# A COMPLEX SYNTHETIC ENVIRONMENT FOR REAL-TIME, DISTRIBUTED AIRCREW TRAINING RESEARCH

**David A. Greschke**
**Simulation Technologies, Inc.**
**Air Force Research Laboratory, Mesa AZ USA**

**Edward Mayo**
**QinetiQ, Bedford UK**

**Stuart C. Grant**
**Defence R & D Canada, Toronto ON Canada**

During November 2001, AFRL (US), Defence R & D Canada and QinetiQ (on behalf of the UK MoD), conducted the first in a series of simulation trials to investigate the potential of an international collective environment for real-time, ground-based aircrew training. The trial involved simulating a mixed air-to-air and air-to-ground package using manned virtual simulators in the US for the friendly force and manned simulators, computer generated forces, and human role players at the Bedford site in the UK for both the friendly and enemy forces. The Canadian site was a passive stealth node on the network. The simulated operational environment known as the "scenario" was designed to be as realistic as possible. Front-line, mission ready crews manned the simulators, while other military personnel took the roles of the command chain for both friendly and hostile forces. This allowed the simulated missions to be run as they would be in a real operational environment, with full pre-sortie briefings, crew planning, sortie execution and debriefing all conducted via a secure long haul link between the countries. The implementation of the trial infrastructure involved significant development and integration effort, covering aspects such as long-haul secure data and voice communications; scenario development and management; data recording and analysis tools; planning, briefing and debriefing systems; and computer generated forces. This paper describes the trial infrastructure, explains its development, and reviews the lessons learned during its development and use.

## ABOUT THE AUTHORS

David A. Greschke is the Senior Technical Analyst at the Air Force Research Laboratory, Human Effectiveness Directorate, Warfighter Training Research Division in Mesa, Arizona. He is also the Manager of the Distributed Mission Training Testbed at AFRL Mesa. Mr. Greschke has over 30 years of experience in flight simulation as an Air Force fighter pilot for 22 years, as Program Manager for the Simulator for Air-to-Air Combat, and as the lead engineer for DMT engineering research and development for the onsite contractor at the Mesa Research Site since 1992. He has been responsible for many national and international real-time technical experiments and training demonstrations using distributed simulation. Currently the Chairman of the NATO SAS-034 Technical Task Team, he is responsible for developing a six nation distributed, real-time virtual simulation network that will be used to demonstrate the potential utility of mission training via distributed simulation in Exercise First WAVE in early 2004.

Edward Mayo is employed at QinetiQ plc where some of his duties include trials integration for research relating to air training. Previously he was a technical leader within Future Systems Technology Division at DERA. His first five years within DERA had been spent in the Centre for Defence Analysis (CDA) and its forerunners analyzing future military airborne concepts. Prior to joining DERA he worked for British Aerospace (Military Aircraft Division) as an Aerodynamicist after leaving Queen Mary and Westfield college with a degree in Aeronautical engineering.

Stuart C. Grant is a Defence Scientist with Defence Research & Development Canada. He conducts human factors research on the use of emerging technologies for training and mission rehearsal, including virtual reality technologies and intelligent agents. Current projects include simulation for dismounted combatants and the acquisition of team skills in virtual environments. He received his Ph.D. in cognitive psychology from the University of Toronto in 1994.

# A COMPLEX SYNTHETIC ENVIRONMENT FOR REAL-TIME, DISTRIBUTED AIRCREW TRAINING RESEARCH

**David A. Greschke**
**Simulation Technologies, Inc.**
**Air Force Research Laboratory, Mesa, AZ USA**

**Edward Mayo**
**QinetiQ, Bedford UK**

**Stuart C. Grant**
**Defence R & D Canada, Toronto ON Canada**

Since Coalition and Combined Air Operations have in recent years become more and more common (e.g. Balkans, Afghanistan, Iraq, Gulf War), there is a renewed interest and a recognised value in live training exercises demonstrated by the various flag exercises such as Red Flag in the USA and Tactical Leadership Program in Europe. However, the opportunities for aircrew to practise and rehearse live coalition training to any significant extent beyond the mentioned venues above are few and far between.

Through the year 2001, and continuing into 2002, QinetiQ plc, Bedford, UK, the Air Force Research Laboratory in Mesa, Arizona, and Defence R&D Canada in Toronto are performing a number of simulation trials to confirm the potential of a long haul collective environment for real-time distributed aircrew training. Including this first trial, known as *Trial VirtEgo*, the Coalition Mission Training Research Program, CMTR, will place a number of international teams, drawn from front line mission ready aircrew, in a representative operational scenario and provide them with all the facilities that would be available to them when performing a real operation, from appropriate briefings to a representative, fully populated simulation environment. The trials are being conducted under a Project Arrangement (PA) governed by The Technical Cooperation Program, TTCP.

A vast amount of technology and many civilian and military personnel from the UK, US and Canada, have been brought together to provide the high fidelity simulation environment for CMTR. This paper describes some of the reasoning that has taken the research down this path, the scenario used within the trials, and the underlying technologies that have been employed to provide the crews with this collective training environment.

## Trial VirtEgo

One of the main objectives of the trials programme has been to create a virtual environment that represents, as accurately as possible within the constraints, a realistic, operational theatre (Crane, Tomlinson, and J. Bell, 2002). To that end a scenario based on recent real-world operations was chosen. The specifics of the scenario were based on recent operational experience of US and UK aircrew.

The trial was designed to cover three days. Day 1 was a familiarisation day. Day 2 was a Medium Level (ML) Thermal Imaging Airborne Laser Designator (TIALD) mission against a fixed facility. Day 3 was a Medium level TIALD mission against a deployed Scud (with on-scene commander option).

More specifically, the missions were designed to exercise the aircrews' team interactions with the addition of 'trigger events', which were not expected by the aircrew. These included events such as intelligence updates during mission planning, radio communications jamming, munitions unavailability, system malfunctions, and engagements by previously unknown ground based air defence (GBAD) sites.

The assets simulated and their types are listed in Table 1. For each of the primary missions, the main package of coalition aircraft included the four Jaguars (as the bombers), four Tornado F3s (as fighter escort), four F-16Cs (as either fighter escort or in a swing role), four F-16CJs (in the suppression of enemy air defences (SEAD) role) and an EA-6B as an escort jammer. The other

assets in Table 1 played a supporting or hostile role in the trial.

| Asset | Simulation Type |
|---|---|
| *Coalition Air* | |
| UK Jaguar GR.1<br>UK Tornado F.3 | UK Virtual |
| US F-16C | US virtual |
| UK Harrier GR7<br>UK E3D<br>UK Nimrod R<br>US F-15E<br>US F-16 CJ<br>US EA-6B<br>US KC-135 | UK constructive |
| *Threat Air* | |
| MIG 25<br>MIG 23 | |
| *Threat GBAD* | |
| Early Warning Radar<br>SA-2<br>SA-3<br>SA-6<br>Roland<br>KS-12<br>KS-19<br>KS-30<br>S-60 | |

***Table 1 Trial VirtEgo Asset List***

## SIMULATION DESCRIPTION

### Simulation Sites

***United Kingdom.*** The UK used the RTAVS family of simulators (Greig, Mayo, & Crush, 2000) in two forms: RTAVS-immersive (Figure 1), RTAVS-Mission (Figure 2). The RTAVS simulators are based upon PCs using high-end graphics cards (from Primary image) for outside world generation. Both UK systems used a common sourced database. The RTAVS system has been developed in-house by QinetiQ to meet research requirements. All of the systems were DIS compliant and this was the prime means of interconnection. RTAVS makes use of PC technology as it has matured and has been used by QinetiQ for studies in the Synthetic Environment (SE) field.

The RTAVS system is able to provide a cockpit environment to support both air-to-air and air-to-ground aircraft types, in this case Tornado F3 (two seat) and Jaguar GR1 (single seat), respectively. Although the cockpits are generic in nature they provide the aircrew with all the necessary information that they would get in the real thing. Two of the RAF Aircrew flew the ground attack missions in an immersive visual environment using RTAVS simulators. The simulators provide a 270$^{o}$ field of view, a generic cockpit with three representative head down displays and the necessary controls to operate the aircraft and weapon systems including the Thermal Imaging and Laser Designation (TIALD) system. A Jaguar aircraft armed with sidewinders for self-protection and either carrying a reconnaissance pod, solely Paveway II (Laser Guided Bombs (LGBs)) or a combination of TIALD and Paveway II (depending on the exact mission type and the role of the aircraft) was simulated. The Jaguar pilots flew the bombing mission whereby one aircraft designated the target and the other dropped the LGB. Two RAF instructors flew the mission using the RTAVS mission simulators.

RAF Aircrew flew the four Tornado F3 fighters whose role was to escort the bombers to the target area and protect them from airborne threats. The Tornado F3's were armed with AIM-120 and AIM-9L missiles. Four students (two sets of F3 crew) flew the escort mission using the RTAVS-immersive simulators and the two instructors flew using the RTAVS mission simulators.

***Figure 1 RTAVS immersive***

***United States***. The US site participated with four F-16C Block 30 Multi-Task Trainer (MTT) simulators at the Air Force Research Laboratory's Distributed Mission Training Testbed facility in Mesa, Arizona. Qualified F-16 pilots flew the simulators during the exercise.

On the first day of the mission the F-16s played an air-to-ground role. They were equipped with General Purpose 500 lb bombs, AIM-120 and AIM-9 missiles. On the second day the F-16s took an air-to-air role and carried AIM-120 and AIM-9 missiles. The AFRL F-16 simulators are full fidelity cockpits each with a 360-degree field of regard visual display system using the M2DART. The simulator complex and supporting facilities are described further in Mack and Bell (2001).

***Figure 2 RTAVS mission***


***Figure 3 F-16C MTTs at AFRL Mesa***

The high fidelity nature of the F-16 MTT required that some systems be disabled in the simulators for the trial. This proved to be a minor work item, once identified, owing to the modular nature of the simulator designs at the US site. Being a research and development facility, alternative systems models with suitable security classification were available, as were the personnel to make the substitution. A similar ability might prove desirable in future operational training installations.

***Canada.*** Canada participated as a stealth-viewing node on the network as an initial step in participation in large scale, long haul simulations. As such, the Canadian site did not host any virtual or constructive simulation. Rather, the site was intended to allow viewers to observe all stages of the trial and was therefore equipped with a 3D stealth viewer, a data recording and logging system, teleconference facilities, and a voice comms station in addition to the long haul data communications equipment.

The stealth viewer consisted of a personal computer with a consumer graphics card running ModIOS Perspective Stealth View Display software. Custom coding, as well as the software tools Polyworks by Innovmetric Inc. and Polytrans by Okino Computer Graphics, allowed a radical reduction in size of the database used by the UK and US virtual simulations. The number of polygons and the photo texturing memory requirement were reduced, sacrificing terrain detail, but preserving graphics power for rendering the targets and entity models. This provided acceptable stealth viewer performance, highlighting the range of image generators that can and should be supported within long haul networks. It generated imagery of the simulation events for display on a 61" plasma screen. The same display was connected to the teleconference system and electronic whiteboard (Figure 4). The voice comms station ran the ModIOS Voice software.

***Figure 4 DRDC Stealth View Suite***

**Long Haul Secure Networks**

The network topology for the trial was based on an IP point-to-point architecture using the US site as the hub and extended spokes to the UK and CA sites. The US – CA spoke was a leased T1 line dedicated for the trial and established as a point-to-point link. A multiplexed bundle of 24 ISDN lines (T1 equivalent) created the US – UK spoke.

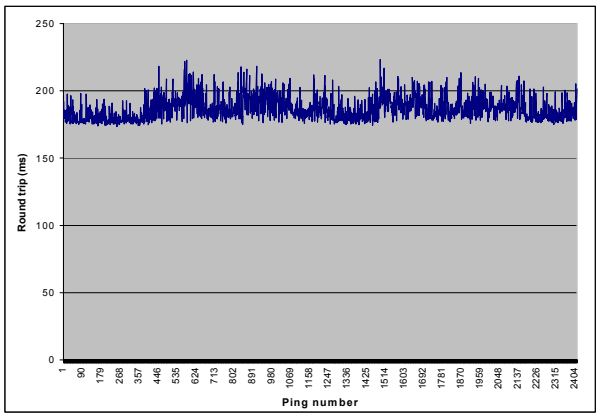
***United States.*** The US site is a facility accredited for processing of classified data. Existing procedures, equipment, and systems were in place and, therefore, very little incremental effort was required to satisfy security concerns.

Within the US facility, the local area network was based on a 10/100 Base-T system. The local network was connected to two wide area gateways (one for T1 and one for ISDN) via standard COTS switches and routers. KIV-7 encryption units were used in both gateways. The trial was conducted at the SECRET level.

The ISDN lines obtained for the US – UK spoke did not allow the US site to accept dial-in from UK. It was felt at the time of the original installation at AFRL that not having a phone number assigned would add to the security protection since the line would not have a dial-in capability. This proved to be an unnecessary and costly mistake. When using ISDN lines it does not matter which end ISDN line initiates the call. However, the site initiating the call is the billed party. The fact that only the US could call the UK and not vice versa, and that the US supplier of the ISDN service was unable to solve the telephone number problem within the timeframe of the trial, AFRL had to pay the entire ISDN cost for the test, integration and trial periods. That cost was $78,000. A lesson to be learned for future multi-site ISDN based networks.

***United Kingdom.*** Due to time-scales and as a risk reduction option for the first trial, help was requested from the Air Force Research Laboratory in Mesa. This request was supported by sending communications and network specialists from Mesa to QinetiQ for the duration of the trial. They brought with them the KIV-7 encryption device, which was compatible with the existing ISDN dial-up connection. Since this device was an already approved encryption system by the UK accreditation authority, approval was obtained for its use for this trial.

All simulation data and voice packets were sent over the communications infrastructure using the DIS 2.0.4 protocol. Separate frequencies were assigned for tactical voice and exercise control. Prior to mission start each day the data lines were also used for video and voice communications for intelligence briefings and pre-mission planning. The video comms were terminated prior to mission start. Due to what was believed to be an equipment anomaly at the UK site, only 16 of the 24 available ISDN channels were used for Trial VirtEgo. This made the bandwidth of the data pipe approximately 1.024 Mbps. The average round-trip 'ping' was of the order of 190ms, well within the 240ms round-trip time desired for DIS. Graph 1 below shows the round-trip times between the US and UK for a realistically loaded network. Regardless of the load, the average round-trip latency remained below 200ms. Once the ISDN link was established between Bedford, UK, and AFRL Mesa, AZ, it was very stable throughout mission execution. This is almost identical to the latencies experienced by AFRL in the AFA 2000 demonstration that connected Mesa, AZ, Wash DC, and Crawley, UK (Greschke & Bell, 2002). As expected, the encryptors had little noticeable impact on latency (10-15ms) and there appeared to be no noticeable packet loss. The maximum bandwidth used was of the order of 60%. Network traffic filtering was also used to make maximum use of the available bandwidth over the WAN.




***Graph 1 Round-trip time between UK and US with a realistic simulation load***

Using an SGI Octane AFRL pinged the ASTi radio system located in the UK. This test included the encryption devices. Packets of 176 bytes at rates from 100 Packets Per Second (PPS) to 1000 PPS were tested. Rates above 500 PPS showed a marked increase in latency indicating that the throughput of the system had been exceeded.

Data for these cases was ignored when looking at minimum, average and maximum latency values. Between 100 and 500 PPS, 14 different rates were used (100, 150, 175, 200, 225 PPS, etc.), and each case was repeated twice for a total of 28 cases. Each case performs 3000 pings for a total of 84,000 pings performed. The results are listed in the table below.

| | Min (ms) | Ave (ms) | Max (ms) |
|---|---|---|---|
| Average of All Cases | 182.2 | 196.5 | 219.1 |
| Minimum of All Cases | 179.1 | 192.1 | 209.8 |
| Maximum of All Cases | 188.7 | 203.6 | 241.9 |

In addition to the above, a replay of last year's scenario was replayed and ping tests were performed at one-second intervals. 1,980 pings were completed during this replay. Two pings of 340 ms (the first ping and one other half way through) were way out of line with all other data and were therefore discarded. These results are listed in the table below.

| | Min (ms) | Ave (ms) | Max (ms) |
|---|---|---|---|
| Replay Ping Test | 176.3 | 196.0 | 242.6 |

The replay packet rates are variable and therefore show the maximum range of variability, while the average agrees very well with the stand-alone ping test.

Analysis of the Trial VirtEgo DIS data packets revealed the following breakdown of PDU type contributing to the overall load. After entity state PDUs, the signal PDU used to carry the DIS voice traffic is the most data intensive PDU type.

| PDU type | % of PDUs | % of data |
|---|---|---|
| Entity state | 41.9 | 41.7 |
| Signal | 15.9 | 27.7 |
| Electro magnetic | 20.3 | 15.4 |
| Comment | 6.1 | 6.7 |
| Transmitter | 9.1 | 6.2 |
| Receiver | 5.2 | 1.2 |
| Other | 1.5 | 1.1 |

***Canada.*** The Canadian site was created within existing laboratory space from new equipment for the purposes of the Trial VirtEgo. Equipment procurement was a minor work item, but preparing the site for the processing of classified data was a major hurdle. Not only did the process consume resources, it also consumed time. The managerial, technical, and regulatory work entailed a substantial delay in the initiation of classified testing.

This was unfortunate because serviceability of the long haul portion of the network was also an issue for the T1 line connecting the US and Canadian sites. The long distance network provider made several errors in configuring the T1 line between the two sites. The link was initially inoperable and extended testing was needed to determine the cause and establish connectivity. This consumed the time that was allotted for establishing network interoperability testing between the two sites. The connection eventually carried 1.536 Mbs with 'ping' indicating 0% packet loss. The reliable connection, however, was not accomplished until after Trial VirtEgo was complete. Therefore, the Canadian site had to observe the exercise played back later over the network by the data logger which was successful.

**Exercise Management**

The ExMan systems deployed at QinetiQ, Bedford for the trial can be split into two distinct, although related, groupings – those to aid the White Force in their understanding of the scenario as it unfolded, and those that enabled the role-players to interact with the simulation. For the trial, the former consisted primarily of a prototype system called "The ROC", the Real-time Observers Console.

The philosophy behind the design of the ROC was to concentrate on providing the information that the White Forces felt they required in order to assess the collective (rather than individual) performance of the teams. An important element of the trial was the use of 'injects' to trigger specific types of team behaviour. It was important that the ROC and other ExMan systems allow the White Force team to judge the appropriate time in the scenario to perform the inject, and then allow them to monitor the outcome.

The ROC included a system to generate event-markers in the network simulation log to aid subsequent replay and analysis. These could

either be automatic (i.e. generated without human intervention when certain conditions are met) or manual, with the operator being able to select from a list of pre-defined event types or manually enter a new descriptor.

A number of 'Role-Player Stations' were produced to allow those members of the White Force team required to interact directly or indirectly with the experimental subjects. These included an AWACS display and a SOC RAP display. These were variations of the same system, and basically provided the role-player with a view of the synthetic battle-space as perceived by the forces (both human and CGF) under their control.

Additionally, the ExMan system included data logging and replay facilities to allow post-sortie and post-trial analysis of the exercise. This included voice and video recording of the briefing and debriefing sessions, as well as in-mission recording.

The ExMan was manned by the White Force who were active duty (serving) RAF personnel from the Air Warfare Centre (AWC). The White Force comprised of an AWACS controller, a Tornado F3 controller / observer, a Jaguar GR1 controller / observer, an overall exercise controller ('the boss'), a blue force CGF controller, a red force CGF controller and a red force GBAD controller. The technical team supported the White Force but in essence it was the White Force who ran the show. The ExMan system has been laid out so that White Force members were able to access the information pertinent to their roles. This information was displayed to them in a variety of ways including, ROC GUI, 2D/3D tactical displays, stealth views, comms channel viewer, aircrew voice, comms boxes and repeats of Tornado and jaguar HDD (see Figure 5). In addition to this the White Force personnel responsible for the control of the CGF were able to control the CGF via voice commands, which worked with varying degrees of success. The US Exercise Control Station is shown in Figure 5a.


***Figure 5 UK Exercise Management Facility***


***Figure 5a US Exercise Control Station***

**Data recording and analysis tools**

Data recording at the US and CA sites used the AFRL Distributed Mission Training Control Station Software (DCS). This software has a broad range of functionality, but the logging, replay, and visualisation capabilities were of primary importance in this trial. In the UK, the in-house developed NuNu DIS logger software recorded the DIS data packets including data and voice. These systems were used together for remote playback of mission events during debriefing. While the DCS system from AFRL has the ability to be controlled from remote sites allowing synchronized debrief of the data files, this feature was not used due to training requirements of the Air Warfare Center in the UK. The remote controlled, synchronized debrief capability will be utilized in future CMTR trials.

**Radio Communications Suite**

The overall comms system can be broken down into five separate areas:

i. Controller / Exercise Management comms
ii. Aircrew comms
iii. Monitoring of aircrew channel selection
iv. Long haul comms link
v. Voice comms recording

The UK site used in-house technology to provide the comms local area comm channels which were then input into an ASTi radio communications PC which output the DIS protocols necessary to connect to the ASTI system in the US and the ModIOS Voice system in Canada.

**Planning, briefing and debriefing systems**

The actual time spent flying was a relatively small part of any one trial day. For every hour spent flying in the simulation environment, five hours were spent in briefing, planning and debriefing sessions. For the purposes of realism the aircrew brought their own mission planning equipment, the output of which was downloaded into simulators. In short, each day comprised of the issue of an Air Tasking Order (ATO), followed by a Met (weather) brief, an intelligence brief, planning session by the aircrews, a Mass brief and finally a formation brief before climbing into the cockpits. Debrief sessions were conducted for the individual squadrons and for the package as a whole followed by a Mass debrief conducted by the Mission Commander. The planning session was aided and abetted by an adjoining CAOC cell that injected information into the aircrew planning sessions, information such as latest met reports, intelligence reports and last minute reports that required the aircrew to re-plan, e.g. non-availability of support assets. The layout of the briefing, planning and debriefing sessions was as close as possible to reality.

To carry this out over a long haul link necessitated a suite of equipment that allowed aircrew on different continents to plan and brief together. This included the use of video teleconference equipment, Smart Board digital whiteboards, Microsoft NetMeeting software, and more mundane equipment such as microphones at each site (Figures 4, 6, 7). The use of the video link required careful control of scene content to retain acceptable system performance. In addition, the aircrew did not have prior experience with conducting briefings in this manner, and they were understandably conservative in their use of the system. They showed a preference for using cameras, telephones, and fax machines to enable their conventional planning tools across the long distance rather than employing the newer technologies.

***Figure 6 AFRL US Briefing/Debriefing Room with Long Haul VTC and SmartBoard technology***

***Figure 7 AFRL's Digital Debriefing System***

**Computer Generated Forces**

The CGF were provided using a combination of JointSAF (the STOW development of ModSAF) and an in-house system (based on the RTAVS modelling framework). Six PC-technology Linux workstations running JointSAF version 4.8 were used to provide all of the air-based CGF entities, which were split into three functional groups to ease management – ‘package’, ‘support’ and ‘hostile’. The integrated GBAD systems were provided by RTAVS-based systems running relatively high fidelity models of the SAM sites, AAA sites and early warning radar systems. These were operated in a semi-autonomous mode, with a human role-player tasking them and monitoring their behaviour. A voice interface for controlling the CGF is being researched in the UK and was employed for control of some CGF. The system

proved beneficial but it was not yet developed to a state where it could be used exclusively.

The CGF fulfilled all those roles that were not manned, role-played or who had any direct manned decision making involvement, e.g. EMCON measures by the threat GBAD forces. This amounted to about 40 (depending on mission type) airborne assets requiring simulation for both hostile and friendly platforms. The CGF was primarily supplied by ModSAF and typically consisted of F-16CJs, Harrier GR7s, F-15E, EA-6B, F-15C, an E-3D, a KC-135, a Nimrod R, MiG-23s and MiG-25s. The CGF mission planning was carried out prior to the missions being flown due to the number and complexity of the mission types. For the mission to succeed as planned it was important that the CGF members of the scenario met their time on targets and fulfilled the role that they had been tasked. To this end it was important that the aircrew took off when they were tasked as those CGF flying from airbases further from the combat arena were already airborne and had been flying for up to an hour prior to the aircrew take-off times. It was very important that the CGF and manned players flew under a tight a formation and with close timings as possible.

***Role-player systems.*** The role of the AWACS was to provide a Recognised Air Picture (RAP) that was then fed to the Tornado F3s (via the Joint Tactical Information Distribution System (JTIDS) and voice comms), F-16Cs (via long haul voice comms) and to the Jaguar's (via voice comms). An AWACS emulation was used that enabled the AWACS role player (a serving RAF officer) to fulfil his role as an AWACS operative. His role was to provide stimulus into the scenario and provide the aircrew with the correct cues.

***CAOC.*** The purpose of the Combined Air Operations Center (CAOC) was to provide the exercise management cell (White Force) with the necessary information so as to insert trigger events into the scenario. This enabled the CAOC role player (a serving RAF officer) to fulfil his role as a CAOC operative. The CAOC was positioned in the white team cell so he had a lot of information at his disposal from which to provide stimulus into the scenario.

***SOC, AAA, SAM & EW Radar.*** The red Sector Operations Centre (SOC) was manned by a serving RAF intelligence officer who had a detailed knowledge of the scenario and the equipment deployed by the threat. His role was to provide a stimulus into the scenario by coordinating the threat systems, both air and ground based. The red SOC operator was located in the same room to the white cell and Computer Generated Forces (CGF). A ground truth 2D tactical display gave the red SOC operator his RAP which enabled him to control his Anti-Aircraft-Artillery (AAA) and Surface-to-Air Missile (SAM) assets in a coordinated manner with other White Force participants.

The GBAD threat environment consisted of nine AAA units (KS-12, KS-19, KS-30, S-60), eight SAM units (SA-6, SA-3, SA-2, Roland) and several EW units (Spoonrest). The AAA, SAMs and EW, were operated from three separate PC's and all had the option to be operated man-in-the-loop. The AAA units could be fully automatic, i.e. radar laid firings, man-in-the-loop firing or an emulation of man-in-the-loop firing. The SAM units could be operated automatically, i.e. radar laid firings or an emulation of blind firing could be opted for. The EW radar could all be switched on and off by command. A single person operated all the AAA, SAM and EW. Each individual AAA, SAM and EW unit was manipulated as the scenario and evolution of the combat dictated employing strict emission control (EMCON) procedures.

***'Voice Actors'*** – SEAD, ATC, etc. The missions were planned from take-off to landing. It was not necessary or cost effective to simulate all the support roles required to add realism to the exercise. Where this was not the case, then the white cell acting in these parts performed these roles. For example, the Air Traffic Control (ATC) tower and enroute traffic control function was performed by the white cell, as was the role of the SEAD voice communications with the package. The SEAD voice communications was a trigger event where by the EA-6B Prowler was late to station due to equipment failures and so the manned package had to hold before entering threat airspace. The 'Actor' at this point played the role of the EA-6B operator although the actual platform was being simulated by a CGF entity.

## DEVELOPMENT OF THE SYSTEM

Development of the system entailed the configuration, reconfiguration, or modification of existing simulation facilities in the US and UK and the stand-up and configuration of a new facility in Canada. To coordinate these efforts, advance joint

meetings, joint teleconferences, and direct one-to-one communications were employed.

Joint meetings early in the project addressed the highest level issues and issues that could be easily identified or anticipated. These meetings selected the network simulation protocol, basic scenario, encryption devices, and voice communications systems. A key achievement of these meetings was the establishment of a test schedule early in the project.

Teleconferences were scheduled at first monthly and then weekly as the exercise date approached. The teleconferences provided a forum in which more detailed issues could be discussed and where new business could be raised. Specific and detailed questions were handled through individual telephone calls and email.

Offline, additional information was exchanged via email and courier. Some data sets, such as the terrain database, proved to be too large for sharing via email or ftp, thus courier shipments of storage media were used. Email was suitable for small data sets, test plans, test results, and technical documents. This was serviceable, but targeting email attachments to the correct recipients proved challenging in a large international project. Furthermore, given the time differences between sites and the busy schedules of the participants, arranging for the resending of email attachments could take up to a week.

These methods allowed each site considerable independence in its use of resources and time while readying itself for the trial. However, some aspects of development and configuration were done collectively. A successful example of collective action was the terrain database development. The UK provided their terrain database to the other sites. The other sites then adapted it for their individual image generators. This worked well because each site had its own terrain database tools. Furthermore, the fact that the primary focus of Trial VirtEgo was on team and inter-team coordination, minor terrain database changes made at each site were tolerable without resending each of the site changes to the other locations.

Collaboration was less successful in relation to encryptors. The versatility of encryptors, national differences in the certain aspects of encryptor employment, and their exacting nature presented a problem too difficult for the coordination and data exchange methods used elsewhere in the system development. Resolution required the sites to exchange personnel and drawings at the lowest level of detail. Because of the very long lead times required to procure encryption devices, particularly through the National Security Agency, the UK was unable to obtain their own device requiring the US to get permission to send a KIV-7 to the UK along with two US personnel to maintain control of the encryption keys and equipment.

Because of the time it took to get permission to operate at the Secret level and the unanticipated failure of the UK to obtain their own equipment, almost all of the time allotted to test and integration was spent sending pings and running an unclassified replay between the US and UK site using JSAF. Permission to operate at the SECRET level was given one week. This was barely enough time to insure interoperability, but several days of testing did prove each site could see the other's entities on the net. However, more time for testing and characterizing overall system behaviour would have resulted in substantial improvements. For example, the previously reliable CGFs (during unclassified JSAF to JSAF testing) occasionally exhibited non-representative behaviour in this new environment and the performance of the teleconference system was sub-optimal.

## LESSONS IDENTIFIED AND RECOMMENDATIONS

### Network links and network providers

Each site experienced problems with the long-haul link provided by their local telephone companies. These problems were especially vexing because their resolution was outside the control of the participating laboratories. Moreover, the telephone companies did not approach the problem with the same degree of commitment and urgency. In no case did the telephone companies in Canada, the US, or the UK deliver the requested service within the time frame required. This resulted in Canada's participation being reduced to receiving a replay of the log files, unexpected financial expenditures in the US, and reduced network performance in the transoceanic link. Since the use of telephone company links are nearly impossible to avoid for distributed training exercises, having one's own expertise in the telephone company's equipment is helpful in assisting them in their troubleshooting. Furthermore, it is hoped that support from the local

network providers will improve as their experience in supporting classified data networks grows.

**Integration testing**

A long haul integration plan had been defined and its intention was to use this to undertake the integration and testing phase. The integration and testing phase was originally split between 20% of the time undertaking unclassified testing and 80% of the time undertaking classified testing. The unclassified testing phase was completed satisfactorily with latency measurements being undertaken for a variety of bandwidth loadings and unclassified systems tested together (e.g., voice system). It also enabled the technical team to work together and test the robustness of the link.

Unfortunately, due to encryptor availability the classified element of the testing was not undertaken until the week before the trial. This only allowed some elements of the integration plan to be tested. It is a credit to both the UK and US systems that with this limited amount of testing (one week) it did not adversely effect the trial due to system crashes. If more time had been available, it was planned, obviously, to test all possible entity interactions to ensure that each entity behaved and responded in an appropriate manner. The number and types of interactions had been derived by analysing all of the entities and the systems they carried and to ensure that each interaction worked appropriately, e.g. Mig-23 radar would activate F-16 RWR in TWS and STT modes. The integration testing did allow adequate testing of the VTC systems and the ASTi radio communications systems.

In short, although a lot was achieved in a week and if it were not for the mature DIS simulators that were being hooked up it may not have been enough. When conducting integration testing it is vital to have knowledge of the underlying system models so that the data contained within DIS PDUs can be sensibly, and in our case, expeditiously interpreted.

Time must also be set aside for the training day process. A run-through of how the VTC, SmartBoards, etc. were to be used should have taken place much sooner. The processes required to make the day run as smoothly as possible needs to be understood, put in place, and tested with the actual participants.

**Security adds stresses to system development**

Running a classified system puts additional strain on the development of the system. Perhaps the most obvious stress is to timelines. Obtaining clearances from a large number of agencies to field and use encryption is a lengthy process and should not be underestimated. When it is multi-national, the approval process is even longer. Furthermore, the complexity of the network is substantially increased with the addition of encryption devices. Although the devices can be transparent once operating correctly, they introduce additional non-trivial faults and errors that must be considered during troubleshooting and accounted for in timeline development. As well, hidden network configuration errors that are normally tolerable when operating locally can become intolerable once encryption and multiple sites are introduced.

**Team Development**

When operating in a multi-country, multi-continent environment, time of day management becomes a significant issue. In Trial VirtEgo, a seven-hour time difference existed between the UK and US sites. Opportunities for real-time interaction are fleeting unless extended operating hours are available. When extended hours are used, the burden imposed must be understood and ameliorated, if possible, by the other sites. For example, the “day” started at 0000 local Arizona time and 0700 UK time. This was done in our case to accommodate the UK Air Warfare Center pilots who were the principal subjects for the research.

The establishment of a working rapport is important and worthy of specific consideration because the interconnected nature of the project requires a wide variety of people to work together. Differences in age, field of expertise, experience, status, and culture provide ample opportunities for misunderstanding. Organizational differences are also relevant. Recognizing that other sites may have fundamentally different mandates, fiscal frameworks, authorities, and commitments provides important contextual information and subsequent exercise process management challenges.

Face-to-face contact between team members in work and social settings is obviously helpful, but not always feasible in these projects. Those that did occur were beneficial, and more would have proved valuable. A visit by even one team member

to the other sites can be helpful, however. Not only does that team member benefit, but that team member invariably provides informal liaison and orientation functions that benefit all. Finally, scheduled teleconferences are very valuable. Their scheduled nature ensures that the collaboration retains a profile with all participants. Furthermore, it provides a forum for rapid decision-making and shared situation awareness.

## REFERENCES


Greig, I., Mayo, E., & Crush, D. (2000). *A Complex Synthetic Environment For Aircrew Training Research.* Proceedings of the 2000 Interservice/ Industry Training Simulation and Education Conference, Nov 2000, Orlando, FL.

Mack, I., & Bell, H. (2001). *United States – Canada Joint Training Research*. Proceedings of the 2001 Interservice/Industry Training Simulation and Education Conference, Nov 26-29 2001, Orlando, FL, 1244 – 1253.

Greschke, D., & Bell, H. Training for Dynamic Aerospace Control: *An Experiment in International Distributed Mission Training*. Proceedings of the 2002 International Training and Education Conference, April 9-11, 2002, Lille, France.

Crane, P., Tomlinson, B., & Bell, J. (2002). *Similarities and Differences in the Implementation of Distributed Mission Training*. Proceedings of 2002 Interservice/Industry Training System and Education Conference, Orlando, FL: National Security Industrial Association.