVCT Test Engine (TE) runs ETCs to stimulate and to check responses from the SuT. The IVCT reports a successful or unsuccessful verification of IRs.

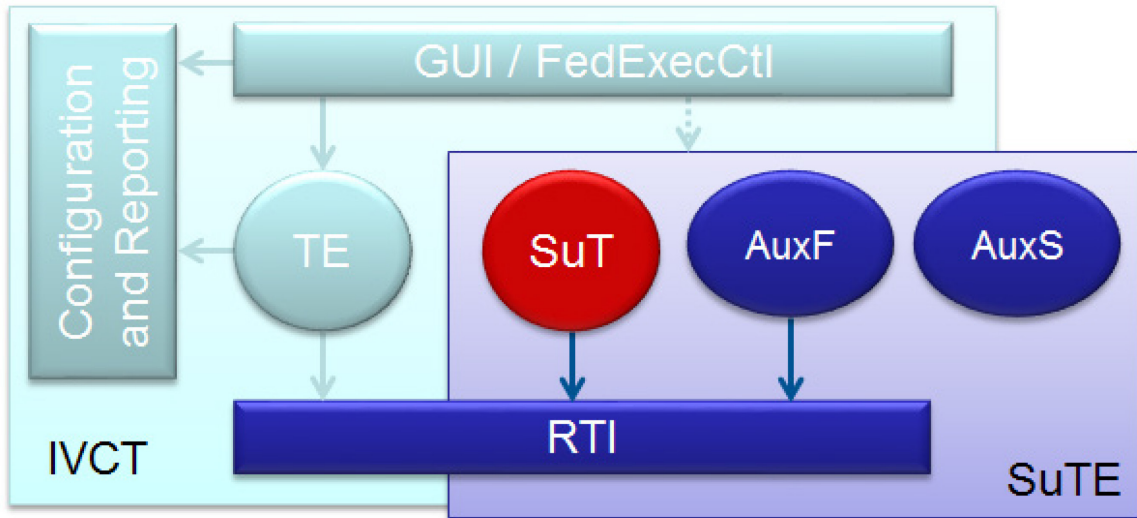


Figure D-2: Using IVCT.

MSG-134 has implemented a first version of IVCT including the core Test Engine (TE) and supporting modules. The IVCT is implemented and provided as Open Source and is maintained by the NATO CE.

REPORT DOCUMENTATION PAGE			
1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TR-MSG-134-Part-II AC/323(MSG-134)TP/841	ISBN 978-92-837-2168-0	PUBLIC RELEASE
5. Originator	Science and Technology Organization North Atlantic Treaty Organization BP 25, F-92201 Neuilly-sur-Seine Cedex, France		
6. Title	NATO Simulation Interoperability Test and Certification Service – Concept of Operations (CONOPS)		
7. Presented at/Sponsored by	Version 1.0 D7. Developed by NATO MSG-134.		
8. Author(s)/Editor(s)	Multiple	9. Date	September 2019
10. Author's/Editor's Address	Multiple	11. Pages	102
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	<p>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.</p> <p>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, provide an easy way for stakeholders to recognize the interoperability capabilities of a federate.</p>		





BP 25

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



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 et 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 Bakanlıklar – 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/>).



BP 25

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



**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
S DFA – 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 Bakanlıklar – 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>).