Multilateral Interoperability Programme
MIP Test Reference System

Michael Gerz
Fraunhofer FKIE
Fraunhofer Institute for Communication, Information Processing, and Ergonomics
Neuenahrer Straße 20
53343 Wachtberg
Germany

email: michael.gerz@fkie.fraunhofer.de

ABSTRACT

Semantic interoperability of Command and Control Information Systems (C2ISs) is a vital prerequisite for efficient combined and joint operations. However, semantic interoperability does not come for free, especially in the military domain, in which each nation has built its own proprietary C2ISs for many years.

Defining a common semantics for information exchange that is agreed upon by a large community of interest is an ambitious task. It is the merit of the Multilateral Interoperability Programme (MIP) to have specified an interoperability solution that is supported by no less than 27 nations and NATO.

In this paper, we give an introduction to MIP and its approach to achieve semantic interoperability. In particular, we will highlight some of the features that will be available by the latest specifications, which will be released officially as MIP Baseline 3 in 2009. Next, we will present the MIP Test Reference System (MTRS). This test system provides a unique way to ensure conformance of national C2IS to the MIP specification. Finally, we will give a short outlook and highlight some of the interoperability challenges that should be addressed in the future.

1.0 THE MULTILATERAL INTEROPERABILITY PROGRAMME

The purpose of the *Multilateral Interoperability Programme* (*MIP*) is to “achieve international interoperability of Command and Control Information Systems (C2IS) at all levels from corps to battalion, or lowest appropriate level, in order to support multinational (including NATO), combined and joint operations, and the advancement of digitization in the international arena.” [1] MIP is mainly driven by the operational needs of the land forces and their requirements for information exchange with navy and air force in joint operations.

MIP is a voluntary programme that does not have a common funding. By September 2009, 28 members have joined the programme, including 21 NATO nations, 5 nations of the Partnership for Peace (PfP) program, Australia, and NATO Allied Command Transformation (ACT).

The deliverables of MIP are a set of specifications that define the interoperability solution. The *MIP Solution* is based on consensus to ensure greatest possible acceptance within the community. It covers operational, technical, and procedural aspects. Based on operational information exchange requirements, system requirements are derived, which finally result in a concrete technical solution.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **NOV 2009**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**
4. TITLE AND SUBTITLE **Multilateral Interoperability Programme MIP Test Reference System**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Fraunhofer Institute for Communication, Information Processing, and Ergonomics Neuenahrer Straße 20 53343 Wachtberg Germany**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADB381488. RTO-EN-IST-088, Interoperability Issues (Questions d'interoperabilite).

14. ABSTRACT
Semantic interoperability of Command and Control Information Systems (C2ISs) is a vital prerequisite for efficient combined and joint operations. However, semantic interoperability does not come for free, especially in the military domain, in which each nation has built its own proprietary C2ISs for many years. Defining a common semantics for information exchange that is agreed upon by a large community of interest is an ambitious task. It is the merit of the Multilateral Interoperability Programme (MIP) to have specified an interoperability solution that is supported by no less than 27 nations and NATO.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**12**	

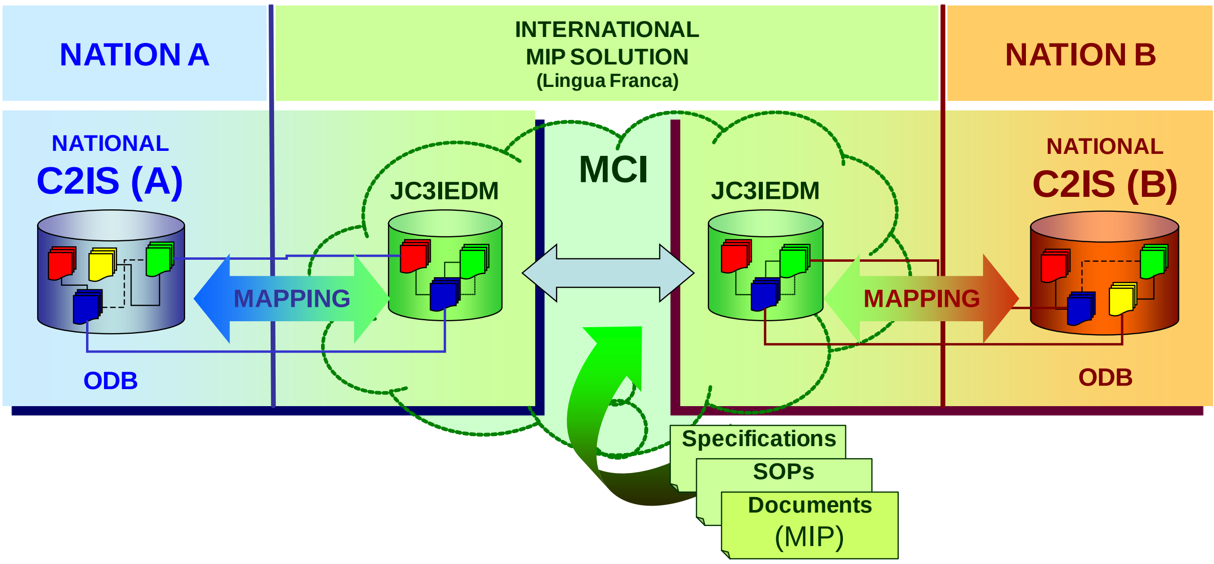

Figure 1: The MIP Solution (updated version of [1])

A high-level view of the MIP solution is shown in figure 1. The part of the C2IS that provides the MIP common interface (MCI) is called MIP gateway. A core asset of the MIP solution is its common information model, the latest version of which is called *Joint Consultation, Command, and Control Information Exchange Data Model* (*JC3IEDM*). Each C2IS has to map its information, which may be described by means of a proprietary data model, onto the JC3IEDM and vice versa. The JC3IEDM is described in detail in section 1.1.

On the technical level, MIP defines two information exchange mechanisms. The *Message Exchange Mechanism* (*MEM*) is based on ESMTP and used for (email) exchange of formatted messages. The *Data Exchange Mechanism* (*DEM*) is a publish-subscribe protocol used for database replication. In the latest release of the MIP specifications – MIP baseline 3 – the MEM is only used for the exchange of a few system management messages and NBC (nuclear, biological, chemical) messages, whereas the DEM is used to exchange all kinds of operational information that can be expressed in the JC3IEDM. The DEM is explained in section 1.2.

In addition to the JC3IEDM and the MEM/DEM, the MIP solution comprises standard operating procedures. For instance, there is guidance for the MIP gateway administrators on how to set up the MIP solution and how to recover in case replication of data fails. Moreover, there are guidelines regarding security. MIP also provides an operational handbook for staff officers that describes the concepts of the MIP solution from a user's perspective.

MIP defines its interoperability solution in a system-independent way. Implementing the MIP solution is a national issue, i.e., there is no common hardware and software development by the programme. In order to support national implementation efforts, MIP provides comprehensive test specifications and organizes interoperability test sessions. There are both system-level tests that check the functional behaviour of the C2IS and operational-level tests that validate the MIP solution with regard to its underlying operational requirements (see section 1.3).

The Multilateral Interoperability Programme has been established in 2001. It has released its first baseline at the end of 2003, followed by another baseline at the end of 2006. MIP baseline 2 has been implemented in many national systems, e.g. in two German C2ISs. The latest set of specifications, MIP baseline 3, is supposed to be approved in 2009. Its in-service period will start after approval and last until 2012.

The major new operational requirement addressed by MIP baseline 3 is the exchange of plans and orders in accordance with STANAG 2014. Another objective was to simplify the data exchange mechanism of baseline 2 and make it more robust. The technical assessment has finally resulted in a complete redesign of the DEM protocol stack. Significant improvements have also been made with regard to testing. Thanks to a better coordination of test specification activities, better tool support, and a better document management, MIP managed to increase the number of test cases by a factor of 5 to 10 (varies among the different test levels).

1.1 JC3IEDM

The *Joint Consultation, Command, and Control Information Exchange Data Model* (*JC3IEDM*) defines a common semantics for information exchanged between two C2ISs. It supports Article 5 operations and crisis response operations (CROs) as well as joint information exchange requirements.

The JC3IEDM is the result of cooperation between MIP and NATO. It is ratified as NATO STANAG 5525. The latest draft version of the JC3IEDM is 3.0.2. The final version will be published as part of MIP baseline 3.

The JC3IEDM is an entity-relationship model specified in IDEF1X. Its logical view consists of 271 entities, 1460 attributes, and 233 relationships (excluding subtype relationships). Many attributes are enumerations with a fixed set of domain values. For every single data element – from the entities down to the individual domain values – a definition is given in textual form to define its semantics.

The ER model of the JC3IEDM is complemented by a comprehensive documentation. Moreover, there is a large number of business rules that serve two purposes: *Integrity rules* define invariants on the data model that cannot be expressed within IDEF1X itself. For instance, some combinations of attribute values do not make sense from the C2 domain perspective. Moreover, there are rules on valid associations among entities (“an engineering capability can only be assigned to engineering equipment”). Many integrity rules are needed due to the generic structure of the JC3IEDM. In contrast, *transformation rules* define mappings from the JC3IEDM onto tactical symbols according to APP-6a.

The conceptual view of the JC3IEDM is given in figure 2. The data model is based on a few generic concepts such as object item (i.e., a concrete object in the real world), object type (i.e., a class/category of objects), capability, affiliation, and location. Each of the afore-mentioned entities is the root of a detailed subtype hierarchy.

The JC3IEDM allows to describe militarily relevant objects, including their status and position, their current and expected capabilities and equipment, and their affiliations to geopolitical, ethnic, religious, and functional groups. It is possible to specify task organisations and orders of battle (ORBATs). The location model can be used to define the position and the geometry of objects.

Tasks and events can be specified in a formal manner using the *ACTION* sub model. Each action is characterized by its objectives, resources, effects, rules of engagement, and its functional and temporal relationships to other actions. The JC3IEDM also supports the specification of plans and orders that consist of free-text paragraphs according to STANAG 2014. Elements of a textual plan can be linked with structured information that, e.g., can be displayed on a map.

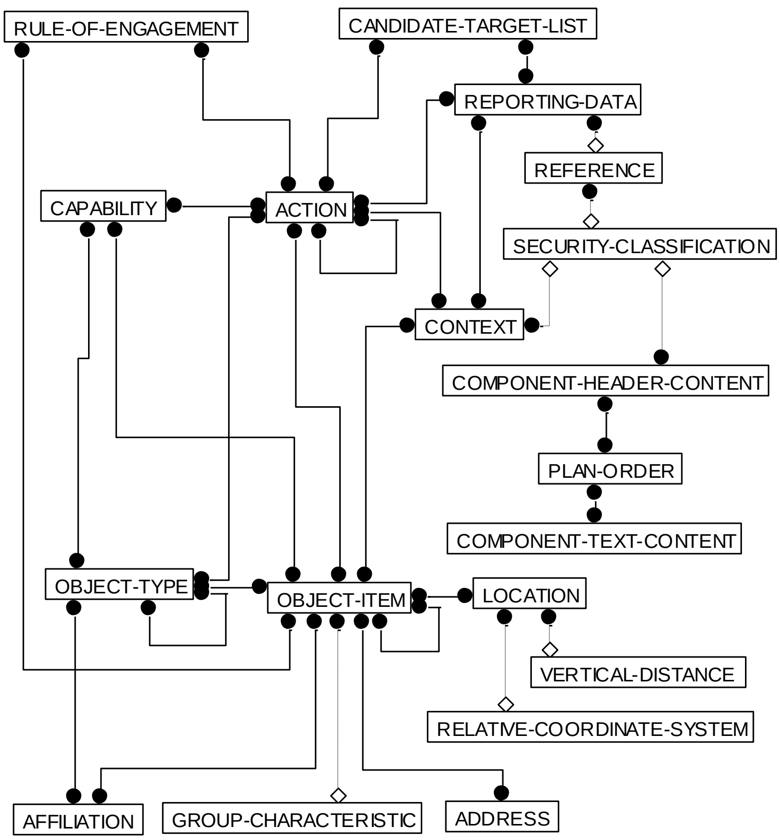

Figure 2: Conceptual view of the JC3IEDM [3]

Information, which may change over time or may be reported by different organisations or persons (intelligence information), is associated with meta information (entity *REPORTING-DATA*). This meta information includes the reporting organisation, date and time when the information was reported, accuracy and credibility, and references to external documents related to the information.

Operational information can be placed in groups (entity *CONTEXT*). For instance, a group may represent a graphical overlay. A special type of group is an *Operational Information Group* (*OIG*). OIGs are not only used for structuring information but also for controlling their distribution. OIGs are described in detail in the next section.

Apart from plans & orders, several new information exchange requirements have been taken into account for the JC3IEDM of MIP baseline 3:

- Additional capabilities for objects (maintenance, support, transmission)
- Air Tasking Order (ATO)
- Maritime Mine Warfare (MMW) / largely extended harbour model
- Chemical Biological Radiological Nuclear (CBRN)

For a detailed description of all new features, see [2].

1.2 Data Exchange Mechanism

The primary means to exchange operational data in MIP is the *Data Exchange Mechanism* (*DEM*). The DEM is a technical solution based on data replication, i.e., the DEM is used to replicate data from one MIP gateway to another one. The payload of a DEM protocol data unit conforms to a schema that directly relates to the structure of the physical view of the JC3IEDM. Although there is no explicit requirement by the MIP specification to do so, virtually all national MIP gateway implementations comprise a relational database, whose schema is derived from the JC3IEDM. If the C2IS also stores its data internally, data have to be mapped between both data stores.

The DEM uses a publish-subscribe approach. If a MIP gateway opens a connection to another MIP gateway, the latter responds with a list of available Operational Information Groups that the staff commander wants to share. There are six predefined OIG categories:

- Friendly and Neutral (Organisational)
- Friendly and Neutral (Non-Organisational)
- Uncorrelated Enemy and Unknown
- Correlated Enemy and Unknown
- Globally Significant
- Plans & Orders

Each unit has its own set of OIGs – exactly one OIG for the first five categories and an arbitrary number of Plans & Orders OIGs. Only the unit owning an OIG is allowed to add new information to the group.

A data receiver may subscribe to one or more OIGs that are offered by the data provider. Once a subscription is established, the data provider will replicate all database content that is related to the respective OIG. Depending on the operational needs indicated by the data receiver when subscribing, the provider will transmit all historic data or only the most recent data.

Besides subscribing, the DEM allows the data receiver to unsubscribe from an OIG and abort a subscription in case the data provider has sent erroneous data that could not be processed. Moreover, the data provider may send an updated list of available OIGs at any time. Depending on the network topology, a MIP gateway may not be able to connect directly to another MIP gateway, because they are located in different subnets. For that purpose, a MIP gateway may also forward OIGs.

The DEM aims at reducing transmission redundancy, i.e., the same data within an OIG should not be replicated twice. On the other hand, the DEM demands that referential integrity of data must be ensured on the receiver’s side. In addition, the DEM requires that semantic completeness be maintained. For instance, an object shared between multiple OIGs must have a hostility status in each individual OIG.

In order to reduce bandwidth, all operational data are compressed using the *DEFLATE* algorithm (which is used by, e.g., the well-known UNIX tool *gzip*), before they are exchanged. To enable fast resynchronization after a connection loss, each DEM data message is labelled with a synchronization point. When a MIP gateway re-subscribes to an OIG, it can specify the synchronization point of the last data packet received for this OIG. Then, the data provider is expected to replicate only those data that were created after the previous subscription.

Technically, the DEM relies on TCP/IP, i.e., a reliable, connection-oriented service. The MIP solution assumes that it is used in a secure local area network. In practice, nations will use their secured communication infrastructure and set up a virtual private network to exchange data with a remote system.

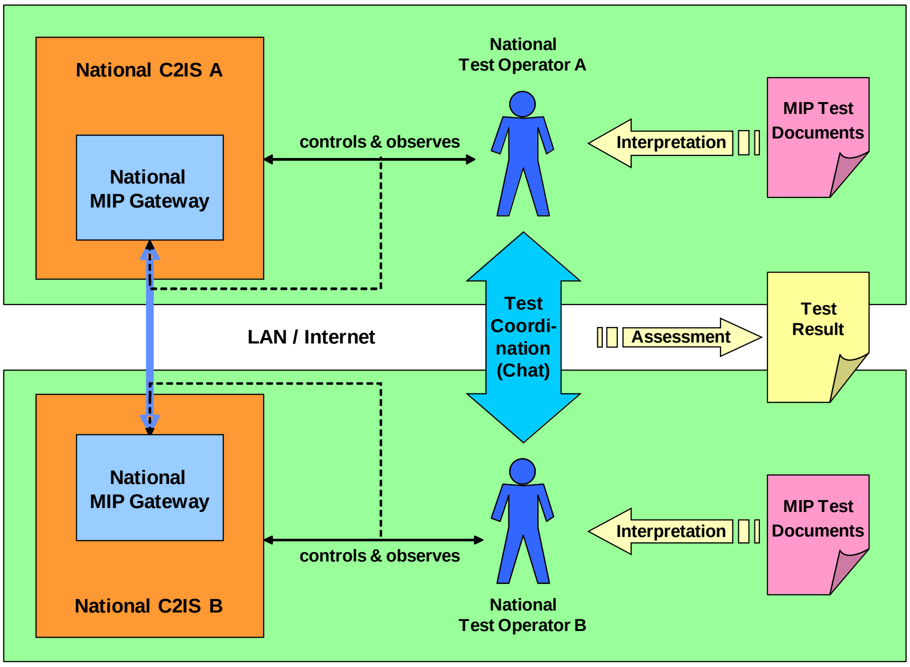

Figure 3: Bilateral Interoperability Testing

1.3 MIP Interoperability Testing

In order to support the implementation of its interoperability solution in national systems, MIP provides a set of test specifications that can be used to perform bilateral or multilateral interoperability tests. Tests should be performed for all aspects of the interoperability solution. In MIP, functional system tests are specified on three levels:

- In the first step, the communication protocols (as implemented in the MIP gateway of the C2IS) are tested. For instance, it is checked whether a MIP gateway is able to exchange configuration information with another MIP gateway, and whether it can subscribe and unsubscribe from an OIG. Advanced tests consider the interaction of a MIP gateway with multiple gateways simultaneously.
- In the second step, database replication and processing of (possibly erroneous) operational data is tested. Many test cases are based on the principle that a MIP gateway must replicate the *right subset* of all data available, depending on the established subscriptions.
- In the third step, end-to-end information exchange is tested, i.e., information created by a user with one C2IS has to be presented in a semantically equivalent way by another C2IS. Technically, these tests focus on whether C2IS information is mapped correctly onto/from the common data model.

In addition to the test specifications, MIP arranges a series of interoperability test sessions as part of its development process. Tests take place over the Internet or are executed collocated in Greding, Germany.

The general approach for bilateral interoperability testing is depicted in figure 3. Each national C2IS (including the national MIP gateway) is controlled and observed by a test operator that is familiar with the handling of his/her national system. Both test operators refer to the MIP test specification that defines a sequence of test events and test criteria to decide whether an interoperability test was passed successfully.

During test execution, both test operators must coordinate their activities and, by the end of the test, agree on the test verdict.

This way of testing has several theoretical and practical limitations and weaknesses:

- First, tests are executed manually by test operators. This means that testing consumes many human resources. Please note that test preparation (organisation and technical setup) makes up a significant portion of the total efforts. If tests are run over the Internet, additional scheduling problems may arise if the participants live in different time zones.
- Because the test specifications are only described in a semi-formal way, they are subject to interpretation and different test operators may execute the same test in a slightly different way. This may also have an impact on the test verdict.
- Moreover, it is difficult or even impossible to test the behaviour of a C2IS in response to invalid input from another system, because C2ISs are not designed for sending corrupted data but for conforming to the MIP specification.
- If a test fails, it can become quite challenging to identify the cause of the problem or even to decide which of the participating C2ISs has behaved incorrectly. For instance, if the position of some unit is replicated between two C2ISs and the position on the map is different on both systems, the problem might have occurred in the user interface layer of either C2IS or when mapping the information onto/from the common exchange data model.
- Similarly, errors introduced in two C2ISs may compensate each other and thus may not be discovered.
- If a test has uncovered a bug, depending on the severity of the problem, the test session may have to be interrupted for an indefinite time to fix the software.
- Due to the enormous resources needed, it is close to impossible to perform regression tests on a large scale. On the other hand, both draft specifications and national implementations evolve over time, which requires regular re-tests at least for specific aspects of the specification and the implementation.

2.0 MIP TEST REFERENCE SYSTEM

To support testing, the Fraunhofer Institute for Communications, Information Processing, and Ergonomics has developed a conformance test system, which has been adopted by the MIP community as the *MIP Test Reference System* (*MTRS*) [4]. Its purpose is to improve the test specifications by using formal notations and to reduce the test effort by automating the test process.

The MTRS is funded by the Federal Office of the Bundeswehr for Information Management and Information Technology. It is provided as a free service to the MIP nations. The MTRS has become a mandatory tool of the MIP system-level testing strategy.

2.1 Conformance Testing Architecture

As indicated above, the purpose of the MTRS is to check *conformance* of a C2IS to the MIP interface specification. This means that a C2IS must interact with the MTRS in a way that is in line with the MIP specifications. Please note that the internal structure and behaviour of a C2IS is not constrained by the MIP specifications but only its external behaviour. Accordingly, the C2IS is considered as a black box. It is stimulated with some input and its response is observed and compared with the anticipated reaction.

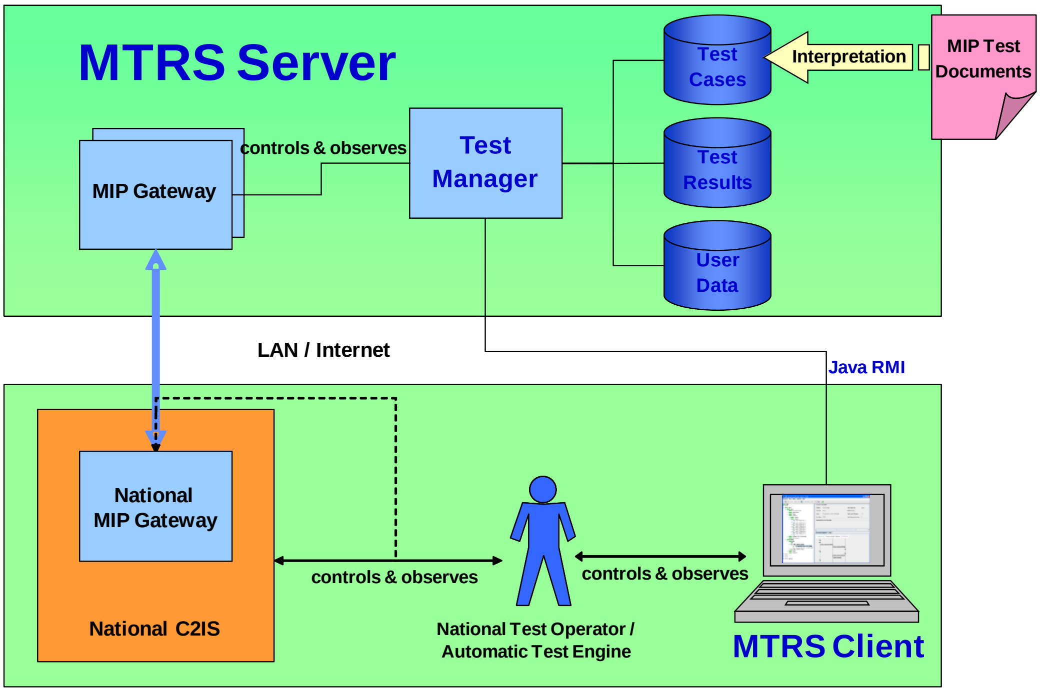

Figure 4: Conformance Testing with the MTRS

The MTRS is able to test the response of a C2IS to inopportune and invalid input. Inopportune input means unexpected input that is valid according to the specification (such as closing a connection immediately after opening it). Input may be syntactically and semantically broken both on the network protocol level and on the operational data level. For instance, operational data may violate domain value restrictions or business rules defined by the JC3IEDM.

Test operators can use the MTRS over the Internet. Since it runs tests automatically, it is available at any time and independently from other test operators. Accordingly, the need for coordinated test sessions is significantly reduced (although interoperability testing still has its merits once systems have checked their conformance, because national C2ISs may cover different, non-overlapping parts of the interoperability solution).

The distributed test architecture of the MTRS is depicted in figure 4. The MTRS consists of a client and a server component. Each test operator uses a client application to connect to the central MTRS server. The client allows to browse the test suite, start and stop test cases, analyse errors in case of failed tests, generate test reports, etc. There are two kinds of clients:

- an interactive client with a graphical user interface and
- a Java Application Programming Interface (API) for integrating the MTRS into a national test environment.

When starting a test case via the client, the test manager on the MTRS server executes a test script. It runs in a separate thread that is isolated from other test processes. That means that several users can use the test system in parallel without noticing each other.

Depending on the specific test case, one or two MIP gateways are set up that interact with the national C2IS. During test execution, the test script triggers its associated gateway(s) and controls and logs all

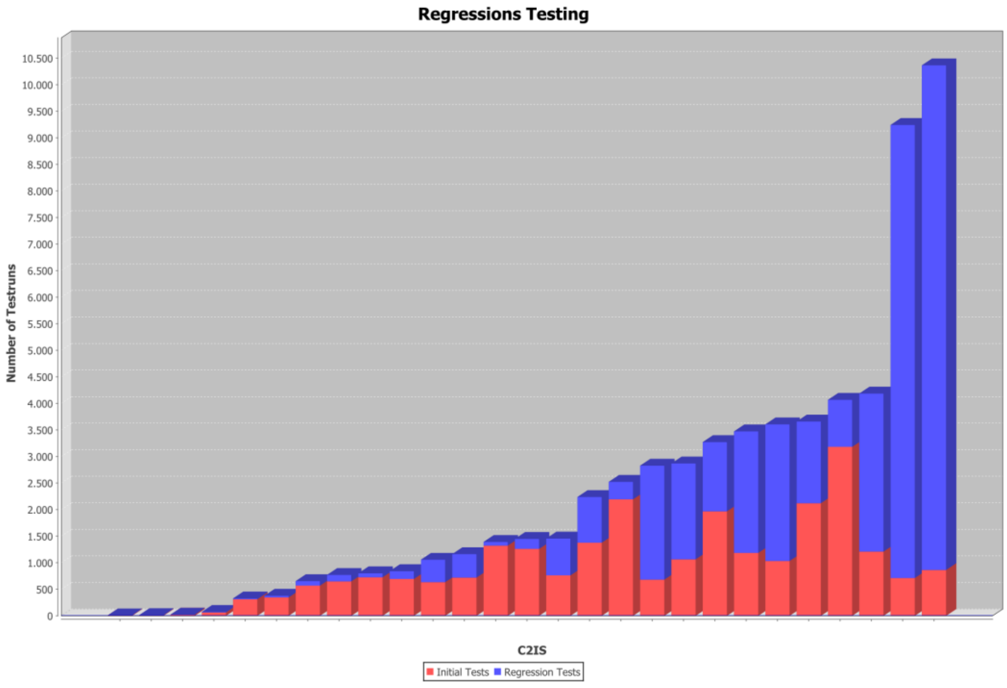

Figure 5: Nations' test activities

communication between the MTRS gateway(s) and the national C2IS and between the components within the MTRS gateway(s). Therefore, the test operator can trace and analyse the processing of the data exchanged between the C2IS and the MIP gateway. For that purpose, analysis tools are integrated into the client. At the end of a test case, the test verdict is determined automatically by the MTRS.

An important prerequisite for automatic test execution is the availability of a test suite, whose test cases are specified in a formal manner. For that purpose, a formal test language is needed that can be interpreted by the test system. As part of the MTRS development, a general-purpose test language based on Java has been designed and implemented. Moreover, a domain-specific language has been developed to describe JC3IEDM mapping test cases on a proper level of abstraction.

The MTRS test suite consists of 107 tests for the DEM communication protocols, 171 database replication tests, and 356 JC3IEDM mapping tests (in both directions). All tests are specified formally and can be executed automatically by the MTRS.

2.2 Test Results

As of September 2009, the MTRS has been used for 26 C2ISs from 24 nations; two more systems are going to start testing soon. In total, nations have run more than 70,000 test cases. Users were logged into the MTRS for about 476 hours.

Figure 5 shows the testing activities for the participating systems. There are two interesting aspects: First, there are two systems with 9,000 to 10,000 tests runs. This enormous number of tests was enabled by the MTRS API, which allows nations to fully automate test execution even on the C2IS's side.

Second, we can see that many C2ISs were checked with many regressions tests. (In this context, regressions tests are defined as tests that were repeated although they have been passed successfully before.) This indicates that the MTRS is an efficient means for testing. Moreover, it indicates that the

MTRS is not considered as an obligation to prove conformance of one's own C2IS but is voluntarily used even at the later stages of development.

3.0 SUMMARY AND OUTLOOK

The MIP solution supports semantic interoperability based on a common information exchange data model and a data exchange mechanism. The JC3IEDM conglomerates more than 20 years of C2 modelling experience and covers a large number of individual information exchange requirements (IERs). These IERs have been merged into the data model in order to exploit the benefits of sharing common data elements.

The MIP Test Reference System has proven to be a valuable contribution to MIP baseline 3 testing efforts. Since it was available at an early stage, many problems in the specifications could be identified and resolved. Due to the automatic execution of test cases, the number of test runs could be increased significantly, resulting in more stable system implementations and, ultimately, in better interoperability.

In the future, additional information exchange requirements will be reflected in the data model. Therefore, keeping the entity-relationship model, the business rules, and the accompanying documentation consistent becomes a challenging task. The MIP community investigates and develops new tools based on the Unified Modelling Language (UML) to simplify the configuration management. Migrating the model to UML will also enable implementers to quickly derive software artefacts from the JC3IEDM, applying the Model-Driven Architecture (MDA) approach.

Since the JC3IEDM satisfies many different information exchange requirements, C2ISs may not support all aspects of the data model. In the future, an interoperability solution is supposed to be based on individual capabilities that are supported by services on the technical level. Each service may employ a specific subset of the JC3IEDM. This way, capabilities and services can be delivered incrementally at a higher rate.

Semantic interoperability is the "ability of computer systems [or humans] to communicate information and have that information properly interpreted by the receiving system [person] in the same sense as intended by the transmitting system [person]" [5]. However, it does not ensure that the actors, i.e., the C2ISs, the staff officers, and commanders, act in a coordinated way based on the information that they receive. In order to reach the next level of interoperability, *pragmatic* interoperability, it is important to describe the overall processes. Understanding the operational actors, their activities, etc. also helps to better identify the technical requirements of an exchange mechanism for a specific capability. An architecture framework, such as the NATO Architecture Framework (NAF), helps to achieve that purpose.

REFERENCE

[1] Multilateral Interoperability Programme (2006). MIP Standard Briefing. http://www.mip-site.org.

[2] N. Bau, M. Gerz, M. Glauer, H. Schüller (2007): Multilateral Interoperability Programme – Advancements in MIP Baseline 3. 12th Internal Command and Control Research and Technology Symposium (ICCRTS), Newport, RI.

[3] Multilateral Interoperability Programme (2009). The Joint C3 Information Exchange Data Model. Edition 3.0.2. http://www.mip-site.org.

[4] MIP Test Reference System (2009). https://trac.fkie.fgan.de/MTRS .

[5] Wikipedia (2009). Semantic Interoperability. http://en.wikipedia.org/wiki/Semantic_interoperability .