Modernizing OMIS, an operational air force C2 system, using COTS hardware and software products

J.G. Stil
ICT Division
National Aerospace Laboratory NLR
P.O. Box 90502
1006 BM Amsterdam
The Netherlands
E-mail: stil@nlr.nl

Abstract

This paper outlines some experiences, gained with the modernization of an existing and operational air force Command and Control (C2) system using Commercial-Off-The-Shelf (COTS) hardware and software products and the adoption of standards, from a practitioners perspective. It describes examples of functional areas where requirements could be met using COTS products alone and where requirements couldn't be met and what strategies were followed to meet these requirements.

1 Introduction

This paper presents an example of the application of COTS hard- and software products for the modernization of an operational air force C2 system. The system consisted of a tailor made application running on COTS hardware. The application has been modernized using as much as possible COTS software products and the hardware has been replaced by leading edge technology hardware. The aim of this modernization was to come to a system based on state of the art technology. The new system had to be easier to use, have capabilities for interoperability, lower maintenance costs and it had to form a solid base for future functional extensions.

The paper describes how COTS products are applied to fulfill the military requirements, with emphasis on the application software. This paper also explains what measures have been taken to satisfy requirements where COTS products alone are not sufficient.

2 COTS products in a military environment

In the last decade more and more COTS information technology (IT) products become employed in military environments. Personal Computers, operating systems, office suites, database management systems, etc., originally meant for the consumer market, appeared to be usable to fulfill the military requirements. Implementation of these leading edge technology products in defense applications has become an attractive alternative for custom made systems and is generally seen as an effective way to cope with reduced budgets and staff. Advances in technology are no longer driven by military applications, but rather the military market only needs to exploit technology that exists in the commercial market [6].

Besides the lower costs, application of commercial available products can result in shortened acquisition times and a shorter *time-to-deployment* and therefore could provide military advantage, as stated in [2] and [7]. The earlier a leading edge technology becomes deployable in the battlefield, the better. The products are available relatively fast and the prices for these products continuously decrease. Furthermore, if products are available from multiple suppliers, dependency on a single supplier reduces.

Note however that in some situations application of COTS products alone is not sufficient, especially when

Paper presented at the RTO IST Symposium on "Commercial Off-the-Shelf Products in Defence Applications "The Ruthless Pursuit of COTS"", held in Brussels, Belgium, 3-5 April 2000, and published in RTO MP-48.

requirements are very military specific. COTS alone often results in a so-called 80 percent solution, which is generally what the COTS solution represents in terms of a comparison toward the customed desired or customed tailored requirements [3].

In many situations the missing requirements can be met by implementing glue code or by making modifications to the COTS product. In other situations it not possible to determine whether requirement can be met with a certain COTS product. In these situations it is often no longer possible to treat the COTS product as a black box. More (inside) details about the product might be necessary [5] and possibly involvement of the manufacturer.

M. Lockey and J. Briggs even state: "By definition, any development project cannot be completely COTS. There must always be some glue to integrate components or customize them which implies some level of understanding and involvement" [4].

Following paragraphs describe how COTS are applied in an operational military environment and what measures have been taken to cope with the shortcomings of the applied COTS products.

3 Overview OMIS

The example presented here describes the modernization of OMIS. OMIS is the Operations Management Information System which is in use by the Royal Netherlands Air Force (RNLAF) at Volkel Air Force Base in The Netherlands since 1983. OMIS is a command and control (C2) system which has as main goal to support the RNLAF in its task to prepare aircraft for missions to be flown. OMIS assists in the communication of all necessary information between different control centers and units and provides all users with consistent and up to date information, needed to perform their task. A schematic overview of the OMIS functionality is shown in figure 1.

The system met all requirements with respect to functionality, way of operation and security. The functionality was assured through continuous maintenance and adaptation of the application software to fit the changing needs of Volkel Air Force Base with respect to their business rules. The operational availability was assured by adding redundancy through application of multiple computers which mutually synchronized all information. Security was assured through the implementation of a sophisticated access control mechanism based on *the need to know* principle. The system was approved by military intelligence and was intensively used for the daily operations and during exercises.

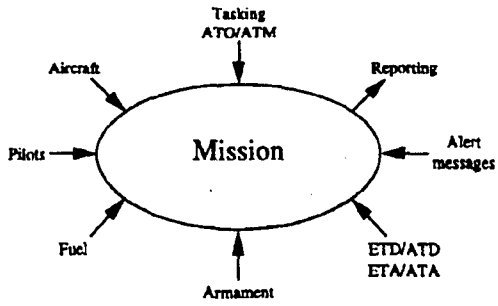

Figure 1: OMIS functionality

OMIS consists 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 (see figure 2). The OMIS application software was developed by the National Aerospace Laboratory (NLR) in the Netherlands, under responsibility of and in close cooperation with the RNLAF.

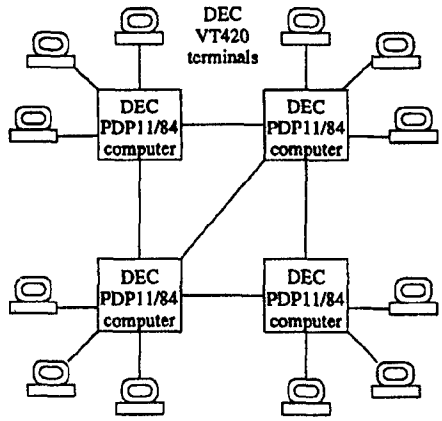

Figure 2: The OMIS network architecture

Not only the application software was tailor made. Functionalities that are less application specific, like database management and data replication, were also tailor made.

4 System life-cycle and modernization

4.1 Life-cycle aspects

In the mid 90's it became clear that it was no longer cost effective to maintain the current OMIS. The main problem was that the hardware had become obsolete. Spare parts became scarce and expensive maintenance contracts where necessary keep the systems up and running. Besides that, the OMIS software was of a former generation of software that lacked standardization and the capabilities for extension and interoperability. However, because the system was constantly adapted to fit the changing needs, the functionality was still valid and absolutely required to support the execution of the daily operations. Officers from Volkel AFB often say: "We can't fly without OMIS".

The RNLAF also had the intention to introduce OMIS at other bases in the Netherlands. Therefore the RNLAF decided to modernize OMIS. The resulting system had to be functional equivalent to the original system and had to meet the same requirements with respect to functionality, way of operation and security.

Further in this document the original OMIS will be called OMIS-1 whereas the modernized version of OMIS will be referred to as OMIS-2.

At the same time the RNLAF decided to realize a complete new IT infrastructure at all their bases. This new infrastructure, called KLuIM, had to be realized using COTS hard- and software products. KLuIM forms an *implementation middle layer* and should be used as the basis for all future applications. This new information infrastructure is intended to provide a multilevel secure environment in which command and control applications and office-like applications are used simultaneously.

Another justification to modernize OMIS was the changing operational role of the RNLAF. Till the late 80's the main task of the RNLAF was the defense of NATO territory during the cold war. This role has now changed to a role in which the RNLAF participates in multinational peace keeping operations, possibly where operational units are temporarily deployed *out-of-area*. This new operational task requires communication with other participating forces and therefore *interoperability* with other forces's information systems.

A technical, but certainly important, argument for modernization was the fact that the OMIS application and the operating system were judged not Y2K compliant.

4.2 Choices made

Two options for the modernization of OMIS were distinguished. The first option was to upgrade the hardware only and run the application software on an up to date platform, using emulators of the original hardware. This option guaranteed the operational continuity (only the Y2K problem had to be solved), but the resulting system still would lack standardization (at least at software level) and capabilities for interoperability and extendibility. Another draw back of this option was that emulators were only supplied by the manufacturer of the original hardware. This would result in a lack of freedom of supplier. This option was considered not very attractive.

The second option was to upgrade to the new COTS products based information infrastructure, existing of a new hardware platform, a new operating system and a new network, and to re-design and implement a functional equivalent of the application software using as much as possible COTS software products and standards. The application would be brought to state-of-the-art technology. The functionality of OMIS itself is defense unique, even air base unique. The type of application however is not defense unique and could be applied to non-defense environments, so it seemed to be possible to apply COTS products.

An argument for the second option is on standards for interoperability. Because the software had to be redesigned, the RNLAF also had the possibility to conform to a standardized data model to enable interoperability. The ATCCIS standard was adopted for OMIS-2 and adapted to the air force situation.

The RNLAF had plans to introduce OMIS-2 at other air bases also and therefore has chosen for the second option because this option offered a better maintainability and more opportunities for future extensions, which were indeed defined.

5 Hardware

5.1 General configuration

The choice of the hardware was, amongst others, influenced by the requirement that it had to be possible to run a wide variety of commercially available office applications and to use OMIS-2 for out-of-area operations. It had to be possible to use a small OMIS-2 configuration at locations where an operational unit of the RNLAF is deployed temporarily, possibly connected with the OMIS-2 configuration at the home base.

A choice was made for an Intel based computer platform running under the Microsoft Windows NT4 operating system. This choice allowed the application of a wide variety of Personal Computers, from laptop to large server, depending on the needed capacity and size of the configuration and a lot of office-like software products are available for an Intel/Windows based computer platform.

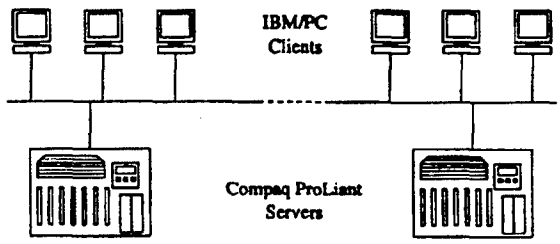

Figure 3: The OMIS-2 network architecture

The client computers are equipped with removable hard disks. This offers the advantage that defective systems can easily be replaced while the workstation related data stays available for the user, under the assumption that no disk failure occurred. Another advantage is that the disks of classified workstations can be locked in a safe outside operating hours.

Choosing de-facto PC standard hardware allows easy system upgrades to meet increasing performance requirements. At the start of the modernization, leading edge hardware could hardly meet the performance requirements. When the system was operationalized, which was about two years later, the advances in hardware technology happened so fast that the performance problems were no issue anymore.

5.2 Security

The new information infrastructure had to provide a multilevel secure environment at the operational air bases in the Netherlands. The need for a multilevel secure environment resulted from the requirement to be able to run office-like and command and control applications in the same environment. However, COTS network encryption hardware was not available due to the absence of military accreditation for these products. Accreditation was absolutely required because OMIS-2 needed to run on NATO SECRET level.

The KLuIM infrastructure was not available on time for the modernized OMIS and therefore the RNLAF decided to build a separate network. This network was realized conforming the standards that were defined for KLuIM and is used for command and control applications only. Later, when the encryption hardware becomes accreditated, this network will be used for office-like applications also.

The network that is implemented is an ATM-switched fiber optic network. For security reasons, not only the backbone is realized using fiber optic equipment but also the end user workstations are connected to the network via fiber optic cables also (no copper cables). This separate network is accreditated to run NATO SECRET.

5.3 Survivability

To assure failsafe operation at hardware level and continuity in emergency situations, the OMIS-2 configuration at Volkel AFB consists of multiple server computers, each located it a secure location. Whenever a server fails or gets lost, the other server(s) take over its tasks, mainly related to operating system and network management, so that the system stays available for the operational users.

Reliability of the servers itself was increased by applying hot pluggable RAID-5 (Redundant Array of Inexpensive Disks) disk units. This technology allows replacement of defective disks without interrupting system operation.

6 Application Software

During the modernization of the software, four important functional areas were encountered where COTS software products alone were not sufficient to fulfill the OMIS-2 requirements. These areas were security (especially access control), logging, survivability and interoperability. Following paragraphs describe what measures have been taken to satisfy the requirements.

6.1 General approach

General approach was to apply as much as possible COTS software products to meet all requirements. Some requirements that couldn't be met by the application of COTS products alone were satisfied by implementing missing capabilities on top of the COTS products using COTS available development tools. Other requirements could be satisfied by tailoring parts of the COTS software products.

The new OMIS had to be a client-server application in which all user interface related functionalities

were performed by clients and data management activities mainly by the server(s). The data stored in the servers had to be structured in a model compliant with the ATCCIS standard model.

Data management requirements could be satisfied by commercial available Relational Database Management System (RDBMS) products from Oracle. Database design tools from Oracle provide design capabilities compliant with ATCCIS modeling techniques.

In the future it might be possible that the applied COTS software products have to be upgraded to newer versions. To minimize the risk that the newer versions are no longer compatible with tailor made parts of the system, only capabilities of the COTS software products are used that are not de-supported by the manufacturer. Hardware and operating system specific features were avoided completely.

The original OMIS software contained some capabilities, especially related to security, logging and survivability which could not be provided by COTS software products alone. These issues will be detailed next.

6.2 Security

OMIS-2 required an access control mechanism following the *need to know* principle. This mechanism had to control the access to particular parts of the application and to the data accessed by those parts. Classification levels of the user and the location of the workstation had to be taken into account also when determining whether access was allowed or not. For example, parts of the application might only be accessible from a workstation located in a secure place such as a bunker.

The access control data had to be available on all participating database servers and be consistent. In a typical OMIS-2 configuration, multiple server computers are applied to assure continuity in case a server becomes unavailable. This means that users must have access to more than one server using the same user name/password combination.

Modifications to the access control data had to be made via a *two-men concept* to prevent security violations by administrators.

The access control mechanism provided by Oracle7 is only based on rights to access data stored in the database. Access to specific parts of a client application couldn't be controlled by this mechanism directly. This problem was solved by implementing a custom access control mechanism on top of the standard Oracle7 mechanism. This mechanism is used by the client application to determine access to the different parts of the application.

Standard Oracle7 also did not provide facilities to maintain a centralized user administration for distributed and replicated database servers. This problem was solved by implementing a mechanism which periodically synchronizes the distributed user administrations of the multiple server computers.

The problem related to the maintenance of the authorization related data was solved by implementing a special authorization data maintenance application using the COTS software development tools. This application forces administrators to apply changes on the authorization related data via the *two-men concept*. This means that modifications have to be made twice, by two different operators and within a certain time frame. After the first administrator has made modifications to the authorization data, this little application temporarily stores the modified authorization data in the database, so it can be used for comparison when the second administrator makes the same modifications. Only when the modifications, made by both administrators within the preset time frame, are exactly the same, the modification is accepted.

6.3 Logging

The original OMIS used a very extensive logging mechanism. For all modifications made to data in the database, the old and new values, the user making the modification and the time the modification was made, were registered. Besides a log of data mutations, an event log was maintained to register user actions. Both logs offered the capability to reconstruct the series of activities and mutations in case of system malfunctioning or security violations.

OMIS-2 required a similar logging mechanism to register all data manipulations and user activity. The mechanism provided by the Oracle7 database server (*tracing*) was not suitable for OMIS-2 because at some levels it did provide too detailed information whilst at other levels it did not.

This problem was solved by implementing a simple logging mechanism in the databases. This logging mechanism is based on a generator which generates logging facilities for specific data sets. By applying this technique the logging subsystem can easily be updated whenever changes to the structure of a data set have to be made.

6.4 Survivability

In OMIS, survivability was assured by applying multiple computers, each with a complete set of data stored on it. A tailor made replication mechanism kept the data on the different computers synchronized. For OMIS-2 this functionality had to be realized using Oracle capabilities.

Standard Oracle7 provides mechanisms to setup distributed databases and for database replication. The database replication mechanism takes care of the distribution of modifications made on one server to the other servers participating in a replicated environment. The replication mechanism provides facilities to detect conflicting simultaneous data manipulations on separate servers and methods to solve these conflicts.

The standard mechanisms couldn't be applied directly because the conflict detection techniques did not allow simultaneous updates on different attributes of the same object which was absolutely required by OMIS. For example, it had to be possible for a logistic officer and an operations officer to assign an aircraft and a pilot respectively to the same mission simultaneously when connected to different server computers.

The Oracle7 replication mechanism was slightly modified so that above mentioned operations could be performed. Also the conflict detection and resolution mechanism needed some simple modifications. The modifications made to the standard software are temporary since newer versions of Oracle ($\geq$Oracle8) provide required capabilities standard.

6.5 Interoperability

A new requirement for OMIS-2 was the capability to interoperate with other C2 systems. For OMIS-1 there was no such requirement and therefore this system lacked capabilities to interoperate.

At network level the interoperability requirement was met via the application of standard network hardware and software. At application level this requirement resulted in a complete re-design of the data model. The ATCCIS standard data model was used as basis for the new data model. All entities in the OMIS-2 functional environment were re-analyzed, normalized and placed in a so-called *ATCCIS-able* data model. Adoption of the ATCCIS concept facilitates future coupling with other national and possibly international (COTS based) Command and Control systems that are based on the ATCCIS model.

Application of a COTS relational database management system offered the possibility to utilize leading edge database technology for OMIS-2. The Oracle Relational Database Management System provided the enough functionality to implement the new data model. Database design tools from Oracle were used for the design of the database. These tools allowed automatic generation of the database.

7 Concluding Remarks

The modernization of OMIS showed the successful application of COTS products for a functional re-hosting. The re-hosting resulted in a system with a 100 percent equal functionality, but based on leading edge technology and with improved capabilities for future extensions and an improved ease of operation and management.

The application of standard PC hardware for the modernized OMIS showed that an assurance level at least equal to the assurance level of the original OMIS is possible.

The presented example showed that not all functionality could be realized directly by the COTS products itself. It appeared not to be possible to meet requirements related to security, logging and survivability using COTS products alone. These requirements were satisfied by implementing small modifications to the COTS products or by successfully using applying COTS software development tools to implement missing functionalities.

The requirement for interoperability was satisfied by using the ATCCIS standard for the data model. The resulting data model was implemented using COTS data management products without any problem.

Mid 1999, OMIS-2 is installed and operationalized at Volkel Air Force Base in the Netherlands. The configuration consists of multiple servers placed at secure locations, and client workstations all over the base. Minor problems were encountered during the installation, mostly related to the scaling of the system. After the installation it took only three days to operationalize OMIS-2. From mid October 1999 the modernized OMIS runs smoothly. Intensive usage during large exercises did not result in problems.

References

[1] *First Workshop on Ensuring Successful COTS Development*, May 22 1999.

[2] Emmett Paige Jr. (assistant defense secretary for command, control, communications and intelli-

gence). Striving for Information Superiority. *Defense Issue*, 11(72), June 22 1996. Prepared remarks to the 311th Theatre Signal Command Activation Dinner.

[3] Lloyd Mosemann (deputy assistant secretary of the air force). COTS in the Air Force - Success Story. 1995. Prepared statement to COTS'95 Conference.

[4] Micheal Looney and Jim Briggs. Some experiences and comments on the use of COTS Software in UK Naval Combat Systems. In *First Workshop on Ensuring Successful COTS Development* [1].

[5] Norman F. Schneidewind and Allen P. Nikora. Issues and Methods for Assessing COTS Reliability, Maintainability and Availability. In *First Workshop on Ensuring Successful COTS Development* [1].

[6] Richard Scott. Putting COTS in command. *Jane's Navy International*, 102(4), May 01 1997.

[7] Paul G. Kaminski (undersecretary of defense for acquisition and technology). Investing in Tomorrow's Technology Today. *Defense Issue*, 10(46), March 28 1995. Prepared statement to the Research and Development Subcommittee, House National Committee.