Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

NLR-TP-2001-198

A road map to the NATO virtual enterprise

Y.A.J.R. van de Vijver and J.G. Stil

Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

NLR-TP-2001-198

A road map to the NATO virtual enterprise

Y.A.J.R. van de Vijver and J.G. Stil

This report is based on a presentation held at the NATO/RTO Symposium on "Information management challenges in achieving coalition interoperability", Quebec City, Canada, 28-30 May 2001.

Division:	Information and Communication Technology
Issued:	April 2001
Classification of title:	Unclassified

Summary

In this paper information management challenges are described, and ways to achieve coalition interoperability, by defining a road map towards a NATO virtual enterprise. Such an enterprise strongly supports the “interoperable communications”-target of the Defence Capabilities Initiative (DCI), launched at the NATO summit in Washington, April 1999. The building blocks of virtual enterprises will be discussed. These blocks are increasingly becoming standards, therefore allowing higher and higher levels of abstraction in interoperability. Starting from a historical example, and continuing with a Joint Warrior Interoperability Demonstration and results from a recent research program, this paper will describe the journey on the road to the NATO Virtual Enterprise. The paper will be concluded by looking forward to the goal and discuss the road towards it.

Contents

(18 pages in total)

1 Introduction

In the future, more and more military operations will be conducted by a coalition of NATO nations. This places new and more important requirements on the interoperability needed for such operations.

In Section 2, the building blocks, or stepping stones, of the NATO Virtual Enterprise will be described. Although the term “Virtual Enterprise” emerged as one of Information Technology’s hot buzzwords during the 1990s, the first steps on the road toward the Virtual Enterprise have already been set in the Apollo space program by increasing standardisation of hardware and software components. A more down to earth example from NLR’s own history of how standardisation of systems has evolved over the last twenty years will be given in Section 3.
The implementation of virtual enterprises has become increasingly more feasible by recent developments in Information and Communication Technology. Combined with fast data communication, these developments make it possible for geographically distributed teams to work together as if they were co-located. NATO must embrace these developments as stepping stones toward the NATO Virtual Enterprise.

The present state-of-the-practice of the NATO Virtual Enterprise is the level of interoperability demonstrated in present day interoperability trials, for example the 2000/2001 Joint Warrior Interoperability Demonstration (JWID). During this event, a lot of military computer systems originating from various NATO nations are interconnected and operated against the background of an operational war scenario. The Netherlands’ JWID 2000 interoperability demonstration (developed for the Royal Netherlands Air Force by NLR) will be given in Section 4 as an example of current NATO interoperability achievements.

In the long term, NATO Interoperability Frameworks should be aiming at aligning with commercial efforts. A possible road map towards the installation of a NATO Virtual Enterprise should consist of the stepwise adoption of the building blocks of such an enterprise, for instance, a NATO Command and Control Working Environment. Initiatives towards this goal are taken (e.g., NATO C3 Agency’s Virtual Command Centre). Results from research programs may provide additional capabilities to support and improve these initiatives. One example of such a research program is EUCLID RTP 6.1, entitled Advanced Workstation for C3I, which finished end of 1998. This program resulted in a common business model for C2, and in a demonstrator based on a multi-agent system architecture and an ATCCIS-compliant ontology. These were used to develop a dozen agent-based decision support tools from seven European countries, communicating via a CORBA-compliant communication layer. The results of the

EUCLID RTP 6.1 project will be described in Section 5. The road map to the NATO Virtual Enterprise will then be further elaborated in Section 6.

2 The stepping stones towards a virtual enterprise

A Virtual Enterprise can be defined as ”A temporary alliance of parties, come together to share core competencies and resources in order to better respond to opportunities and threats, and whose co-operation is supported by computer software and networks”. It presents an option to exploit opportunities and to provide products/services that no single party may be able or willing to provide alone. Alliances of parties are not new: already in the 1960s a number of aerospace projects, such as the Apollo space-project, satisfied this definition. NATO itself is a prime example. New is the intensity of the use of ICT means, connecting the parties in real-time and enabling real-time situation assessment and decision making.

The ICT means can be joined together into groups of capabilities according to their functionality. These capabilities are considered the building blocks or stepping stones[1], necessary to enable the Virtual Enterprise. The road to the Virtual Enterprise is constructed from these stepping stones starting at the lower level of Communications, and progressing to the level of end-user Applications (see Figure 1). Security and Management Services should be active through all building blocks and require extra attention within international collaboration.

A key enabling technology and catalyst in the set-up and maintenance of virtual enterprises has been the technology of heterogeneous distributed networked environments. These environments, which are part of the Computer Network stepping stones in Figure 1, support instantaneous collaboration across organisational and geographical boundaries, while protecting information and other assets against unauthorised access. Integration of network and information infrastructures can only efficiently be carried out if these rest on open standards which continuously comply with the speed of change in technology and which are supported by state-of-the-art tools.

Early on, NLR’s Information and Communication Technology Division has recognised the need for an organisation-wide solution and piloted basic building blocks for what became part of the SPINEware middleware [5], which shields users from lower level complexities. Commercial vendors now also provide these building blocks, for instance, Samba-server, which allows

[1] Stepping-stone (Collins):

- One of a series of stones acting as footsteps for crossing streams, marshes, etc.
- A circumstance that assists in progress towards a goal

Windows-based PCs to access files on Unix workstations, and VMware, which enables windows-based applications to run on Linux workstations. Within the military community, standardisation of this layer of stepping stones is encouraged by, for instance, NATO OSE and the DII-COE Common Operating Environment specification.

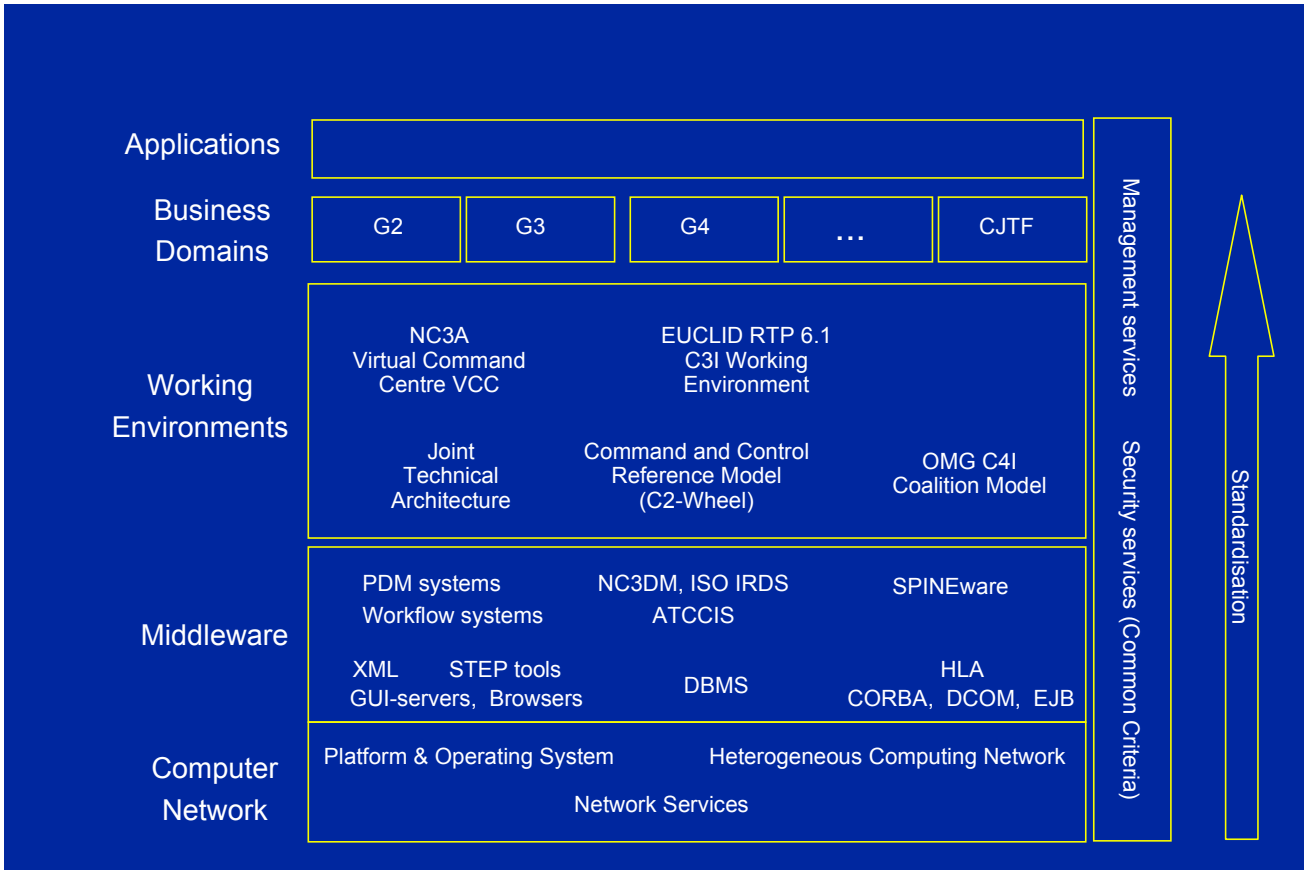

Figure 1 Stepping stones of the Virtual Enterprise

The Middleware stepping stones de-couple application-specific capabilities from any dependencies on the "plumbing" layer that consists of heterogeneous operating systems, hardware platforms and communication protocols:

- Database Management Systems (DBMS) take care of the storage and handling of data.
- Component integrators such as CORBA and OLE/COM/DCOM separate monolithic applications into components, which can be located where it is most cost efficient to execute them (e.g. close to a database engine).
- Web-based user interfaces using a web browser are platform independent and provides the same look-and-feel on any platform.
- Stimulated by the US Department of Defence, the High Level Architecture (HLA) encourages simulation re-use and interoperability.

- Information exchange languages, such as the Standard Generalised Mark-up Language, the HyperText Mark-up Language HTML, and the Extendable Mark-up Language XML standardise information exchange.
- STEP, the Standard for the Exchange of Product Model Data, is a comprehensive ISO standard (ISO 10303) that prescribes how to represent and exchange digital product information. In order to do this, STEP covers geometry, topology, tolerances, relationships, attributes, assemblies, configuration and more.
- Product Data Management (PDM) and Workflow tools can be applied to support standardisation of products and processes. Examples of commercial workflow tools for the latter types of application are Windchill and Enovia. These elaborate packages, that combine product data management with workflow capabilities, are being used by main aerospace industries.
- A common Data Model based on ATCCIS, ISO IRDS (Information Resource Dictionary System Framework [ISO 10027 1990]) and the integrated NC3DM (NATO C3 Data Model) allows sharing of information on a higher level.

The Working Environments stepping stones provide the tools for creating a user-oriented, single, virtual computer that hides the details of the underlying heterogeneous network, and that may be tailored to support particular business domains, such as G2, G3, G4, and also the Combined Joint Task Force (CJTF) Centre. Working environments may cross organisational boundaries and therefore provide the environment for the virtual enterprise. Based on these lower layer stepping stones, Business Domains can be constructed to fully exploit the high level of interoperability created by these stepping stones, without already becoming application-specific. The stepping stones in these layers will be discussed in more detail in sections 5 and 6.

In addition to these functional layers of stepping stones, some general services have to be standardised as well. The security service stepping stones are of utmost importance in a military environment. In a complex and multi-company environment the security policy could apply at different levels: The internal network and systems of each partner, the communication links between partners, the access "doors" to each company network, the communication software between partners (e-mail, ftp etc.), the data, the responsibilities, different national laws, etc.
Each company could have different a security policy and a fundamental issue is the level of trusted relationship that is introduced between the partners companies.
For Virtual Enterprises a simple way of proceeding follows these rules:

- Each party guarantees a basic level of security on its internal systems following policies and procedures;
- Each party applies security mechanisms on the access "doors" to internal systems, complying with internal policies and procedures;

- Common security mechanisms are applied on the communication links and software harmonising security policies and national laws.

To this end stepping stones such as User identification, Perimetrical Security, Data Security, Access Control, Cryptographic Mechanisms, Anti-virus tools and Firewalls should be addressed.

The Common Criteria, which have formed the basis for standardisation of security services, have now been merged with commercial standards, resulting in the ISOIEC 15408 IT-Security Standard for dual-use.

The Operation and Management Services includes the framework for managing the assets of the Virtual Enterprise and/or the projects via which the goals of the collaboration are established. Such a framework usually includes process management with PDM and ERP tools, configuration management tools, quality assurance (as ISO 9000 and CMM), information storage management, performance monitoring and disaster recovery.

3 History shows the way

An example from NLR's history that shows the increasing need for and use of standardized, Common-Of-The-Shelf (COTS) tools is the Operations Management Information System OMIS [4]. OMIS is a command and control system to support the Royal Netherlands Air Force in its task to prepare aircraft for missions to be flown. OMIS has been in use at Volkel Air Force Base in the Netherlands since 1983.

OMIS assists in the communication of relevant information between different control centres and units at an Air Force Base. OMIS provides all users with consistent and up-to-date information, needed to perform their task, for instance, allocation of aircraft, fuel, pilots, and weapons. Air Task Orders and Air Task Messages are processed and communicated as well as reports to higher command levels. Air Traffic Control information on planned and actual times of departure and landing of aircraft are registered. Changes in Alert Status are distributed to all connected units upon arrival. A schematic overview of the OMIS functionality is shown in Figure 2.

The 1983 OMIS consisted of tailor-made application software running on COTS hardware, which consisted of DEC PDP-11/84 minicomputers, interconnected with each other via DECNET (including crypto-devices), and DEC VT-420 terminals. In addition to the application software, functionality that is less application specific, like database management or data replication, was also tailor-made.

The modernisation of OMIS (called OMIS-2) was triggered by the lack of interoperability capabilities and by the technological advances in commercially available hardware and software. The lack of interoperability capabilities led to a complete redesign of the data model at application level. The ATCCIS (Army Tactical Command & Control Information System) standard data model was used as a basis for the new application data model. All entities in the OMIS-2 functional environment were re-analysed, normalised and placed in a so-called *ATCCIS-able* data model. Adoption of the ATCCIS concept facilitates future coupling with other national and possibly international Command and Control systems that are based on the ATCCIS model.

Figure 2 Overview of OMIS functionality

The advances in hardware and software led to the adoption of, for instance, the Oracle Relational Database Management System for implementing the new data model. At network level the interoperability requirement was met via the application of standard network hardware and software (PC's operating with Microsoft Windows NT4). The OMIS-2 user interface is based on the Microsoft Window Multiple Document Interface to display the various windows (in OMIS-2 called totes). OMIS-2 has been installed at Volkel Air Force Base in the Netherlands in the middle of 1999 and has been successfully in operation since.

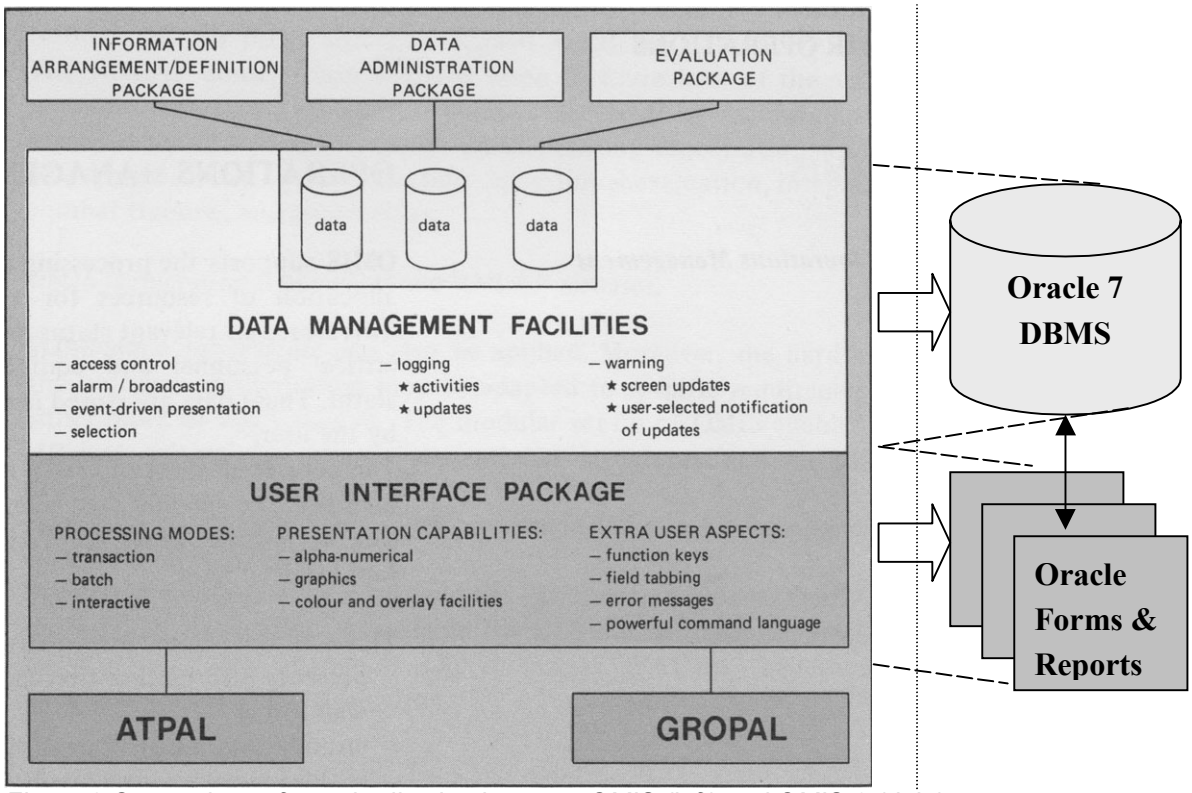

Figure 3 Comparison of standardisation between OMIS (left) and OMIS-2 (right)

Figure 3 shows the difference between OMIS and OMIS-2 with respect to commercially bought and tailor-made hardware and software, and is an example of the progress in standardisation between the early 1980s and the late 1990s. Referenced against Figure 1 (see following section), OMIS used standard platform and operating systems on top of network services, and OMIS-2 added the Database Management System and Graphical User Interface Builders to the standard, and ATCCIS as a first attempt towards a Command and Control business domain definition.

4 The present

As the example in the previous section shows, the current status of standardisation is at the level of middleware (see Figure 1 in Section 2). Database management systems are no longer developed for an application, but simply bought from commercial vendors and tailored to the need of the application. A Graphical User Interface (GUI) is built with the help of tools (called GUI Builders) that produce standard layouts and handlers which, again, may be tailored to the need of the application. Similar stories may be told for communication middleware such as CORBA and DCOM, exchange languages such as HTML, SGML, XML and STEP, the High Level Architecture (HLA) for simulation re-use and interoperability, and increasingly for product and process management tools (PDM, Workflow).

NATO also has a lot of work already in progress to achieve coalition interoperability. An example of an environment where already a lot of interoperability trials are carried out, is the Joint Warrior Interoperability Demonstration (JWID).

JWID interoperability activities concentrate both on the exchange of messages that are formatted according to messages formatting standards and on the information storage structure within military systems. With regard to message exchange standards, both military and civilian standards are considered. Examples of military message text formatting standards are the Allied Data Publication no. 3 (ADatP-3), the US Message Text Formatting standard (USMTF) and the *Over The Horizon-Gold* (OTH-GOLD) standard. Examples of non-military standards are the afore-mentioned SGML and XML. In the context of application-internal information storage structures, a typical example of standardisation is ATCCIS (Army Tactical Command and Control Information System). The Army Tactical Command and Control Information System project is developing specifications to share data automatically between different command and control systems of participating nations. The ATCCIS Replication Mechanism (ARM) enables selective data replication between Command and Control systems that adopted the ATCCIS standard for their internal data structure.

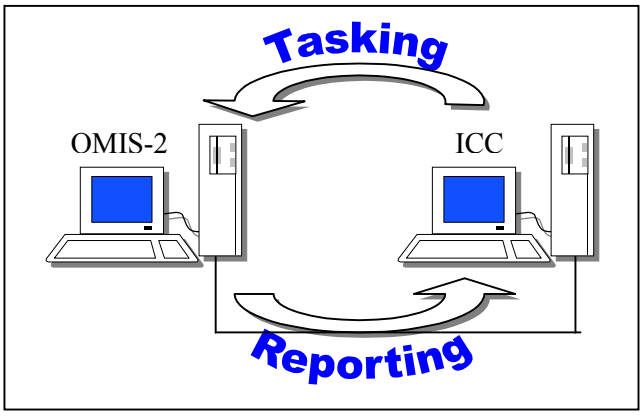

Figure 4 Database Link Principle

The Royal Netherlands Air Force and the National Aerospace Laboratory (NLR) of the Netherlands participated in JWID'00 and demonstrated a prototype of an interface between ICC and OMIS-2 (see Figure 4). ICC (Initial CAOC (Combined Air Operations Centre) Capability) is a NATO system developed by NC3A and operational at CAOC Kalkar. OMIS-2 (Operations Management Information System) is a national Command and Control (C2) system, of which the software has been developed by NLR. It is operational at Volkel Air Force Base. The implemented prototype interface is meant as a replacement for the swivel chair interface that has been operational so far.

Both ICC and OMIS-2 are client / server systems using Oracle databases. The client applications connect to their database via SQL*Net, a standard Oracle networking product on top of the TCP/IP protocol. The interface between OMIS-2 and ICC utilises the same SQL*Net protocol.

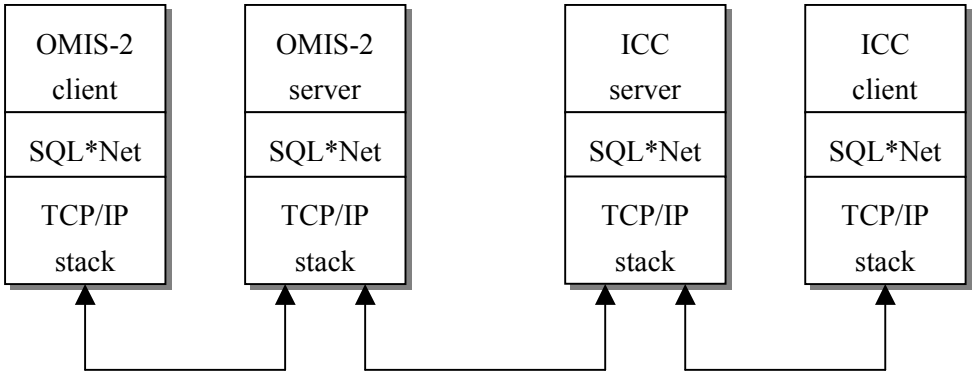

Figure 5 Interface Network Concept

The connection between the two database servers is actually a client / server connection where the OMIS-2 database server acts as client of the ICC database server. The initiative to exchange information comes from the client (OMIS-2). The connection between the two databases is realised using an Oracle database link. This mechanism is part of the distributed database option of Oracle. Database links provide the user access to data stored in a remote database. Remotely stored data can be manipulated in a similar way, as locally stored data is manipulated (see Figure 6). Synonyms in the database are used to make the actual location of the data completely transparent. This technique is also used to access data stored in the OMIS-2 REAL database from the OMIS-2 CPX (exercise) database.

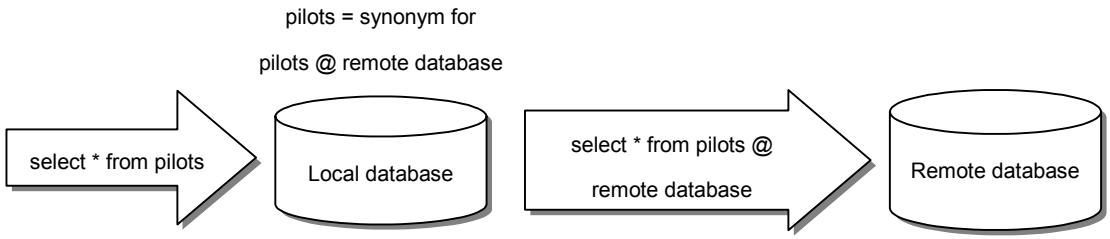

Figure 6 Database Link Principle

5 The next step

As shown in the previous section, the current practice in interoperability and standardisation is at the level of the Middleware stepping stones in Figure 1. These stepping stones may be considered to be fairly standardised and integrated in operational systems to enable interoperability at this level. In the short term, a similar level of standardisation must be sought for the layer of Working Environments. Necessary components for interoperability at this level of abstraction are a common process definition and a common data model definition.

An example of a command and control working environment is the demonstration environment created within the EUCLID (European Co-operation for the Long-term In Defence) Research and Technology Program 6.1, called Advanced C3I Workstation [2]. This workstation consisted of the following key innovative technologies:

- An agent-based information/software architecture to integrate diverse artificial intelligence based applications, and
- An integrated suite of command decision support tools applying AI technologies.

The integration architecture comprises a multi-agent system architecture [3] for developing and running software structured as multiple co-operating, intelligent agents, and a user interface framework that provides the user interface between one or more users and multiple agents, including a map-and-overlay display called the DOHP (Digital Overhead Projector). Both components embrace CORBA object request brokering, enabling multi-agent software to be distributed at run-time across a mixed network of workstations and PCs.

One of the major achievements of the EUCLID RTP 6.1 program has been the development of a general command and control reference model, called the “C2 wheel” (see Figure 7). This reference model is a consolidated process model for army, navy and air command and control, accepted by 7 European countries. This model has been submitted to the Object Management Group OMG during the Coalition Day Event in Manchester, United Kingdom, 18-19 April 1998, to serve as a basis for the OMG efforts to develop a C4I domain and process model (the Coalition Model).

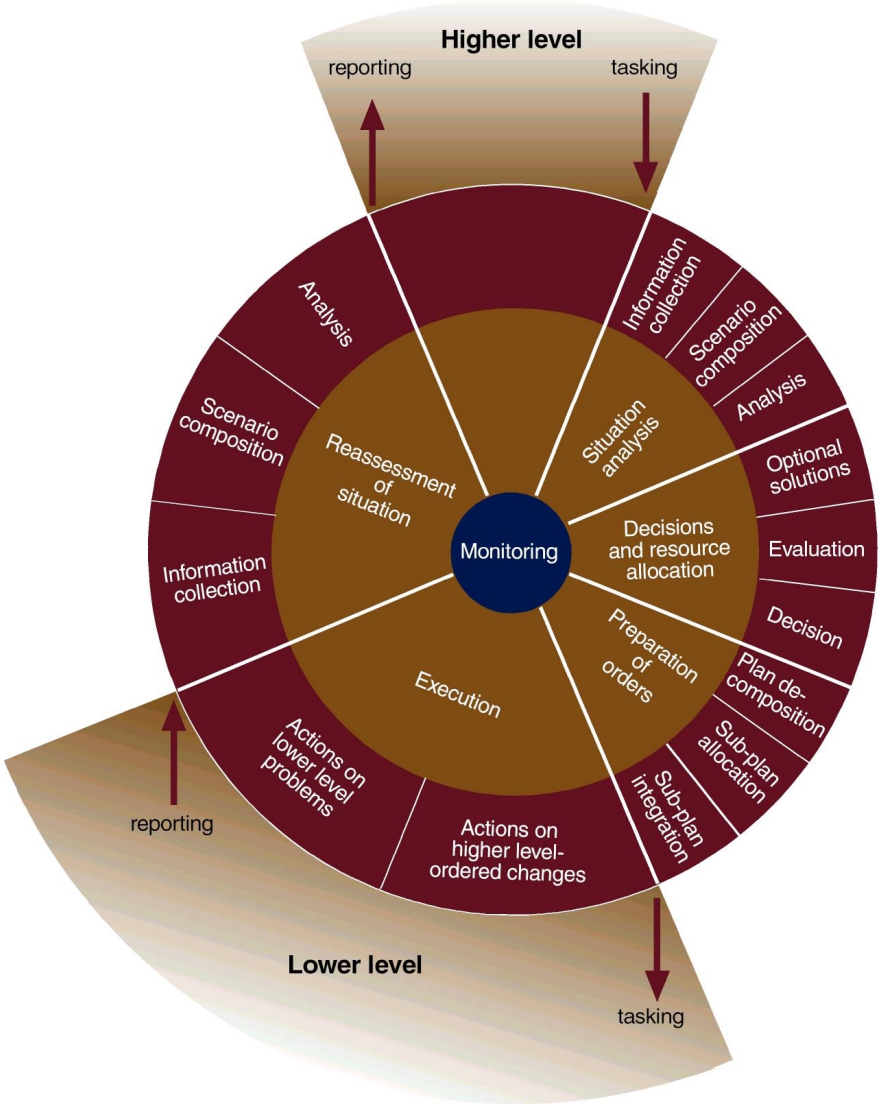

Figure 7 General Command and Control Process (C2-wheel)

The integrated suite of decision support tools in the EUCLID RTP 6.1 Working Environment contains some 14 tools to support different aspects of joint army-air and naval-air situation assessment and planning, grouped according to the C2 wheel:

- For report analysis and situation assessment, decision support tools have been developed for automated message processing, wide area picture compilation, using fuzzy logic and clustering algorithms to identify significant enemy behaviours and groupings, and a publish-and-subscribe mechanism to notify other decision support tools of changes to the wide area picture;
- For army-air decision support, planning and tasking, decision support tools have been developed for storing, displaying and manipulating vector feature data, for automated terrain analysis & mobility corridor construction, for Course of Action comparison based on

Weapon Effectiveness Indices and Weighted Unit Values, for manoeuvre planning, for ORBAT browsing, and for air and fire support resource allocation [1];

- For naval-air decision support, planning and tasking, decision support tools have been developed for engagement co-ordination, for terrain analysis, for terrain exploitation and display, for manoeuvre plan browsing and situation prediction, and for manoeuvre co-ordination and formation planning.

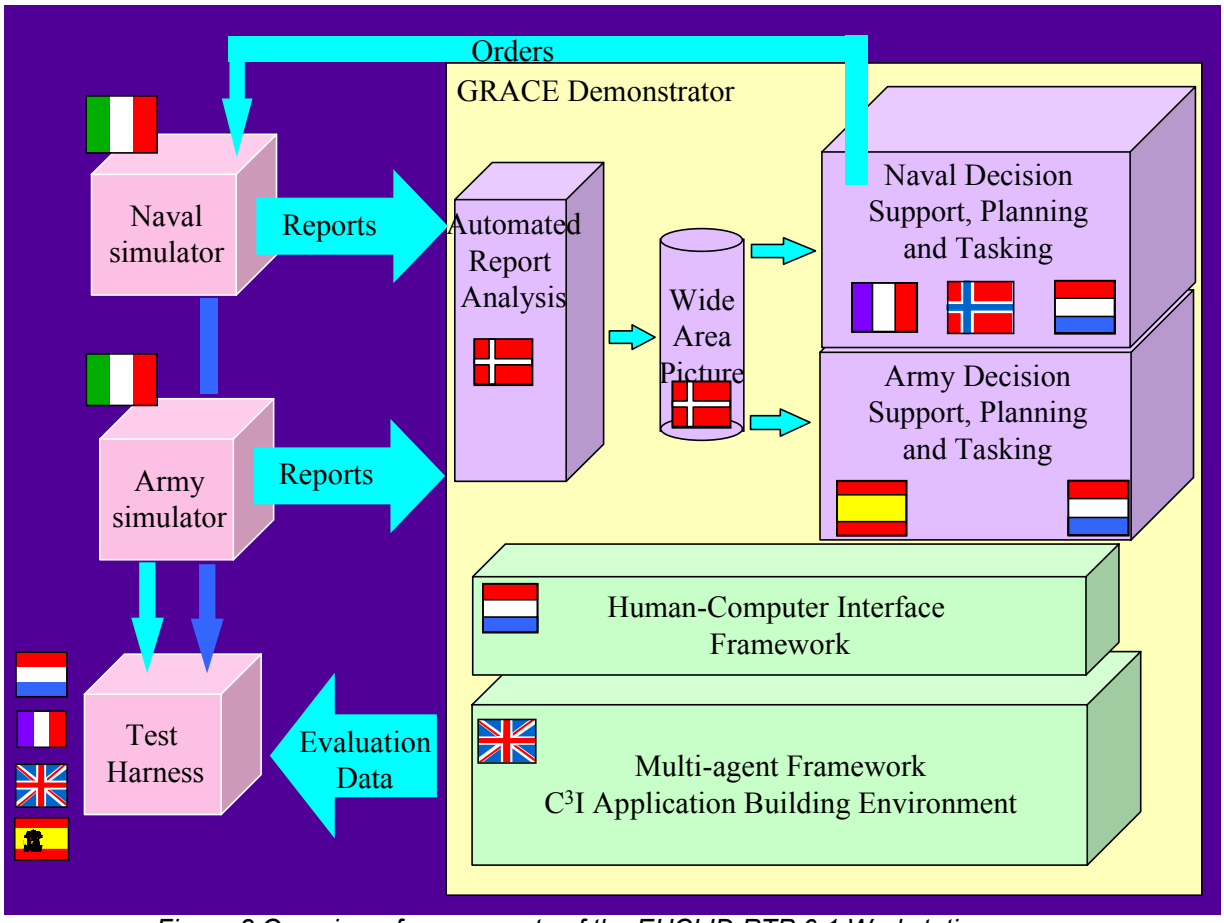

Figure 8 Overview of components of the EUCLID RTP 6.1 Workstation

These tools were generally intended to support the human command team, by automating only those aspects of a task that are better suited to the machine. Each of the tools was evaluated and demonstrated using simulated data from a naval landing force scenario or an army peace enforcement scenario. The benefits from the use of artificial intelligence techniques compared with manual planning are:

- Automatic alerting to significant events or changes in the situation;
- Quicker planning;
- Consideration of more alternative plans;
- Improved consistency and accuracy of plans, e.g. through plan critiquing;

- The ability to take more constraints (time, space, terrain, resources) into account.

One of the other major accomplishments of the EUCLID RTP 6.1 program was the development of a common object oriented data model, based on the ATCCIS model. This data model handles information like:

- Units and Organizational structures, including status, organizational dependencies, position, perception information and encyclopedic keys
- Weather information
- Facilities such as bridges, oilrigs and ports
- Naval and army unit information, including air assets.

The model is used by some components as an internal data storage format, and by all components as an external exchange format. Most of the decision support tools used the common model to structure information associated with the services they provide and request. This is particularly the case for all situation and encyclopaedic information, which is held by the situation analysis component and provided to requesting decision support tools.

Some of the decision support tools do not use the common model as their internal software implementation, because in the program the common model was derived posterior from the information requirements of the different decision support tools. In future developments, the common object model can be used a-priori of the development of interoperable decision support tools. It is worth noting that at the more detailed levels of the model interesting discussions emerged and were resolved about how to represent both army and naval concepts in the same model. Such issues are of increasing importance with the increased need for in joint operations.

A common object model in its own is not enough to ensure valid interactions between distributed components. It is also necessary to have agreed services and service protocols. For the future it would be beneficial to relate these aspects to agent communication mechanisms such as KIF, KQML and the FIPA standards, although none of these are yet sufficiently well established that adopting them yields real interoperability benefits.

6 The road to the NATO Virtual Enterprise

In the previous sections, the Virtual Enterprise concept has been introduced and the effort of ICT on the road to the virtual enterprise has been demonstrated. Common working environments enable crossing of organisational and geographical boundaries. Standards for information exchange are applied successfully, both in civil and military environments.

There are still a large number of open issues requiring further developments. In spite of the fact that most projects are currently focussed on the development of a Virtual Enterprise infrastructure, various aspects remain without proper solution. Much more work is necessary to support the dynamical creation and reconfiguration of virtual enterprises. NATO operations usually are of shorter time-spans and out-of-area. Therefore, the NATO virtual enterprise must be able to be created and reconfigured fast. In addition, the NATO virtual enterprise for such operations cannot always rely on large-bandwidth connections. The NATO virtual enterprise must also be able to cope with temporarily losses of connections and must be safe against information warfare attacks (information assurance). With respect to this last item, the dual-use ISO/IEC 15408 IT-Security Standard is particularly worth mentioning.

These special NATO requirements on virtual enterprises are not the focus, or at least not to the required extent, of commercial developments. Therefore, NATO research must concentrate on these specific problems and on technology to integrate solutions with commercially, and for dual-use, developed virtual enterprise technology. In this way, NATO may benefit largely from the commercial research and move quickly ahead on the road towards the NATO Virtual Enterprise. In doing so, special emphasis must be placed on business modelling. A further elaboration of the presented C2 wheel, for instance in the C4I model adopted by the Object Management Group OMG, could be an excellent starting point.

7 Conclusions and further work

In the future, more and more military operations have to be conducted by a coalition of NATO nations. This places new and more important requirements on the interoperability needed for such operations.

In this paper has been described how information management challenges may be met in achieving coalition interoperability by defining a road map towards a NATO Virtual Enterprise. Such an enterprise strongly supports the “interoperable communications”-target of the Defence Capabilities Initiative (DCI), launched at the NATO summit in Washington, April 1999.

An example from NLR’s own history of how standardisation of systems has evolved over the last twenty years has been given in order to show that the first steps on the road towards virtual enterprises has already been taken years ago. The implementation of virtual enterprises has become increasingly more feasible by recent developments in Information and Communication Technology. The stepping stones toward a virtual enterprise have been described. NATO must embrace these developments as stepping stones toward the NATO Virtual Enterprise. Further work within NLR will concentrate on a further elaboration of the C2 wheel, on ontology, and on

joint business models. Working environments will be based more and more on COTS, thereby pushing the level of standardisation upwards.

An example from the 2000/2001 Joint Warrior Interoperability Demonstration (JWID) has been given to indicate the current NATO interoperability achievements. An example of a research program has been given to indicate possible ways forward in the short-term future. In the long term, NATO Interoperability Frameworks should be aiming at aligning with commercial efforts. A possible road map towards the installation of a NATO Virtual Enterprise has been described.

8 References

1. Y.A.J.R. van de Vijver, *Time-critical allocation of Tactical Air Resources to Targets*, In: Proceedings of the NATO/RTO Symposium on Advanced Mission Management and System Integration Technologies for Improved Tactical Operations, Florence, Italy, 27-29 September 1999, NLR Technical Publication NLR-TP-99308.
2. http://public.logica.com/~grace
3. Chris Dee, Paul Millington, Ben Walls, and Tim Ward, *CABLE: A multi-agent architecture to support military command and control*, In: Proceedings of the Practical Application of Intelligent Agents and Multi-agent Systems (PAAM'98), London, 1998.
4. J.G. Stil, *Modernizing OMIS, an operational Air Force C2 system, using COTS hardware and software products*, In: Proceedings of the NATO/RTO Symposium on Commercial-Off-The-Shelf Products in Defense Applications "The Ruthless Pursuit of COTS", Brussels, Belgium, 3-5 April 2000, NLR Technical Publication NLR-TP-2000-085.
5. B.C. Schultheiss, E.H. Baalbergen, *Utilizing supercomputer power from your desktop*, HPCN Europe 2001 conference, 25-27 June 2001, Amsterdam, the Netherlands, NLR Technical Publication NLR-TP-2001-181.