Collective Mission Simulation in The Netherlands Key Problems & Solutions

Jeroen Voogd, Klaas Jan de Kraker, Lesley Jacobs, Frido Kuijper
TNO Defence, Security and Safety
The Hague, The Netherlands
{jeroen.voogd, klaas_jan.dekraker, lesley.jacobs, frido.kuijper} @tno.nl

Michel Keuning
National Aerospace Laboratory
Amsterdam, The Netherlands
keuning@nlr.nl

Rombout Karelse
Simulation Expertise Centre, Netherlands MoD
The Hague, The Netherlands
RJ.Karelse@mindef.nl

ABSTRACT

Simulation has established itself as a powerful tool for the military domain. Collective Mission Simulation involves the use of mission simulation - the execution of (parts of) a tactical or operational mission in a (partly) simulated environment - for one or multiple teams. The Royal Netherlands Armed Forces have exploited Collective Mission Simulation (CMS) through participation in a number of virtual exercises. The potential of collective mission simulation has been recognized and the requirement for a CMS capability was formalized.

The need for a CMS capability has led to a Dutch national research into a collective mission simulation environment that can support training, exercises, mission rehearsal and experimentation. Such a simulation environment that supports collective missions in combined and joint settings is characterized by effective realism, interoperable systems across domains, and seamless information flow. Within the next few years the Royal Netherlands Armed Forces wants to establish a validated, reusable, interoperable mission simulation environment that will support the distributed simulation of tactical and operational missions at varying degrees of security classification. Clearly, the Royal Netherlands Armed Forces intends to also use the CMS capability in the international context of NATO and bi-lateral exercises/events.

In this paper we describe the challenges and shortcomings associated with applying collective mission simulation by the Royal Netherlands Armed Forces. We present our vision for a future CMS environment and the building blocks that are necessary for obtaining it. There are four building blocks that will enable the development and operation of a CMS environment: a defined CMS policy and a suitable organizational structure, guidance on procedures and technical standards (e.g. handbooks), the CMS Common Technology Framework to connect distributed simulation assets and facilities, and a set of services to allow smooth operation of the CMS environment.

ABOUT THE AUTHORS

Jeroen Voogd is a member of the scientific staff in the Defence, Security and Safety Division at TNO. He holds a Ph.D. (1998) in Computational Physics from the University of Amsterdam in the field of modelling and simulating of biophysical systems on parallel and distributed computing platforms. Currently he is involved in projects on simulating group behaviour, operational analysis studies of army operations and connecting C4I infrastructure to simulators. A recurring theme in his work of the last years is the quality of simulations. This involves issues like fidelity and VV&A of simulator assets, as well as quality assurance within TNO (e.g. audits).

Klaas Jan de Kraker is a member of the scientific staff in the Defence, Security and Safety Division at TNO. He holds a Ph.D. (1998) in Computer Science from Delft University of Technology. He has a background in Computer-Aided Design and Manufacturing, collaboration applications, software engineering (methodologies), meta modelling and data modelling. Currently he is leading various simulation projects in the areas of simulation based performance assessment, collective mission simulation, multifunctional simulation and serious gaming.

Lesley Jacobs is a member of the scientific staff in the Defence, Security and Safety Division at TNO. She works as training and simulation specialist in the department of Modelling and Simulation. She has been involved in various (inter)national projects concerning Mission Training through Distributed Simulation (MTDS). Currently, she is programme leader of the Dutch national research programme on Collective Mission Simulation. Lesley holds an MSc in Educational Science and Technology from the University of Twente, with a specialization in Simulation.

Frido Kuijper is a member of the scientific staff in the Defence, Security and Safety Division at TNO. He has a broad background and experience in real-time distributed simulation related research. His current assignment is the lead scientist for the research programme on natural synthetic environment modelling within TNO. Frido holds an MSc in Computer Science from Delft University of Technology with a specialization in Computer Graphics.

Michel Keuning is a senior scientist with the NLR, working at the training, simulation & operator performance department. His career at NLR began in 1996 in the field of safety critical software for airborne systems; by the turn of the century he had moved into the field of human-in-the-loop real-time simulation with focus on distributed mission simulation. He holds an MSc in Computer Science from the University of Twente.

Rombout Karelse is head of the Simulation Expertise Centre of the Royal Netherlands Armed Forces. He is tasked with standardization, interoperability and re-use of M&S.

Collective Mission Simulation in The Netherlands
Key Problems & Solutions

Jeroen Voogd, Klaas Jan de Kraker, Lesley Jacobs, Frido Kuijper
TNO Defence, Security and Safety
The Hague, The Netherlands
{jeroen.voogd, klaas_jan.dekraker, lesley.jacobs, frido.kuijper} @tno.nl

Michel Keuning
National Aerospace Laboratory
Amsterdam, The Netherlands
keuning@nlr.nl

Rombout Karelse
Simulation Expertise Centre, Netherlands MoD
The Hague, The Netherlands
RJ.Karelse@mindef.nl

INTRODUCTION

Mission simulation has established itself as a powerful tool for the military domain. Its value has been demonstrated in application areas such as operational analysis, system acquisition, training, and mission rehearsal. Mission simulation differentiates itself from platform simulation in that mission simulation involves tactical or operational aspects of a military mission. When involving multiple, potentially geographically dispersed, simulators, we talk about Collective Mission Simulations (CMS). In CMS, interactions between the simulated entities and between these entities and their simulated environment are of prime importance.

To date, the Royal Netherlands Armed Forces have exploited collective mission simulation only to a limited extent. Through participation in a number of virtual exercises, such as exercise JPOW, see (Wiel, 2006) and exercise First WAVE (RTO-TR-SAS-034, 2007), the potential of collective mission simulation has been recognized.

Due to a number of developments in the past decade, the relevance and importance of CMS is increasing strongly. Some of these developments are:

- Growing number of out-of-area operations, often with short preparation times;
- Frequently changing missions in complex (urban) environments, e.g., joint and combined, multi-national coalitions (e.g. Iraq, Afghanistan);
- Increasing peace-time limitations for live mission training and rehearsal, due to e.g. budget and system life time limitations, environmental constraints, security and safety issues;
- Decreasing availability of operational systems for mission training and rehearsal (due to more and longer operational deployments);
- Rapidly increasing simulation capabilitieswithin the Royal Netherlands Armed Forces, such as the introduction of the Tactical Indoor Simulator (TACTIS) for collective manoeuvre training;

All of these developments lead to a growing need for a collective mission simulation environment that can support mission training, rehearsal and experimentation.

Within the next few years the Royal Netherlands Armed Forces want to establish a validated, reusable, and interoperable mission simulation environment that will support the distributed simulation of tactical and operational missions at varying degrees of security classification.

Therefore, the Royal Netherlands Armed Forces is further extending their knowledge on the subject of CMS and is supporting developments of new processes, methods and technologies to improve CMS effectiveness. For this purpose a new national research programme was initiated by the name of “Collective Mission Simulation”. Also, a national M&S policy has been developed to create an integral vision to acquire and exploit M&S capabilities, including CMS.

This paper presents a vision on CMS from the perspective of the Royal Netherlands Armed Forces. This vision is placed in context with the present situation and the way to overcome present challenges. The “Collective Mission Simulation” programme plays an important role in achieving this vision and addresses some of the most urgent issues that currently challenge the use of CMS.

The remainder of this paper is organised as follows. First, we describe the key problems that currently occur when applying CMS. Next, we present our vision on CMS that addresses these challenges and presents solutions to the key problems. Subsequently we elaborate on the building blocks that should enable our vision. Lastly, we present our conclusions and plans for future work.

KEY PROBLEMS

Although Collective Mission Simulation (CMS) has a huge potential, it appears difficult in practice to actually realize such simulations. Our experience has shown that many hurdles have to be taken every time such event is carried out. Our experience in this area is are based on, for example, NATO Exercise First Wave, and various national projects including the Unit Level Trainer -Joint Operations Integrated Network Demonstrator (ULT-JOIND), which is illustrated in Figure 1.

Based upon these experiences we developed a vision and way ahead regarding CMS, identifying the key problems that hinder effective and efficient realization of a CMS environment. The first type of problems concerns various issues that we found to be lacking in the Netherlands. They are: Policy and Organization, Methods and Procedures, and Facilities. The second type of problems concerns various CMS issues that are to date unresolved. They are: effectiveness, interoperability, and security issues.

As we are developing a CMS vision for the Royal Netherlands Armed Forces, we describe the key problems that apply to the Dutch situation. However, we believe that these problems are relevant from a more general perspective as well.

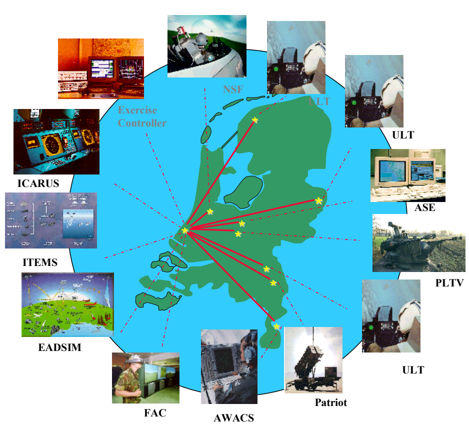

Figure 1. The ULT-JOIND network, a national CMS demonstration that involved air and ground simulation assets.

Policy and Organization

The first identified problem area concerns organizational issues. The key problem in this area is that there is no joint organization in the Netherlands that is responsible for establishing and exploiting CMS facilities. For example, there is no CMS Operations Centre that could provide CMS services and specialists, and there is no Joint Training Command to state the need for common CMS capabilities. An effect of the lack of a central CMS organization is that every individual CMS event performs similar activities, often in an ad hoc fashion. Typical recurring CMS activities are developing a system architecture, establishing a (secure) network, coupling different simulators, developing scenarios, and dealing with terrain databases.

Since funding is allocated to individual (and often single service) CMS activities, instead of a joint CMS organisation, there is hardly or no room for acquiring joint facilities and/or services that meet overall common requirements. So far, the work in the Netherlands on defining an M&S architecture has lead to standardization, but not to the development of common services. We conclude that the lack of a joint organization that is responsible for CMS facilities is holding back the operational exploitation of CMS capabilities.

Methods and procedures

The second main problem area is the lack of well-defined methods and procedures that assist in initializing CMS events. It appears often difficult and time consuming to initialize a CMS environment for a particular exercise or experiment. Getting all systems and databases ready for execution can be nightmarish. This does not only concern making the systems available. It also includes other aspects, for example taking care of security issues and arranging payment for system use.

A CMS environment shall have a well-documented set of practical methods and procedures that describe how the environment can be used efficiently and effectively. Step-by-step instructions shall be provided, that incorporate lessons learned from previous events and that should avoid that users are solving the same recurring problems time and again.

Facilities

The third main problem area that holds back CMS is the very practical fact that the required facilities to support CMS are lacking. Simulators are available at various locations and some may even have networking capabilities. However, components essential to CMS like secure networking at appropriate bandwidth, distributed (de)briefing facilities, and logging and analysis functions are simply not available throughout the country.

Effectiveness

The fourth main problem area concerns issues of realizing appropriate levels of effectiveness in CMS events.

The difficulty in this area is to develop a CMS environment that is fit for purpose. If a CMS environment is not fit for purpose, effectiveness problems will show up. In a distributed mission simulation training event, for example, realizing training effectiveness for multiple training audiences and training levels is a challenge. In a large scale training event many different trainees have different roles and objectives, making it increasingly difficult to meet these different individual training needs in an appropriate manner. The fact that CMS events are often conducted from dispersed locations is another complicating factor, especially in the area of distributed debriefings.

Training value may also decrease rapidly (or even result in negative training for participating units) when elements that are important for real world effectiveness are not reproduced with sufficient fidelity in the simulation environment.

In addition, the different applications that can benefit from CMS (e.g. training, mission rehearsal, analysis, tactics and doctrine development), each pose different requirements on CMS systems. For example, a training application typically requires a level playing field that provides fair fight conditions for all trainees (Boomgaardt and Kraker and Smelik, 2007). The virtual terrain database may very well be geo-typical rather than geo-specific. A mission rehearsal application on the other hand, typically requires that the simulation terrain database resembles the actual mission terrain very accurately. The problem here is that such aspects are often not addressed adequately during the development of the CMS environment, which results in simulations that are not validated for their particular use and thus may have low or negative effectiveness.

Interoperability

The fifth main problem area concerns issues of CMS systems interoperability.

Although significant efforts have been undertaken to develop simulation interoperability standards such as DIS and HLA (including reference FOMs), see (HLA Wikipedia, 2008) and (HLA IEEE 1516, 2000), and although such standards have been available for several years now, achieving interoperability in CMS in practice is still problematic.

The difficulty in this area lies in the fact that many of the currently used simulators were never designed to be connected into a CMS environment, and therefore have only limited solutions to do so. Current (legacy) simulators, and probably also many future simulators, are mostly systems that are closed black boxes. They often do not provide good means for interoperability and reuse. Moreover, making any changes to a simulator, such as replacing a terrain database or upgrading a simulator system component, often requires support from the manufacturer. This vendor lock-in makes CMS operations very costly and time consuming to realize.

Other problems in this area concern multinational aspects and multi-level training. When setting up a CMS environment in a multinational context, one is confronted with many different architectures (and associated security regulations) which logically enlarge the interoperability problems.

Security

The sixth and last problem area that we distinguish is the well-known area of security.

Network security, or in other words the risk of unauthorized entities tapping networks, is largely solved by using current security regulations and cryptography devices. However, practical problems remain. For example, the current security regulations are very time consuming, the availability of identical devices in a multinational context is an issue, and using cryptography devices may cause performance implications.

From the perspective of multinational CMS, security problems originate from the requirement that nations do not wish to share the detailed performance characteristics of their systems (platforms, weapon systems and sensor systems) with other nations. This causes extensive practical problems when setting up a CMS environment. On the one hand nations do want to perform multinational CMS, but on the other hand they are often hindered by security regulations to provide their simulators for such use. In our view the problem is that there's a lack of simulators whose fidelity and security classification can be adjusted to the needs of the specifics of a CMS exercise. We can safely state that taking away such security-related problems is key to successful applications of multinational CMS.

CMS VISION

This section presents our vision on CMS. It first describes the key characteristics of an ideal CMS environment and then gives an overview of the associated CMS facilities.

CMS environment characteristics

The CMS environment provides easy to use facilities to CMS users that fulfil their training and analysis needs. It takes away any hurdles that exist today, for example, in setting up the CMS environment for a particular experiment and in processing the experiment's results. Therefore, the CMS environment is highly adaptable and configurable to any application and use. For example, when using the CMS environment for a mission rehearsal session, a synthetic environment model of the mission area at hand is uploaded into the CMS environment and is automatically distributed to the various participating simulators, in their required format and fidelity. Also, the participating simulators are configured automatically with the (sensor and weapon) systems that occur in the mission rehearsal scenario. This is done in such a way that a level playing field is established and that fair-fight conditions are guaranteed.

The 24/7 environment allows easy joining of exercises by requiring human operated systems and Computer Generated Forces (CGF) to be interchangeable. The CGF are of high quality and validly mimic the behaviour of real entities. Besides the use of CGFs, large multi-national/coalition exercises can be conducted by easy coupling of the CMS environment with international CMS facilities.

Regarding issues of security, the elements of the CMS environment (i.e. the simulations) are able to adapt their classification level based on the required level of fidelity of the experiment. The CMS provides procedures and guidelines for doing so that are efficient and that comply with the current security regulations.

Furthermore, the CMS environment satisfies the needs of different military roles, or in other words it supports multi-level training. It provides facilities for multi-level briefing and debriefing and for full mission support including C4I systems. Performance assessment is partly automated and support is provided for the different debriefing levels.

Lastly, in our vision a CMS environment is not a fixed asset but instead is extendible in order to be future proof. Therefore provisions are incorporated for adding new players/nations and for transforming into a future Live Virtual Constructive (LVC) environment. The concept of LVC implies that besides virtual and constructive simulations, also live entities can participate in an exercise (Bizub and Cutts, 2007). The concept can provide very powerful training environments, and its development has gained a strong momentum in recent years.

CMS facilities

In Figure 2 the envisioned CMS environment is depicted schematically. Training facilities as well as operational units in the Royal Netherlands Armed Forces can participate. The "glue" in this environment is a CMS Operations Centre (CMSOC). The CMSOC is connected to the network and offers services to users. One of the services is to route all interactions via a service to ensure fair-play. It is also the place where exercise control can ensure that all training needs are fulfilled.

All participants are connected through the national CMS Common Technical Framework (CTF). For security reasons, all participants use security devices in the gateway to the CMS CTF. The gateway also allows interoperability of local systems with the other systems in the CMS environment.

The national CMS CTF can be coupled with the international CMS CTF. The roles of the national CMSOC is then partly taken over by the international CMSOC.

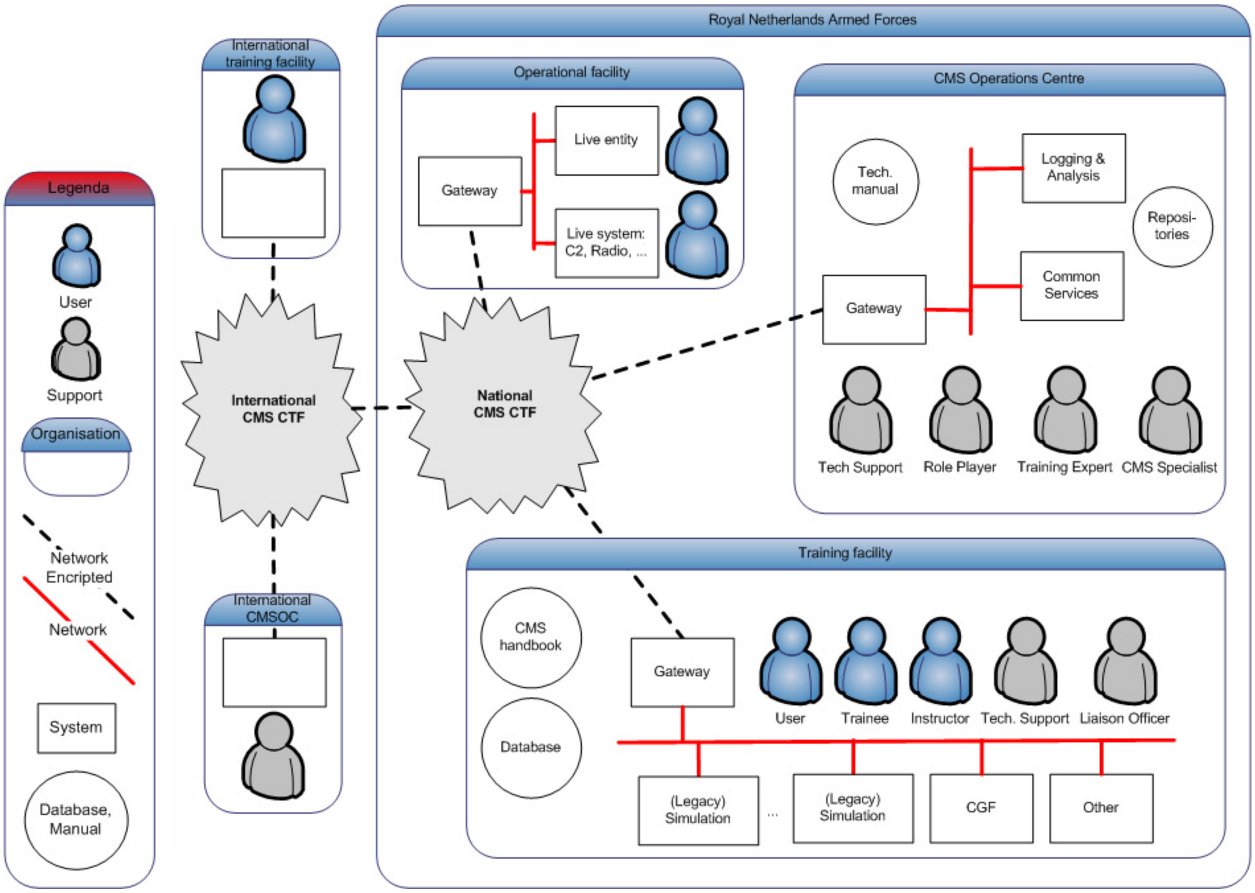

Figure 2. Overview of the envisioned (inter)national CMS environment.

ENABLING BUILDING BLOCKS

This chapter presents the building blocks that are required to realize our CMS vision. These building blocks provide the solutions to the key problems that were identified earlier. The building blocks are:

- Organization
- Guidance handbooks
- Common Technical Framework
- Common Services

Figure 3 visualizes the mapping of the key problems to the proposed building blocks. This illustrates that the building blocks each cover parts of the problem domain. Together they form the integrated constituents of a CMS environment.

Each of the building blocks is briefly described below and we discuss which parts of the vision a building block covers and which problems it addresses.

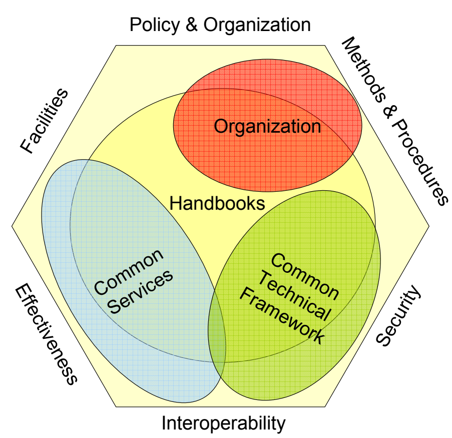

Figure 3. Mapping of Key problems to enabling building blocks.

Organization

This building block covers the important organizational aspects of the vision. The presented vision calls for two organizational structures: one to deal with long term aspects of the CMS vision, below denoted as the CMS Command, and one to deal with the more day-to-day practical aspects, further called the CMS Operations Centre (CMSOC). Below, first the CMS Command is described, then the CMSOC.

The task of the CMS Command is to develop and maintain the overall CMS vision and the management of the overall organizational aspects of CMS. This command serves as an umbrella for a number of subsidiary CMS Commands, one for each major CMS application. Thus specialized CMS Commands can exist for e.g. training & instruction, mission rehearsal and tactics & doctrine development, see Figure 4. These subsidiaries may be located in another part of the organization. For example the "CMS Joint Training Command" can be located in the "Joint Training Command" organization.

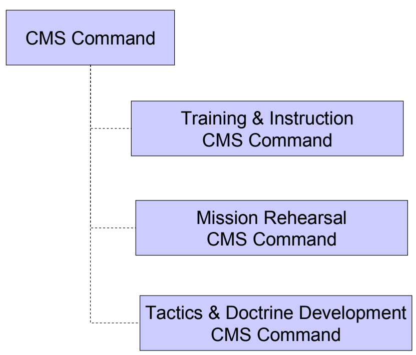

Figure 4. CMS Command organization

One of the key aspects of the work of the CMS Command is to promote the vision on and advertise the use of the CMS environment. To maintain and enhance an overall CMS vision it is necessary to keep track of the needs of the potential users of CMS and a harmonization with other visions such as presented in the national Modelling & Simulation Policy. To attract users it is necessary to get key personnel involved. They must promote the concept of CMS and simulation in general, and convince potential users to adopt and adapt to the CMS vision. With the increase in interest in CMS and a growing CMS capability, it should become easier to raise funding to fully implement a CMS environment.

The adoption of the CMS vision in the organization requires the adaptation of a number of processes in the defence organization and the definition of a number of new processes. The adaptations typically deal with provisions that are needed to work with the CMS environment. Where appropriate, specialized handbooks and manuals should be developed, see the next section.

One of the managerial tasks of the CMS Command is to make sure that the CMS environment remains relevant and up to date. This includes providing support to simulator acquisition projects, to ensure that newly acquired simulators are compliant with the CMS environment. CMS Command is also tasked with management of efforts that support the development of relevant emerging standards (e.g. CBML), development of a NL defence wide architecture, and international architectural solutions (e.g. LVC).

The CMS Command will also serve as a liaison point for international contacts, e.g. for the co-ordination of large exercises or experiments with the CMS environment. Nationally, it manages contacts and formalizes cooperation with e.g. the Royal Netherlands Army Geographic Agency for use of geo-data.

The CMS Command should implement effectiveness evaluation of the CMS environment and security and validity accreditation of the overall systems. The subsidiary CMS Commands are responsible for the effectiveness and validity of the CMS environment for their specific application area. This means that they specify what "fit for purpose" and valid use of the CMS environment means, see (Brade and Jacquart and Voogd and Yi, 2005). The result of this specification is captured in handbooks. This assessment also determines which systems can join the CMS environment in a valid way, and which systems can not. The subsidiaries have direct contact with the users of the CMS Environment and should record and handle lessons learned such that they can be processed in handbook updates. This will for example include guidelines on how multi-level training can be accommodated by joining various systems together in a way that all users get training value from the exercise.

The actual maintenance and daily operation of the CMS environment is taken care of by a separate organization: the CMS Operations Centre, CMSOC. It offers centralized services to be used during CMS exercises or experiments. Part of the tasks of the CMSOC is performed "on-line", i.e. in preparation of or during exercises and experiments, other tasks are performed off-line. The off-line tasks include support in development of the various handbooks. The CMSOC has the detailed technical knowledge of building and running the CMS environment, therefore it can contribute to handbooks regarding for example interoperability issues, security, rapid exercise set-up, validity and effectiveness assessment. The CMSOC can also contribute practical experience on making the CMS environment future proof by precluding vendor lock-in through the specification of requirements on the openness and flexibility of still to acquire systems. The

CMSOC will provide recommendations on such issues to the CMS Command for its policies. The CMSOC should also have personnel to give technical support on all mentioned topics for the benefit of new participants in the CMS.

The CMSOC will manage a number of systems to offer on-line central services. It has to do cost-benefit analysis on these assets and when necessary look for improvements or extensions. To keep up to date, the CMSOC can participate in research on e.g. increasing the level of interoperability between systems, fair play and obtaining a common playing field.

The CMSOC can maintain repositories of scenario's and databases (terrain, GIS, physics properties, entity interaction models) for general use in a standardized format. This can help to attain a common playing field among the participants.

The on-line services that the CMSOC must offer includes co-operation and co-ordination in (international) CMS events, mission planning support and facilitating the 'white force': role players and exercise control. In order to do this, the CMSOC must for example have systems for (de)briefing, scenario tools, multi-exercise planning tools, and logging and analysis. The CMSOC has a central role in ensuring a level playing field to allow for fair fight. The CMSOC can offer a central service that handles all interactions between entities and with the virtual environment in a fair manner.

One of the objectives is to have permanently available facilities that can either operate 24/7 or at least can be set-up on short notice. The CMSOC needs to be able to facilitate this.

Handbooks

An important building block for a coherent CMS environment consists of having guidance on how to build, operate and maintain such an environment. In the above vision on organization it is said that the guidance is developed by the CMS Command and its subsidiaries with contributions from CMSOC.

This guidance will be documented in a number of handbooks, each on a different topic and targeted to a specific audience. The guidance documents include technical, operational and organizational topics. There will be handbooks for use by the different levels of

1. the CMS Command and its subsidiaries,
2. the CMSOC, and
3. the operators of the various facilities that want to connect to the CMS environment.

The collection of handbooks tells the complete story for running a CMS organization, from planning, implementation, execution and evaluation of a CMS session, down to specific technical details. This will include, for example, a description of how to effectively integrate legacy simulators in a CMS exercise.

The first level concerns handbooks for the CMS Command. These handbooks deal with organizational aspects concerning security aspects for all systems and procedures for joining (international) exercises. There must be a set of rules that make sure that secure data never ends up on unsecured networks. The CMS Command handbooks must contain instructions on how to build for the future, i.e. specifications for open and flexible systems. This handbook is to be used during acquisitions and upgrades.

The subsidiary CMS Commands use handbooks in which it is specified what validity and effectiveness means, and how it can be measured, for their specific topic. It can also specify requirements on standards that must be adhered to for all systems and e.g. scenario files, terrain databases, etc.

The second level of handbooks, for use in the CMSOC, contains information on how to build and operate a CMS environment. One of the aspects is when and how to make the evaluation of what assets to use for a specific application in the CMS environment, effectiveness and validity aspects are here used together with the specific goal of a CMS run. For the identified applications of the CMS environment the handbook specifies a set of acceptance criteria that have to be met in order to have a valid simulation, and it specifies the process to do the validation for a specific CMS run. It can thus be determined which systems (where each trainee has its own goals) can be joined in a given scenario in a useful valid way. This information should also be recorded in a handbook, such that validation results can be reused. The handbooks for use in the CMSOC also contain guidelines on configuration management and test procedures.

The third level on which handbooks specific for CMS are used are the operators of facilities that are joined into the CMS environment, possibly by using the CMSOC services. These handbooks shall describe all the CMS related elements and how to make systems interoperate with the envisioned CMS environment, such as the FOM to use. Also the use of the CMSOC central services is described in detail. These services include those to ensure a level playing field, but also how to get and use scenarios, the logging and analysis service and how to connect to centralized (de)briefing equipment.

The training facilities that connect to the CMS environment are locally responsible for executing guidelines for validation to see which system can join the CMS environment given the exercise purpose and security demands. These facilities will each have to give regard to security instructions to make sure that their secure data only ends up where it is supposed to go. This may mean that degraded data has to be used.

Parts of the three levels of manuals described above can be specified as an overlay on the HLA FEDEP. Although other processes could also be used, the FEDEP is a general and often used development process description. There already exist a number of FEDEP process overlays. See Figure 5 for an illustration of the draft VV&A overlay from (SAC-PDG-VVA, 2006).

For the CMS specific elements a similar overlay can be envisioned. For each step in the process a number of tasks can be described that handle the CMS specific elements. Both the technical and organizational elements can be placed in this overlay. Besides the tasks also the flow of needed and produced information can be indicated.

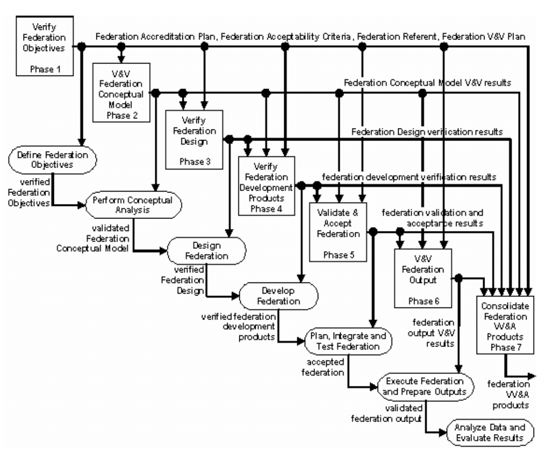

Figure 5. FEDEP VV&A Overlay

Common Technical Framework
This building block covers the necessary elements to connect the various systems in a secure and meaningful way. The Common Technical Framework (CTF) provides so-called Points of Presence (POP) that allow (national) facilities to connect to the CTF. Figure 6 depicts an example international CMS CTF and national CMS CTF including the associated POPs. A POP describes the gateway and security specifications that must be met by the facilities.

The gateways play an important role in making systems interoperable on a technical and semantic level. By providing protocol translation and performing other translation functions, the gateways can allow legacy systems to join the CTF. Besides these functions, gateways can also perform additional functionality such as filtering. Data can be filtered for entities of interest and region of interest.

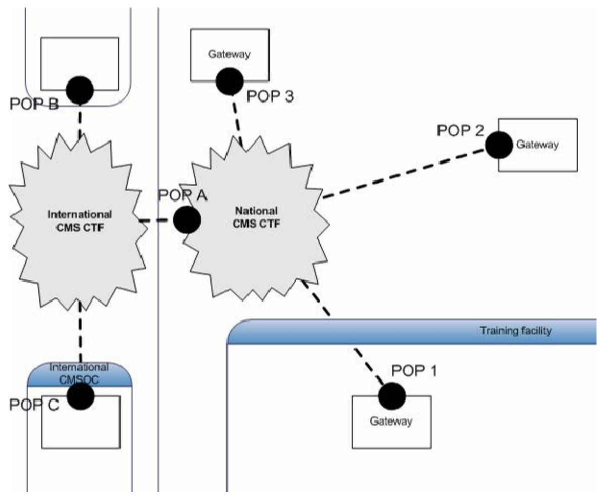

Figure 6. Common Technical Framework example

The gateways have to have an internal structure that allows easy upgrade to newer architectures and protocols because standards evolve while the CMS environment is supposed to exist for a long time. A plug-in structure allows building a dedicated plug-in for each legacy simulation.

The gateways can also perform a security function. It can make sure that within a facility "private" data of e.g. weapon systems data is used, while on the outside of the facility this data is not visible and e.g. an interaction service from the CMSOC is used. This solves the security problem of not wanting to share your data. The implementation of this security function is in the form of crypto boxes. These allow secure data to be sent over an unsecured network. For different exercises or cooperation with different users, different levels of security may be necessary, i.e. multi-level security. This may mean that different crypto boxes have to be used. These crypto boxes and organizational guidelines must assure a workable and secure environment.

Besides the simulations that can be connected to the CTF via gateways, operational systems can also be connected. This means that data coming from data links with command and control devices and radio links with entities such as aircraft and vehicles need to be supported. This should also include voice communication. Joining these operational systems allows for LVC co-operation. Drawbacks may include that "magic moves" and instant replay can not be supported for live entities.

The vision calls for an environment that can either be set up on short notice or even 24/7. This means that the CTF must at least have a high readiness. For the part of the vision that suggest a 24/7 environment, it will also be necessary to have a 24/7 CTF in operation. It should be easy to connect and disconnect from the CTF.

Lastly, the network itself. The (international) network must have sufficient quality of service to allow all the needed data traffic, i.e. high bandwidth, low latency. Especially when used for international exercises, the network will have to deal with different standards and architectures. These may have to be coupled by using translation services in a national or international CMSOC.

Common Services

In the proposed CMS vision it is made clear that in order for the CMS environment to operate smoothly and simulations to run fair for all parties, a set of common services shared by all CMS users is necessary. Some of these services are centralized, typically operated by the CMSOC; some have to be fulfilled by the facilities connected to the CMS environment themselves. Below first the central services are discussed and then the responsibilities of the facilities.

A number of central services are necessary for setting up the CMS environment for an exercise. For a quick set up it is necessary that the CTF is managed centrally, this can assure a high readiness of other central services. Especially for the 24/7 availability it will be necessary to automate all central services as much as possible. This may mean that the CMSOC has to have a number of CGFs running in exercises that can be replaced by human operated systems when requested. Due to the central role of the CMSOC it is also in a good position to handle the federation management.

The CMS environment must ensure a common playing field. This is most easily obtained by letting the CMSOC create and manage centrally available databases. These include databases for terrain, GIS, physics and scenario's. By distributing these source databases to the various facilities problems with correlation can be diminished, thus allowing for a common playing field. The facilities that receive the databases possibly have to translate the databases to a suitable format for their own systems.

The CMS environment must also provide a fair playing field. A centralized interaction handler, as has been proposed by (Boomgaardt and Kraker and Smelik, 2007), can be envisioned that handles all interactions between entities and between entities and the environment, and even multi-level interactions e.g. between entities and aggregates. Figure 7 depicts the architecture of the interaction handler prototype. An interaction reference database can be used to have fair sensors, lethality, protection and manoeuvrability. These services can also be used to generate and distribute dynamic aspects of the environment such as terrain, weather and sea state. Besides these entity and environment interactions, it must also be possible to handle radio interactions to allow for disturbances coming from the atmosphere, jammers and terrain features. Realistic secure communications can also be facilitated as a common service.

An important function that should be co-ordinated from the CMSOC is the accommodation of the white force. The white force includes exercise control and role players. The white force prepares and handles (de)briefing and video/audio conferencing. The central facility should offer services for (de)briefing, data logging and analysis, and facilitate video/audio conferences.

Figure 7. Interaction handler architecture

An important function that should be handled centrally from within a CMSOC is the accommodation of the white force. The white force includes exercise control and role players. The white force prepares and handles (de)briefing and video/audio conferencing. The central facility should offer services for (de)briefing, data logging and analysis, and facilitate video/audio conferences.

The facilities wishing to join CMS exercises must have a number of local services. As already mentioned, these include preparing the centrally offered databases for use in their local systems. A number of central services mentioned above also have local counterparts in order to work smoothly (e.g. (de)brief facilities, based on centralized data but also on data from local mission planning, logging and after action review tools).

CONCLUSIONS AND FUTURE WORK

The need for a Collective Mission Simulation (CMS) capability identified by the Royal Netherlands Armed Forces has led to national research into a collective mission simulation environment that can support training, exercises, mission rehearsal and experimentation. The current facilities show a number of shortcomings:

- the organization is not optimally structured for developing, and using a CMS environment and policies are lacking for gaining the most out of the current facilities,
- method and procedures need to be adapted or new ones constructed for operating an CMS environment,
- facilities need to be tailored for (distributed) CMS by offering specific services, and being flexible, reusable and future proof,
- effectiveness and fit-for-purpose need to be defined for the different applications,
- system interoperability can be expected to be a problem when systems built for such diverse backgrounds are connected on a large scale,
- security issues need to be tackled in an effective way before users are allowed and willing to use a CMS environment.

We have developed a vision that addresses these shortcomings and that is aimed at obtaining a CMS environment that supports collective missions in combined and joint settings. This vision transforms current ad hoc practices into a new paradigm that effectively and efficiently supports the delivery of the combat readiness of the Dutch Armed Forces. This is characterized by providing effective realism, reusable, valid, interoperable systems across domains, and seamless information flow, at multiple security classification levels. To realize this vision, a number of enabling building blocks need to be instantiated. The identified building blocks are:

- the current organizational structure needs to be changed in order to develop and maintain a CMS environment,
- handbooks need to be present on various levels of the CMS organization to coherently acquire, build, operate and maintain the CMS environment,
- a Common Technical Framework (CTF) is necessary to connect the necessary elements in a secure and meaningful way,
- a set of centralized services with their distributed counterparts are needed for smooth operations and a level playing field.

The Dutch national CMS environment will have a strong international component. International cooperation is therefore sought with coalition partners and NATO, such as for example NATO's LVC initiative. We have a strong interest in international M&S visions, and in the development of relevant standards such as HLA evolved and languages for interoperability of simulation with C2 equipment such as the Joint Battle Management Language (JBML), and in the subject of simulation model validation. As such, the envisioned CMS environment will be a significant step forward for the Dutch armed forces on the roadmap towards the effective - national and international - use of CMS.

REFERENCES

Bizub, W. & Cutts, D. (2007). *Live, Virtual Constructive (LVC) Architecture Interoperability Assessment*, I/ITSEC 2007

Boomgaardt, J.J. & Kraker, K.J. de & Smelik, R.M. (2007), Achieving a Level Playing Field in Distributed Simulations, *Proceedings of Fall Simulation Interoperability Workshop*, Orlando, FL, September 2007, 07F-SIW-009.

Brade, D. & Jacquart, R. & Voogd, J.M. & Yi, C-H. (2005) *"WEAG THALES JP11.20 (REVVA) Results and Perspectives",* 05E-SIW-021.

HLA IEEE 1516 (2000). *IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA)*, IEEE 1516.

HLA Wikipedia, (2008). *High Level Architecture (HLA).* Retrieved January 5, 2008, from http://en.wikipedia.org/wiki/High_Level_Architecture

RTO-TR-SAS-034 (2007). *Mission Training via Distributed Simulation and First WAVE: Final Report,* NATO Research and Technology Organisation.

SAC-PDG-VVA (2006). *Draft Recommended Practice for Verification, Validation, and Accreditation of a Federation, Overlay to the High Level Architecture Development and Execution Process*, SISO

Wiel, W. van der (2006). J-ROADS Air Defence Simulation Support during the 2006 JPOW IX Missile Defence Exercise. *NATO Modeling & Simulation Conference,* RTO-MP-MSG-045, paper 12.