A Reference Test bed for the Experimentation, Testing and Validation of NATO Communications and Information Systems

The NATO CIS Interoperability Experimentation, Testing and Validation (IETV) test bed

Alberto Domingo
NATO Consultation, Command and Control Agency (NC3A)
The Hague, The Netherlands
alberto.domingo@nc3a.nato.int

***Abstract*—The NATO Interoperability Experimentation, Testing and Validation (IETV) reference test bed is part of a capability in support of NATO expeditionary operations interoperability assessment and improvement. The IETV addresses the complete mission life-cycle, from planning to pre-deployment, and all functional levels, from transmission to user applications and INFOSEC. This paper describes the initial findings out of the IETV concept development, and proposes a model of operation for the capability. It describes the validation/certification cycle, the IETV capability concept, the basic architecture and design, the business model (model of use, the different stakeholders, the cost model and the potential funding mechanisms) for the long-term capability implementation and operation. It also derives a set of conclusions and recommendations and proposes further expansion to the capability.**

Keywords-reference test bed; certification; validation; interoperability; deployable CIS.

I. INTRODUCTION

Expeditionary operations constitute nowadays the paradigm of (deployed) missions in NATO [1]. Deployed Command and Control (C2) systems and the subordinate forces in expeditionary missions require extensive Communications and Information Systems (CIS). Those systems are spread over a number of geographical sites, which are then interconnected among them and also with the static headquarters and other organizations. CIS for these NATO deployed missions include wide area communications, local distribution (packet switched, circuit switched and Time Division Multiplexing -TDM-), core Information Systems, Tactical data Links (TDL) and Functional Services (or FS, which are the applications that support information warfare for the end users).

At each geographical location, CIS assets are provided and operated by NATO but also by the different (NATO and non-NATO) coalition Nations. Effective interoperability of CIS at all levels of command is then a key requirement to allow proper information sharing in the battle-space, leading to the required information superiority. Since Nations periodically rotate to fill-in NATO force requirements, ensuring CIS interoperability is a rolling and permanent effort that must be undertaken with the proper level of exertion and the adequate tools [2]. In addition, new CIS concepts and technology evolutions are constantly implemented, and interoperability of those new technologies with existing assets needs to be assessed before the system is declared ready for deployment.

To address the interoperability assurance requirements derived from the scenario described above, a comprehensive representative test bed is needed. The test bed should support CIS interoperability assessment at several levels (from core communication services to the most sophisticated C2 applications). It should support testing and validation of nationally-provided CIS, interoperability issues resolution, and also experimentation for concept development and technology insertion [3].

This paper describes a reference CIS test bed developed by the NATO Consultation, Command and Control Agency (NC3A). The reference test bed, called IETV (Interoperability Experimentation, Testing and Validation) is a tool in support of systems certification, interoperability enhancement and experimentation in scenarios related to multinational, NATO-led expeditionary operations. The paper describes the NATO force certification process and the resulting motivation for the test bed development. It outlines the test bed architecture, design and current level of implementation. It also addresses the underlying processes and documentation required to effectively use the test bed. Finally, the paper analyses the business model that justifies the efforts to build and operate the test bed, including the identification of stakeholders, the identification of cost components, the potential allocation of costs to stakeholders (funding arrangements) or the access criteria to define who (military or not) can benefit from the capability and how to do so.

II. FORCE CERTIFICATION AND CIS VALIDATION PROCESS IN NATO

A. Certification, Validation and Verification

Certification is the result of a process in which a force formation is prepared, evaluated and validated by a higher

This work was made possible thanks to the NATO Consultation, Command and Control Board (NC3B) 2006 program of work on NATO Response Force (NRF) and NATO Network-Enabled Capability (NNEC).

headquarter in the chain of command. In NATO, certification is a pre-requisite for a Nation to contribute forces to a given mission [4].

An essential pre-requisite for the force certification is the preparation, evaluation and validation of the underlying CIS, from basic communications services to consolidated information sharing [5]. This is especially true in multinational expeditionary missions, where NATO and several Nations will provide different CIS assets that need to effectively operate together. The validation needs to be conducted in a formal manner, to ensure that all relevant aspects of the CIS readiness are evaluated, and that the evaluation is systematic, complete and consistent for all the potential missions, and for all the participants in a generic mission. The assessment of the validation results also needs to be done formally, to ensure homogeneity and repeatability of results.

But validation in itself is a loose term. Validation is the act of proving that something is sound, and conformant to a set of needs. Validation of NRF CIS is then, the act of proving that a CIS system is able to fulfill the needs of a mission. "*Able to fulfill the needs*" is quite a vague definition, just because vague is the adjective that comes to mind when defining in a few words CIS capabilities which are inherently complex in nature. In contrast with "*validation*", "*verification*" means proving that something is correct. Validation of complex capabilities (as CIS) then, should be based on formal verification.

B. Implementation of the CIS validation process

CIS validation then needs to look at the different dimensions and components of the problem to finally assess the validity of the solution. This multidimensionality arises from the fact that in addition to service layers (transmission, communications, information systems, functional services and data links), it includes cross-dimensional components such as INFOSEC and management, with an overarching set of operational requirements. This complexity rules out CIS validation in a single stage/venue, but rather forces to decompose it into a number of stages. At the time of writing this document the most widely developed and accepted CIS validation process in NATO [5] is based on 4 stages, as depicted in figure 1. Those four stages are:

Unit level assessment, performed nationally, where the Nation has to prove that the nationally-provided system is compliant with NATO architectures, is adequate to perform the expected C2 function and is compliant with INFOSEC policy. The result of the Unit-level assessment is a nationally assessed CIS system.

Assessment against a reference test-bed. The nationally-provided system is then evaluated in terms of its ability to interconnect and interoperate with other NATO and National systems. It also allows assessing interoperability conformance of new concepts and technologies. To remove ambiguity and ensure reproducibility of results, this verification needs to be done against a well known technical criteria, and using a reference test-bed. Both of them, criteria and the test bed, are the subject of this paper. The result of the assessment against the reference test-bed is a CIS system compliant with the technical requirements for CIS validation.

Assessment of CIS interoperation with other units. Then the unit's CIS is interconnected with other C2 elements from different nations/formations. Since all those other functions have (ideally) also been tested against the reference test-bed, most of the first-time interconnection issues should have been already resolved and testing/validation can focus on real-time information sharing interoperability issues. The above assessment is conducted during a NATO interoperability Exercise, and the outcome is a technically validated CIS.

Operational CIS Assessment. Finally, the missing link towards full CIS interoperability validation is the assessment of the ability of the setup to conduct actual missions. This involves not only adequacy of CIS infrastructure and ability to interconnect and operate it, but also the adequate force composition, the C2 capabilities, their readiness, their ability to deploy and the sustainability aspects. This last assessment validation activity is conducted during a NATO operational exercise. The result is an operationally validated CIS system for NATO expeditionary operations.

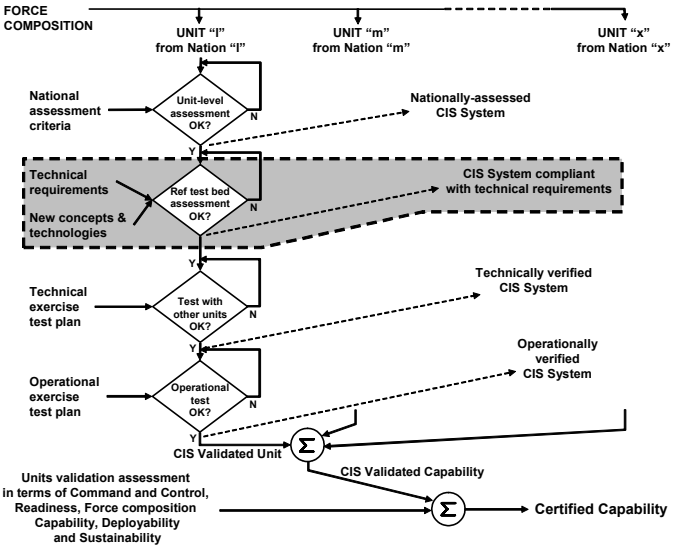

Figure 1. Stages in the CIS validation process. Within the shadowed area, the scope of the IETV reference test bed

C. Resolution of interoperability issues, concept development and experimentation.

In addition to validation, NATO CIS are expected to incorporate operational concepts and the supporting technology and tools as soon as they become stable enough. Operational or technical prototypes in concept development phase are incorporated into the reference test bed as early as feasible, and tested as soon as they are mature enough for such purpose. Once the new technology has been technically validated using the test bed, and operationally assessed, it becomes part of the scope of certification for next NATO missions.

III. REQUIREMENTS FOR THE IETV REFERENCE TEST BED

To play the role identified in the Figure 1 above, the IETV reference test bed needs to satisfy a number of requirements [6]. The most relevant ones are outlined in the paragraphs below:

From the ***functional*** standpoint, the IETV shall be representative of all CIS in use for NATO deployed operations. This includes basic wide-area and local-area communication services (voice, data, and data links, both secure and non-secure), core information systems (Alliance's directory, messaging, web-services, etc.) and functional services (for air, land, maritime and joint operations, logistics, intelligence, etc.). The test bed shall have the ability to support a coordinated spectrum of experimentation and test activities. Those activities range from technology experimentation and demonstration, through standards development and implementation, to inter-system interoperability testing. They also cover field testing of systems during CIS exercises and demonstrations, and pre-deployment testing of operational systems.

From the ***interface*** point of view the test bed is required to emulate the whole set of NATO strategic and tactical interfaces, at the complete IO-OSI layers 1 to 7, as well as provide support for the interface with specific national systems.

From the ***performance*** perspective the test bed shall be able to model and emulate the capabilities of NATO deployed systems, with special emphasis on the impact of limited infrastructure and communications bandwidth available at deployed locations, performance constraints derived from multiple satellite hops or INFOSEC restrictions, to name a few.

In terms of ***security***, the IETV shall incorporate NATO CIS INFOSEC and management policy and concepts, implement the whole spectrum of INFOSEC mechanisms that the CIS assets will face when deployed, including INFOSEC driven architectures and systems.

Operationally speaking, the test bed shall allow representing the actual information flows traversing CIS in a deployed mission, with the tempo and characteristics of an actual battle rhythm of a mission.

From the ***implementation*** viewpoint the test bed shall be commensurate with the current (limited) level of funding, and to that extent shall make maximum re-use of current, existing NC3A test beds, laboratories and assets. To enable this, the IETV shall be composed of a mixture of a static component and a deployed footprint, interconnected through the NATO strategic or any other wide-area network. The static component is located at NC3A premises, and groups all existing development, experimentation and test laboratories with significance in deployed operations. The deployable component extends the static component into the remote location where validation/testing is to be conducted, providing on-site identical interfaces and the required support and assistance to the unit under validation. To reduce the effort and cost of successive validation/testing campaigns, test automation shall be implicitly built into the IETV.

Finally, the IETV shall strictly follow a modular design approach, to ensure that the different building blocks (normally provided by different NC3A labs and facilities) can be engaged and disengaged for the different validation and testing campaigns, and new modules can be added whenever new technologies and concepts demand so. Reusability shall be then a key aspect in the IETV implementation.

IV. ARCHITECTURE OF THE NATO IETV

The Interoperability Experimentation, Testing and Validation (IETV) Capability is made up of four essential components. The IETV reference test bed is just one of them, and provides the required testing infrastructure and equipment facilities (hardware, software and supporting installations). The capability is complemented with appropriate testing criteria and supporting documents, processes and the required *know-how*. Figure 2 shows this structure, and the following sections describe each of the four components separately.

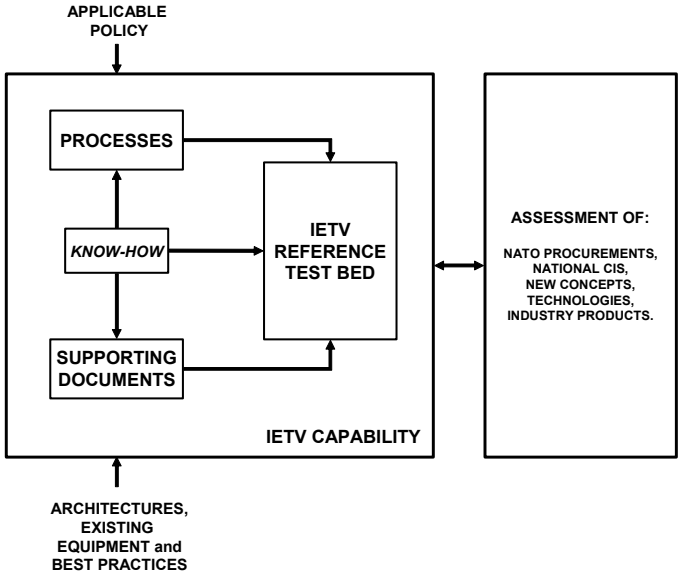

Figure 2. Components of the IETV Capability

A. *IETV reference test bed*

The ability to satisfy the complexity and heterogeneity of the military operational requirements demands a sophisticated deployable CIS. This sophistication needs to be reflected in the IETV test bed architecture, which must provide representative functions, interfaces, performances and implementation constraints associated with any deployed mission environment. Figure 3 shows the result of the functional analysis conducted to define the architecture of the test bed. The test bed groups DCIS into a number of functional clusters, including interfaces (with the national systems), transmission, bandwidth management, voice/video/VTC services, information exchange, network services, core IS services, functional services, information assurance and management. Each cluster then groups individual functions which are required to provide a CIS service. This clustering allows easy re-use of assets currently existing at other more specialized test beds and labs in NC3A. But it also allows an easy split up of the test bed into a static part (which stays in The Hague to avoid costly transportation and deployed manning) and a deployable footprint, to be shipped to wherever the validation/testing campaign is going to occur. The deployable part interconnects to the static part in The Hague, for management and control, and to access the static facilities providing the most sophisticated assets of the test bed.

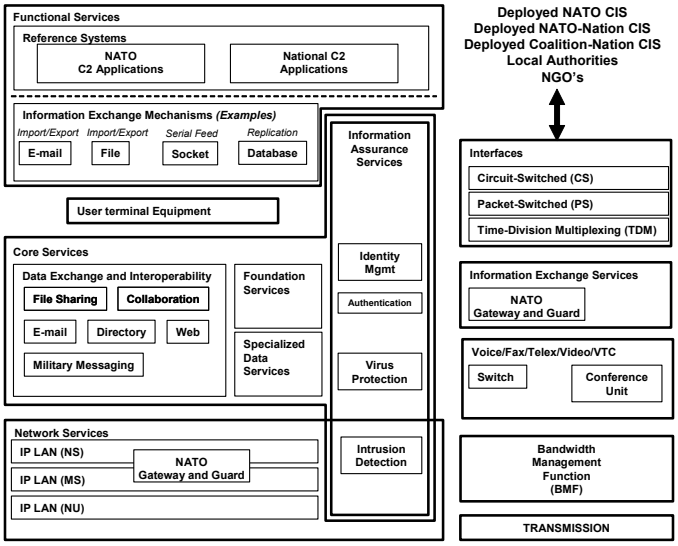

Figure 3. Architecture of the IETV test bed

A deployable footprint of the IETV has been built for the 2006 validation, testing and experimentation campaign. Strictly required functions (such as interfaces, transmission and information exchange) have been embedded into the deployable element. This would typically suffice for a normal scenario. However, due to a number of mainly logistic reasons, plus the convenience of deploying a self-sufficient IETV test bed for demonstration purposes, a number of other functions like network services, core services, exchange mechanisms and information assurance elements have also been configured into the deployed part. The outcome of the 2006 deployable footprint is depicted in Figure 4.

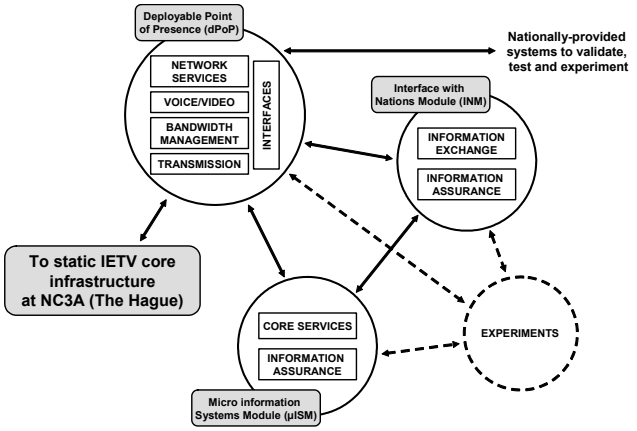

Figure 4. 2006 deployable footprint of the IETV test bed

The figure shows that the deployable part of the test bed includes three main items: a generic transmission function (the Deployable Point of Presence or dPoP), providing secure and non-secure voice and data transport services, a deployable miniaturized Information Systems Module (the µISM) providing generic NATO Automated Information Systems, and a security gateway (the Interface with Nations Module, or INM) to implement and test INFOSEC compliant interconnections between NATO and Nationally-provided networks. Systems to be tested and validated using the IETV, and experiments envisaged for the 2006 campaign will connect to these kits, which in turn will use the NATO strategic wide-area network to provide reach-back to the static part of the IETV, sitting in The Hague, from where high level functions (such as functional services) and control are provided. Figure 5 shows the deployable footprint of the IETV test bed that was used during the first validation and experimentation campaign that took place in the fourth quarter of 2006, during a NATO Exercise in Turkey.

Figure 5. 2006 deployable footprint of the IETV test bed.

B. Processes

To run validation and experimentation campaigns, a formal set of processes is required. Processes determine when and how are campaigns performed, how partners access the IETV test-bed, how to use it, and how results form those campaigns are formally assessed. Processes need to be systematic, measurable and repeatable. Formally agreed processes are needed to ensure that all Units or other testing partners know in advance how they are going to be evaluated, and to ensure that all of them are treated equally.

As part of the IETV, processes are being developed in support of Nationally-provided CIS validation and assessment. They are mostly derived from outstanding NATO policy such as [2] and [4]. At the moment, the main reference is the IETV Concept Paper [6], currently under approval.

C. Supporting documentation

Supporting documentation is needed to guide testing partners and experimentation users during the validation and experimentation process. Supporting documentation comprises handbooks and validation criteria. The handbooks describe NATO CIS and how NATO partners and other users should design and configure CIS systems to enable interoperability with NATO and other National CIS. At the moment, there are handbooks under development that describe NATO deployable CIS architectures and systems for expeditionary operations [7], configuration templates for users intending to interoperate with NATO [8], and a number of technical notes providing guidance on specific interoperability issues handling and resolution.

Once users have gained a common understanding of the main NATO interoperability aspects, they need the CIS validation criteria that NATO will use to validate their (CIS) readiness to support an expeditionary mission. This is because CIS technical validation is essentially a process of assessing compliance against a given technical criteria. Therefore there must exist agreed, formal, objective and measurable criteria before validation can start.

The technical criteria for CIS validation mainly derive from outstanding Minimum Military Requirements (MMR) and applicable policy, but also from information about existing architectures and systems in NATO. These documents are, however, far from the verification/testing level, and cannot be directly used to support a certification campaign using a reference test bed for CIS validation. Development of a proper technical criteria was, then, key to enable a real test bed capability that could be substantiated over agreed principles.

To overcome the above situation, NC3A has developed [9], where the high-level operational requirements from the Commanders are translated into technical requirements governing interoperable national CIS contributions to the deployed C2 structure. The requirements look at all technical aspect of compliance assessment, including functional assessment, performance assessment, interface assessment, implementation assessment, and INFOSEC assessment.

Figure 6 below shows the methodological approach followed for the development of the technical specification criteria.

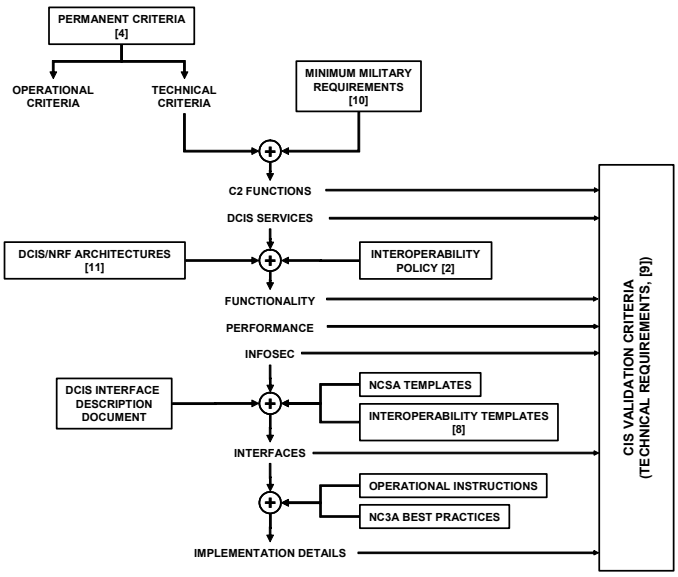

Figure 6. Methodology for the specification of interoperable CIS

The methodology takes as a departure point the NATO Permanent Criteria [4], which is the formal, Nations-approved reference for the Commander's certification of forces. Since the purpose and level of detail of the Permanent Criteria and the Technical Specification are very different, a number of policy and technical documents have also been used, as inputs for detailing the technical criteria. They include the Minimum Military Requirements for NATO Response Forces [10], Deployable CIS architectures and concept of operation [11], policy guidance in terms of services at the points of interconnection between C2 functions/Units [2], existing interface descriptions, etc. Those sources have been then completed, when possible, using first hand best practices, practical information and know-how from NC3A, the NATO CIS Support Agency and other relevant NATO bodies.

The outcome of the technical specification for interoperable CIS is the set of technical requirements that Nationally-provided Units need to meet in order to ensure proper interoperability with other NATO and National assets. They are also the requirements for which verification support from the IETV is needed.

D. NC3A know-how

To complement the processes, the supporting documentation and the IETV test bed, the capability requires a substantial amount of *know-how* on existing NATO and National systems, NATO operations, actual interfaces configuration, information sharing principles and mechanisms. It also demands a good understanding of operational C2 aspects related to how NATO conducts deployed operations. Currently, the IETV team at NC3A includes relevant experts and tools to provide the required *know-how* in all those areas for any generic validation, testing or experimentation campaign.

V. USE OF THE IETV TEST BED

The IETV is a complex and sophisticated capability, and its use requires substantial manpower and capital effort. In addition, the test bed itself comprises existing labs and assets at NC3A and other national facilities, which sometimes are fully engaged in other activities. Access to the IETV needs then to be planned and scheduled in advance, and de-conflicted if needed following a priority plan that gives preference to military units engaged in upcoming missions. This section summarizes the protocol developed to de-conflict the use of the IETV, but also to maximize the analysis versus the testing part of a validation campaign, to both increase the availability of the test bed and reduce the manning and operation costs per validation campaign.

A. Access to IETV capability

The current protocol for access to the IETV establishes that priority is given to Units that are earmarked to support on-going or upcoming NATO missions, followed by those who offered their forces to contribute to a future rotation of NATO high-readiness or graduated-readiness forces. Then, the NATO scientific and experimentation programs of work and all other units with a need to validate/test their systems can gain access to the capability, followed by national military research and experimentation centers, Industry and academia.

B. The validation and experimentation campaigns

To initiate a validation/testing campaign, the Unit (or equivalent) receives the list of technical requirements for interoperability with NATO (available in [9]) and states its compliance with the checklist. This is the outcome of the "*Unit-Level Assessment*". For requirements for which

validation approach is based on analysis, the Unit provides sufficient information to conduct the analysis and assess a positive result before connecting to the IETV test bed. Interoperability issues detected during the analysis phase are processed with support from NC3A/IETV for resolution/testing. A test plan is prepared to test the compliance with the technical requirements. The test plan is prepared specifically for each Unit, and implements only the subset of the technical requirement applicable to the Unit, which could not be verified by other methods (analysis, demonstration or inspection). A number of supporting manuals and templates need to be prepared to guide the Unit during the validation process. The tests are performed against the reference test bed in the IETV. Results are documented in existing NATO interoperability databases. A result assessment is done based on the analysis of the test results, risk analysis and potential risk mitigations for detected non-compliances. When the outcome is going to be used for force certification purposes, the force Commander gets as inputs the technical requirements compliance checklist, the test results and the recommendations out of the assessment. This process is depicted in Figure 7. As can be seen, the validation process is divided into three main sub-processes: unit-level assessment (within a dotted line, but out of the scope of this paper), verification using the IETV test bed (in the shadowed area), and verification results assessment (the grayed box, also relying on the IETV capability).

For experimentation campaigns, the process is usually less formal, and starts when the IETV team receives an outstanding requirement to resolve an interoperability issue, or a draft test plan for the experimentation campaign. The campaign implementation details are worked out for each specific event between the experimentation party and the NC3A.

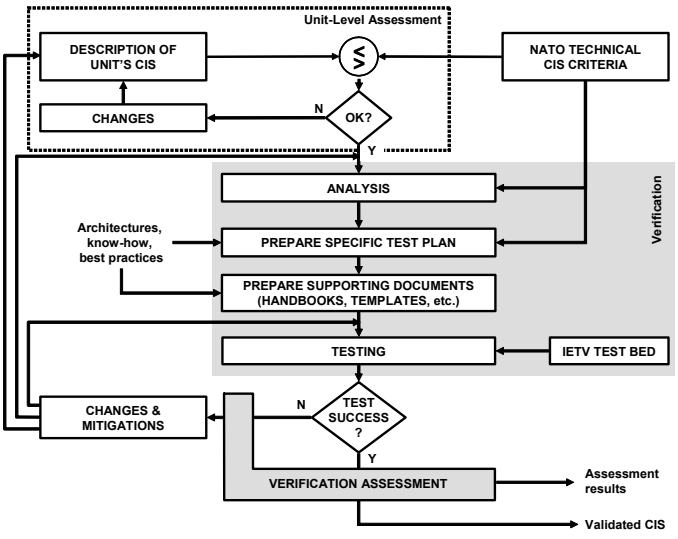

Figure 7. The CIS technical validation process

C. *Verification process*

Figure 8 looks in more detail into the verification part of the process described before. It depicts the detailed sub-process of verifying each of the outstanding technical requirements.

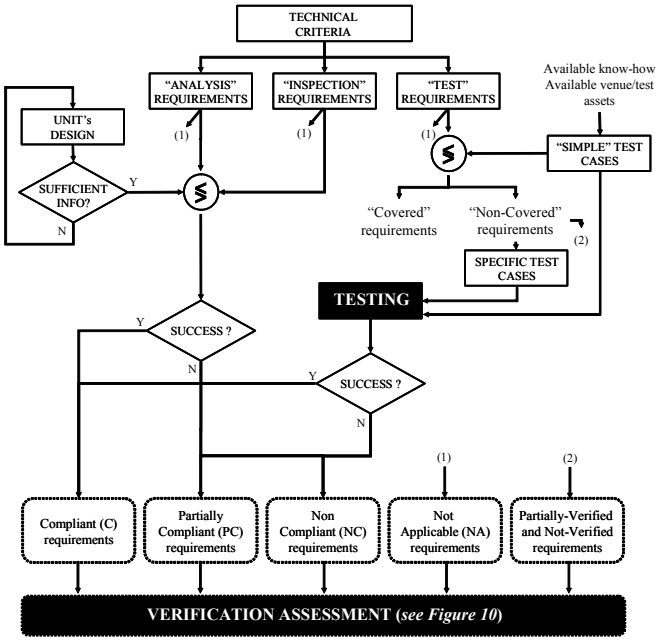

Figure 8. CIS verification sub-process

The figure shows that distinction needs to be done between requirements subject to verification by "*testing*" and other (verifiable by "*analysis*", "*demonstration*" or "*inspection*") requirements. Typically, non-testing requirements are verified before the actual test-campaign, and easily rule-out many of the potential interoperability issues that might arise during the testing campaign. Furthermore, verification of non-testing requirements is in general much less expensive than testing, and do not preempt the test bed for other activities. Therefore, it is typically worth paying sufficient attention to this phase, to avoid lengthy and expensive testing phases afterwards. On the other hand, "*testing*" requirements do need of specific tests to be conducted. To minimize testing time and cost, a set of generic tests is prepared, and covers most of the testing requirements in one go. Further specific test-cases might be needed to cover particular requirements or requirements hard to verify.

Based on the performed verification, for each requirement a verification output will thus become available. The output can reveal Unit's CIS compliance, non-compliance and partial compliance with the requirement, plus a number of outstanding comments.

D. *Assessment process*

The compilation of results of the verification (analysis and test) campaign determines the suitability of the national CIS system to fulfill the intended role. They also provide good descriptions of the interoperability gaps that the Unit needs to resolve to become 100% compliant, if so is the case. The two together (compliance status and interoperability gaps) constitute the main input for the CIS validation assessment process, and a very good indication on the ability of the Unit's CIS to perform the role as expected. Figure 9 shows the sub-process used to perform the formal assessment based on the recorded verification results.

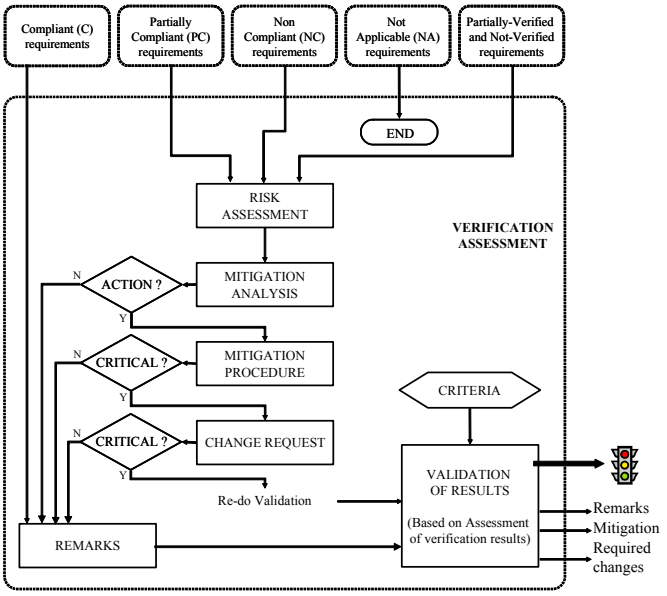

Figure 9. CIS validation assessment sub-process

The figure shows that the main objective of the assessment sub-process is to determine Unit's CIS level of readiness. But it also shows that there is a main side product of the assessment process: the collection of information about CIS readiness, which is used to (a) formally describe the potential interoperability issues, (b) assess potential consequences of those issues, (c) identify practical short and long term solutions, (d) increase Unit's awareness and (e) collect and document relevant historical logs.

The outputs from the validation (including verification and assessment) process have been formatted to produce the required outputs for the NATO interoperability databases and documentation tools. They are also summarized into a CIS verification report for the Unit, that states (a) the Validation assessment executive summary (validation result and "*one-line*" justification, major high-level issues, criticality, and high-level proposed solutions), (b) the current limitations identified during the verification process (description of non-compliances and partial compliances, impact and potential mitigation and summary of interoperability consequences), (c) the technical recommendations for improvement of the Unit's CIS readiness, based on the assessment results, and (d) the complete test results.

VI. BUSINESS MODEL FOR THE NATO IETV

NATO is a non-profit organization which does not aim to generate direct revenue out of capabilities and assets like the IETV test bed. However, a proper business model supporting the foreseen use-cases allows ensuring that the resulting test bed capability is useful to the stakeholders, matches the level of ambition, is cost efficient and is in line with the Alliance's affordability and the existing lines of funding. In the following sections, the basic business model that supports the on-going IETV development is summarized.

A. IETV Stakeholders

There are a number of prime IETV stakeholders with an interest in the successful implementation and usage of the capability. They are involved in the IETV implementation and operational usage cycle, including the concept definition, design, implementation, operation and funding processes. Their main interest is ensuring that NATO has access to a capability able to enhance NATO to Nations and Nations to Nations interoperability at all levels. The most relevant stakeholders identified so far in this category include several NATO policy bodies, such as the NATO Military Committee, The NATO C3 Board (NC3B) and the NATO Strategic Command ACT (Allied Command for Transformation).

From the operational standpoint, the core stakeholder is the NATO Allied Command for Operations (ACO), which is mainly interested in the availability and usability of tools in support of force certification. In close relationship with this ambition, additional operational stakeholders include Nations participating in upcoming or planned NATO missions, other NATO and non-NATO partner Nations, and the NATO CIS Services Agency (NCSA).

From the budgetary and programmatic perspective, IETV stakeholders include NATO security investment programs and projects, which benefit from a single, common test bed rather than acquiring individual ones for each NATO procurement project. Finally, other NATO Agencies and Program Offices and other NATO and National test-bed facilities and laboratories have also shown preliminary interest in accessing and using the IETV capabilities. The later also have an interest on liaising with the IETV program to ensure technical coordination and compatibility. Furthermore, Industry has also declared their interest in gaining access to the IETV, either in support of on-going projects for NATO or simply to access expertise and resources not commonly available in the civil sector.

B. Cost components in IETV

There are a number of cost items to consider when estimating the cost of setting-up, maintaining and operating the IETV capability. Costs components have been split into fixed and variable costs. The main, fixed cost components include the cost of requisition of existing (at NC3A) assets, the cost of existing assets initial set-up and preparation (including the procedures and supporting documentation preparation, and associated engineering effort), the cost of existing assets maintenance, replacement and upgrade and the cost of regularly procuring additional assets and services to enhance and keep the test bed updated. Main variable costs are normally associated to specific campaigns, and include the cost of testing, validation or experimentation campaign preparation, the cost of the actual testing, validation or experimentation campaign execution (including proper documentation of results), and the cost of supporting Nation(s) and other NATO bodies during the process.

The analysis of these cost components allows estimating in advance the required level of funding for the capability. Furthermore, it allows allocating them to the different stakeholders, under the principle of "*costs lay where they fall*".

C. Potential funding sources for IETV

Based on the analysis of stakeholders and cost components, potential lines of funding can be identified. The identification of adequate, stable lines of funding is pivotal to a successful long-term implementation of the IETV. At the time being, a number of founding sources are identified as adequate to support the IETV global costs. They include most of the IETV stakeholders, including the NC3A, but also stress the importance of getting permanent sources of funding from NATO organizations which maintain a rolling program of work to support transformation (like ACT), operations (like ACO), interoperability (like the NC3B) or procurement of new CIS assets (like the NATO Security Investment Program, NSIP). National budgets to support validation of National Units are also (currently potential) candidates for funding, while Industry contributions are also possible, provided that they aim to achieve outcomes consistent with the IETV main spirit and purpose.

D. IETV funding mechanisms

Funding mechanisms (which have to be agreed by all stakeholders) are developed by allocating cost components to potential funding sources. There are many possible variations on this mapping process, and the optimal will be the one that balances allocation of costs to actual generators, while enabling stable, long-term funding mechanisms.

To enable proper discussion of the funding model, NC3A has developed an initial apportionment of cost components among funding sources. This model is currently under discussion, seeking approval. The model aims to subsidize most of the fixed IETV costs through permanent, stable lines of funding, such as the NC3B program of work for interoperability, the ACT scientific and experimental programs of work, the ACO program of work to support operations, or the NSIP for infrastructure acquisition. The variable costs associated with actual testing, validation or experimentation campaigns are candidates to be funded directly by the parties involved in the campaign or seeking the results of it.

The overall outcome of the model is depicted in figure 10. The figure maps cost components (in vertical) to funding sources based on the type of activity performed with the capability (in horizontal). The proposed funding model foresees a fixed budget to set-up and maintain the capability, plus a "*pay-per-use*" component to ensure a rational use of the facilities. While this theoretical allocation is seldom easy to achieve, it provides a very useful tool to discuss and allocate budgets with each of the different IETV stakeholders.

Regarding actual costs of use of the IETV, those very much depend not only on the type of campaign, but mostly on the number and type of assets required to perform the necessary testing, validation or experimentation. As an example, estimates of the costs involved in validating a mid-size, all services national system in support of NATO expeditionary missions might be in the order of 85 KEUR, while resolving and testing a relatively simple interoperability issue through experimentation might cost in the order of 40 KEUR.

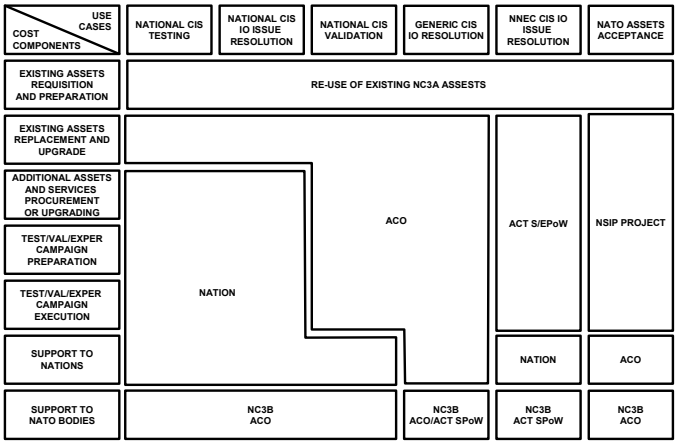

Figure 10. Example of a potential IETV funding model based on apportioned cost sharing

VII. INITIAL AND ON-GOING TEST BED ACTIVITIES

The IETV concept was originally developed in late 2005, and a first capability concept was implemented during 2006. The capability included the necessary CIS assets that the reference test bed comprises, but also the underlying supporting processes and documentation required for a sensible use of the IETV test bed. Therefore, part of the initial capability development was the development of the National CIS validation process, the development of the supporting documentation (interoperability handbooks, templates and technical criteria) and the development and implementation of the IETV test bed itself.

The initial IETV capability was deployed to SteadFast Cathode 2006 (SFCE 06), a NATO interoperability Exercise in support of NATO to Nations interoperability and certification for the NATO Response Force (NRF) type of expeditionary missions. The Exercise took place in October 2006, in the vicinity of Istanbul (Turkey).

The 2006 IETV test bed comprised the set of configured NATO CIS functions and interfaces that a Nation needs to verify compliance with NATO and other national systems. The outline of the test bed is depicted Figure 11. It mainly consisted on a deployed footprint, able to connect and be remotely configured/managed from the static IETV facilities in The Hague. The deployed part of the test bed included three main items: a generic transmission function (the Deployable Point of Presence or dPoP), providing secure and non-secure voice and data transport services, two deployable miniaturized Information Systems Modules (the μISM) providing generic NATO Automated Information Systems, and two security gateways (the Interface with Nations Module, or INM) to implement and test INFOSEC compliant interconnections between NATO and Nationally-provided networks. The described set-up provided services to a number of deployed user communities, including local and remote, NATO and National, at two different security domains. Automated testing devices were also used to speed-up the national CIS validation process, where required.

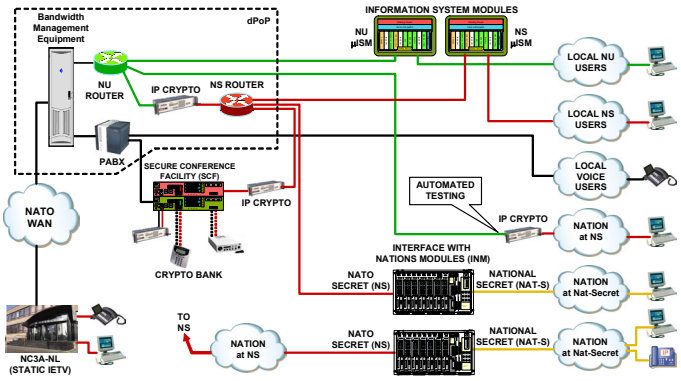

Figure 11. IETV test bed as deployed to exercise SteadFast cathode 2006

Using the IETV, the following three main activities took place during the validation and testing campaign:

Proof of concept of the validation of a nationally-provided system. The process and the procedures outlined in this paper were exercised to formally validate a national CIS system. It also allowed assessing the test bed itself, collecting relevant feed-back on the usability and usefulness of the IETV capability.

Proof of concept of IETV to resolve an outstanding IO issue. The IETV was used to implement a solution for an interoperability limitation identified by a Nation. The IETV implemented a secure cross-domain gateway function to securely activate selected information exchanges between a national-secret system and the NATO secret networks, in compliance with applicable INFOSEC regulations. To achieve this, the Interface with Nations Module (INM) of the test bed was configured to implement the interconnection in compliance with outstanding NATO INFOSEC architectures and policy, removing an air gap that currently prevents automatic data exchange between the NATO and the (specific) national system.

Proof of concept of IETV to experiment a future interoperability enhancement. The experimentation capabilities of IETV test bed (to develop, test and validate solutions in support of the implementation of CIS enhancements that will satisfy upcoming operational requirements) were also used during SFCE Exercise. An experiment was incorporated into the IETV to implement a deployable secure conference facility (SCF) that enabled end-to-end secure voice communications between Nations, even when they used non-interoperable cryptographic equipment. In particular, it provided a solution to provide end-to-end secure voice between all-IP Voice over IP (VoIP) converged networks and systems using ISDN-based secure voice systems.

In addition to the above, another main activity conducted during the validation and test campaign was the assessment of the test bed itself. In particular, relevant feed-back on the usability and usefulness of the IETV capability was collected, and has been processed to define next steps in the capability (and test bed) evolution.

VIII. Future Activities

Upon successful completion of foreseen 2006 activities, a number of more ambitious objectives have already been set for the upcoming period. The following short-to-midterm objectives for the IETV capability are foreseen at the moment:

Once consolidated the implementation of basic communications, information and INFOSEC systems on the IETV, the test bed and associated processes should focus on the full incorporation of NATO and National Functional Services (FS). While data exchange mechanisms exist nowadays between NATO and National FSs, full automated information sharing is not always a reality. One of the short term goals of the IETV is then the development and testing of automated data filters and gateways between dissimilar FSs that need to share information.

Another short term objective is the full enabling of the distributed nature of the test bed. For 2006 the most critical elements have been installed and configured in the deployed footprint of the IETV, leaving control and some applications in the static component in The Hague. Maximizing the distributed nature of the IETV means deploying only essential modules to guarantee identical interfaces and security gateways. This reduces deployment costs and also optimizes the *know-how* by making available all expertise that usually sits in the NC3A and other nationally-provided static labs.

In addition to the above, to enable full distribution further work in the area of integrating remote national labs into the IETV needs to be done. Candidate efforts go in the direction of interconnecting national facilities that are responsible for the development of national Functional Services, to enable full interoperability testing and issues resolution even before the application rolls out, but also allows to offer the specific FS as part of the IETV capability at any validation, testing and experimentation campaign.

Last, but not least, some of the upcoming efforts will be devoted to consolidating and agreeing on a stable funding model for the IETV capability, which ensures smooth operation while preserving the basic principles of allocating costs to those who directly generate or benefit from them.

IX. Conclusions

NATO has been looking at length for a comprehensive CIS capability in support of validation of national assets, experimentation and interoperability enhancement, and NC3A has been tasked to develop such capability specifically in support of expeditionary operations. The capability should support all existing and foreseen CIS services, and cover the specificities of NATO management and INFOSEC systems as well.

Out of the analysis performed by the NC3A, the first conclusion is that the required capability is much more than a test bed, and that a number of process, procedures, tools and *know-how* need to be built around the test bed to achieve the required objectives. The subsequent design and implementation activities have also shown that a representative initial IETV capability for NATO expeditionary operations interoperability enhancement is feasible and can meet the requirements of the

outstanding policy. The analysis of the potential stakeholders reveals that a large number of NATO and non-NATO bodies (including research facilities and Industry) will benefit from the implementation and use of the IETV capability.

The comprehensive scope and complexity of the capability demands it being implemented in phases. The initial (2006) phase has produced a limited IETV in functional scope and abilities, but covers all essential service types, and all key interoperability issues in a typical NATO deployed mission, including transmission, service provisioning, communications, information systems, Functional Services, Tactical Data Links and INFOSEC.

For the architecture of the IETV test bed a highly modular structure based on a small deployable footprint connected to static assets in NC3A has been selected. This approach allows maximizing re-use of existing NC3A assets, eases the configuration of the tool for each specific use campaign case (by selecting only those modules which are actually needed), and facilitates deploying a small footprint with only those modules required to sit next to the user premises.

However, the analysis has also shown the need to carefully look at issues derived from reusability of assets. It has been estimated that pure hardware costs are just a fraction of capital costs involved in providing the IETV capability. Dominant factors are kits and prototypes development, cost of distributable software licenses, cost of manpower for analysis, configuration and testing, cost of INFOSEC accreditation and cost of facilities to host the capability. Re-usability principles [12] should not focus merely on pure hardware sharing, but rather concentrate on exploiting the knowledge base currently associated to other NC3A existing test beds. Furthermore, preliminary experience shows that the use of the existing test beds and equipment for the IETV activities needs to be carefully regulated by some scheduling criteria, so that equipment and operators are not tied up in other activities, and give NC3A the necessary preparation and configuration time to set up the test environment and to allow for proper INFOSEC accreditation for every test series.

When trying to establish a funding model to satisfy the costs of the IETV capability, the diversity of funding sources based on the mixture of stakeholders reveals the relevance of the test bed for the community. However, care must be exercised as this variety brings complexity to the funding process and even to the billing procedures. A pure pay-per-use model has shown to be inadequate, as does not provide sufficiently stable funding to guarantee proper capability maintenance and enhancement. On the other hand, a model merely based on permanent funding of the IETV does not encourage rational use of the capability, nor helps resolving scheduling conflicts when they arise. Rather, a mixed model based on permanent lines of funding covering capability maintenance and updating, plus specific attribution of costs to testing/experimentation campaigns is therefore the preferred option for supporting the IETV costs.

Finally, it must be said that a test bed could never replace, but rather complement, testing and validation efforts at NATO Exercises, or the Commanders assessment of the IETV validation results. But as a complement to the above, it is expected that the first increment of the (IETV) capability implementation, including functional capabilities, mode of employment, cost and potential funding models, addresses the main issues of NATO and Nations concern, and allows a fruitful discussion on how to make the IETV a useful, value for money, capability for the Alliance.

REFERENCES

[1] North Atlantic Military Committee. Military Concept for the NATO Response Force. Military Decision MC 477, April 2003.

[2] AC/322-D(2205)0050. ISC Report to the NC3B on NRF C3 Interoperability. NC3B-Interoperability Sub-Committee, 14 December 2005.

[3] Matthew T. Reynolds. Test and Evaluation of Complex Systems. John Wiley & Sons; 1 edition, January 14, 1997.

[4] Supreme Headquarters Allied powers Europe. Promulgation of revised NRF Permanent Criteria. 2100.15/DFCG/0512/05-106526, 20 December 2005.

[5] A. Domingo, M. Rudack. Support of Steadfast Cathode (SFCE) Exercise to NATO Response Force (NRF) Certification. NC3A TN-1127, Edition 1.0, December 2005.

[6] A. Domingo. Concept Paper For The Interoperability Experimentation, Testing And Validation (IETV) Capability. NC3A TN-1176, unpublished.

[7] A. Domingo, N. Hatton, S. Kuhene. NATO to Nations CIS Interoperability Handbook. NC3A TN-1173, in press.

[8] M. Bommezijn, A. Domingo, M. Gerritsen, N. Hatton, H. Kalkman, S. Kuehne, A. v. Zanden NATO To Nations CIS Interoperability Templates. NC3A TN-1175, unpublished.

[9] A. Domingo, M.A. Rico. Technical requirements for NATO to Nations CIS service interoperability in expeditionary operations. NC3A TN-1174, unpublished.

[10] MCM-0083-2005: NATO Response Force Minimum Military Requirements (NRF MMR) for common funded deployable CIS and HQ CSS equipment, 7 July 2005.

[11] A. Domingo, H. Wietgrefe, NATO DCIS Target Architecture. NC3A TN-1009, Edition 3. March 2005.

[12] M. Suzuki, H. Hazeyama, Y. Kadobayashi. Expediting experiments across test beds with AnyBed: a test bed-independent topology configuration tool. Tridentcom 2006, Barcelona, March 2006.