16th ICCRTS
"Collective C2 in Multinational Civil-Military Operations"

Title of Paper
Towards Semantic Interoperability between C2 Systems Following the Principles of Distributed Simulation

Topic(s)
Architectures, Technologies and Tools
Networks and Networking
C2, Management, and Governance in Civil-Military Operations

Name of Authors
Vahid Mojtahed
Swedish Defence Research Agency
SE 164 90 Stockholm, Sweden
Vahid.Mojtahed@foi.se

Martin Eklöf
Swedish Defence Research Agency
SE 164 90 Stockholm, Sweden
Martin.Eklof@foi.se

Jelena Zdravkovic
Department of Computer and Systems Sciences, DSV
Stockholm University
Forum 100, SE-164 40 Kista, Sweden
jelenaz@dsv.su.se

Point of Contact
Vahid Mojtahed
Swedish Defence Research Agency
SE 164 90 Stockholm, Sweden
+46 8 5550 3705
Vahid.Mojtahed@foi.se

Towards Semantic Interoperability between C2 Systems Following the Principles of Distributed Simulation

Vahid Mojtahed, Martin Eklöf
Swedish Defence Research Agency
SE 164 90 Stockholm, Sweden

Jelena Zdravkovic
Department of Computer and Systems Sciences, DSV
Stockholm University
Forum 100, SE-164 40 Kista, Sweden

Abstract
Increased focus on multi-functional and multi-national operations brings new requirements to military command and control, in addition to other capability requirements. Parallel but separate from this development, interoperability has been of major concern within Modeling and Simulation (M&S) for years, especially in connection with standards for distributed simulations, e.g. High Level Architecture (HLA). Both areas share a need to create configurations of systems where elements of information exchanged are interpreted similarly among all participating parties, preserving the intended meaning (i.e. semantic interoperability). An effort to address this need is currently under development within NATO IST-094, Semantic Interoperability Framework (SIF), which includes tool and methodology support for harmonising data/information models on a semantic level, as well as mediators to translate between heterogeneous abstractions. The framework builds on a knowledge-based approach utilizing emerging semantic technologies, such as ontologies. In this paper we investigate how, and to what extent, concepts, solutions and experiences from the distributed simulation community can help fulfill the requirements of the SIF. Based on this, a common process is presented which is aimed at governing the development and execution of system configurations to meet expressed business requirements.

1. Introduction

1.1. Background

Coordinated efforts, collaborations and interdependencies have increased the need for information exchange between heterogeneous systems that are owned and designed by different organizations. *Semantic heterogeneity* is a particularly challenging form of heterogeneity which occurs when there is disagreement regarding the meaning, interpretation and intent of information or when information is described in different ways in two different systems.

Semantic heterogeneity causes new and unexplored problems in decentralized information systems. Multiple interpretations of data by different users in different contexts must be handled. In current information systems, much of the semantics of a system resides in the application code, or in the assumptions which the application makes about the data rather than in a conceptual schema. Such a situation can be accepted in a centralized system in which the applications use a shared set of assumptions, but in a decentralized environment it gives rise to severe problems. It is therefore important to develop methods, tools, and techniques for achieving *semantic interoperability*, i.e., cooperation among semantically heterogeneous systems [1].

1.2. Problem

The ongoing globalization poses new challenges for military operations. In particular, it has become much more common to carry out activities together with other nations' civil and military organizations, i.e. to interoperate in multinational and multifunctional contexts. In order to cooperate efficiently, it is necessary for different organizations to exchange information between their command and control (C2), management and information systems (IS), i.e., to be interoperable. It is therefore essential to develop future IS that can adapt to different types of situations in which the information exchange needs are not known in advance. A prerequisite for an improved interoperability between IS of different organizations is to create standards, methods and tools which can align different terminology, and facilitate translation of data between heterogeneous systems.

Successful operations involving organizations which are not trained together requires at least one very important function - reliable communication of critical information like threats and risks. This, in turn, requires that any two co-operating parties are interoperable on a *semantic* level. Problems related to the use of different data formats, or pure connectivity issues, all too often distract from what is really the main problem - to understand and interpret information in a consistent manner. The importance of this aspect cannot be emphasized enough, especially so when information exchange is taking place between multiple domains. The aim of semantic interoperability is to achieve a common understanding of one or more domains before the exchange of operational information between systems takes place. Since current development processes do not take into account the preservation of the intended meaning of terms in the exchange of information, any attempt to integrate heterogeneous systems for multi-national operations without taking semantic interoperability into consideration will be insufficient.

Thus, it is of a great importance that command and control systems are developed with flexibility in mind, in order to be able to adapt to different situations in which the need to exchange information between systems exists. Within NATO, semantic interoperability (SI) has been consequently identified as a core capability for future command and control systems. Semantic interoperability may contribute to various capabilities of the armed forces, but is above all expected to increase the safety of international operations. Despite this, semantic interoperability has not yet been identified as a requirement for information exchange between different systems. SI is formally defined in Section 2.

1.3. Our contribution

Interoperability problems have been a major concern within the Modeling and Simulation community for years, especially in connection with standards for distributed simulations. As in the C2 domain, there is a need to create configurations of systems where elements of information exchanged are interpreted similarly among all participating parties, preserving the intended meaning (i.e. semantic interoperability).

As mentioned, an effort to address this need in the military world is currently ongoing within NATO, with the proposal of a Semantic Interoperability Framework (SIF). Therefore, it is of great interest to study and gain experiences from the M&S community which has struggled with similar interoperability issues for many years and apply that knowledge to the SIF which is still under development.

The distributed simulation community has been successful in creating conditions for integration of simulation models, but has historically been most concerned with interoperability at the syntactic level. However, two very important results from this domain are of interest when developing SIF. The most important concerns the achievement of a standardized process for development and execution of distributed simulations. The other one concerns component-based development which relies on simulation components (models) being interoperable in different configurations without much need for manual work.

In this paper, theories and best practices that have been accumulated by the distributed simulation community are adapted and applied to SIF in order to develop a robust framework for semantic interoperability of C2 systems. In particular, we investigate how, and to what extent, concepts, solutions and experiences from the distributed simulation community can help in fulfilling the requirements of SIF. By doing so, we aim at conceptualizing a common process for governing the development, execution and analysis of heterogeneous systems in a C2 context, meeting semantic interoperability requirements.

1.4. Paper layout

The rest of the paper is organized as follows. Section 2 introduces the concept of semantic interoperability, as well as other levels of interoperability both below and above the semantic level. The concept of ontology is defined and its role in a knowledge based solution for semantic interoperability is described. Section 3 introduces the Semantic Interoperability Framework – SIF, which proposes an augmented ability of information systems to facilitate exchange of data and share information and knowledge. After a brief description of SIF, its main components and functionality are described. Section 4 gives a brief introduction to distributed simulation standards, the High Level Architecture (HLA) and the Federation Development and Execution Process (FEDEP). In Section 5 a general comparison of distributed simulation efforts and SIF's requirements is provided. Based on that, and a survey of other, collaboration- and interoperability-related management processes, a similar process for SIF is defined. The process is named Semantic Interoperability and Development Execution Process (SIDEP). In this study, SIDEP is explored to a high-level meta-model and the major activities are defined. Section 6 concludes the paper by summarizing our current research results and pointing out intended future work.

2. Knowledge-based solution

In this section we recall the basics of knowledge-based solutions for semantic interoperability.

2.1. Semantic Interoperability

Wikipedia defines Semantic Interoperability as the ability of two or more computer systems to exchange information and have the meaning of that information accurately and automatically interpreted by the receiving system. NATO's primary research group in this field, NATO RTO IST-075, has slightly modified Wikipedia's definition and defines Semantic Interoperability as *the ability of two or more computerized systems to exchange information for a specific task and have the meaning of that information accurately and automatically interpreted by the receiving system, in light of the task to be performed* [2].

Hence, two actors that are semantically interoperable can not only exchange information, but can also interpret and understand the intended meaning of the information in a common way. This is a key issue in the interaction between groups that do not share common frames of reference acquired through a common culture or through education. Support for semantic interoperability is therefore a prerequisite for the ability to participate in international operations with allied forces.

Interoperability is more than only the technical compatibility of systems. In a Network Centric Warfare scenario, the C2IS of all engaged elements must be connected (physical interoperability), exchange data in such a way that automatic processing is possible (syntactic interoperability), exchange information and guarantee identical interpretation (semantic interoperability), cooperate and realize situational awareness (pragmatic interoperability) that assures the coherent cooperation of all participating actors (social/cultural interoperability).

2.2. Utilizing ontology for Semantic Interoperability

Knowledge-based solutions for semantic interoperability often exploit the ontology notion. Within the knowledge engineering community, ontology is defined as an explicit, formal specification of a shared conceptualization [3]. Here, *conceptualization* refers to an abstract, concept-based model of some phenomenon in the world. *Explicit* means that the type of concepts used, as well as the constraints on their use, are explicitly defined. *Formal* refers to the fact that the ontology should be machine-readable. *Shared* reflects that an ontology captures consensual knowledge, that is, the knowledge accepted by a group.

Every term used in natural languages has several meanings. In an ontology we constrain the semantic interpretation of these terms, and provide formal definitions. This is called ontological commitment and means mapping between ontology terms and their intended meanings. The major task here is to determine precisely what meaning the term has.

Ontologies have been proposed for the following uses [4]:

- sharing common understanding of the structure of information among people or software agents,
- enabling reuse of domain knowledge,
- making domain assumptions explicit,
- separating domain knowledge from operation knowledge, and
- analyzing domain knowledge.

More recently, ontologies have become recognized as an emerging mechanism for dealing with semantic interoperability of Information Systems. This is entirely aligned with the lately recognized fact that semantic understanding and interoperability is a key challenge for organizations and their systems to successfully and competitively provide their services. By specifying the conceptualization in terms of an "agreement" on meaning between the parties involved, the ontology becomes a reification of an agreement on knowledge.

2.3. A solution for Semantic Interoperability

The traditional means of exchanging information between systems do not guarantee that the intended meaning of information (the semantics) is preserved. To ensure that meaning is preserved, we need shared terminologies (ontologies); every message between communicating actors may then include references to one or several ontologies according to which the message should be interpreted.

Common representation of semantics through ontologies represents one important step towards information interoperability. However, in addition to the use of ontologies and related tools, a consensus on a common process is needed, i.e. on how they are to be used in the lifecycle of a system interoperability task. One way to achieve semantic interoperability between two systems is to align the ontologies of those systems. Ontology alignment is the result of an ontology matching process which is the task of determining correspondences between the concepts of different ontologies. Ontology matching and alignment are required when two heterogeneous systems want to harmonise their ontologies in order to achieve semantic interoperability. This process of harmonising two different ontologies is known as ontology reconciliation [5].

FOI (Swedish Defense Research Agency) has as of 2007 worked to clarify the concept of semantic interoperability, to build skills in this area, and to propose solutions. In cooperation with NATO's primary research group in this field, NATO IST-075, a general logical framework in the shape of an architecture for semantic interoperability has been developed, called Semantic Interoperability Framework (SIF). The framework will be explained in next section.

3. SIF - Semantic Interoperability Framework

In this section we describe the Semantic Interoperability Framework (SIF) proposed in the report of NATO task group IST-075 [2].

3.1. Background

Semantic Interoperability (SI) is difficult to measure, and the challenge of achieving SI between independent and heterogeneous systems is far too complex for any "one-size-fits-all" universal solution. Nevertheless, in order to achieve a common view and describe this challenge, the NATO group IST-075 has conceived a framework, called SIF - Semantic Interoperability Framework, intending to provide a generic approach to SI. This section briefly introduces SIF, gives an overview of SIF, and finally outlines the requirements for it to function efficiently.

IST-075 was an RTG (Research and Technology Group) coordinated by the IST (Information Systems Technology), and included members from several countries that cooperated, for the period 2007-2009 under the umbrella of NATO RTO (Research and Technology Organization). The group worked on the problem area "semantic interoperability" with a focus on ontologies and created SIF as one of its results. The Swedish Defense Research Agency - FOI - received a mandate from the Swedish Armed Forces to join, follow and contribute to this work during that period. A continuation group IST-094, which FOI also joined and supports, proceeds with this activity for the period 2010-2012.

3.2. Overview of SIF

In order to ensure semantic interoperability of several systems, an architecture is needed which includes a party-wise set of common ontologies between communicating parties, which the involved systems can understand and use. Such is always implied by actors who exchange messages (otherwise communication is impossible), but in this architecture it is made explicit. This allows each message between communicating parties to be provided with references to one or more of the ontologies according to which the message should be interpreted. SIF is a high level view of such architecture that supports semantic interoperability among heterogeneous information systems. In terms of features, SIF is a middleware that performs interoperability in a communication medium and not as part of the communicating systems. SIF applies means of knowledge-based systems, using ontologies, for mediation purposes.

SIF can be described from various perspectives - from a functional point of view one could say that SIF has a preparatory phase and an implementation phase. During the preparatory phase, all necessary information about the participants in the communication is collected or created in the form of ontologies. During the implementation phase a number of different ontology methods and mapping tools are applied on those ontologies. The end result is a transformation of the message structure from one information system A to another information system B with preserved semantics.

3.3. Assumptions and Conditions

The application of SIF assumes that the lower levels of interoperability have already been achieved between the concerned systems. This means that the systems are connected (physical interoperability is established) and that they can exchange data in such a way that automatic data processing is possible (syntactic interoperability is also established). It also assumes that semantic descriptions of systems can be obtained in some way. These descriptions can more or less automatically be (partly) derived from systems, but in order to achieve the necessary quality of the descriptions the process normally requires human intervention.

It is important to note that the starting point for SIF is that existing systems have a need to share information in order to be able to interact in some kind of coalition. This must also be done without claiming major changes to the systems, and without any requirements of knowing the other systems' intention beforehand. Nations will unlikely change their C2 systems in order to be able to interact with other nations. Nor is it likely that they want to adapt their C2 systems every time a new nation will integrate. The optimum for each C2 system is to "talk and listen" in their own language. In addition, the general situation is that of a sender creating a message without knowing in advance who the receiver will be.

3.4. Brief description of SIF, its main components and functions

The basic idea of SIF is to foster the use of a semantic description of all of the information to be exchanged and then take advantage of a number of existing and emerging semantic technologies, mainly ontologies, to improve interoperability. Figure 1 shows an overall view of SIF which can be described as follows. SIF mediates an exchange of information between systems A and B, which do not necessarily know each other. Furthermore, the assumption is that the systems information structures are different and therefore the exchange of information cannot happen painlessly. This means that to make the communicated information correctly interpreted in accordance with the semantics of system B a transformation is required for all information that system A communicates. A number of ontology operations take place in order to define and produce the rules necessary for these transformations. Input to these ontology operations and transformations are not only semantic descriptions of systems A and B, but also references to potential shared concepts and definitions which will exist in the "Common Ground" (CG).

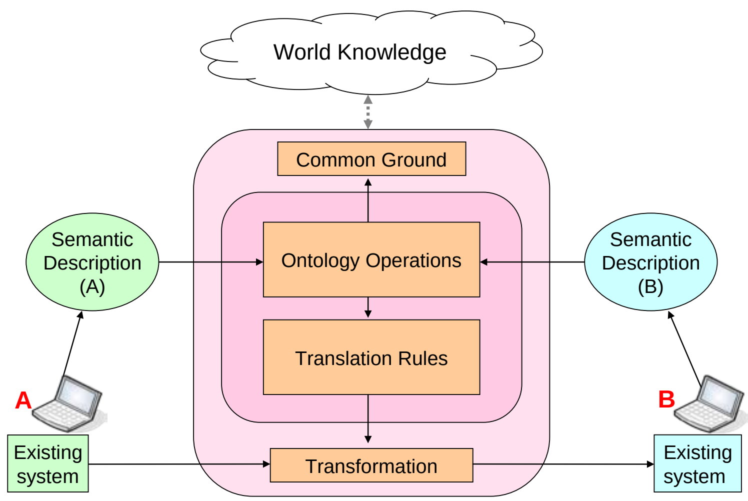

Figure 1: An overall view of SIF.

The most important components of SIF according to Figure 1 are as follows.

The main purpose of *Common Ground* (CG) is to provide knowledge resources that will serve as common references for the semantic descriptions supplied by independent systems, in order to produce accurate ontology mappings. The idea here is that a portion of "all knowledge" available in the world, either exist or can be made available in machine-readable form. If this available machine-readable knowledge proves to be useful, reliable and validated for military use, it can be placed in CG to support SIFs ontological activities. An ontology manager within SIF provides services for *ontology operations* that identify similar concepts across ontologies and otherwise harmonise and align ontologies. *Translation rules* are the output of the mappings between concepts in the Common Ground, schema definitions, etc. *Transformation* is used to convert a message from a form which was suitable for system A into a form which is appropriate for system B. It is important to note that the structure of the message is converted without loss of semantics. For more details on SIF the interested reader is directed to NATO IST 075 Final Report [2].

The major functionality of SIF is to facilitate the exchange of messages (information) by the help of above described components. The information exchange is orchestrated into a number of stages, which we have directly considered when proposing our solution for a semantic-interoperability process (Section 5).

4. Modeling and Simulation

Modeling and simulation (M&S) technologies play an ever-increasing role in supporting military applications such as training, research and development, analysis, test and evaluation. The M&S community has tackled interoperability-related problems for many decades. Since the late 1980's, there have been serious efforts to address the related problems of interoperability and reuse by encouraging the development of simulations according to well-defined standards. The Simulation Interoperability

Standards Organization (SISO), which has played a major role in these efforts, has succeeded in establishing standards for distributed simulations.

Distributed simulation is concerned with the execution of simulations on geographically distributed computer systems interconnected via a local area and/or wide area network. It can be viewed as a collection of autonomous virtual, live, and constructive simulators, each generating its own representation of the battlefield from its own perspective. In order to achieve interoperability among separately developed simulators, a set of standards have been developed, e.g. the High Level Architecture (HLA).

4.1. Distributed Simulation and HLA

Today, the High Level Architecture (HLA) is one of the most widely adopted standards for distributed simulations in the military domain. HLA has its origins in the (US) Defence Modelling and Simulation Office's (DMSO) effort during the 90's, which aimed at increasing the support for reuse and interoperability of models maintained by the Department of Defence (DoD). Since then, the HLA has matured and standardized through IEEE. HLA 1516-2010, which builds upon previous HLA 1516-2000 and HLA 1.3 standards, is the latest release (published in august 2010).

An HLA-based distributed simulation is referred to as *federation*. Individual simulation models, that together form a federation, are called *federates*. Federates interact in a federation execution (simulation) through services provided by a run-time infrastructure (RTI). The RTI can be seen as a distributed operating system, implementing the HLA standard. The standard itself comprises the following core parts:

Framework and Rules – This part defines the HLA, i.e. specifies its components and describes the responsibilities of federates and federations. The latter comprises two set of rules that federates and federations must follow [6].

Federate Interface Specification – The HLA relies on a standardized inter-federate interaction interface. The Federate Interface Specification describes this interface in terms of six types of RTI services, e.g. services for federation management, synchronization and message distribution [7].

Object Model Template (OMT) Specification – The OMT could be seen as a template for documenting information in HLA federations, i.e. it defines the format and syntax. It comprises two different templates, namely the Federation Object Model (FOM) and the Simulation Object Model (SOM). The former is used to specify the data exchange for a set of federates of a federation, whereas the latter specifies capabilities of a federate [8].

In addition to the above mentioned parts, there is a recommended best practice for development and execution of federations: *Recommended Practice for High Level Architecture Federation Development and Execution Process (FEDEP)*. FEDEP does not replace project management or systems development practices, but should be seen as en overarching framework within which these are integrated and adapted for a given purpose [9]. See next section for details.

4.2. FEDEP

Figure 2 shows the phases of FEDEP. Note that FEDEP is an iterative process where the steps are not necessarily implemented in a strict sequential order. Below, a brief description of each phase in FEDEP is given.

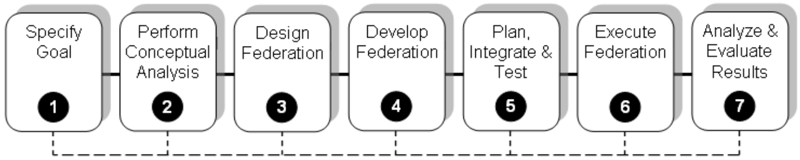

Figure 2: Federation Development & Execution Process.

Specify Goal – In this step, the user's, or project sponsor's, needs/problems, which should be addressed by the federation, are specified. The needs are expressed in terms of objectives, at a relatively high level of abstraction, which is sufficiently concrete to allow for evaluation, i.e. post federation execution (i.e. how well objectives were met). In addition to this, a comprehensive plan for the "project", used for management of subsequent process steps, is described.

Perform Conceptual Analysis – In this step a conceptual model, covering the part of reality that is of primary interest, is created. In this work one or more scenarios are created addressing the current problem. The purpose of a scenario is to provide a scope for the development of the conceptual model. A conceptual model is created describing all relevant entities and their possible actions, and mutual relationships. Based on the conceptual model, specific requirements for the federation are then specified. These should be detailed enough to serve as a basis for implementation at a later stage.

Design Federation – In this step, the simulation environment (the federation) is designed, according to the requirements specified in the previous step. This includes the selection of federates that might be reusable in the given context, and/or design of new federates if the existing models do not meet current requirements. Responsibilities of representing entities and actions, defined in the conceptual model, are given to identified federates or new federates. A detailed plan for the development of the federation is established.

Develop Federation – In this step the federation is developed. From an overall perspective, this is carried out in four steps. First, a Federation Object Model (FOM) is developed that support the information exchange requirements, i.e. specifies all data that can be exchanged within a federation. Secondly, important aspects, not covered in the FOM, are captured in a set of federation agreements. Thirdly, needed changes to existing federates, or development of new federates, is performed. Finally the infrastructure needed for federation execution is implemented, configured and initialised.

Plan, Integrate and Test Federation – In this step the execution of the federation is planned, all connections between federates are established, and testing of the federation is carried out. An exhaustive description of the execution environment is created, such as the technical requirements that federates impose on the underlying infrastructure. The operational planning is also in focus to describe who is involved in the federation execution, needed support, time-scheduling, and required education. The overall objective of the tests is to ensure that the federation can be executed and hence that the individual federates can interoperate, in an intended manner, given by specified goals.

Execute Federation – In this step the federation is executed according to the plan that has been established. Data generated during federation execution are collected. Data can be collected and stored locally, by individual federates, or collected by dedicated tools with interfaces to the federation and the RTI. In this step the collected data is also prepared for analysis and evaluation.

Analyze and evaluate the results – At this stage, collected data are analyzed and evaluated. The results are packaged and reported back to relevant users and project sponsor. It is their task to determine if the goals of the federation have been achieved or not. Another important part of this last step is to ensure that as many as possible of the federation components are made available for reuse. This applies to FOM / SOM, conceptual models and scenarios, and federates. It is also desirable to document the experiences of developing and executing the federation.

4.3. Interoperability & reuse

One of the main objectives of HLA is to enable reuse of simulation models, being able to efficiently combine simulation components (federates) to fit a specific scenario (federation). A federate should not, in the ideal case, be designed and developed with a specific federation in mind, but should be reusable in several contexts. In the process of developing a federation, one of the key questions to address, in relation to reusability, is to assure that a configuration of federates is "meaningful", e.g. that assumptions of an individual federate are consistent with those of all other federates. However, the HLA standard is primarily focused on describing the interface syntax of federates and is less concerned with specification of the "internals" of a federate. Thus, an additional HLA-related standard, Base Object Model (BOM) has been promoted and standardized within SISO (Simulation Interoperability Standards Organisation) to overcome these limitations. The BOM standard provides means of describing the conceptual model of a "simulation component" along with associated metadata. Furthermore, it provides grounding to the HLA OMT which enables mapping from conceptual model to component interface specification, where the latter may be expressed in terms of the HLA OMT. The current version of BOM was standardized within SISO four years ago. Recently, a PDG (Product Development Group) of SISO released a *BOM Experimental 2010 Schema* with several enhancements.

The data exchange of most federations is usually based on a standardized FOM, e.g. RPR-FOM (Real-time Platform Reference FOM) [10]. This is similar to the approach often used in the C2 systems domain, where a standardized data exchange model is applied, usually in the form of JC3IEDM – Joint Command Control Consultation Information Exchange Data Model, to enable systems connectivity. The drawback of this approach is that a monolithic, centralized model is difficult and costly to maintain. To overcome this problem, the concept of FOM modules has been introduced as of HLA 1516-2010. Through FOM Modules, HLA object models are handled in a more scalable and flexible manner, e.g. by separating local specialisations from standardized core models and providing a function for introduction of new concepts in an already active federation execution [11].

5. SIDEP – Semantic Interoperability Development and Execution Process

5.1. Reflecting Modeling and Simulation to Semantic Interoperability Framework

HLA and SIF are both frameworks that address how to inter-connect distributed, and potentially heterogeneous, systems. In both cases the integrated system must meet several interoperability requirements, ranging from common network connectivity to semantic agreement requirements.

The cornerstones of the HLA, the Framework and rules, Federate Interface Specification and the Object Model Template, correspond on a conceptual level with the constituents of the SIF. C2 systems participating in a SIF configuration must adhere to certain rules. These rules should not be too constraining, but a basic level is needed in order to reduce heterogeneity and ease an integration effort. Similar to the interface specification of the HLA, SIF must specify a standard set of services that the run-time component of the SIF architecture exposes (the broker). Finally, a standardized way of describing a system in a SIF context must be provided similar to the HLA OMT, i.e. a formal specification of the semantics of information handled by the system. Apart from this, a governing process, similar to FEDEP is required to control integration/development and use/execution of a C2 system configuration. The next sections outline a blue-print for this process.

5.2. Concepts and Activities of SIDEP

Similar to FEDEP in HLA, it is possible to define a formal process for configuring and using C2 systems in the context of SIF. Since such a configuration task can be rather complex, an integrated, process-centered approach for managing activities is needed. A well-defined semantic interoperability management process can be used to guide the ordering of SI activities and thereby make the whole SI task more systematic and efficient.

Following the proposal for SIF described in Section 3, as well as the given descriptions of HLA and FEDEP (Section 4), in what follows, we have defined a management process for SIF, namely SIDEP - Semantic Interoperability Development and Execution Process. A number of related collaboration and interoperability frameworks, such as ebXML [12], Open-EDI [13] and COA [14], have been jointly considered to distinguish major SIDEP phases. FEDEP has then been considered as a related basis for the elicitation of particular activities in each of the process phases.

We view SIDEP as *the process of preparing and executing a semantic interoperability task between two or more C2 systems*. A high-level conceptual meta-model for SIDEP is shown in Figure 3.

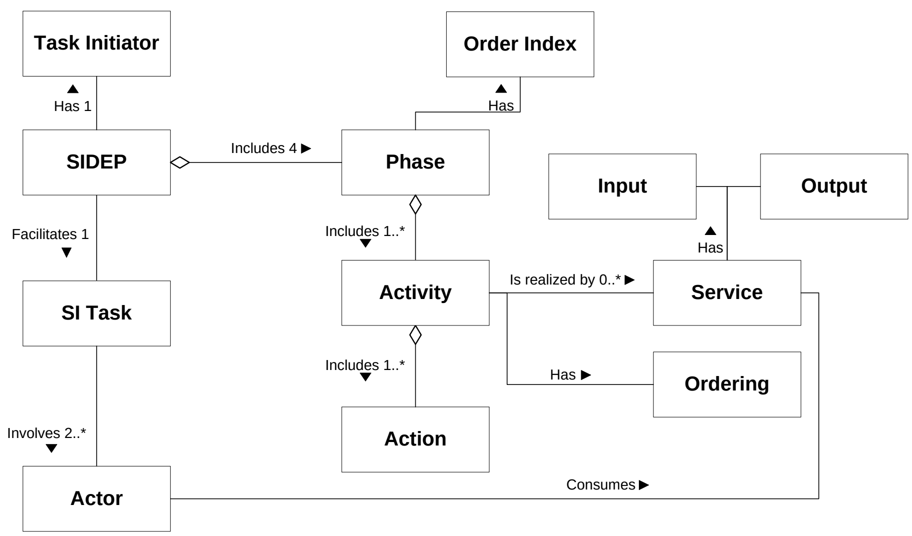

Figure 3: A high-level conceptual model for SIDEP.

In the meta-model, the SIDEP concept represents a management process consisting of four *Phases* - *Preparation*, *Configuration*, *Operation* and *Post-Operation*. SIDEP facilitates a *SI Task* initiated by *Task Initiator* and involving at least two *Actors*. Every Phase is a distinct sub-process within SIDEP, having an *Order Index* that determines its position in the phase sequence. A SIDEP Phase includes one or more *Activities*, which are executed according to *Ordering*. An *Activity*, containing one or more *Actions* is considered to be implemented as a *Service* of SIF. A service can be internal to SIF, or external, when consumed by an *Actor* participating in a semantic interoperability task. Every service has *Input* and/or *Output*, which represent required and produced artefacts respectively.

In Figure 4, the four major SIDEP phases are depicted, together with containing activities.

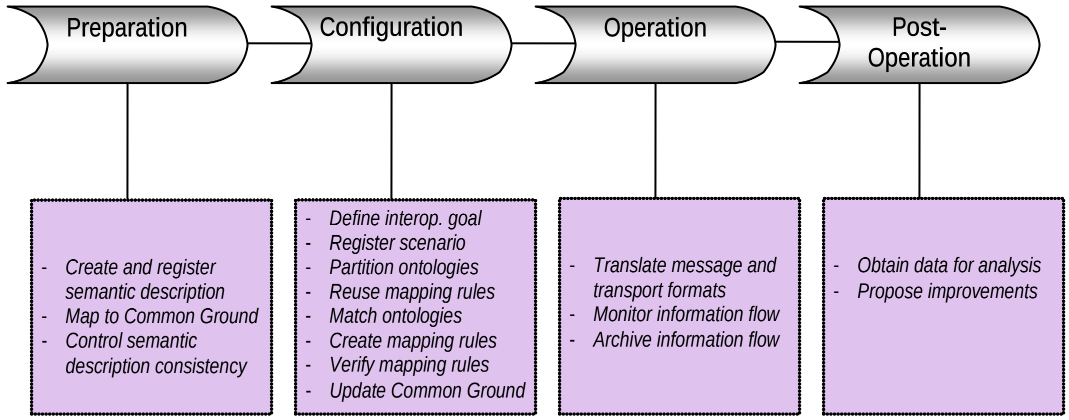

Figure 4: SIDEP phases and activities.

The phases are: Preparation, Configuration, Operation and Post-Operation. The Preparation is an "off-line" phase, where the military organizations accommodate their system by new capabilities required for knowledge based semantic interoperability according to SIF. When a certain operation and the goal for it have been specified, the Configuration phase will start to harmonise the semantic descriptions of the heterogeneous participating systems in the operation. The Operation phase is the only online phase from a military perspective where the configuration is completed and the SI tasks are executed with the support of SIF realizing the message exchanges between the involved systems. The last phase, Post-Operation, concerns analysis and evaluation of the results to be able to propose improvements for future uses. Below, we describe in details the responsibility of each of the phases.

Phase 1: Preparation

The Preparation is an "off-line" time segment in SIF. During this phase, individual actors such as military organizations or units use SIF (independently of each other) to perform a number of grounding activities.

FEDEP itself does not encompass such grounding activities, as the process starts by the publication of a common simulation goal. However, the Preparation phase could be compared to the Planning phase in the Open-Edi framework [12], where each actor interested in an e-collaboration, is responsible to define and register the actions which he will perform in the transaction. In the SIF context, the focus is on managing information, i.e. semantic-level descriptions of each actor planning to be engaged in a SI task using SIF. We have elicited the following set of the activities for the Preparation phase:

1. *Create and register semantic description*

   Here, the actor is supposed to create and submit the model of its knowledge-base to SIF in the form of a semantic-level description. The core requirement here is that the given document must describe the included information on a *semantic level* and in a *machine-readable* form. This may include different kinds of ontology descriptions, i.e. descriptions provided in RDF [15], OWL [16], or some other semantic-level language. The semantic description should provide a structure of all the information concepts, their relationships and constraints expected by the actor to be relevant for his future SI tasks. Following the meta-model given in Figure 3, this activity, as any other, is implemented as a SIF service. The input of the service is the semantic description, which is checked by SIF for compliance with accepted formats for semantic-level artefacts. If the semantic description complies, the document is stored in the semantic description repository of SIF, otherwise the actor has to re-design or edit its semantic description and then re-submit it to the framework.

2. *Map semantic description to Common Ground*

In this activity, the registered semantic description will be mapped to a reference knowledge-base of resources that act as a semantic foundation within SIF. These resources will be used in order to create consistent ontology mappings between the semantic descriptions delivered by the independent actors. Thus, all the information resources that can be useful for bridging the semantic gap between the systems that interact should be addressed in the Common Ground; these resources must have a formal representation that can be processed by computers, e.g. ontologies. This activity is realized with a corresponding service internal to SIF.

3. *Control consistency of the registered semantic description*

   Here, an internal service of SIF is executed, to perform a detailed consistency checking of the registered semantic description. In case of the use of OWL for semantic description representation, both the classes and the individuals are checked, by invoking a reasoner (a software tool that automatically checks the consistency on both the class and individual levels). In this way the semantic description is verified for the correctness, such as if the class part is correctly structured, and if the individuals follows the relationships and the constraints of the related classes, etc.

Phase 2: Configuration

According to FEDEP, preparing the execution of a federation is the most extensive effort. It encompasses five phases, starting from “Specify goal” to “Test federation”. Similarly, the Configuration phase in SIDEP encompasses all the essential activities related to the constitution of a common semantic base for a given interoperability task.

The activities considered for this phase, are as follows:

1. *Define and register the interoperability goal.*

   In the FEDEP process step “Specify goal” the stakeholders document an end-goal for a simulation. Similarly in SIDEP, a need or decision for undertaking a semantic interoperability task involving a number of actors must be elicited in form of an objective. Thus, it is the responsibility of the unit enrolling as a task initiator/leader to submit a description of the task objective. This activity is realized by submitting a goal document through the corresponding service of SIF.

2. *Register scenario*

   The FEDEP step "Perform conceptual analysis" describes what resources / entities are involved in a specific context (operation / mission), their behaviours, and their peer relationships. The result is a set of requirements that forms the basis for the actual integration in a later step. Here, Base Object Models (BOM) may play an important part as a basic building block when constructing the conceptual model. In the SIDEP context this step is equated to the need for defining a scenario, where the functions to be performed and the responsibilities (i.e. actors) are clearly described and related. The task initiator submits the scenario as a structured document through the corresponding service of SIF. As a result, the scenario is registered as a SI task (corresponds to the SI Task concept in the meta-model).

3. *Partition ontologies*

   The FEDEP step "Design federation" designs a new federation, either from “scratch” or by reusing existing designs. Within SIF, this step corresponds to the need for relating a registered scenario to the semantic descriptions of the actors involved in the scenario. In particular, ontologies retrieved from a semantic description, which may be huge, are reduced so as to cover only the vocabulary relevant to the given scenario, i.e. to the SI task. This ontology modularization facilitates a more efficient ontology management throughout a SIDEP. In [17], we have argued that military tasks can be of different size - in certain situations a task could be described with a single sentence, while in others, it may require a longer scenario. Following that, we proposed a “task”-oriented ontology modularisation (i.e. partitioning), i.e. an approach where the boundaries of the extracted semantic descriptions are derived from the given task description.

4. *Revisit mapping rules and ontologies*

   This activity is used to retrieve the mapping rules between the considered ontologies, if such exists from previous SI task executions. The corresponding service is thereby implemented to search the SIF repository for existing mapping rules of the ontologies in the task consideration.

5. *Match ontologies*

   The FEDEP step "Develop federation" corresponds to the ontology matching step in SIDEP. In this step, ontology operations are invoked (on the ontology repository) to match ontologies, i.e., to find the relationships between semantically related concepts across ontologies. The output of the activity (i.e. service) is a list of similarities between concepts.

6. *Create mapping rules*

   Here, the goal is to establish mapping rules (translations between ontologies) based on the concept matches found in the previous step. This mapping process is a tedious process, commonly requiring the use of different techniques to determine correct levels of similarities between the concepts. In other words, an attempt is made to identify and analyze the correspondences between what system A can send and what system B can receive. The result of ontology mapping operations is used to define the transformation that must be performed on the information to make the recipient able to interpret the contents in a semantically correct way. Transformations must be computable, i.e. readable, in a programmatic sense on how to process the input message to create the output message.

7. *Verify and Validate mapping rules.*

   Following the “Test federation” step in FEDEP, in a corresponding activity in SIF, the results of the aligned ontologies are verified and validated by testing the mapping rules against a limited number of concept instances (i.e. on a small scenario part), to ensure correctness of the mappings.

8. *Expand Common Ground*

   In this activity, the validated mapping rules and the concepts to which they concern are added to the reference knowledge-base of SIF (i.e. Common Ground) for the future reuse.

Phase 3: Operation

The FEDEP process step "Execute Federation” corresponds in the SIF context to the “Operation” phase where the configuration is completed and the SI task is executed with the support of SIF realizing the message exchanges between the involved systems. The corresponding activities in SIF are accordingly structured:

1. *Translation*

   In the case of FEDEP, a federation integrates federates through the services that the run-time infrastructure provides. In a similar way, SIF provides "run-time” services, primarily focusing on the translation between different message representation formats, and contents according to the mapping rules defined in the Configuration phase. Those services are internal to SIF, i.e. once the execution is initiated by an actor, the rest of the actions are done by SIF.

2. *Monitor information flow*

   As in FEDEP, the ongoing executions are monitored and registered. Exchanged messages are monitored by a SIF internal service in order to trace and present the information flow.

3. *Archive information flow*

   The complete flow of data is in addition registered in a log-based structure of the SIF repository to enable subsequent offline analysis.

Phase 4: Post-Operation

The FEDEP process step "Analyze and Evaluate Results" gives rise to corresponding activities in the phase "Post-operation" in SIDEP. In this phase the execution of the SI task is completed and experiences from the activities undertaken are collected and documented. From the SIF perspective, it is of the major importance to determine *if the information exchange has met the task objective*, i.e. if the given scenario is realized and in what extent (i.e. how the information exchange have satisfied a required precision / quality). In addition, the obtained results should be used as a basis for improvements of executions of further SI tasks. Post-operation is mostly done “offline” using the execution-time data. It involves a number of activities:

1. *Obtain data for operation analysis*

   This activity relies on a corresponding SIF service, which can be invoked to obtain different data artefacts, such as: applied mapping rules, the list of exchanged messages, applied conversions, reported errors, etc. Further activities are performed by the involved actors, i.e. outside of SIF.

2. *Perform analysis and propose improvements*

   As many as possible of the artefacts, such as mapping rules created during a SIDEP, should become available for future use to facilitate more efficient collaborations. It is therefore of the interest for each actor who participated in the executed task to engage in a number of analysis and improvements activities, such as:

   a. Analyse “conversions” to perceive how the information alignment can be more effective in the future.
   b. Propose improvements.
   c. Change definitions of organisation concepts and terms to update semantic descriptions according to the proposed improvements.
   d. Propose extensions to/changes of Common Ground according to the recommended improvements.
   e. Propose changes to the organisational policies according to the proposed improvements.
   f. Propose technical improvements in the framework, e.g., additional activities and services or change of existing ones.
   g. Rehearse the SI task to test in a local and limited context the proposed improvements.

The above proposed meta-model for SIDEP and the included activities and services scope a high-level architecture for a semantic interoperability framework. The two middle phases of SIDEP, Configuration and Operation phases, are highly important as they are mandatory in managing SI tasks (i.e. even when actors have not changed their knowledge bases (i.e. semantic descriptions), at least setting the task goal, and realizing it through an execution are mandatory activities). On the other hand, Preparation and Post-Operation phases are also important as the first one manages creation or changes in the semantic descriptions of the actors, and the last one is essential for improving efficiency of future SI tasks.

6. Conclusion and Future Work

In this paper we have investigated how concepts and methods from the Modeling and Simulation (M&S) research discipline could facilitate in fulfillment of the requirements for SIF, a NATO-initiated semantic interoperability framework. The framework builds on a knowledge-based approach utilizing emerging semantic technologies, such as ontologies.

We have argued that both SI and M&S areas share a need to create configurations of systems where information exchanged are interpreted similarly among all participating parties, preserving the intended meaning. Therefore, it is of a great interest to revisit the results from the M&S community which has studied similar issues for many years and apply these results to SIF which is still under development.

Interoperability has been of major concern within M&S for years, especially in connection with standards for distributed simulations, such as High Level Architecture (HLA) and Federation Development an Execution Process (FEDEP). Distributed simulation has successfully created conditions for integration of simulation models, but has been mostly concerned with interoperability at the syntactic level. However, two very important results from distributed simulation seem to be relevant to SIF. The most important result is FEDEP, the standardized process for developing and execution of distributed simulations configurations. Following the activities of FEDEP and their ordering, we proposed a management process for semantic interoperability, namely the Semantic Interoperability Development and Execution Process (SIDEP).

SIDEP is aimed at governing the development and execution of system information exchange to meet expressed business requirements on interoperability tasks. To formalize the aspects of SIDEP we have defined a core meta-model where the four distinct process phases of SIF are in focus, followed with included activities and the services realizing those activities.

As already discussed, this is a high-level conceptualization of a semantic interoperability framework. Looking ahead, we intend to further refine its aspects, especially in respect to flexibility of use and service orientation. In order to facilitate a system-based validation of correctness of individual SIDEPs, we also plan to formalize further the SIDEP meta-model in the form of an OWL ontology [16], and to describe executable SIF services on a semantic level, using an ontology for Web services such as OWL-S [18].

Further more, we intend to implement SIF and its management process SIDEP in a service-centric semantic broker and use the prototype to validate and evaluate the usability and efficiency of SIF and SIDEP. We assume that this activity will provide additional input for further improvements on both technical and conceptual design levels.

7. References

1. Semantic Interoperability Context, Issues, and Research Directions (1994), Paul Johannesson, M. Hasan Jamil, Proc. of the Second International Conference on Cooperative Information Systems, 180 – 191.
2. Semantic Interoperability, Final Report of NATO Task Group IST-075, RTO Technical Report TR-IST-075, 2010.
3. Gruber, T.R., “Toward Principles for the Design of Ontologies Used for Knowledge Sharing”, In: Guarino, N., Poli, R. (Eds) International Workshop on Formal Ontology in Conceptual Analysis and Knowledge Representation, Padova, Italy, Kluwer Academic Publishers, Deventer, The Netherlands, 1993.
4. Noy, N.F. and McGuinness, D., “Ontology Development 101: A Guide to Creating Your First Ontology”, Technical Report, Stanford University, 2001.
5. Hameed, Adil, Preece Alun and Sleeman Derek, Ontology Reconciliation. In Steffen Staab and Rudi Studer, editor, Handbook on Ontologies, Chapter 12, page 231-250. Springer Verlag, Berlin (DE), 2004.
6. 1516-2010 IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) – Framework and Rules.
7. 1516.1-2010 IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) – Federate Interface Specification.

8. 1516.2-2010 IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) – Object Model Template (OMT) Specification.
9. 1516.3-2003 Recommended Practice for High Level Architecture (HLA) Federation Development and Execution Process (FEDEP).
10. SISO-STD-001.1-1999 Real-time Platform Reference Federation Object Model (RPR FOM 1.0), http://www.sisostds.org/DigitalLibrary.aspx?Command=Core_Download&EntryId=30823.
11. B. Möller, K.L. Morse, M. Lightner, R. Little, R. Lutz, HLA Evolved – A summary of Major Technical Improvements, 08F-SIW-064, Fall Simulation Interoperability Workshop, 2008.
12. EbXML, OASIS Standard for E-Business Colalboration, http://www.ebxml.org/, last accessed 30.01.2011.
13. Open-Edi ISO/IEC, "Operational aspects of Open-edi for implementation", ISO Standard 15944-1, 2002.
14. COA, Jericho Group Collaboration Oriented Framework, http://www.opengroup.org/jericho/COA_v1.0.pdf, last accessed 30.01.2011.
15. RDF, W3C Resource Description Framework, http://www.w3.org/RDF/, last accessed 30.01.2011
16. OWL, W3C Web Ontology Language, http://www.w3.org/TR/owl-features/, last accessed 30.01.2011
17. Mojtahed V., Eklöf M. and Zdravkovic J., FOI report on Semantic Interoperability, "Semantisk Interoperabilitet – Slutrapport för projektet Semantisk interoperabilitet, 2007-2009", FOI-R-- 2846—SE, 2009.
18. OWL-S, W3C Web Ontology Language for Web services, http://www.w3.org/Submission/OWL-S/, last accessed 30.01.2011.