

Cross Domain Solution Configuration Management in the Simulation Training Environment

Bonnie Page Danner, James R. Multeri
Northrop Grumman Information Systems
Orlando, Florida
Bonnie.Danner@ngc.com, James.Multeri@ngc.com

Heath T. Morton
USAF AFMC 677 AESG/SYCB
Dayton, Ohio
Heath.Morton@wpafb.af.mil

ABSTRACT

The implementation of Combat Air Force (CAF) Distributed Mission Operation (DMO) cross domain solutions (CDS) in the dynamic world of simulation training introduces new and significant management challenges. One key challenge is the maintenance of cross domain solution security assurance and the associated approvals to operate in an environment where changes to mission training centers (MTCs), network infrastructure, participant sites, security classification guides, and training requirements are the norm. The effects of these changes on the approvals to operate the CDS can range from a requirement for re-accreditation with significant impact to little or no impact.

This paper describes the development and practice of configuration management for CDS in the DMO training environment. It provides an overview of the initial plans for implementing a CDS configuration management process involving key stakeholders participating in a review board. This paper addresses early lessons learned and describes an evolutionary process which is still being worked to improve and streamline the overall approach to configuration management. The CDS configuration controls required for secure operations in a constantly changing environment are complex, but essential for protection level 3 accreditation maintenance. A major challenge described in this paper is how to achieve clear understandings with stakeholders to help balance the need for retesting cross domain solutions for security approval maintenance and still meet the warfighter needs for daily training. This paper presents some of the configuration control issues, resolutions, and remaining challenges for CDS in the mission training environment.

ABOUT THE AUTHORS

Bonnie Page Danner, CISSP, has more than 25 years experience in systems engineering, software development, and information assurance. She is currently managing DMON CDS Services and the Specialty Engineering Team on the DMT Program. She has technical and PM experience on a variety of DOD and civil federal programs including R&D for DARPA and the USAF. Ms. Danner's specialty is high assurance systems. She has more than 11 years of security engineering experience in the training, modeling and simulation environment. Ms. Danner has published a variety of articles in journals and conference proceedings on information assurance, software engineering, and field theory. She received a BS degree from Virginia Tech and a MS degree in Mathematical Sciences from Virginia Commonwealth University.

James R. Multeri, CICM, has more than 27 years experience as a manager of configuration and data management and 6 years as a systems engineer. He is currently managing the configuration/data management office for both the CAF DMO DMT and the DMON CDS projects. He has configuration/data management experience on DOD and civilian programs, both white and black world programs. He is International Certified at the Manager level for both hardware and software configuration management. He received a BS in Systems Engineering and Design from Roosevelt University and Certifications in: Configuration Management of Software Programs and Systems Analysis.

Heath T. Morton, has more than 12 years experience in systems engineering. He is currently managing the DMO O&I engineering efforts for the USAF. He has worked for NAVAIR and ASC on multiple platforms including UAVs, B-1, and simulators. His modeling and simulation experience has enabled him to work with most platforms in the USAF inventory. He received his BS and MS in Engineering from Wright State University.

Cross Domain Solution Configuration Management in the Simulation Training Environment

Bonnie Page Danner, James R. Multeri
Northrop Grumman Information Systems
Orlando, Florida

Bonnie.Danner@ngc.com, James.Multeri@ngc.com

Heath T. Morton
USAF AFMC 677 AESG/SYCB
Dayton, Ohio

Heath.Morton@wpafb.af.mil

INTRODUCTION

Rigorous control of the configuration items affecting the trust of secure system operations is an extremely important security requirement. The challenges and resources associated with strict Configuration Management (CM) of systems requiring significant certification and accreditation (C&A) assurance are often underestimated. Planning well for the CM required to maintain the assurance and approvals to operate is essential for continued use of systems such as cross domain solutions (CDS). Over the years, a historical lack of CM guidance and foresight for higher assurance systems has plagued the operators and maintainers of these systems once they were approved for operation.

In the early days (1980's) of Department of Defense (DOD) and Intelligence Community (IC) automated security guard/controlled interface implementations (called CDS today) there was a great deal of emphasis on meeting the requirements for multi-level security (MLS) using high assurance techniques including formal, mathematical proofs of system security. While the development and assurance activities for these systems was challenging enough, the maintenance and configuration control of the security assurance turned out to be an even greater and more challenging task. The configuration management (CM) of high assurance systems frequently required new statements in formal security policy models necessitating expensive rework including redoing formal mathematical proofs, conducting certification testing, and updating the associated accreditation documentation. These expensive efforts were necessary to maintain the security approvals to operate.

The primary author first experienced this challenge after the successful implementation of a MLS high assurance guard for USAF-NASA shuttle communications. Unfortunately, the costs associated with maintaining the formal assurance were not anticipated well, and maintainers were faced with a choice between making improvements requiring an expensive reaccreditation or living with the existing

baselined system. In environments that can sustain system operations with little or no changes, the system CM required to maintain security approvals to operate is manageable without additional process control considerations. However, not all situations are stable, and software and hardware changes are usually inevitable to correct flaws, improve system operations, and address technology advances. Recognizing in advance the key role of CM to maintain security approvals is essential for most security applications, especially today.

Distributed Mission Operations Network (DMON) Cross Domain Solutions (DCDS) Configuration Management

Security approvals to operate Combat Air Force (CAF) Distributed Mission Operations (DMO) security-based systems must be maintained in an extremely dynamic environment. In a situation where changes to mission training centers (MTCs), network infrastructure, participant sites, security classification guides, and training requirements are the norm, the CM challenges are exacerbated. The effects of these changes on the approvals to operate CDS systems can range from a requirement for re-accreditation with significant impact to little or no impact. This paper addresses the CM challenges associated with the DCDS implementations that were evident from the beginning of the certification efforts in 2006 and continue to evolve.

BACKGROUND

Configuration control of the DMON DCDS security configuration items is challenging primarily due to the dynamic environment associated with the Mission Training Center (MTC) simulator software changes. The CM challenges also are directly tied to the requirement to maintain the security assurance for the approvals for cross domain operations involving the MTCs on the DMON.

DMON and DCDS Overview

The CAF Distributed Mission Operations (DMO) is the primary sponsor for simulation training capability between USAF warfighter MTCs distributed across the globe. The DMON provides a secure environment that allows two or more simulation training centers to participate in a pre-scheduled training event. The DMON Portal is a key facilitator for DMON operations. The DMON Portal translates simulation training center message traffic and enables interoperability between different simulation protocols.

Figure 1 illustrates the DMON Protection Level 2 (PL2)¹ (single level operational) architecture. The DMON simultaneously supports cryptographically separate training missions for different security domains. Each PL2 training mission is conducted within a single security domain. Routinely, the DMON supports training events for significantly more than two different security domains. For simplicity only two partitioned domains are illustrated in Figure 1.

Figure 1 shows the Distributed Mission Operations Center (DOC) management of MTC enclaves participating on the DMON in their partitioned security

domains. The three dots on each side in the figure are used to indicate that additional MTCs with similar Portal kit interfaces may also be involved in an event in the respective enclave.

The DOC is the classified operations center for the DMON. The cryptonet management system located in the DOC manages all DMON encryptors locally and remotely manages MTCs. The DOC event managers control the encryptor security associations.

DMON Common Security Operating Instructions (CSOI) and internal security procedures govern event management processes for the DOC and the O&I contractor MTC site agents. DOC Help Desk, Security, and Event Management personnel provide the necessary support for event execution. Operations center activities include support for scheduling, events and providing pre-event security coordination, event network set up, and network take down for each DMON event. Only accredited, authorized sites having signed Interconnectivity Security Agreements (ISAs) in advance are allowed to connect to the DMON to participate in events.

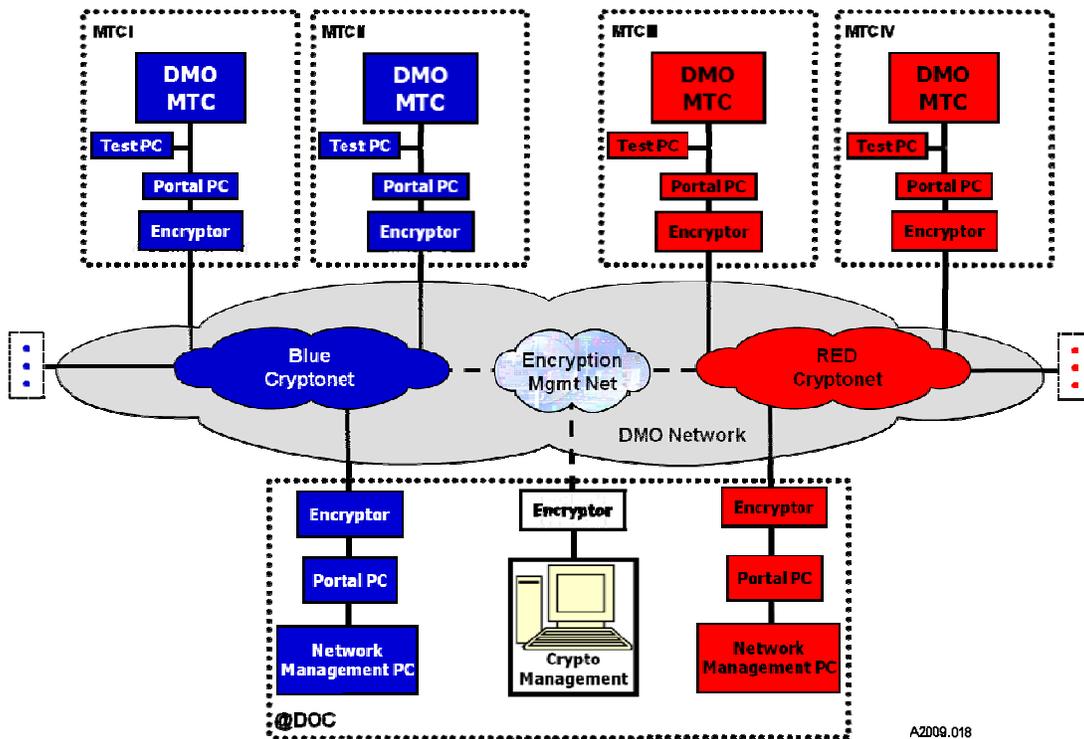


Figure 1. Two Domain Example: DMON (PL2) Conceptual Operational Architecture

Site personnel at each participant site perform their local support activities in accordance with the DMON

CSOI and site internal security procedures. The DMON assets at each participant site include Portal

kits containing the Portal machines, test machines and encryptor devices as shown in Figure 1.

Cross Domain Events

Security configuration management considerations for this paper are focused on assuring the continuity of cross domain event execution on the DMON. Figure 2 illustrates the DCDS Protection Level 3 (PL3)ⁱⁱ (cross domain operational) conceptual architecture for cross domain event operations.

The DCDS at Protection Level 3 (PL3 as described in JAFAN 6/3) consists of two main subsystems, the

controlled interface located at each DCDS site, and the management system located at the DOC.

Figure 2 shows the PL3 controlled interface located at the high security domain site and managed through a dedicated cryptonet by the PL3 management system resident in the DOC. A high security domain contains information that at least one participant in the low security domain is not authorized to access. Cross domain events may be conducted between high security domain enclaves and low security domain enclaves as depicted in Figure 2.

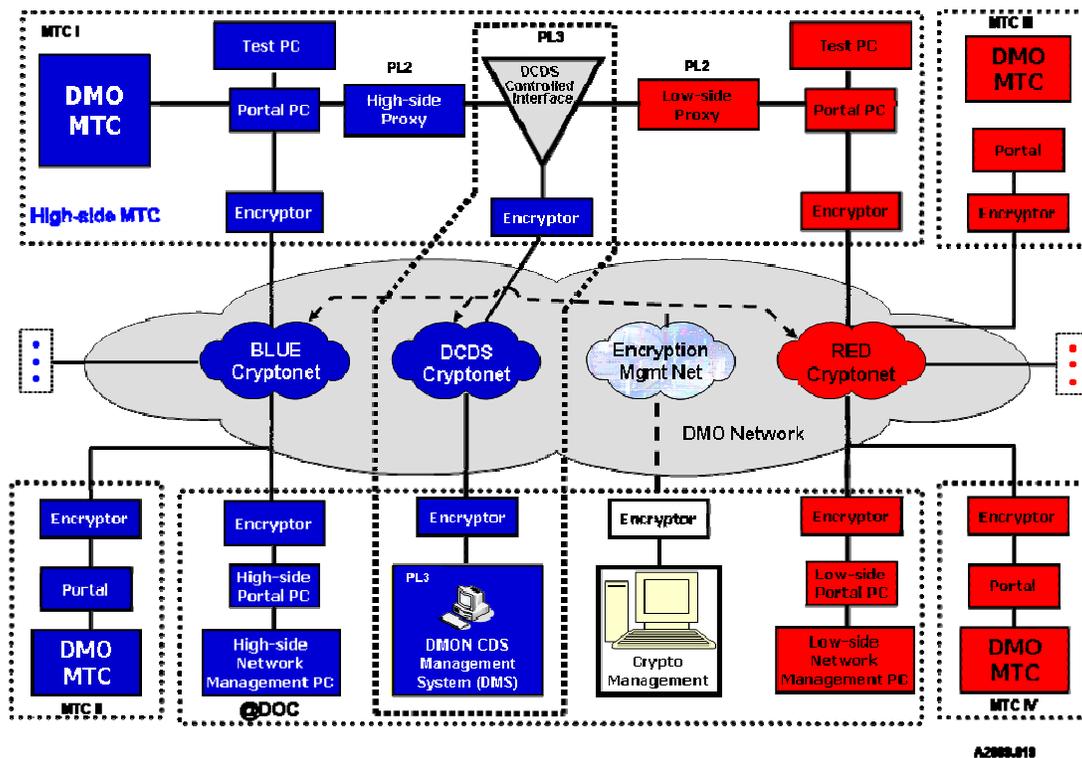


Figure 2. DMON DCDS (PL3) Conceptual Operational Architecture

The controlled interface is supported by PL2 non-security relevant, data conditioning proxy machines on both the low and high-side interfaces. The controlled interface performs all the security relevant decisions that govern the information flow between security domains. The deployed rule set on the controlled interface determines whether or not information will be passed without alteration, modified and passed, or blocked between the security domains.

By January of 2010 eight DCDS sites received approvals to operate (ATOs) from the SAF/AAZ Designated Approval Authority (DAA). Some of the sites received approval for two different rule sets. However, only one rule set can be deployed at a time

on a controlled interface during the conduct of an event.

UNIQUE CM CHALLENGES FOR DMON CDS SECURITY

Simulation and Training Environment

The DMO simulation training environment presents unique security baseline control challenges with airframe MTCs not only performing routine software maintenance, but also undergoing a dynamic software and hardware evolution necessary for simulators to keep up with aircraft changes. Simulator-related system

updates occur frequently. The various MTC simulator contractors are required to practice internal CM in accordance with their own corporate CM policies.

For MTCs that participate in cross domain training events on the high side of the DCDS controlled interface, changes to the software could potentially impact the data stream and affect the security rules implemented in the cross domain solution. Every change (hardware and software) in the high-side security domain must be evaluated with respect to the impact to the secure functioning of the DCDS and its rule sets. Therefore, the high-side MTC sites, as cross domain event stakeholders, must submit change requests along with impact statements to a DCDS security configuration review board (CRB).

Exacerbating the problem across the existing eight sites is the effectivity and timing of the changes. The installation of the changes to an MTC may be staggered in such a manner which requires maintaining accreditation at site 1 of a platform, while testing site 2 with the software changes in place. As more and more sites receive CDS capability, the challenges associated with managing the multiple baselines will grow.

Maintaining Approvals for Cross Domain Events

Only approved changes to high-side system components are allowed for the execution of cross domain training events. To maintain the ability to continue cross domain training participant high-side sites must be operating with an approved software version and must indicate the site software version to be used when providing their information for a cross domain event. The network event managers at the DOC obtain the information concerning the current version to be used from each high-side site planning to participate in the cross domain event. The event manager then verifies that high-side system/software versions are CRB-approved before connecting the site to the DMON for a CAF DMO cross domain training event.

As a result of the dynamic nature of MTC software updates, the control and monitoring of approved changes and versions become significant challenges. Additional controls are required for tracking and assuring that only the CRB-approved software versions are in use for cross domain events. These extra steps are necessary to maintain the approvals to operate the DCDS.

DAA Involvement

The DAA for the DCDS emphasized the importance of strict control of security baselines in early discussions prior to the first approval to operate a persistent solution. Understanding the necessity for frequent airframe simulator updates, the DAA also recognized that only reviewed and approved security baseline versions would be acceptable for DCDS use. With the goal to facilitate successful warfighter simulation training across different security domains, all participants desired a security configuration control process that would handle frequent changes efficiently, allowing rapid responses; especially for changes that were categorized as non-security-relevant.

Effective Control and Monitoring

The security CM process needed to enable a variety of stakeholders to participate and communicate changes, security impacts, degree of testing, and software/system version monitoring to continue use of the cross domain solution. Two key stakeholders in the process are the USAF DMON oversight organization and the DCDS DAA. These stakeholders are the signature authorities on configuration item changes to ensure that the approvals to operate remain viable. The greatest challenge continues to be the implementation of a control and monitoring process that can be performed with as little disruption as possible to the warfighters who require simulation training in a cross domain environment.

DCDS SECURITY CM PRACTICE AND CRB

The governing document for the DCDS change control process is the Security Configuration Management Plan (CMP). The DCDS Security CMP defines the DCDS security configuration items, the CM processes, the CRB, CRB membership, and participant roles and responsibilities. In a distributed maintenance environment including critical systems that interface with the PL3 DCDS, it is particularly important that changes to the baseline system's security configuration items be strictly controlled.

Security Configuration Management Purpose

The DCDS Security CMP describes the specific processes required to manage the security-relevant DCDS baselines controlled by their respective stakeholders. Configuration control of security baselines is essential to ensure continuation of secure operations, sufficiency of rule sets, and maintenance of the PL3 security approvals for operation.

Strict configuration management is required for the PL3 components and the associated rule sets including documentation. Changes to the DCDS security configuration items of the MTCs and support systems involved in cross domain events, to the DCDS PL3 system, and to the rule sets must be reviewed for security relevance and potential impact to rule set implementations. The CRB reviews the resulting security impact analyses and approves security-relevant changes before they can be tested as directed, and a new system/software version can be approved for use in cross domain events. The CRB is led by the government with members from key stakeholder organizations including a representative for the Air Combat Command (ACC) and USAF security representatives.

Primary Change Drivers

Three primary occurrences may trigger changes to the approved security baseline and the need for CRB activities. These occurrences are as follows:

1. Changes to the Security Classification Guides (SCGs) that govern the protection policies for the sites. These changes may affect configuration item baselines and/or affect technical and operational rules. Possible reasons for SCG changes include changes in aircraft capabilities, changes in tactics, and corrections or changes to program security policy. These changes could affect the DCDS rules and/or affect simulator implementation.
2. The need for upgrades and/or corrective measures that drive changes to the Mission Training Center (MTC) software loads and their associated configuration items; similarly, upgrades and corrective measures that drive changes to the contractor support systems and associated configuration items. Simulator software must keep pace with the changes made to the actual aircraft. In addition, changes in the CAF DMO standards may drive the necessity for software modifications. DMO participant software data formats must meet the standards and be certified to allow interoperability between different platforms. Support software must also be kept compliant with the standards and remain interoperable with the systems in place.
3. The need for upgrades and/or corrective measures that drive changes to the DCDS system baseline including the approved rule

sets. Changes to the simulator software may affect the DCDS coded rules and even impact the English Language Rules. Changes in technology may drive a need for DCDS system improvements or platform upgrades. Any significant change to the DCDS system baseline will require additional security certification activities.

Changes to the approved DCDS security baselines may be minor enough to require only reporting without requiring any testing. However, it is more likely that changes will require some level of testing for security assurance and maintenance of the approvals to operate. These changes present challenges for the continued operation and maintenance of the DCDS which can be made even more significant with high system usage and personnel turnover within the government oversight organizations.

Security CMP Overview

The Security CMP was developed to ensure that any changes affecting the security of the DCDS system would be accomplished in a manner consistent with well defined guidance, and therefore, maintain the associated systems approved PL3 security posture. The focus of the DCDS configuration management is the continuation of security assurance that depends on the baselined configuration items.

The DCDS Security CMP centers on sustaining security. It describes the actions required to test and obtain approval for any baseline changes affecting system security prior to such changes being implemented for cross domain events. The CMP presents the CRB processes and the specified steps for CRB participants. The plan provides the guidance for stakeholders to coordinate, communicate, and strictly maintain the approved security baselines necessary to ensure continued PL3 operations.

The specific DCDS stakeholders who support maintenance of the security configuration items for cross domain operations include USAF program managers, USAF security and engineering oversight staff, USAF approval authorities, MTC contractors, and DCDS contractors. These core participants in the protection of the DCDS security domain data and approved baseline maintenance perform the following roles:

1. Government stakeholders – USAF teams perform technical, security, and management oversight and provide security approvals.

2. DCDS contractor personnel - A distributed team supports security engineering, test, operations, and maintenance of the DCDS.
3. MTC Providers – Contractor teams engineer, test and maintain training systems software for sites participating in training events.

The security configuration items that must be maintained to ensure continuity of DCDS approvals to operate are varied. Not only are the MTC system (hardware and software) versions potential configuration items, but changes to the version of any software/system on the high side of the DCDS could potentially impact the security of the DCDS. The high-side data stream to the controlled interface and its rule sets must be interpreted and processed correctly before allowing data to pass to a lower security domain.

The DCDS and its rules are also key configuration items. Changes to the DCDS or to rule sets are by their nature, security-relevant changes. Changes to the high enclave software systems may or may not be security relevant, but must be examined before making such a determination. These examinations are required for changes to all systems involved in the high-side data stream including the simulators, the Instructor Operator Systems (IOSs), the Computer Generated Threat Systems (CGFs), and other computers that manage the protocol data units (PDUs) on the high side of the DCDS. Other significant items to manage from a security perspective are the security classification guides (SCGs) and the DCDS Security CMP.

The following list illustrates the kinds of configuration items that must be managed by the DCDS configuration review board and its stakeholders.

- ▲ DCDS Controlled Interface
 - ▲ Hardware and software at each site and related documentation
- ▲ DCDS Management System
 - ▲ Hardware and software located in the DC and related documentation
- ▲ English Language Rule Set Plan
 - ▲ Describes the content of each rule, technical and non-technical
- ▲ DCDS Implemented Rule Sets
 - ▲ Developed and tested rule sets
- ▲ Rule Set Implementation Report
 - ▲ Describes test results, rules pseudo code and additional assurance detail
- ▲ High-side Support Equipment
 - ▲ High-side proxies hardware and software versions
 - ▲ High-side Portal hardware and software versions
- ▲ Simulation Implementation Protocol
 - ▲ MTC hardware and software versions

- ▲ PDU list, structure, and security-relevant content
- ▲ Battlespace implementation details affecting rules assumptions

Each security configuration item change requires a formal configuration change request, a designated change level (proposed by the requester), a description of the change, and a security impact statement relevant to the change. As described below, the changes must then be reviewed by the DCDS engineering team and by all formal participants on the DCDS CRB.

The change levels are defined in as follows:

Level I: A request for a change to the baselined DCDS System Requirements or system that requires DCDS changes and/or new rule sets. A Level I change is of a level of severity or sufficient impact to require re-accreditation of the DCDS system.

Level II: A request for change to the Rules or to a software implementation. A Level II change is of a level of severity requiring re-certification of DCDS rules.

Level III: A request for change that has no security impact. This level of change constitutes a release-based change that does not affect the security posture of the DCDS system. SAF/DAA retains the right to re-classify this level. The specific testing required for a Level III change to obtain the associated software/system version approval is directed by the CRB.

Level IV: A request for change that addresses non-security relevant MTC and high-side support software or hardware that does not affect information that flows between the high and low sides of the network which impacts the baseline version. No testing is required for Level IV changes and any associated version approvals.

Configuration Change Requests are submitted using a form posted on the unclassified, protected DMODMT.com website for DCDS CRB use. The requester provides unclassified versions of the change description including a proposed change level that can be posted for rapid dissemination. If classified change descriptions are also necessary, the requester must send these descriptions via appropriate channels to the DCDS contractor security engineering team for review and dissemination as needed. The DCDS security

engineering team provides a written assessment and recommendations to the CRB stakeholders.

CRB stakeholders may also provide comments on the change request. All CRB members have the opportunity to respond and to request a CRB meeting for more detailed discussions if they consider this necessary. The responses must be provided within a defined time frame. The CRB secretariat consolidates the information and posts an agenda for either an electronic or a face-to-face CRB meeting. He/she also provides a summary of all comments on the approval forms to be signed by the CRB co-chairs representing the government oversight and the DAA organizations.

Once the government signs CRB approvals, the DCDS engineering and operations team must follow up with the recommendations for actions necessary to sustain the DCDS ATOs. These actions may include full certification and accreditation testing and documentation for a re-accreditation, some level of certification testing to achieve an ATO update, regression/confidence testing with a confirmation report that the DCDS secure operations are not affected, or no testing. Notification of the approved software versions to event managers and to CRB members must be strictly maintained following the implementation of changes at high security domains that participate in cross domain events.

DCDS CM ISSUES AND CHALLENGES

Trust in the acceptability of residual risks for the approvals to operate is essential for cross domain warfighter training in the distributed simulation environment. With the security approvals in place, simulator changes required for currency and interoperability as well as network availability become challenges; however, they are required to achieve effective training across security domains. Consequently, the most significant CM challenge results from two opposing requirements. The first is the requirement to maintain the security accreditation of the baselined high-side systems including the cross domain solution. The second is the requirement to continue distributed training network availability for warfighters as the various contractors incorporate changes in the simulator environment to model airframe equipment improvements and to correct software problems. This CM challenge drove a need for frequent and rapid change control actions by the DCDS CRB resulting in a variety of DCDS CM issues during the first year of the DCDS CRB.

Classified Information Sharing

The closed environments for high-side simulators require information security safeguards that affect the ability of the CRB to disseminate classified information in a rapid manner. The DCDS CRB change control process requires the completion of baseline configuration change requests (CCRs) by the organization initiating the change. The CCR is then reviewed by the DCDS engineering team to validate the security impact statements and proposed levels of change. The engineering team's analyses are then disseminated to the CRB membership for review and concurrence as appropriate. Classified aspects of the change descriptions and security impact analyses need to be disseminated to a number of stakeholders. Not all stakeholders are able to access electronic networks approved for all high-side security domains. This accessibility issue slows down the DCDS CRB electronic information exchange process and affects the ability of the board to accomplish decisions in a timely manner.

Infrequent Face-to-Face Meetings

DCDS CM issues result from such things as inadequate communication between stakeholders including an inability to ascertain changes to security classification guides when they occur. With senior advisors and key participant availability a factor, DCDS CRB events could not be scheduled on a monthly basis as was originally planned. The infrequency of face-to-face correspondence was a major reason for some communication inadequacies experienced by the DCDS CRB in its first year of operation.

Need for Low-side Subject Matter Expertise

Cross domain test events focus on the necessary security certifications for protection of the high-side security domains and not on the impacts to the low-side participants. However, experience has shown that test and training events with a focus on low-side impacts is also important to determine the feasibility of rule constraints for overall training effectiveness. Initially, the DCDS test teams were slow to glean low-side participant information from training events that affected rule sets. Any impacts necessitating rules changes would require DCDS CRB review and approvals along with additional security testing. In some cases obtaining low-side subject matter experts who could provide knowledgeable feedback to the high-side stakeholders was a challenge.

Rapidity of Simulator System Changes

The dynamic nature of some simulator environments resulted in too-rapid software and hardware updates from a DCDS CRB and approved security baseline perspective. These rapid changes have to be managed either by using separate, older version drives to continue cross domain operations or to halt cross domain operations until the new baseline can be approved by the CRB and adequately tested for continued approvals to operate. Maintaining adequate configuration control is an essential security assurance task. Managing the approved software baselines when there are frequent changes can become a significant issue for secure network operations and for the high-side participant mission training centers.

It is important to note that once a Level I, II or III change is implemented into the high-side enclave, the cross domain training across the DMON in a CDS environment halts when the MTCs are using the changed software. The site does have the ability to train locally and at a single security domain on the DMON, but must wait until the proper paperwork and testing have been completed to train with the CDS across the WAN. This testing re-asserts the information assurance confidence necessary to conduct distributed training during a PL3 connection.

Additionally, identification of future modifications to the primary change drivers is critical for minimizing the down-time of CDS capabilities. Proper coordination with the Federate System Provider (FSP) is vital for identifying when an install will occur and thus when testing can occur. Proper coordination with the site is also vital to support the required testing.

Personnel Transitions and Heavy Workloads

Another issue, common in many military environments, is the frequent transition of key stakeholder personnel causing a loss of subject matter expertise. This loss affects the rapid and knowledgeable decisions necessary for the DCDS CRB and slows down the overall review process. In addition, the heavy work load many decision makers frequently experience causes time delays in scheduling DCDS CRB meetings and impacts timely electronic responses.

ADDRESSING THE ISSUES AND REMAINING CHALLENGES

Refining the Change Levels

At the first DCDS CRB meeting, the government oversight team recommended a fourth level of configuration change that could be readily handled by the CRB and not affect the use of the DCDS systems for training events. Level IV changes that are not security relevant and do not require regression testing for security impact (for example, some simple hardware swaps) once defined as a possible Level III changes, could then be disposed of quickly by simple electronic dissemination to the CRB and government approval.

Initially, the non-security relevant Level III changes requiring only simple regression testing and the non-security relevant Level IV changes requiring no additional testing still required approval from the DAA as well as the government oversight team. This places additional burden on the DAA organization and adds to the time required to achieve the go-ahead for continued operations for the DCDS systems. Currently, the DAA is reviewing a recommendation to delegate the non-security relevant change approvals to the oversight organization to streamline the DCDS CRB approval process. On hind sight, the very cautious approach the DCDS CMP took with respect to change approvals may have been too strict with respect to addressing the management of non-security relevant changes.

Change Control Forms

Some immediate improvements resulting from lessons learned centered on addressing the specific entries in forms that present the change descriptions of the DCDS configuration items. The need to conduct electronic DCDS CRBs to achieve review and approvals in a timely way became obvious very early in the CRB process. Having frequent face-to-face meetings proved difficult for the membership, especially with the number of change requests submitted for approval exceeding initial expectations.

The need for achieving more clarity and more specific understanding about the planned changes including details about where and when they were to occur became more obvious as the change control efforts were put into practice. Forms that seemed to provide lines for sufficient information turned out to need more details and guidance to achieve the necessary understanding for approvals to proceed and to conduct the necessary security confidence testing.

Improvements to these forms continue as the CRB functions and use of the forms evolve.

Accurate Presentation of Approved Versions

A major challenge that continues to require improvement is effectively documenting and disseminating the numerical versions for all of the CRB approvals for the participating high security domain systems to ensure only the approved versions are being used for cross domain operations. This final and crucial step in the security CM process turns out to be one of the most difficult to perform due to the dynamic nature of the simulator systems. The DCDS CRB stakeholders are currently focusing on this particular aspect to both ensure the security of DCDS operations and to avoid unnecessary delays in the use of the DCDS for recurring team training.

Remaining Challenges

Significant challenges remain to achieve timely CM for the persistent operations of the DCDS for daily team training. The DCDS CMP acknowledges in its introduction that it is a living document, and it has already undergone a series of changes based on the early application of the DCDS CM processes. The forms used for change control requests and for approvals have continued to evolve. The processes described in the document continue to be worked based on experiences and lessons learned. The DCDS CM process will necessarily require continued efforts to apply lessons learned and improve due to the complexity and rapidly evolving nature of the modeling and simulation environment.

REFERENCES

- CAF DMO O&I Contractor (2004). *Draft DMON MLS Guard O&I Contractor Workshop Report*.
- CAF DMO Tailored Distributed Interactive Simulation (DIS) Standard, Version 8.0 dated 31 January 2008
Configuration Management Plan (CAF DMO CMP) Version 2.0, 31 August 2009
- Director of Central Intelligence (DCI) (1999). *DCI Directive (DCID) 6/3 for Protecting Sensitive, Compartmented Information Systems and Manual*.
- DMO Security Classification Guides for specific air frame Platforms (classified); various dates
- DMT O&I Contractor (2001). *DMO Integration Standards and DMO Common Definitions*
From:
<https://secure.dmodmt.com/standards/index.cfm>
- DMT O&I Contractor (2002). *Multi-Level Security Feasibility in the M&S Environment, IITSEC 2002, Paper 167*.
- DMT O&I Contractor (2005). *Multi-Level Security Assessment for the Distributed Mission Operations Network, IITSEC 2005, Paper 2165*.
- DMT O&I Contractor (2006). *A Distributed Mission Operations Cross Domain Solution for Recurring Team Training, IITSEC 2006, Paper 2775*.
- DMT O&I Contractor (2008). *Cross Domain Solution Policy, Management, and Technical Challenges, IITSEC 2008, Paper 8343*.
- DMT O&I Contractor (2009). *Cross Domain Solution (CDS) Certification and Accreditation for Persistent, Simulation Training, IITSEC 2009, Paper 9142*.
- DMT O&I Contractor (2009). *Cross Domain Solution Challenges Transitioning from Concept to Operations, IITSEC 2009, Paper 9133*.
- DOD (2000). *Memo for Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8510, Department of Defense Global Information Grid Assurance*. DOD I 5200.40 (1997).
- Department of Defense Information Technology Security Certification and Accreditation Process DITSCAP*.
- DOD, *Joint Air Force, Army, Navy (JAFAN) 6/3 and Manual* (2004).
- NSA (2003). *Guard Certification Test and Evaluation (CT&E) Handbook Version 2.0*.
- NSTISSAM (1999). *Common Criteria for Information Technology Security Evaluation*.

NSTISSAM COMPUSEC (1999). *Advisory Memorandum on the Transition from the Trusted Computer System Evaluation Criteria to the International Common Criteria for Information Technology Security Evaluation.*

NSTISSP 11 (2000). *National Information Assurance Acquisition Policy Combat Air Force Distributed Mission Operations*

ACKNOWLEDGEMENTS

The authors would like to thank the many government and contractor participants in the early stages of the DCDS CRB who provided insight and guidance as the security CMP and the related processes evolved. In particular, the authors appreciate the ongoing help from SAF/AAZ, ACC, and the 677th AESG organizations. The authors also appreciate the wisdom and ongoing engineering support from Northrop Grumman Corporation, Cobham, SERCO, Boeing Corporation, and Plexsys Systems technical participants.

ⁱ Confidentiality security Requirements for Protection Levels are defined in the DOD, *Joint Air Force, Army, Navy (JAFAN) 6/3 and Manual* (2004)

ⁱⁱ Protection Level 3 details are defined in the DOD, *Joint Air Force, Army, Navy (JAFAN) 6/3 and Manual* (2004)