Enabling Distributed Mission Training

Sanjay Khetia
QinetiQ
Farnborough, Hampshire, UK
skhetia@qinetiq.com

ABSTRACT

The UK MOD has a vision of providing Mission Training through Distributed Simulation, or UK MTDS. The UK MTDS Capability Concept Demonstrator (CCD) programme developed a RAF facility comprising of 4-fast-jet Tornado GR4 and 4-Typhoon simulators, a 7-seat AWACS mission crew training system, and an extensive exercise management capability (including virtual role players and Computer Generated Forces (CGF) and After Action Review (AAR) facilities). In a representative Planning, Briefing and Debriefing (PBD) daily cycle, training participants performed a series of air battlespace missions with joint and multi-national collective teams in a series of nine events. Each event provided evidence and identified lessons addressing various key issues associated with the UK MTDS vision.

This case study will identify real examples of lessons learnt in simulator interoperability between collocated and dispersed training sites utilising air, land and maritime synthetic training environments (STE). To enable interoperability technical issues associated with Local and Wide Area Networking (LAN/WAN), including security protocols and how best to achieve connectivity with other sites and countries will be discussed.

The distributed training model of a hub linked to main operating bases was largely validated during the MTDS CCD programme. Prior research indicated that being distributed from the hub site can reduce training benefit; the MTDS CCD programme demonstrated that this can be mitigated by providing robust Planning Briefing and Debriefing (PBD) equipment, sharing common visual models and providing higher fidelity training equipment.

The experience gained from the MTDS CCD demonstrates that many of the procedures for security accreditation are open to interpretation, and that there is a need to build and maintain personal relationships within the accreditor community to achieve timely approval.

In summary, this case study will both guide technologists in real lessons learnt and challenge the simulation community through practical experiences.

ABOUT THE AUTHORS

Sanjay Khetia graduated with a degree in Computing and Economics he joined QinetiQ in 1999 as a software developer initially on satID systems. In 2001 Sanjay started working on Human in the loop simulations playing an important role in the specification and development of a new generic simulation system. Sanjay has extensive experience of exploiting simulation technology for customers in the Air and Land domains leading QinetiQ technical teams on a number of large UK programmes delivering Synthetic Operational Training. Sanjay is the Capability Group Leader for Joint Training Solutions Group and has been the MTDS CCD and DSALT Technical manager for the last 4 years.

Enabling Distributed Mission Training

Sanjay Khetia
QinetiQ
Farnborough, Hampshire, UK
skhetia@qinetiq.com

INTRODUCTION

Simulation to provide Synthetic Operational Training (SOT) has been in operation for some time. The use of synthetic environments (SE) augments the more expensive live flight training in operational platforms. The Mission Training through Distributed Simulation Capability Concept Demonstrator (MTDS CCD) programme ran from 2005 to 2008 at the Air Battlespace Training Centre (ABTC) at RAF Waddington. The programme was developed to study various elements of synthetic training and provide guidance for the UK MOD on the technical and operational issues in implementing a distributed training program for fast-jet and other aircrew. This programme was managed by the Flight Simulation and Synthetic Trainers Integrated Project Team (FsAST IPT) with research support from the Defence Science and Technology Laboratory (Dstl), RAF Air Command and their manpower support contractor, Inzpire Ltd.

The main purpose of the programme was to address a number of Key Investigative Areas (KIAs) and wider questions. In order to answer these KIAs, UK, US and Canadian forces and their military personnel from air, land and maritime service participated in the MTDS CCD events, during which their requirements for a MTDS capability were captured.

This paper will describe the salient lessons learnt during the MTDS CCD in enabling distributed mission training. Simulation interoperability, Local and Wide Area Networking (LAN/WAN), security protocols and how best to achieve connectivity with other sites and countries will be discussed.

MTDS CCD FACILITY

The MTDS CCD facility consisted of eight fast jet simulators (four Typhoons and four Tornado GR4 aircraft), a seven seat E-3 AWACS capability, and a comprehensive exercise management and control suite.

Figure 1: MTDS CCD facilities.

A 40-seat briefing and de-briefing room and a selection of smaller formation planning rooms were provided. These incorporated standard in-service planning aids and video conferencing, telephone and interactive whiteboard technology so that the subjects could undertake a condensed cycle of planning, briefing, execution and debriefing (PBED).

A classified networking hub allowed for connecting securely with training facilities elsewhere in the UK, US and Canada, including the AH-64 Apache training facility provided by Aviation Training International Limited (ATIL), and the HMS Dryad Frigate Training facility in Southwick Park. The hub also established international training links to multiple locations in the US including the Air Force Research Laboratory (AFRL) in Mesa, Arizona, the Distributed Mission Operations Center (DMOC) at Kirtland AFB in Albuquerque, New Mexico, and finally, into the USAF's DMO network through a

connection at the DMO Operations and Integration (O&I) contractor facility in Orlando, Florida.

DISTRIBUTED CONNECTIONS

The MTDS CCD facility connected to AFRL through a direct serial T-1 connection with a 1.544 Mbs capacity provided by UK Defence Communications Services Agency (DCSA). This AFRL circuit was highly reliable and had low latency.

A single Attack Helicopter site at RAF Dishforth was linked to the MTDS CCD facility via a private ATM 2Mbs network link. Provided by the DCSA under the Global Communications Systems (GCS) IPT, the link was maintained by Telindus.

The Joint Multi-National Interoperability Assurance Network (JMNIAN) network was utilised to connect the CCD facility to HMS Dryad for investigation of connectivity to a legacy Royal Navy Frigate Simulator. The link was a 4 Mbs pipe, providing a portion of that bandwidth for DIS and the remaining for VTC, VoIP, and SMARTBoard & Bridgit™ applications.

For the last CCD distributed training event, it was decided that the QinetiQ Civilian Telecommunication Officer (CTO) in Malvern would act as the network bearer provider. This event used a 4Mbit/s WAN connection to the USAF DMO NOC (Network Operations Centre) in Orlando, Florida. This provided the CCD programme with access to the US Distributed Missions Operation Network (DMON).

While the MTDS CCD program used various solutions, technologies, and providers for communication bearers, the common theme in implementing a WAN was the allocation of sufficient calendar time to properly test the connection, the division of responsibility and ensure the link was providing the agreed to bandwidth capacity.

Several hurdles existed in the creation of WAN links to external sites for the MTDS CCD programme. The following issues had to be addressed for Team ACTIVE to be able to answer the network-related KIA's:

• Working with WAN link bearer providers to define a network which would meet the simulation performance requirements.
• Interfacing to legacy simulation facilities which may not have network capabilities
• Creation of a secure link to protect the simulation data on the WAN
• Development of international agreements for provision of a distributed training capability

Latency

The success of a distributed simulation relies upon a significant number of factors, one of which is the latency of network links. The WAN latency of geographically distributed sites can be a significant impact, especially for international coalition exercises involving a large amount of data relating to fast moving aircraft and missiles. It has been established by the Distributed Interoperability Simulation (DIS) standard (IEEE 1278.2) that the maximum amount of latency for tightly coupled engagements should be 100ms (this equates to a ping latency round trip time of 200ms). The DIS standard allows a maximum latency of 300ms for loosely coupled engagements. With latency greater than this, anomalies appear within the SE .

SIMULATION INTEROPERABILITY

The MTDS CCD facility used IEEE 1278 DIS (Distributed Interactive Simulation) simulation protocols as the information transport layer between the synthetic environment components. The scope of DIS utilisation was covered in a CCD specific Interface Control Document (ICD).

The main DIS producing applications in the CCD were:

- GR4 Tornado Simulators x 4 – based on QinetiQ's Real-Time All Vehicle Simulator (RTAVS)
- Computer Generated Forces (CGF) system – Boeing BigTAC
- Real-time viewer/ After Action Review (AAR) / CGF tool suite – Boeing Insight
- Communication system – based on the ASTi radio system
- Red Air role player stations – RTAVS

- Typhoon aircraft Simulators x 4 - RTAVS
- Airborne Warning And Control System (AWACS) Simulator – Southwest Research Institute
- Forward Air Controller (FAC) station x 2 – Meggitt
- CGF system – Joint Semi-Autonomous Forces (JSAF)
- CGF system – Combined Arms Tactical Trainer (CATT)
- Apache (AH) helicopter role player station - RTAVS
- Tactical Unmanned Air Vehicle (TUAV) role player station – RTAVS

In addition a number of DIS applications have been linked in externally over the WAN during distributed exercises from sites in the UK, US and Germany (albeit a US base in Germany). This has included connections to the US through the DMOC and DMON.

- Apache AH-64 Simulators at Dishforth, UK
- Naval Type 42 simulator at Southwick park (formerly HMS Dryad), UK
- F16 & A10 Simulators at AFRL (MESA), US
- F15 simulators at Langley, US
- F15 & AWACS simulators at Albuquerque, US
- AWACS E3-C Simulators at Tinker, US
- A10 simulators at Spangdahlem, US airbase in Germany
- Joint Tactical Air Controller at AFRL (MESA), US & Defence Research and Development Canada

SIMULATION DATA FILTERING

When carrying out distributed exercises there are various external constraints that limit the time and scope of what can be done to achieve full interoperability between all the components in a synthetic exercise.

One of the major issues in achieving interoperability was that often there was limited scope, if any, to modify existing legacy devices.

Internal to the MTDS CCD facility and on its wide area network interface DIS filtering and data changing applications were used as the major component to enable interoperability between all the systems. The use of these LAN-LAN and LAN-WAN filter boxes to separate the disparate network segments has proved a success in the MTDS CCD exercises. These gateways allowed us to block and modify data when applications could not be altered or fixed.

Data Filtering

The LAN-LAN and LAN-WAN gateways used in the MTDS CCD provided the ability to both block and change data based on run-time user configurable input files. Blocking PDUs based on their type or content is done for two reasons. Firstly, to reduce network-load by preventing unnecessary information passing, and secondly to prevent specific PDUs being received which are causing local applications problems. Ideally where we are blocking data for the second reason it would be preferable that the faulty applications were actually fixed but as discussed previously this is not always possible.

These gateways could also be configured to enforce particular DIS standards. This means blocking PDUs whose format or content is not fully compliant with the DIS standards or whose content lies outside of the MTDS CCD ICD.

Data changing/filtering potentially adds latency into the system, particularly if incoming data need to be referenced against some internal data-store. The filtering applications used within the MTDS CCD operated with minimal latency and did not present any problems within the MTDS CCD exercises.

Data Changing

Data changing is again necessary to correct faulty PDU outputs or applications that cannot handle valid input. Usually this involves changing individual fields in a PDU from one value to another. Data changing does have ramifications when it comes to logging and analysis, as now different components of the SE are receiving variants on ground truth data. In instances where this involves changing positions the affect of this on the exercise must be understood to ensure that what is being done remains valid.

WHERE SIMULATION GATEWAYS AID

This section will highlight some of the areas where interoperability issues arose during the MTDS CCD

programme and provides real examples of how the gateways proved useful.

Visual Modelling & Database Correlation

The large number of different simulators used during the MTDS CCD programme, including legacy simulators, meant that there were a large number of uncorrelated terrain databases used in the various events.

Where possible, efforts were made to achieve correlation between simulations, by the building of new databases and sharing of source data where possible, but frequently it is not always feasible for all systems to integrate new visual databases. As a result the majority of systems operated using ground clamping. Although this helped enable a coherent visual scene to be achieved, interactions between different simulations proved more complicated. Having altered ground-truth the local model must adjust all sensor inputs/outputs and munition fire/detonation events to correct for the adjustments it has made in ground-clamping. The MTDS CCD exercises highlighted that very few systems actually seem to carry out this processing adequately.

Entity Representation Using DIS

Having displayed an entity at its correct location and orientation there can still be correlation issues if the model displayed is inconsistent between systems. With some legacy systems this may be because the exact vehicle model type is not available and so the nearest 'best fit' is used or worse still is to not display any entity at all.

As well as the entity types issue there are a number of Entity State PDU (ESPDU) bit-mapped fields that describe the appearance and status of the entity. It is important that all systems correctly visualize these affects and in a consistent manner. In particular, damage, smoke and dust effects, if not consistently displayed, can slew the fidelity of an SE. During the MTDS CCD a number of systems were found to be erroneously interpreting these appearance and environmental fields i.e. a smoke plume on one system might be large enough to act as a general navigation point, but on another be so small as to be barely noticeable. These errors could not be fixed and it was necessary to remap these values within the gateways to correct the incorrect appearance.

Sensor Modelling Using DIS

The MTDS CCD ICD defined all system types, their associated beam types and the beam type expected modes that were to be supported within the MTDS CCD. As extra components where introduced this list expanded and extra items where added. When linking externally it was necessary for them to support the emissions as described on the MTDS CCD ICD. Part of local integration testing prior to any new exercise involved testing that new system/beam/mode configurations were correctly interpreted by the existing core systems. The flexibility to add the correct responses to new emission types proved to be not as good as it should have been. In fact, it proved impossible to correct the behaviour of certain systems, instead gateways had to be used to alter the PDUs to be something that the legacy system did support.

Weapons modelling using DIS

During the MTDS CCD exercises the correct handling of detonations by all systems was problematic. Many systems only process targeting detonations specifically targeted at themselves and therefore do not react correctly to detonation events within their immediate proximity. Other applications were only sensitive to specific munition types and completely ignored unknown types rather than falling back to some reasonable default behaviour. Unexpected warhead, fuse and detonation-result fields also caused problems. The solution to these short-falls during the MTDS CCD was to use the gateways to alter these unexpected values to known expected values.

Entity Regeneration

Due to the dynamic nature of the scenarios that were executed during the MTDS CCD, it was beneficial to have the ability to regenerate entities that had previously been killed, or alternatively dynamically insert threats. Although it is possible to regenerate entities within some CGF systems, sometimes (dependent on systems) this can only happen at the entities' initially planned position and only after regeneration can these entities be relocated. It was also found to be beneficial to be able to generate 'pop-up' threats and have dormant surface-to-air missile (SAM) sites that could be activated during the scenario; however these entities can still be constrained as defined above.

The dynamic relocation of entities that existed within scenarios generated a number of issues during the MTDS CCD. Where the entity to be relocated was directly, or indirectly, providing situational awareness for other participants, there was a danger of losing immersion for the training audience. This was evident where entities generating Link16 PPLI messages or IFF messages would suddenly 'teleport' to a new location, resulting in confusion for any player that was monitoring this information such as Typhoon Link16 or AWACS. Additionally, Link16 PPLI and IFF codes proved troublesome for the AWACS training audience when entities were regenerated. This arose as the regenerated entities used the same modes and codes as before their death or removal from the scenario; this led to confusion amongst the AWACS operators as entities had apparently returned from the dead.

SECURITY & EXPORT CONTROL

Whilst there may be major advances and lessons learnt with networking and simulation interoperability technologies the biggest hurdle to overcome during the MTDS CCD was security. Whilst the simulation gateways and WAN links facilitate synthetic operational training for the war-fighter, for coalition training to be effective, it is necessary to provide systems with a high level of fidelity and realism.

This level of fidelity will typically result in a higher protective marking (PM) for the simulation information exchange. When that data exchange must occur between networked facilities in different nations, the level of security protection greatly increases.

Such a data transfer will need authorization from the national government as well as departments of defence. The highest level of fidelity attracts the highest PM therefore encryption will be required for protection of information in transit. Building of such a secure network requires development of authorization to include Codes of Connections, Interoperation Agreements, Memorandums of Agreement, or other necessary documents.

Cryptographic Equipment

The classification of simulation facilities both in the UK and the US leads to the requirement for an encrypted link between the training facilities. Throughout the MTDS CCD programme a number of connections were used to external sites with a different WAN connection implying different cryptographic requirements. Data over the UK JMNIAN WAN is transmitted over ATM network clouds, requiring a different encryption device than point to point connections. During MTDS CCD,

Encryption is used to protect information in transit and, in general, these protocols are not visible outside the encryption devices. Approved encryption devices are chosen for their compatibility with the network, their throughput performance and their availability and reliability.

While most equipment in simulation networking is readily available Commercial Off The Shelf (COTS) equipment, the encryption devices and Cryptographic Key Material (CKM) are approved and/or provided by a nation's respective Communication Security (COMSEC) agency. A program wishing to set up a secure network must submit the appropriate system design documentation prior to purchasing the crypto equipment and requesting the CKM.

UK Secure Network

There are various issues to consider when planning a connection to a secret WAN. The Joint Multi-National Interoperability Assurance Network (JMNIAN) is a secure UK Asynchronous Transfer Mode (ATM) WAN using the Defence Fixed Telecommunications Service (DFTS) flexible high bandwidth service. This has the advantage of being a managed network that supports various security levels.

While the JMNIAN network can support multiple levels of security, current operational policy is for all distributed simulation training facilities connected together on a network to be running at the same security level. To implement a secure WAN, it is important that all custodians are aware of the planning requirements and that the necessary authorisations are in place to hold CKM and issue it.

Another consideration when planning a UK Cryptographic installation is the documentary requirements. Defence Security Standards Organisation (DSSO) advice must be sought with sufficient time to obtain Security Accreditation. Ensuring that all CKM issuing authorities are correctly briefed and authorised to receive the crypto and, importantly, to reissue to the user, have adequate courier arrangements in place and

trying to reduce dependency on the Defence Courier Service, can all prove important in reducing time scales. Similarly, UK secure communication facilities require approval by Site Coordinator Installation Design Authority (SCIDA) before any installation work can take place. Allowing lead time for the production of CKM is therefore required. This all has timing implications upon UK secure WAN connection integration and testing.

Coalition Secure Network

Connection to another country's secure networks for the purpose of coalition training presents numerous issues in the technical and procedural arenas. The US may mandate US national encryption for such data exchanges, while other nations may have their own encryption requirements that need to be coordinated.

Currently, government approved encryption is not interoperable between nations. As a result it is necessary for an agreement to be made for a UK/US WAN link. UK/US crypto equipment will have to be mutually agreed upon by the respective governments and documented in the Interoperability Agreement. In order to obtain US cryptographic devices it is necessary to have a Department of Defense (DoD) Foreign Military Sales (FMS) case submitted and supported by an Information Sharing agreement which is sponsored by a DoD department.

Where procedures for security accreditation within a nation are defined clearly in security manuals, the approach to accreditation for multi-country simulation training is not so straightforward. In cases not so clearly defined, security procedures are subject to agreements between accreditors. This highlights the need for the facility or network security officer to build and maintain close working relationships with the accreditors. Those relationships provide the security officer a clearer understanding of what the accreditors deem necessary and allow the accreditor to understand better the approach taken by the contractors to ensure security within the facility.

For connection to foreign government simulation systems an agreement on the type of encryption device has to be sought. This process will involve both the Directorate of Defence Security (DDefSy) and Communications-Electronics Security Group (CESG) as the UK National Technical Authority. In the main for connection to US networks the encryption device will be a US national device. For connection to other foreign networks then the selection and approval for use of a UK device will have to be obtained from Government security accreditors.

LESSONS LEARNT

The need to provide further training in tactics and operational command and control have introduced a number of equally necessary training requirements which require the air crews and other forces to operate in a realistic training environment. As a result of the MTDS CCD further requirements are being identified for training with other nation's forces in Joint and Coalition operations.

The current norm for this type of training would be to develop scenarios and deploy all trainees to a central facility with all the manpower and equipment necessary to conduct a full scale exercise. With budgets being trimmed, the distributed training capability saves money by being able to train in simulators at the aircrew's home base instead of travelling to a central location.

With a distributed training capability in place, the UK will be able to train jointly with other components of the UK Military or in a coalition event with military from the US or other coalition partners.

A key lesson learnt in the MTDS CCD WAN implementation was in getting the customer involved in developing the international agreements which would precipitate the coalition networks. The agreements must be in place between cooperating national governments so that the security accreditations can be completed.

Customer involvement was also critical in getting the WAN links in place and provision of cryptographic key material. Where there existed UK MOD requirements for link provision via a specified government organisation, the customer was critical in developing those bearer relationships to get links in proper time. The cryptographic material must be handled and transferred via governmental organizations, and thus the customer is critical in enabling the secure network.

One factor that facilitated the level of customer involvement in the MTDS CCD programme was having US and UK contractors as members of Team ACTIVE. These contractors knew the international networking security requirements and were able to communicate to their respective governments to enable the international links.

The WAN link provision in the MTDS CCD programme took various paths. Where ATM Links exist (such as the UK MOD's JMNIAN), the connectivity was far simpler to implement and technically more reliable. Those benefits along with the higher bandwidth capacity showed ATM to be a technically superior link.

The provision of new WAN links requires significant schedule time to implement. The lesson learned is that the process for developing a new WAN link requires numerous steps that must be executed in a serial fashion, starting with the development of the interoperability agreement, and proceeding with the design solution and security accreditation. Recognition of this process and constant management of it will enable the WAN link provision to proceed at a faster pace.

CONCLUSION

As a conclusion, the MTDS CCD programme showed successful integration of Synthetic Environment equipment and simulators at RAF Waddington with other distributed simulations both within the UK and in the US. This programme was able to develop WAN links to support the training goals of the customer in a timely fashion and proved that the use of interoperability gateways provided the essential functionality in enabling distributed mission training.

REFERENCES

Dudfield, H.J., Beattie, D., Bruce, F. and Clark, W. (2008) MTDS CCD Final Report, *QinetiQ Technical Report.*

ACKNOWLEDGEMENTS

Grateful thanks for all military UK, US and Canadian training participants, role players and operators. To all members of Team ACTIVE throughout the programme. To AFRL Mesa, for their generosity in sharing Coalition Mission Training Research (CMTR) toolset and data through international collaboration via the UK MOD Dstl. For the support of the FsAST IPT and the three services and commands. In particular, Air Battlespace Training Centre, Air Warfare Centre, RAF Waddington, Inzpire, Dstl, DEC TA, and Air Command.