Computer Generated Forces - Integration into the Operational Environment

Andreas Tolk, Ph.D.

Virginia Modeling Analysis & Simulation Center (VMASC)
Old Dominion University
7000 College Drive, Suffolk VA 23435
+1-757-686-6203
atolk@odu.edu

ABSTRACT

In closed combat simulation systems CGF modules are most often used to generate orders in given or perceived situations. They can be interpreted as command entities getting information about the battlefield and generating the respective orders, information messages, and requests for the superior command, their neighbours, and the subordinate command entities or units.

In order to facilitate the reuse of CGF-modules as the reuse of observations of the real world of Command and Control, it is highly recommended to use a reference data model. This reference data model should address the information exchange requirements (IER) on the battlefield being used by real decision makers. A matured data model being developed by analysing the IER of NATO and national military operations on all levels of command by data modelling experts from several NATO countries is the data model of the Army/Allied Tactical Command and Control Information System (ATCCIS), now becoming a NATO STANAG ADatP-32 as the Land C2 Information Exchange Data Model (LC2IEDM). This data model also is used for data management by the NATO Data Administration Group (NDAG) as well as by some national data management agencies.

This paper gives the architecture, shows benefits and limitations, and introduces a way for real reuse of CGF modules within several federations. The High Level Architecture (HLA) builds the technical framework.

1 Introduction

This paper is dealing with the integration of the results of the research domain "computer generated forces" as a special branch of the wider application field of simulation systems. The content is mainly based on three papers: [Krusche and Tolk 1999], [Tolk 1999] and [Tolk 2000a]. These three papers can be seen as a series of ideas having been born within the Data Mediation Think Tank at IABG within the last three years [Krusche et al. 2000]. These ideas result in a general integration framework for applications of military information technology, i.e., command and control systems, simulation systems, or also computer-generated forces federates.

Originally, the kernel ideas have been born within the academic world of federated databases [Sheth and Larson 1990]. Federated databases are a more general view on distributed databases, where no common data schema for replication is necessary, but the databases themselves can be heterogeneous, autonomous, and also distributed managed. For a general introduction into this domain, the study of the book [Özsu and Valduriez 1991] as well as the articles by Sheth and Larson are recommended. For interested people who are able to understand German, the German book [Conrad 1997] is also a valuable source.

The challenge to merge distributed, heterogeneous, and autonomous data sources into a common operating picture is also formulated for command and control systems. A first try to use the theory of federated database systems to do so was presented during the Joint Warrior Interoperability Demonstration 1999 (JWID 99) and is documented in [NC3A 1999]. Germany and the UK are following this path to gain long-term interoperability for their national systems. Crucial for the benefit of these efforts is a common data management with respective IT support. For this purpose, NATO

Paper presented at the RTO SAS Lecture Series on "Simulation of and for Military Decision Making," held in The Hague, The Netherlands, 10-11 December 2002, and published in RTO-ENP-017.

has established the NATO Data Administration Group (NDAG). However, there are other alternatives that are not pushing forward to such a strong paradigm shift like the federated solution approach.

Anyhow, for the simulation community, the idea of federations is not very new. They are dealing with distributed, heterogeneous, and autonomous data sources since the days of SIMNET, followed by the distributed interactive simulation (DIS), advanced level simulation protocol (ALSP), and finally the high level architecture (HLA). However, the idea of a standardized common information exchange model is also a new challenge to them. The logical idea therefore is to merge the ideas of the high level architecture and federated databases to a new common approach, leading on the long term to a new generation of Warfighter supporting IT systems comprising the necessary functionality (command and control, consultation, intelligence, surveillance, reconnaissance, simulation for training, simulation for decision support, etc.) in modules plugged into a common integration framework like described, e.g., in [Tolk 2000b].

The paper tried to catch the main ideas of the referred papers in a comprehensive manner. For more details, please evaluate the original papers directly.

2 Databases, Data Management and Command and Control Solutions

Each organization in the domain of defence depends on access to information in order to perform its mission. It must create and maintain certain information that is essential to its assigned tasks. Some of this information is private, of no interest to any other organization. Most organizations, however, produce information that must be shared with others. This information must be made available, in a controlled manner, to any authorized user who needs access to it.

At present, almost every defence information infrastructure exists as a collection of heterogeneous, non-integrated systems. Each organization builds systems to meet its own information requirements, with little concern for satisfying the requirements of others, or of considering in advance the need for information exchange. The information sharing that currently occurs is performed through many, point-to-point interfaces, typically through a defined message or file-transfer format. Some message formats are clearly defined (e.g. ADatP-3 and Data Link messages). For the most part, however, information exchange is based on ad hoc interfaces. The result is an extremely rigid information infrastructure that costs months and millions to be changed or extended, and, which cannot cope with the increasing demand for widely integrated data sharing between multiple mission-related applications and systems.

2.1 Federated Databases for Distributed, Heterogeneous, and Autonomous Data

Before starting with the military application of integrating several components comprising the needed functionality into a general integration framework, the ideas of building federated databases for distributed, heterogeneous, and autonomous data will be introduced. Therefore, we will follow the way of [Conrad 1997] starting with homogeneous local databases and coming via the distributed homogeneous databases to federated solutions. The same initial stage is also chosen in [Tolk 2001].

The ANSI/X3/SPARC of the American National Standards Institute standardized the three level schema for homogeneous local databases. The lowest level is the physical or internal schema. This is the system dependent implementation of the system independent conceptual schema, which is the second schema. The conceptual model comprises the complete data that can be stored within the database. As every application may have its own view of the data in doesn't need to know about all the other details (for reasons of security as well as integrity of the data, juristic questions, etc.), there is an external schema for every application comprising just the data subset with the respective rights to read, write, and add new data needed for the functionality provided by the application. Therefore, internal, conceptual, and external schemata are the three standardized levels.

When distributing such a homogeneous database, an additional level is needed. Again, [Özsu and Valduriez 1991] define one external schemata for every application, however, the conceptual data scheme becomes now the common schema for replication, i.e., this is the common data model for all participants/databases. All databases are joining the same common data model. Anyhow, it may not be necessary to store every table and detail in every local database. Therefore, local conceptual schemata are introduced that have to be implemented using the respective local internal schemata. Therefore, local internal, local conceptual, conceptual, and external schemata are the four levels for distributed homogeneous databases. This is the right technique for a homogeneous system, e.g., a network of command and control systems of the same kind within a headquarter. It is also the mid-term way followed in the operational environment. The Warfighter IT systems of the next generation should be able to share data using data replication instead of just sharing and interchanging messages. Especially in the US the efforts to use a common data model – at least for the services – is a favoured idea.

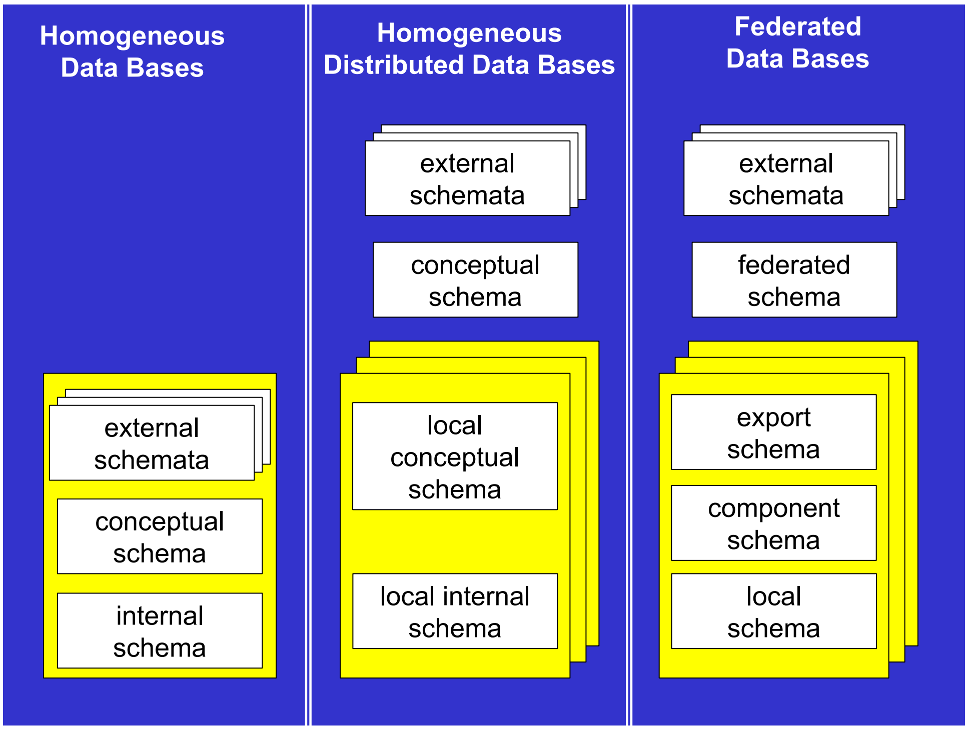

Figure 1: Schemata Levels in Databases

However, when having to deal with the integration of legacy solutions, new approaches are needed. In joint and combined operations, the availability of a common IT environment will be a pure wish for a long time. In addition, the different partners will prefer to work with the system they know the best: their own. The approach using a common conceptual data model cannot be used, as every legacy systems already has one of their own. Within such an environment, integration methods are needed that are able to cope with existing autonomous, heterogeneous systems that have to work together – often on an ad-hoc basis. This can be done using the ideas of federated databases, also used in the domain of electronic commerce, e.g. in the area of Collaborative Product Commerce (CPC), see [Krusche and Tolk 2000] for some details.

Therefore, Sheth and Larson introduce a new five level architecture in [Sheth and Larson 1990]. Every application has again its own data view, the external schema. They are based, however, on a so-called federated schema being the common data exchange data model for all participants. Different from the conceptual schema of distributed homogeneous databases, the federated schema only comprises the shared data elements and doesn't deal with all details of the local autonomous databases.[1] The local

---

[1] This enables the evolutionary growing of the common data exchange model based on the actual information exchange request being formulated between the global applications and the local databases. In the moment, a new data piece is needed in a global application, it becomes part of the federated schema. However, the local databases don'' have to be changed as long as the piece of data is already comprised in one of them.

databases are contributing to this federated schema their part by export schemata comprising the data to be shared by the local database with other databases. Each export schema is part of a local component schema, which is a common presentation of the data elements being comprised in the local, system dependent schema. Therefore, the five levels are external, federated, export, component, and local schemata.

The influence of this technique on continuously interoperable solutions for the Warfighter is described also in [Tolk and Kunde 2000] and [Krusche and Tolk 2000]. Many application examples can also be found in [Krusche et al. 2000].

2.2 Standard Data Elements

Fundamental to any systems' interoperability are standard data elements, i.e. those data elements that have a concise, unambiguous, and agreed, syntactic and semantic definition. These data elements must be considered as an operational asset, which, like other organizational assets, must be managed effectively and organized to facilitate access by those who require it, in accordance with the need-to-know principle and agreed security regulations and constraints. This is also a central idea within the concept of the shared data environment (SHADE), see [DISA 1996].

The definition of standard data elements required for information exchange, the coordination and control of their implementation and use within systems are central objectives of an overall data management organization, which will be described in more detail in the next section.

An important outcome of the data management is a common (shared) data model, which defines how each standardized element of information is represented, and, which also provides a common guideline for system developers of future systems.

In order to meet the migration requirements of existing system components and systems, standard data elements and its common representation must be accompanied by standard mapping rules, which allow the as-is meta data from a system to be defined in terms of the common standard data model when the data meaning is established.

Fundamental to the realization of the migration requirements are standard data access mechanisms, which implement standard data and mappings and allow users to access and interchange as-is data without knowing information about the common, standard data representation. The access architecture contains the data mediation capabilities required to provide the user with this transparency.

The main aspects to achieve systems interoperability,

- a data management organization,
- a common shared data model, together with standard mapping rules, and,
- a common data mediation mechanism for migrating existing system components and systems,

reflect the central conceptual features of the SHADE.

The approach towards systems interoperability, described in this paper, stresses the fundamental meaning of an overall data management, promotes the ATCCIS Generic Hub [NATO 2000] as an appropriate basis for the common, shared data model, and, introduces a data mediation framework as a common mechanism to interconnect heterogeneous system components and systems, thereby extending the SHADE approach.

2.3 Data Management

The overall objective to be reached by introducing a data management is, to coordinate and to control the numerous system projects technically and organizationally, in order to improve the integrity, quality, security and availability of standard data elements. Due to this objective, the following central tasks of the data management organization are proposed:

- Definition of standard data elements across system boundaries,
- Evolutionary development of a common shared data model as a reference representation for standard data elements,
- Representation of standard data elements through a common shared data model,
- Definition of rules and methods for
  - access, modification and distribution of standard data elements,
  - introduction of new information exchange requirements,
- Coordination and Control of system projects using the standard data elements in order to assure their consistent use and interpretation within different applications and systems.

Thus, data management is planning, organizing and managing of data by defining and using rules, methods, tools and respective resources to identify, clarify, define and standardize the meaning of data as of their relations. This results in validated standard data elements and relations, which are going to be represented and distributed as a common shared data model.

An appropriate reference representation of standard data elements, as an important product and outcome of the data management activities directly enables the standardization results to be implemented in future system components (i.e. database systems, applications), and, provides a common basis to interconnect existing systems through a data mediation framework. The following figure depicts the practical use of Data Management for the configuration of Data Mediation Layers as described in more detail in [Krusche and Tolk 2000].

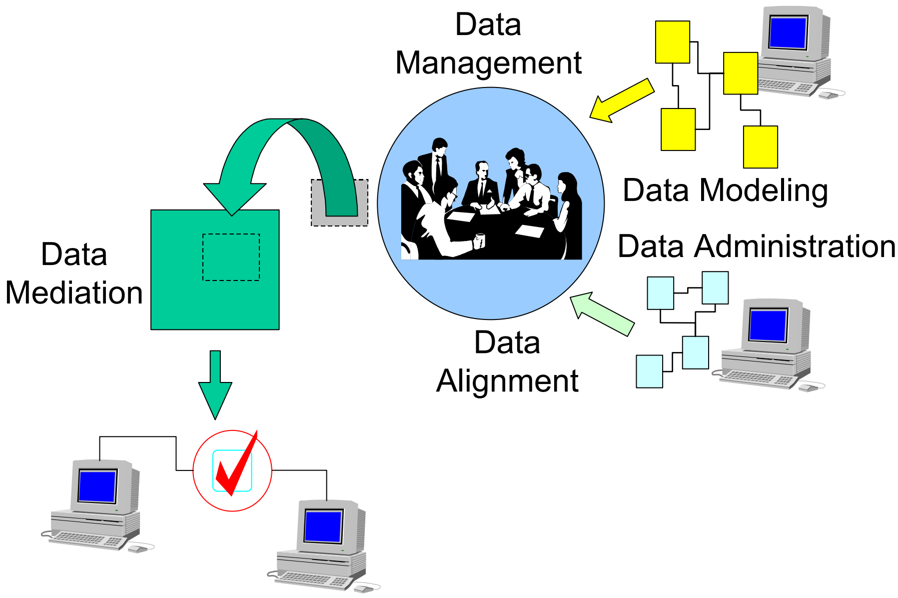

Figure 2: Using Data Management Results for Integration

A common (shared) data model must fulfil the following two main requirements:

- It must capture the information requirements of a wide range of battlefield functional areas. A common shared data model is best characterized as a "to-be" model of the required battlefield information rather than a model that is constructed with direct reference to existing current needs for information exchange.

- For flexible integration of future information (exchange) requirements, the data model must be constructed in a way that future information elements simply extend the model while its existing structure remains unchanged.

The ATCCIS data model [NATO 2000] meets both requirements quite well, as it has been designed to meet exactly these requirements by data modelling experts of almost all nations in NATO during the last 10 years.[2] It will be explained in more detail in the next section.

2.4 Data Modelling with ATCCIS/LC2IEDM

In 1978, NATO's Long-Term Defence Plan (LTDP) Task Force on Command and Control (C2) recommended that an analysis be undertaken to determine if the future tactical Automatic Data Processing (ADP) requirements of the Nations, including that of interoperability, could be obtained at a significantly reduced cost when compared with the approach that has been adopted in the past. In early 1980 the then Deputy Supreme Allied Commander Europe initiated a study to investigate the possibilities of implementing the Task Force's recommendations. This was the birthday of the ATCCIS Permanent Working Group (APWG) that is dealing with the challenge of the future C4I systems of NATO. Today, the ATCCIS ideas have matured sufficiently and, thus, ATCCIS is on its way to become a NATO Standardization Agreement (STANAG).

ATCCIS is much more than just another data model. It is designed to be an overall concept for the future C4I systems of the participating nations.

However, one of the most important topics of ATCCIS is that each nation still can build independent systems with their own "view of the world" and respective applications, business rules, implementation details, etc. Thus, ATCCIS is not designed to be a "buy or be out" product, but is defining a common kernel to facilitate common understanding of shared information and, therefore, facilitating facing the general challenge to reach interoperability.

The Army/Allied Tactical Command and Control Information System (ATCCIS) comprises

- the ATCCIS data model (including a standardized common generic hub and subfunctional areas of national concern),
- the ATCCIS system architecture (with a kernel of common access points to the logical ATCCIS data model on the one side, and access points to standard communication protocols like TCP/IP on the other),
- the ATCCIS Information Resource Dictionary System (AIRDS) with references about information and information structure and context for each data element, and
- the ATCCIS Replication Mechanism (ARM) allowing internal communication by user driven and specified database replication between two ATCCIS compliant systems.

In the context of this paper, we will focus on the data model. When talking about the ATCCIS data model one has to distinguish between the Generic Hub (GH), which is a kernel of data elements common to all application areas of ATCCIS, and the so called Subfunctional Areas (SFA), which extends the Generic Hub to a degree of a special application, e.g., fire support, personnel, etc.

---

[2] Only recently, the work of the Army Tactical Command and Control Information Systems (ATCCIS) Permanent Working Group become considered as a new NATO standard for information exchange. The new name is Land Command and Control Information Exchange Data Model (LC2IEDM). However, it should be stressed that the references ARMY as well as LAND in the data model names are misleading in some way. ATCCIS is not an army data model, but an ontology to structure knowledge of the military domain in a consequent and coherent way. In Germany, the ADatP-3 messages of the Maritime Headquarters and the Destroyers, the Link 11 and Link 16 as well as the OTH Gold messages have been harmonized using the ATCCIS data model, therefore, the model can be seen to be proved to be able to be extended in a controlled manner to comprise information for army, navy, airforce, and joint operations and respective forces.

The ATCCIS Generic Hub data model is intended to represent the core of the data identified for exchange across multiple subfunctional areas and multiple views of the requirements. Toward that end, it lays down a common approach to describing the information to be exchanged in a tactical command and control environment. Thus, the approach is generic, i.e., it is not limited to a special level of command, force category, etc. It moreover tries to catch the idea of object oriented modelling for data modelling by starting with very basic concepts of data – like object items, object types, actions, facilities, etc. – and allowing the specification of, gradually, more and more details in order to match real instances on the battlefield.

To summarize, the data model needs to describe all objects of interest on the battlefield, e.g., organizations, persons, equipment, facilities, geographic features, weather phenomena, and military control measures such as boundaries using a common and extensible data modelling approach.

The following figure shows the key entities of the Generic Hub data model. The five key entities can be described as follows:

- An OBJECT-ITEM is an individually identified object that has military significance.
- An OBJECT-TYPE is an individually identified class of objects that has military significance.
- A CAPABILITY is the potential ability to do work, perform a function or mission, achieve an objective, or provide a service.
- A LOCATION is a specification of position and geometry with respect to a specified frame of reference.
- An ACTION is an activity, or the occurrence of an activity, that may utilize resources and may be focused against an objective

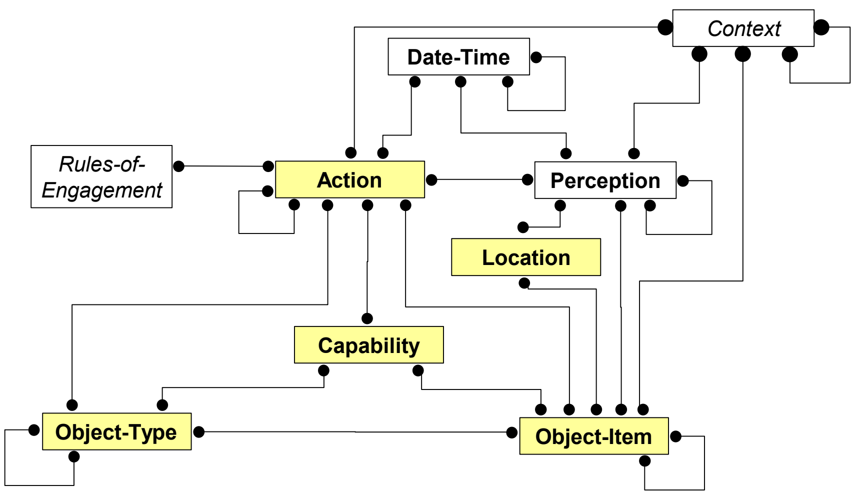

Figure 3: Key Entities on the Hierarchy Level of the Generic Hub

For each key entity, several levels of subtree hierarchies can be derived – and have been standardized to a certain degree – by introducing new categories of OBJECT-ITEMS, OBJECT-TYPES, CAPABILITIES, ACTIONS and LOCATIONS.

The following figure illustrates this for the first two levels of the OBJECT-TYPE and OBJECT-ITEM subtree hierarchies. Each object (be it type or item) can represent an ORGANIZATION, a PERSON, a sort of MATERIEL, a sort of FACILITY, or a sort of a FEATURE as immediate subtypes.

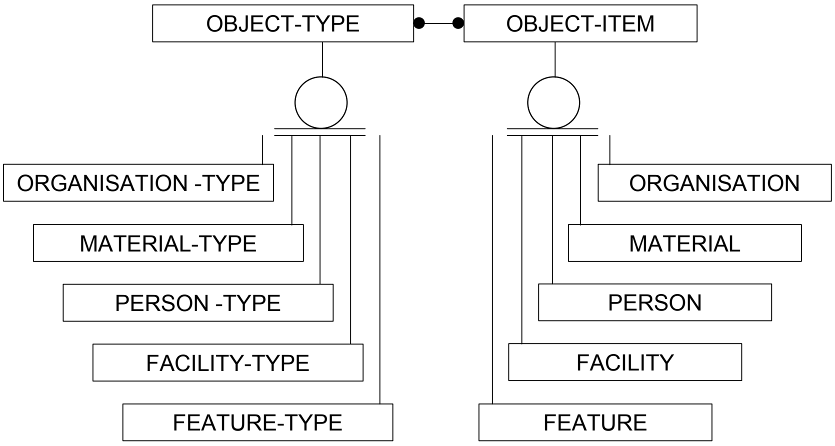

Figure 4: Subtree Hierarchy of OBJECT-TYPE and OBJECT-ITEM

The definitions are as follows:

- An ORGANIZATION is an administrative or functional structure.
- A Sort of MATERIAL is necessary to equip, maintain, and support military activities without distinction as to its application for administrative or combat purposes.
- A PERSON is a human being to whom military significance is attached. This includes not only soldiers, but civilians, refugees, and – if necessary – terrorists, paramilitary forces, or deputies of organizations with significance to the ongoing operations (e.g. Red Cross, NGO, etc.)
- A FACILITY is built, installed, or established to serve some particular purpose and is identified by the service it provides rather than by its content.
- A FEATURE encompasses meteorological, geographic, and control features that are associated with a location to which military significance is attached.

All definitions refer to the standard described in [NATO 2000] where additional examples are given. The data elements belonging to the generic hub of the ATCCIS data model are going to become an agreed standard between the participating nations. In addition to the elements described above they comprise data elements to model establishments, holdings, date and time, perceptions, contexts, etc. It is already possible to model rules of engagement, assessments, tasks, etc.

In order to be able to meet all information exchange requests not only today, but also in the future, it was necessary to establish a procedure to integrate new knowledge to be exchanged seamless into the existing information model. Thus, the subfunctional areas (SFA) were introduced catching special requirements using the same modelling scheme like the generic hub but being of national concern. However, the data elements of the respective SFA can be standardized also, if needed and wished. There is already work going on in the fields of intelligence, fire support, communications and electronics, logistics, and personnel. In a recent study in Germany it has been shown that an SFA for Military Operations Research and Modelling and Simulation can be derived from the analyses of respective data models of simulation systems also.

Every data element within an SFA being shared with another SFA has to become an element of the generic hub that comprises all shared elements. Every data element being special to an SFA is only shared within this area and is of national concern.

2.5 ATCCIS as a Shared Data Model for Command and Control and Simulation Systems

It should be clear by now that every information exchange requirement that exists between two headquarters – or a headquarter and a unit – can be modelled within the ATCCIS approach. Well known information exchange data will be found in the standardized Generic Hub of the ATCCIS data model. New pieces of information being explicitly new within a new operation or scenario can be modelled in a respective SFA for such classes of operations.

As mentioned before, in recent studies in Germany it has been shown that

- ATCCIS can be used as a shared data model for information exchange between C4I systems (including consultation systems) and
- ATCCIS can be used as a shared data model for information exchange between operation research and simulation systems also.

Therefore, ATCCIS can be used as a general shared data model for information exchange between all these systems as well. It will be shown in the next section that CGF modules – when being used as command agents – are simulated data twins of military headquarters. Thus, everything they want to know or want to communicate they can exchange with their counterparts using the language of ATCCIS. It is then part of the simulation – or another CGF module/federate – to retranslate ATCCIS into its own internal data presentation.

3 CGF Modules

Up to now, we have only talked about shared data models and communications between headquarters and units. It is now time to make the connection to the computer generated forces.

Following the definition of the NATO Long-Term Scientific Study LTSS/48, computer generated forces are “A generic term used to refer to computer representations of entities in simulations which attempts to model human behaviour sufficiently so that the forces will take some actions automatically (without requiring man-in-the-loop interaction)“ [NATO 1999b].

In this definition, forces are “Military entities as they are used in conflicts, peace support operations, and other engagements (operations) like disaster relief, and other civilian entities and individuals as they are engaged in actions represented in the simulation system” [NATO 1999b].

In general, CGF can be seen as intelligent simulated elements behaving in a simulated environment like a human or group of humans would do within the counterpart in the real world.

In this paper, the focus of CGF is military headquarters, i.e. simulated entities that have to generate orders for the effective entities within a simulation (combat units, combat support units, etc.). When doing so, they have to take several constraints into account: the objective and orders of their superior commands, their own resources, the perceived intention of the enemy, the situation of the neighbours, etc. Thus, we are focusing not so much on a model for a single person. We are dealing with a model for a group of persons, i.e., a staff making decisions.

3.1 A Modular Concept for Command and Control in Simulation Models

A modular concept for command and control in simulation models has been presented to the NATO SAS Panel on this topic in January 1999 in Paris, France [NATO 1999a]. It comprises effective entities, command and control modules, reconnaissance modules and communications modules.

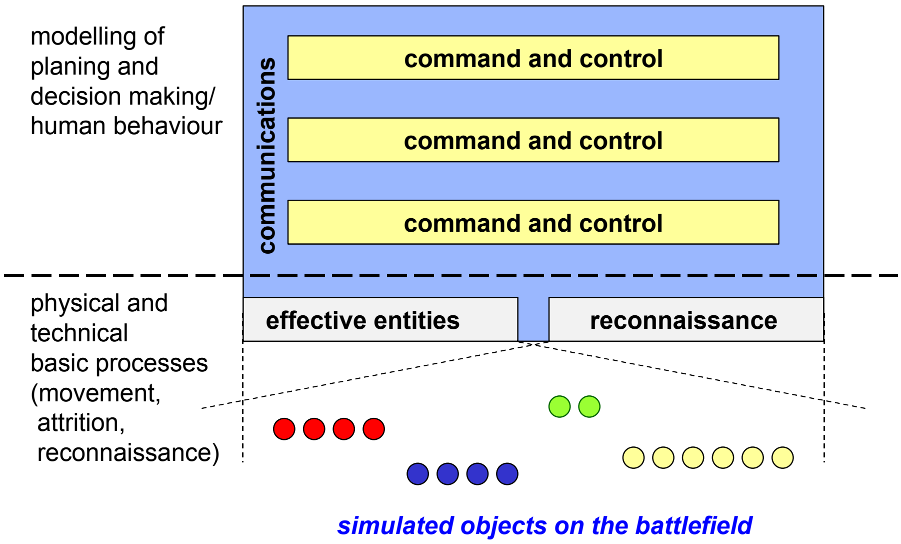

Figure 5: Modules for Command and Control Modelling

- The effective entities are used to model the physical and technical basic processes, i.e. movement, attrition, etc. They just receive orders that tell them what to do. They act and react as predefined taking into account their own actual perception of the situation. On the chosen level of abstraction, the entities receive orders and change their own as other status parameters respectively. This is the part of the simulation model application developers focused on until recently.
- Using a command and control module enables the application developer to model a command post or another element on the battlefield, which receives and generates orders, demands and situation reports. This module is the main topic with this section.
- The reconnaissance module gets orders and generates situation reports. To be able to do so, it groups atomic entities that are able to observe their environment with or without sensors in order to discover the status parameters of the other entities and inform respective command and control modules by predefined reports.
- Every order, demand and situation report must be transported by - i.e. passed via - an incarnation of the module communications. This module receives orders, demands and situation reports and deliver them, perhaps modified due to incoming information operations like jamming or introducing false reports or viruses changing the content of the data packages etc., from the source to the target.

The main driver for this architecture was the urgent need to add command and control functionality to existing or legacy simulation systems without having to rebuild everything. In addition, the new CGF modules were expected to be open and flexible enough to be used within various simulation systems. Therefore, the idea was born to build a CGF federate to be used within an HLA federation and being responsible for the decision processes on the different command levels.[3]

[3] With the simulation model FIT, in the meantime at IABG a respective model implementing this ideas have been successfully introduced. The approach of FIT is a topic of its own and his been presented on various symposia already, see, e.g. [Knoll 2000] or the proceedings of the 39. AORS at Ft. Leavenworth, Virginia, October 2000.

3.2 ATCCIS as a Language for CGF Modules

To be able to define such a federate, a general approach for exchanging information between CGF and other modules was needed. There are three principle types of partners to exchange information with.

- Superior command elements give orders and receive requests. In addition, situation reports are exchanged.
- With neighbours, situation reports are exchanged to be aware of potential dangers.
- Subordinate commands and/or units get orders and give requests. Again, situation reports are exchanged.

Thus, the information exchange comprises orders, requests and situation reports. For these information exchange requirements the data model ATCCIS can serve as a general shared data model. As it was designed to catch exact such information, it can be used to specify the content of the information to be exchanged between the simulated entities also.

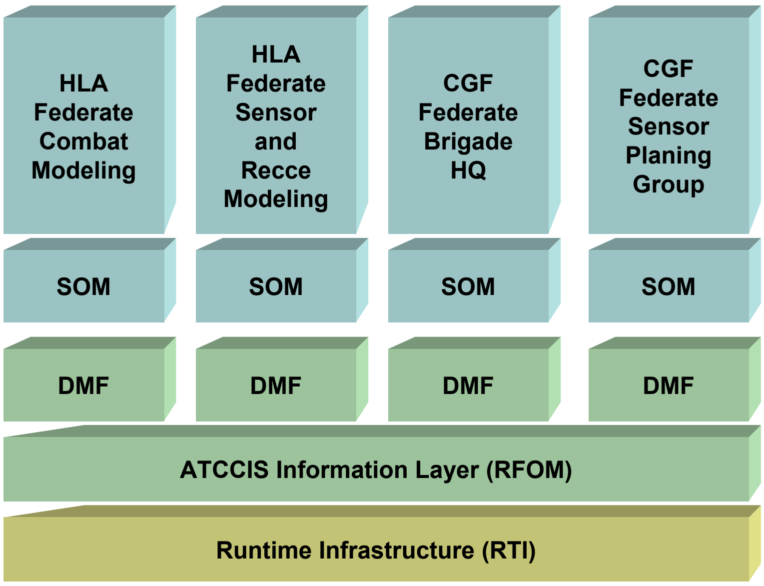

Figure 6: The General Information Integration Framework

The elements of the ATCCIS/LC2IEDM therefore can perfectly well serve as information objects to exchange the necessary data between the application modules of military IT systems.

3.3 Practical Example: The German Communications, Command and Control Model FIT

There are already applicable software implementations of these ideas of modular and configurable command agents. Based on the concepts introduced in this paper, the German C3-Model FIT („*Führungs- und Informationstechnologie*“) has been designed and implemented by IABG to meet the requirements of the German Army within the domain of command and control and C2 support to

- Evaluate the influence of evolution and progress of C2 information systems (C2IS)
- Support the Planning of C2 for specific operations
- Model the use of existing C2 structures in operations for full-scale rehearsal, improvements, and training.

The application also can bridge the gap between the Warfighter and the procurement office, developers and implementers in industry, planers and operators. It is therefore planned by the German Army Office (*"Heeresamt"*) to distribute the model to potential users within the Department of Defence, the Army Office, and Schools of the Army.

The following figure depicts the model architecture reflecting the original ideas quite well. The embedding simulation system HORUS is also a system developed by IABG. Both parts can be coupled either traditionally or using HLA. However, both parts are not yet able to "talk LC2IEDM", but there are already efforts going on to change this.

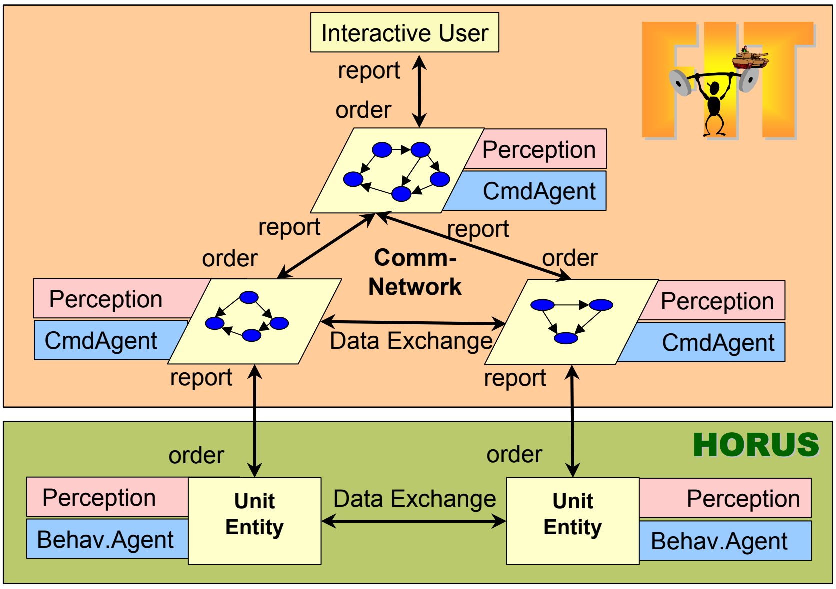

Figure 7: The FIT Model Architecture

Within the domain "Training and Exercises" the FIT model is planned to be used as a computer assisted exercise (CAX) tool for command and control support troops. Within the domain of Support to Operations, FIT can be used for the implementation of realistic command agents to be used for adequate generation of orders for the simulated forces in closed combat simulation systems to be used for alternative courses of action analyses.

A better description can be found in [Eberhard et al. 2001].

4 Information Resource Dictionary Systems

The next idea to be introduced is to use information resource dictionary system (IRDS) techniques to enable the configurable data model translation needed for the already introduced data mediation functionality. More information can be found in [Krusche and Tolk 1999], [Tolk 1999] and [Tolk 2000a] as well as in [Krusche et al. 2000].

The main ideas of an IRDS are defined in the ISO IRDS standard [ISO 1990]. The main purpose of an IRDS is to support data administration and data management. A NATO application example can be found in [NDAG 1999]:

Data administration is an information intensive process involving a wide range of participants. The information required is generated, managed, and used by a large number of participants. Every authority delivering an application to participate in multiple federations – consuming and delivering data from and for the federation – has to be involved in this process of data management. Therefore, it has to be a main purpose of the data administration activities to achieve an effective collaboration between all these participants in the process of establishing a common data standardization lifecycle to gain and preserve a common understanding of the shared data.

An IRDS can be defined as a software system comprising and managing the information resource dictionary in which the information of all participating applications will be recorded. It has been shown, how this idea can be extended in the way, that the IRDS can also be used to support the federate integration process of the high level architecture by making the efforts of the data standardization community usable for the federation builders. The purpose and tasks of data management already have been described earlier.

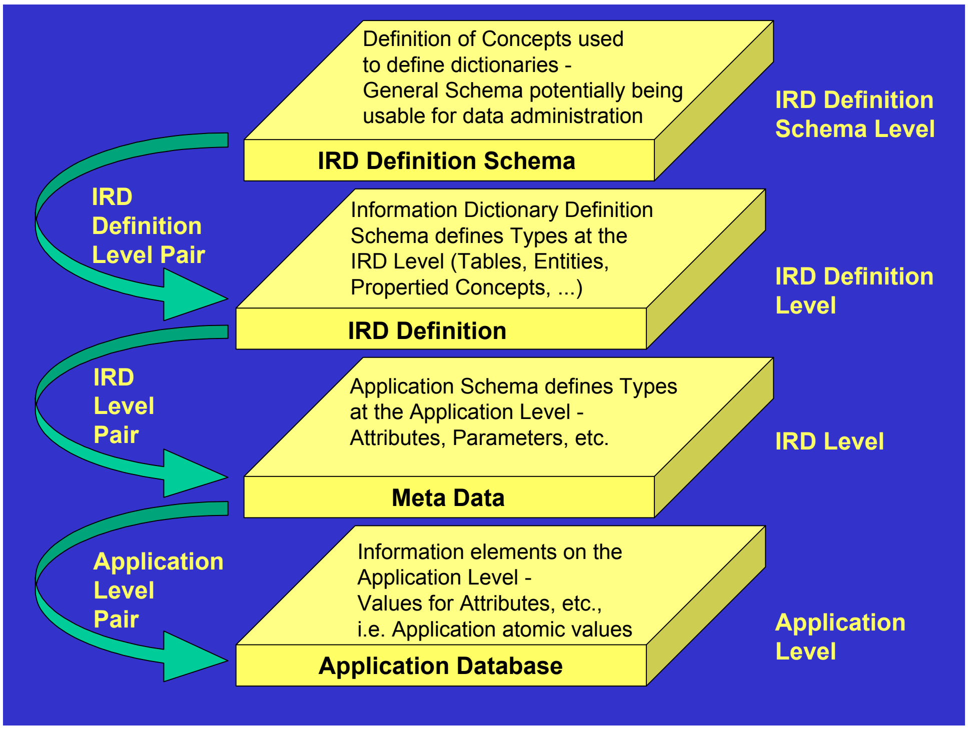

Figure 8: Levels of Information in IRDS

The IRDS framework defines four levels of information. Each level in the framework has a sub-level that consists of the definition of the information contained in its respective sub-levels. Therefore, the use of the ISO IRDS framework allows a gradual introduction of concepts and methodologies from the most abstract form down to most concrete and tangible application and implementation requirements. Thus, the different methodologies of HLA-OMT data modelling, relational data modelling using, e.g., IDEF1X, and object oriented modelling using UML are nothing more or less than different concepts within the IRDS on the respective level.

The idea of level pairs should be described in a little bit more detail. Each level pair consists of a type concept defined in the upper level and an instance concepts being contained in the lower level. Table 1 illustrates the four levels defined by [ISO 1990] and shows the possible level pairs.

***Table 1**: Levels and Concepts of the IRDS Framework*

Level	Illustrative Level Concept
IRD Definition Schema Level	IRD Schema. IRD Table, IRD Column, IRD Object, IRD Template
IRD Definition Level *(Methodology)*	Entity Type, Attribute, Relationship, Table, Column, Constraint, Object, Parameter
IRD Level *(Model)*	Person-Name, Person-Sex, Person-Profession
Application Level *(Data)*	Lara Croft, definitely female, Game Adventurer

In [Tolk 2000a] has been shown that in such an IRDS entity relationship model meta data such as entities, attributes, relationships ends, cardinalities of relationships can be stored as well as the classical and extended concepts of object oriented modelling techniques like classes, types, constructors, inheritance, specifications etc. In the same way, the meta data of HLA-OMT can be contained.[4] On the highest level, the schemas are the objects about what the information has to be interchanged or shared. Thus, on the highest level the concepts are identical. The "technical gap" between the different methodologies vanishes; they can be mediated into each other.

Furthermore, the respective level pairs can be translated into HLA-OMT tables and therefore can be transmitted via the RTI to be interpreted respectively by the receiving federate. Thus, the HLA-OMT not only comprises elements from the application level (as have been the original purpose of the design), but meta as well.

Following the idea of [Tolk 2000a], it is possible to populate the IRDS with different data and or objects models and mediate them into each other using respective mediation services directly deriving from the standardization efforts.

Thus, it is possible to describe a data model within the IRDS, harmonize it with the agreed shared data model to find the matching standardized data elements (SDE) and use the HLA-OMT to describe the respective SDE syntactically. The other model has to be treated in the same way: As having been harmonized with SDEs also, the incoming SDE can be mediated into the object model of the application also. Therefore, both applications can talk to each other using the HLA-OMT without having to agree to a common model or even a common methodology.

All shared information can be translated into the view of the respective application, as not only the application level information is available, but also the meta-information describing its structure. Furthermore, this methodology is open to future standards and extensions also. E.g., it is no problem to define CORBA IRD definitions (which are nearly identical with respective object hierarchies), XML IRD definitions or other forms to structure information. The following figure depicts these ideas.

In other words: To achieve real interoperability and reusability of software components, e.g., simulation systems as federates within several federation, without the need to re-implement the interface for every single federation, it is necessary to gain a common understanding of the shared information first. Thus, the definition of standardized data elements is necessary. The efforts in standardizing the data can be used to populate a respective IRDS. The content of this IRDS can be used to map federate data elements to SDEs. These SDEs can be described in form of the HLA-OMT, no matter in which methodology the respective data or object model has been developed.

---

[4] It was one of the great concerns that the Object Model Template (OMT) of the High Level Architecture (HLA) may not be mighty enough to cope with relational models or object oriented systems. In [Tolk 2000a] it has been shown that these methodologies can be transferred into each other.

Following this way spares time, effort and – therefore – money and guaranties reusability and interoperability of the managed applications of the domain, be it simulation systems or command and control systems or computer generated forces federates.

It should be stated clearly, that actual works trying to define, e.g., a consistent object model for the army to be used within future simulation systems, or works comparing the information content of command and control databases with the information need of simulation systems are very valuable for the effort described in this paper. The better and more complete the models the easier will it be to find good, reliable, and stable reference models that can serve as the needed common shared data models. And, as long as the efficiency of respective algorithms doesn't require another form of a data representation, these models can really serve as common data models for a specific type of domain applications.

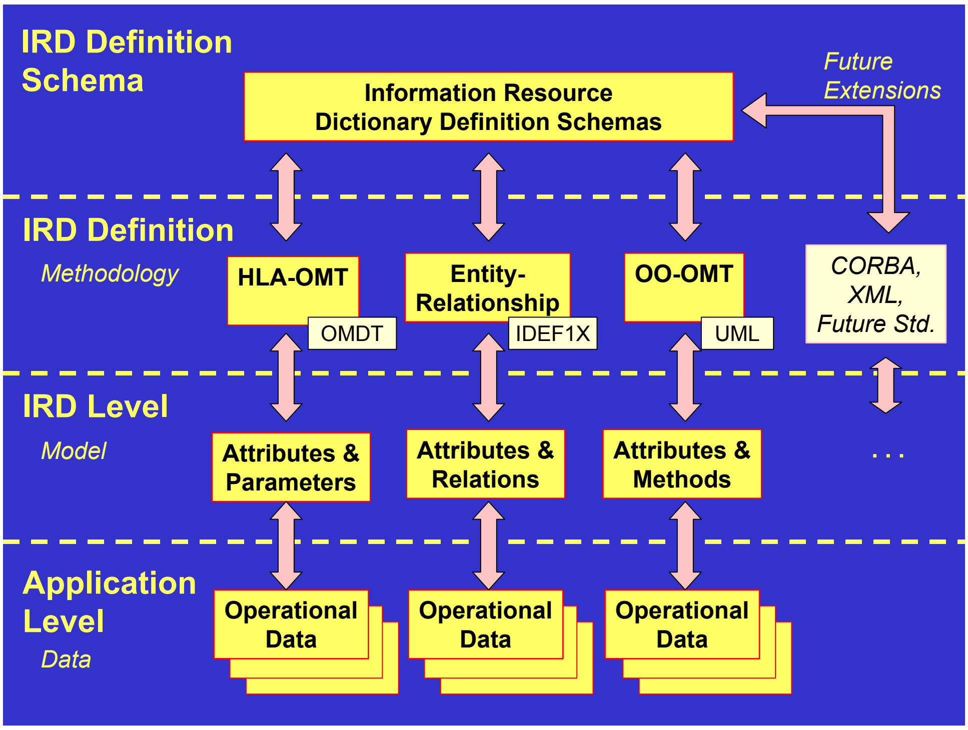

Figure 9: Shared Information Translation supported by an IRDS

5 Recent Developments in the Open Standards Community

Many of the integration efforts being described in the contribution are supported by a new emerging standard being developed by the Object Management Group (OMG). An overview is also given in paper [Tolk 2002] showing also the relations to the operational environment, in particular the High Level Architecture (HLA).

Eleven companies founded the OMG in April 1989. In October 1989, the OMG began independent operations as a not-for-profit corporation. Through the OMG's commitment to developing technically excellent, commercially viable and vendor independent specifications for the software industry, the consortium now includes over 800 members. The OMG is headquartered in Framingham, MA, USA and has international marketing offices in various countries all over the world along with a government representative in Washington, D.C.

The OMG was initially formed to create a component-based software marketplace by supporting the introduction of standardized object software. The organization's charter includes the establishment of industry guidelines and detailed object management specifications to provide a common framework for application development. Conformance to these specifications makes it possible to develop a heterogeneous computing environment across all major hardware platforms and operating systems. Today, implementations of OMG specifications can be found on many operating systems across the world. OMG's series of specifications detail the necessary standard interfaces for Distributed Object Computing.

The OMG has led the way in providing vendor and language independent interoperability standards to the enterprise. Its goal is to enable a global information appliance. To this end, the infrastructure standard CORBA and the modelling standard UML have been introduced by the OMG. In addition to this, a very well accepted standardization process has been established, which as been improved over the recent years to develop – as well as refine - CORBA and UML. The Model Driven Architecture is the next step.

The MDA is based on this idea of meta-modelling as well. It merges the different OMG standards having been developed and used separately so far into a common view by applying common meta models to them. However, it is not necessary to step in too deep into the meta worlds of modelling to understand the underlying concepts. The White Paper [Soley et al. 2000] can be read and understood without requiring outstanding expertise in this domain.

The kernel idea is to use a common stable model, which is language-, vendor- and middleware-neutral. This model must be a meta-model of the concept. The MDA offers concepts for such a model. With such a model in the centre, users having adopted the MDA gain the ability to derive code for various sub-levels. Even if the underlying infrastructure shifts over time, the meta-model remains stable and can be ported to various middleware implementations as well as platforms etc. Figure 10 shows the top-level view of the MDA comprising the stable model in the kernel.

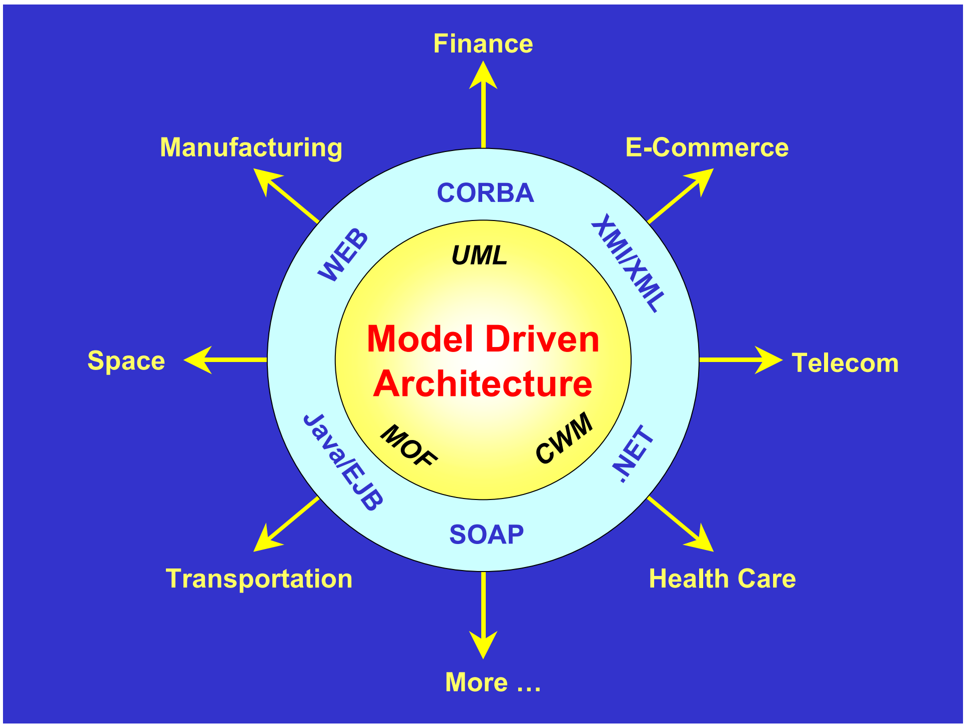

Figure 10: Management View on the Model Driven Architecture

The core of the architecture is based on OMG’s modelling standards:

- Unified Modelling Language (UML)
- Meta-Object Facility (MOF)
- Common Warehouse Meta-model (CWM)

The different views of the core model will represent Enterprise Computing with its component structure and transactional interaction; another view will represent Real-Time computing with its special needs for resource control, etc. In any case, they will be independent of any middleware platform.

The MDA defines an approach to system specifications that separates the specification of the system functionality from the specification of the platform specific implementation. This is done by specifying standards to model the system in a reusable way. This allows two main applications. First, a system can be defined platform independently and then can be realized on multiple platforms through auxiliary mapping standards. Second, different applications can be integrated by explicitly relating their models, even if they do not run on the same platform type.

The first step when creating an MDA-based application is to create a Platform-Independent application Model (PIM). In the MDA, a model is defined to be a representation of a part of the function, structure and/or behaviour of a system; i.e., the definition is usable in the M&S domain quite well. The PIM will be expressed in UML in terms of the appropriate core model. The core models are available in form of UML Profiles of which a number already are well along their way to be standardized by the OMG.

The next step – if the model shall run as an application – is to convert this model from general application to a Platform Specific Model (PSM). The PSM is derived from the PIM using standardized transformation rules. While the PIM defines the necessary functionality, the PSM specifies how this functionality is realized on a special platform.

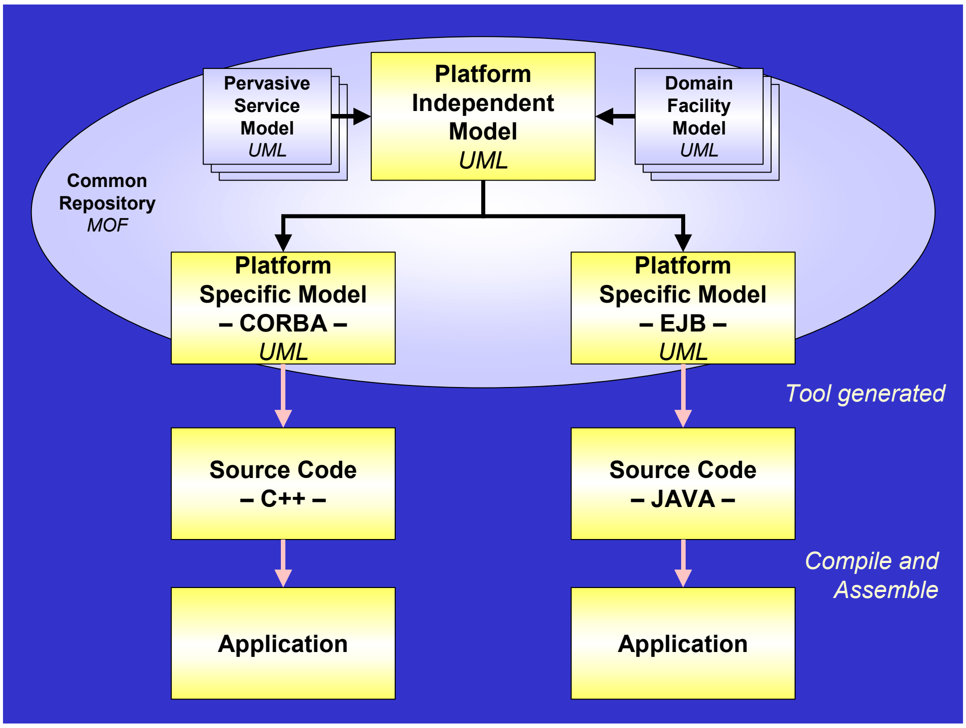

Figure 11: Application Generation using the MDA

The last step is to generate code from these specific UML models. Figure 11 shows the flowchart for the overall process. In this figure, two sets of boxes are shown that haven't been dealt with explicitly so far, the Pervasive Services Model and the Domain Facilities Model:

- The **Domain Facilities Models** are directly connected to the CORBA domains standardized by the Domain Task Forces (DTF) of OMG members. Each DTF produces standard frameworks for standard functions in its application space.

- The **Pervasive Services Model** comprises the definition of the set of essential services that are implemented as CORBA Services and Facilities within the CORBA environment; i.e., services like event notification, object security, transactions, etc. In addition, hardware and software attributes like scalability, real-time, fault tolerance, etc. may be modelled as well, if the user feels the need to do so in order to standardize the model.

This approach is very likely to become a major integration factor for commercial systems in the next decade. In addition, it supports many of the ideas proposed in this contribution to the NATO Lecture Series, such as the Information Resources Dictionary System (IRDS), which is directly connected to the Common Warehouse Metamodel of the Model Driven Architecture, or the decision models which can directly be used to set up respective Platform Independent Models that can be used as a backbone of a respective component that delivers M&S functionality to operational systems later on. It is therefore highly recommended to evaluate the applicability of the MDA to respective system approaches before using proprietary solutions.

6 Summary

The paper comprises the main ideas of federated solutions. A common shared data model introducing a common understanding of the interchanged data is a first step into the direction of continuous interoperability of systems. The idea of federated solutions can also be found in [Tolk and Kunde 2000], where the "house slide" for federated solutions has been described the first time.

The Study Group on Interoperability between C4I System and Simulation Systems (SG-C4I) of the Simulation Interoperability Standardization Organization (SISO) developed a framework to cope with this issues [Timian et al. 2000]. The following figure – introduced by Michael R. Hieb and Andreas Tolk for a briefing of the Simulation Interoperability Standardization Organization (SISO) – comprises the fields to by harmonized and coped with to come to shared solutions.

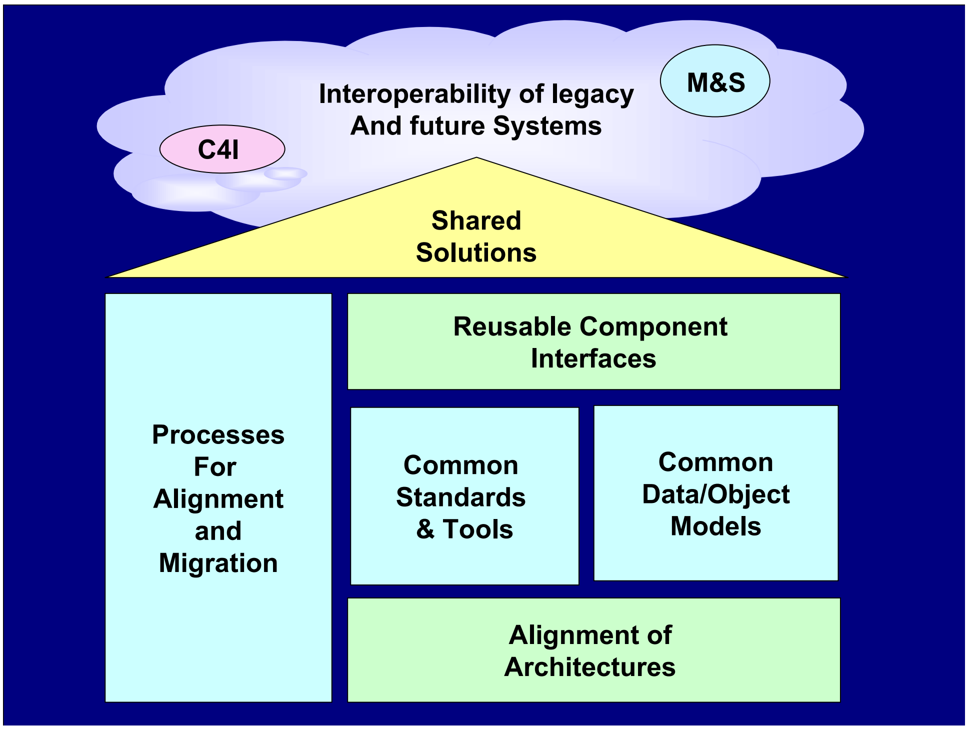

Figure 12: Interoperability Issues of Shared Solutions

First thing to be done is the alignment of architectures, so that components of both worlds are able to talk to another. The next level comprises common data and object models as well as common tools and common standards. This will lead to reusable components. However, to be able to reach real interoperable shared solutions, the processes have to be aligned also (e.g., using the same tools and methodologies) including procedures to migrate legacy systems to this new common world. Thus, more or less a change in philosophy of looking at C4I and simulation systems may be needed, e.g., when looking at M&S in acquisition, requirement analyses, support to operations, and training. Maybe, on the long term there will be no longer the distinction between both worlds but new systems will comprises functionality of both worlds as federates.

Using this techniques it becomes possible to integrate the findings of respective computer generated forces research into the operational environment in the same way that can be used to develop the next generation of Warfighter supporting IT systems.

7 References

[Conrad 1997] Stefan Conrad: "Föderierte Datenbanksysteme" (in German), Springer, Berlin, 1997

[DISA 1996] Defense Information Infrastructure (DII) Shared Data Environment (SHADE), CAPSTONE DOCUMENT, U.S. DoD, DISA, July 1996

[Eberhard et al. 2001] Manfred Eberhard, Hans-Jürgen Rech, Andreas Tolk: "The German C3-Model FIT", Paper 01F-SIW-011, Proceedings of the Fall Simulation Interoperability Workshop, Orlando FL, September 2001

[Hieb and Blalock 1999] Michael R. Hieb, James Blalock: "Data Alignment between Army C4I Databases and Army Simulations", Paper 99S-SIW-034, Proceedings of the Spring Simulation Interoperability Workshop, Orlando FL, March 1999

[Hieb and Sprinkle 2000] Michael R. Hieb, Ron Sprinkle: "Simulation Infrastructure for the DII COE Architecture: The Army Vision", Paper 00F-SIW-035; Proceedings of the Fall Simulation Interoperability Workshop, Orlando, Florida, September 2000

[ISO 1990] ISO Standard IS10027: "IS10027:1990 An Information Resource Dictionary System (IRDS) Framework", 1990

[Knoll 2000] Franz Knoll: "Command and Control Modeling using the Simulation Model FIT", Briefing, German American Workshop on Command and Decision Modeling, Ft. Leavenworth, Kansas, June 2000

[Krusche and Tolk 1999] Stefan Krusche, Andreas Tolk: "A SHADE Approach for Coupling C4I systems and simulation systems", Paper 99F-SIW-004, Proceedings of the Fall Simulation Interoperability Workshop, Orlando FL, September 1999

[Krusche and Tolk 2000] Stefan Krusche, Andreas Tolk: „Information Processing as a Key Factor for Modern Federations of Combat Information Systems", NATO/RTO Information Systems Technology Panel (IST) Symposium "New Information Processing Techniques for Military Systems", Istanbul, October 2000

[Krusche et al. 2000] Stefan Krusche et al.: Data Mediation Forum Homepage (http://www.dm-forum.org)

[NATO 1999a] Uwe K. J. Dompke, Andreas Tolk: "On a Modular Concept for Command and Control in Simulation Models", Proceedings of the NATO Studies, Analysis and Simulation (SAS) Panel TR: Symposium on Modelling and Analysis of Command and Control, Paris, France, January 1999

[NATO 1999b] Uwe K. J. Dompke, Günther Scheckeler: "Computer Generated Forces Technology", NATO Report RTO-TR-11 AC/323(SAS)TP/8, Research and Technology Organization, Neuilly-sur-Seine Cedex, France, March 1999

[NATO 2000] ADatP-32, Edition 2.0: “The Land C2 Information Exchange Data Model”, NATO HQ, Brussels, March 2000

[NATO 2002] NATO Document RTO-TR-9 AC/323(SAS)TP/4. *Code of Best Practice (COBP) for Command and Control Assessment.* NATO RSG SAS-026, Revision 2002, Neuilly-sur-Seine Cedex, France, August 2002

[NC3A 1999] Pre-Feasibility-Study on a “Kernel Application ACE Integrated Database”; IABG Report No. B – CS 2015/01, Ottobrunn 1999, written on behalf of and distributed by the NC3A Information Systems Division, The Hague

[NDAG 1999] NATO Consultation, Command and Control Board (NC3B), Information Systems Sub-Committee (ISSC), NATO Data Administration Group (NDAG): "Feasibility Study for the NATO C3 Information Resource Dictionary System (NC3 IRDS)", AC/322(SC/5-WG/3)WP4, Brussels, September 1999

[Özsu and Valduriez 1991] T. Özsu, P. Valduriez: “Principles of Distributed Database Systems”, Prentice-Hall, Eaglewood Cliffs, New Jersey, 1991

[Sheth and Larson 1990] A. P. Sheth, J. A. Larson: “Federated Database Systems for Managing Distributed, Heterogeneous, and Autonomous Databases”, ACM Computing Surveys, Vol. 22(3): Pages 183-236, 1990

[Soley et al. 2000] Richard Soley and the OMG Staff Strategy Group: “Model Driven Architecture”, White Paper, Object Management Group (OMG), November 2000

[Timian et al. 1999] Donald H. Timian, Jonathan Glass, Michael R. Hieb, Michael J. Staver: “Using Standard Command, Control, Communications, Computers, and Intelligence (C4I) Components to Interface to Simulations”, Paper 99S-SIW-035, Proceedings of the Spring Simulation Interoperability Workshop, Orlando FL, March 1999

[Timian et al. 2000] Donald H. Timian et al: “Study Group Report on C4I to Simulation Coupling”, Paper 00F-SIW-005, Proceedings of the Fall Simulation Interoperability Workshop, Orlando FL, September 2000

[Tolk 1999] Andreas Tolk: “Using ATCCIS as an Information Layer to couple CGF Federates and Closed Combat Simulations”, Paper 99F-SIW-008, Proceedings of the Fall Simulation Interoperability Workshop, Orlando FL, September 1999

[Tolk 2000a] Andreas Tolk: „HLA-OMT versus Traditional Data and Object Modeling – Chance or Shoehorn“, Paper 00S-SIW-024, Proceedings of the Spring Simulation Interoperability Workshop, Best Paper SIW S00, Orlando, Florida, March 2000

[Tolk 2000b] Andreas Tolk: “Heterogeneous Synergy – A Vision for the Next Generation of Warfighter IT Systems”, Paper 00F-SIW-013, Proceedings of the Fall Simulation Interoperability Workshop, Best Paper SIW F00, Orlando, Florida, September 2000

[Tolk 2001] Andreas Tolk: “Bridging the Data Gap – Short, Medium, and Long Term Solutions”, Paper 01S-SIW-011, Proceedings of the Spring Simulation Interoperability Workshop, Best Paper SIW S01, Orlando, Florida, March 2001

[Tolk 2002] Andreas Tolk: “Avoiding Another Green Elephant – A Proposal for the Next Generation HLA based on the Model Driven Architecture”, Paper 02F-SIW-004, Proceedings of the Fall Simulation Interoperability Workshop, Best Paper SIW F02, Orlando, Florida, September 2002

[Tolk and Kunde 2000] Andreas Tolk, Dietmar Kunde: “Decision Support Systems – Technical Prerequisites and Military Requirements”, Proceedings of the 2000 Command and Control Research and Technology Symposium (CCRTS), Monterey, June 2000

The proceedings of the Simulation Interoperability Workshops (SIW) can be found on the SISO web page http://www.sisostds.org following the links to SIW. The proceedings of the Command and Control Research and Technology Symposia (CCRTS) can be found on the CCRP web page http://www.dodccrp.org.