A Survey of Cross Domain Solutions for Distributed Mission Training

Peter Ross, William Oliver, and Peter Ryan
Aerospace Division, Defence Science & Technology Group
506 Lorimer St, Fishermans Bend, Victoria Australia
peter.ross@dst.defence.gov.au
william.oliver@dst.defence.go.au
peter.ryan@dst.defence.gov.au

Keywords:
Distributed Mission Training; Cross Domain Solution; Distributed Interactive Simulation; High Level Architecture; Multi-level Security; Rule Set; Technology Readiness Level

ABSTRACT: *Distributed Mission Training (DMT) exercises integrate dispersed force elements into a common virtual battlespace for collective military training using distributed simulation protocols. Cross Domain Solutions (CDS) are required for running secure DMT exercises by connecting discrete systems that operate at different levels of security in an assured manner. This report surveys the state-of-the-art of CDS for DMT using only open-literature sources for the period 1995 to present. Both deployed CDS for permanent exercises and temporary CDS for specific exercises are discussed.*

CDS operate using rule sets that protect high side (high classification) information being accessed from the low side (low classification). The rule set development process, categories of effects, protection methods, and test and evaluation are explored with sample rules provided for various use cases. Technology Readiness Levels (TRL) for CDS vary across the whole spectrum from 1 (laboratory demonstrator or prototype) to 9 (fielded system). The TRL 1-3 systems are all dated, relating to sensitive-but-unclassified use cases rather than fully classified use cases. Two TRL 4-5 systems were identified and these both recommended hardware solutions to reduce latency. The TRL 6-7 systems are more advanced and some resulted in systems fielded with patents issued for several systems. There are few patented TRL 8-9 systems with several systems dominating the CDS marketplace. A comprehensive list of CDS technologies for DMT is given across all technology readiness levels.

Not surprisingly the US was the major source of CDS literature with only a few papers cited from other nations, mainly from Europe. Interestingly only a few of the papers cited were themselves referenced by other authors perhaps because the entire CDS literature is sparse and there are intellectual property and patent considerations. A distribution of papers across the 1995 – 2020 period showed that these peaked in the 2010-2012 period and have declined since possibly due to the success of the fielded solutions.

1. Introduction

Distributed Mission Training (DMT) is the integration of multiple, physically dispersed force elements into a consistent virtual battle space for the purpose of exercising team skills. DMT has an emphasis on planning, communication and teamwork.

A Cross Domain Solution (CDS) is a type of security capability that is used to connect discrete systems within separate `security domains' in an assured manner [1]. A security domain is a system or collection of systems operating under a consistent policy that defines the security classification, releasability restrictions and special handling caveats for information stored in that domain [2]. A CDS is implemented using a combination of human and machine actions, resulting in the transfer of information from one security domain to another. Rules govern when and how information is transferred from the higher domain to the lower domain.

Traditionally, DMT exercises have required force elements to operate within the same security domain. This has enabled DMT to flourish for some user communities, whereas other communities who use different security domains are unable to more broadly integrate. CDS for DMT would enable these diverse communities to train together, and thus achieve meaningful training outcomes. CDS is critical to enabling greater and continued participation in DMT exercises.

This paper reports on a survey of the state-of-the-art of CDS for DMT using only open literature sources. The full literature survey is published elsewhere [3].

2. Cross Domain Solutions

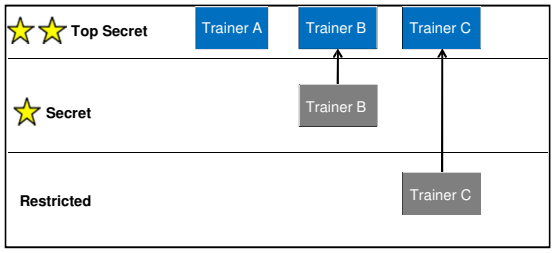
2.1 Concepts and Definitions

The US National Security Agency has developed a set of definitions for key terms in the security domain [4]. The Australian DoD has adopted most of these definitions in its literature [5]. The principal security definitions related to CDS are:

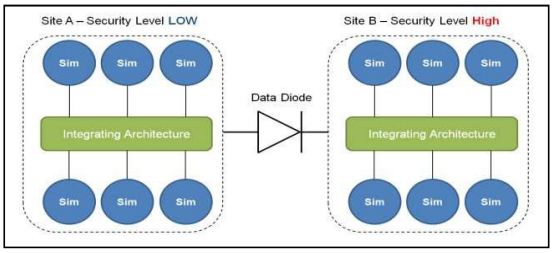
- *Cross domain*: the act of manually and/or automatically accessing and/or transferring information between different security domains.
- *Cross Domain Solution*: A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains
- *Rule Set:* A table of instructions used by a controlled interface to determine what data is allowable and how the data is handled between interconnected systems.
- *Access Cross Domain solution:* A type of CDS that provides access to a computing platform, application, or data residing on different security domains from a single device
- *Transfer Cross Domain Solution:* A type of CDS that facilitates the movement of data between information systems operating in different security domains
- *Multi-level Cross Domain Solution:* A type of CDS that uses trusted labelling to store data at different classifications and allows users to access the data based upon their security domain and credentials.

There are broadly four solutions when integrating training devices across different security domains (reproduced from [6]) as shown in
Figure **1**. These may be described as:

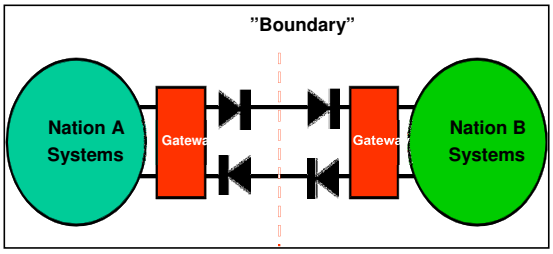
a. *System High*: trainers A, B, and C operate across different levels of security but are all reclassified to the highest level so they can interoperate.
b. *Multiple Independent Levels of Security:* a data diode is employed to prevent high side information being passed to the low side; information can only be passed from low to high.
c. *Information Exchange Gateway:* a gateway is employed between systems from different nations; each nation controls what information is sent across the boundary that can use either diodes or guards.
d. *Multi-level Security:* simulations 1 and 2 operate with system T with simulation 1 only seeing yellow and green information and simulation 2 only seeing yellow and blue information. All information is stored in a trusted system that can release data to each system on a "need to know" basis using a guard.



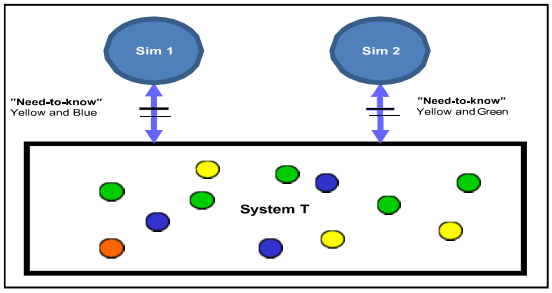
(a) System High



(b) Multiple Independent Levels of Security



c) Information Exchange Gateway



(d) Multi-level Security

Figure 1: Four solutions when integrating training devices across different security domains (reproduced from [6])

2.2 CDS Rule Sets

CDS are implemented to protect high side information from being accessed by low side domain systems. This information can be either operational (system behaviour or existence such as stealth capability), technical (system performance such as range or speed), or representational (how the system is modelled in the simulation). For cases where the security domains are non-hierarchical so that each side has protected information, more complex rules need to be developed and different testing procedures undertaken to ensure certification. The rules employed in CDS can be categorised by their effect on the synthetic battlespace as direct, coupled, or schematic [7] where:

- *Direct effects* refer to protection methods that prohibit warfighter or weapons system actions or state changes. These exclude data from being received by low side training system components such as simulators and constructive threat simulations.
- *Coupled effects* refer to indirect effects resulting from rules that induce a disturbance in the content of the environment which impacts the cognitive agent's response. The environment appears consistent with the mission space design but nevertheless is distorted so that an appropriate response to the altered battlespace would be inappropriate in a real world context.
- *Schematic effects* refer to indirect effects that result from warfighters attempting to under-stand complex causality in uncertain, dynamic situations.

Protection methods can be categorised as either *technical* (performed by machine) or operational (performed by human exercise controllers) [7]. Technical protection methods (rule types) are classified as:

- *Content Blocking*: blocks the passing of protocol information from the high side to the low side of the CDS.
- *Content Guising*: substitutes one set of information for another in the protocol information as it passes from high to low.
- *Interaction Guising:* seeks to represent a battlespace interaction as being of a different character than its simulated form on the high side.

Operational protection methods can be classified [7] as:

- *Behaviour Prohibition*: methods that explicitly prohibit warfighters from performing specific actions, techniques, or procedures.
- *Information Control:* This may be a technical rule that restricts access to specific, protected information to the

high side participants.

- *Certification*: this requires simulation vendors to assert that their modeling implementations follow conditions defined by the rules plan.

2.3 History of CDS

In the mid 1990s, the US released its Defense master plan for Modeling and Simulation [8] that included an approach to multilevel security based on how systems operate in real life on the battlefield. The plan provided guidance for DIS-based simulations to interoperate at multiple levels using PDU labelling, encryption, authentication, and appropriate networks and interfaces.

Post 2000 there was renewed interest in CDS as DMT exercises became increasingly popular with the military training community. The US Joint Forces Command established a Joint National Training Capability to facilitate the expanded exercise program. McGowan and Raney defined and differentiated Multi-level Security and Multiple Single Levels of Security, discussed solutions that have been tested and lessons learned, and assessed the state of MLS for the Joint Warfighter simulation exercises [9].

A NATO study group Security in Collective Mission Simulation (MSG-80) was established in 2010 [6]. Use cases and basic principles for Multi-level security were discussed with definitions for System High, Multiple Single Levels of Security, and Multiple Independent Levels of Security as shown in
Figure **1** above. The study group noted that security solutions need to support simulation protocols, protocols for file sharing and VoIP and other media protocols. Solutions must also provide acceptable performance for real time simulations. The concepts of HLA and Distributed Simulation Engineering and Execution Process (DSEEP) were also introduced to provide exemplars.

2.4 Literature Search Methodology

With the exception of defining terms and security policy, only papers that describe cross domain security in the context of distributed mission training were considered. Papers concerning general-purpose cross domain solutions were considered out of scope together with papers that discuss security issues for a single security domain.

The sources searched included organisations such as IEEE, major simulation conferences such as the Interservice / Industry Training, Simulation and Education Conference (I/ITSEC) and modelling and simulation research journals. Other Defence sources such as the NATO Modelling and Simulation Group were included in the search. Government contract notices and patent searches were also checked. Recognising that there may be classified work in this area, only unclassified sources were included. Research tools employed include the Open Athens system, Google Scholar, Google, and embedded search engines such as those employed by I/ITSEC. Papers were also sourced from electronic databases such as IEEE Xplore, ACM Digital Library, EBSCO and Scopus.

Search terms included, “cross domain solution”, “multi-level security” and “network guard” together with distributed mission training concepts. As the names of influential processes, equipment, software, and authors were discovered, those search terms were also included. It was anticipated that the main source of CDS information would be the US Department of Defense since it has the greatest experience with distributed simulation training exercises. NATO countries, especially the UK, were expected to provide additional information on the state of the art of CDS.

2.5 Literature Search Summary

The literature search results are summarized in the following two figures. Figure 2 shows the number of reports about CDS sourced by country together with datasheets, contract notices, press releases, patents, and standards. Not surprisingly the majority of papers were sourced from the US. There is a total of 97 items.

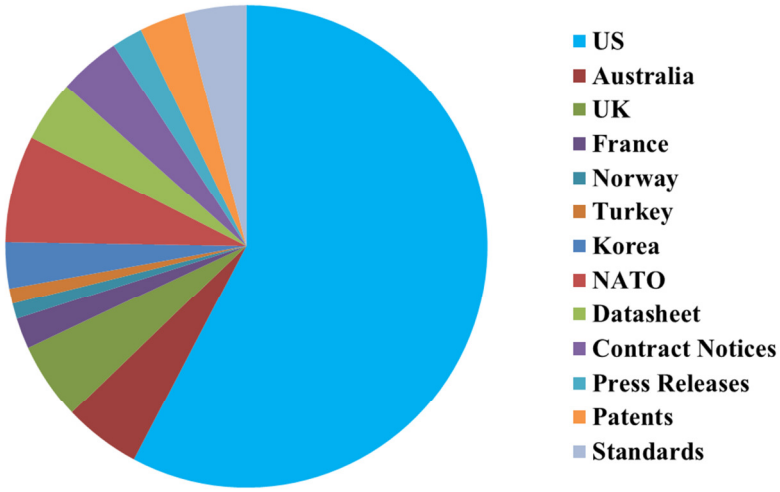


Figure 2: Distribution of papers and reports across countries together with standards, patents, contract notices, press releases, and datasheets

Figure 3 shows the number of papers published each year across the period 1998 – 2019. This shows a peak in the 2010 – 2011 time period and a decline since then.

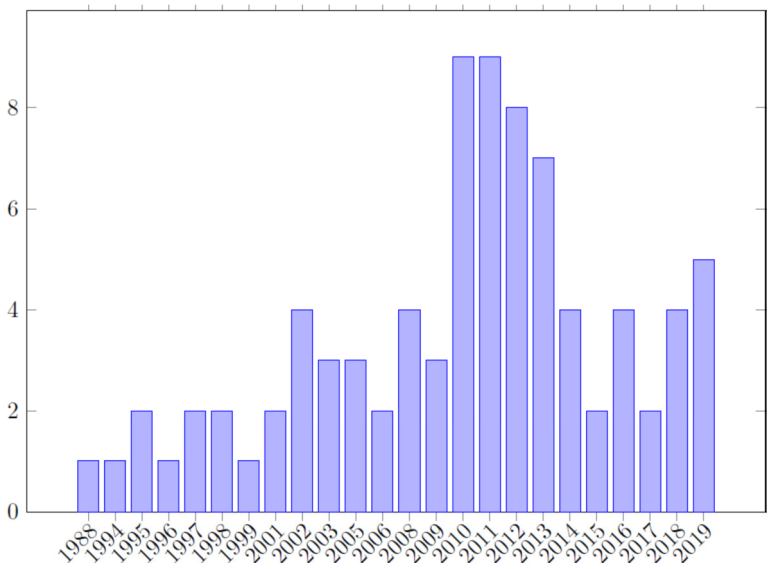


Figure 3: Papers on CDS reported each year from 1998 - 2019

3. CDS Applications

Several CDS are actively deployed in US training environments. These systems are rated at Technology Readiness Level 7 or higher and are used routinely to enable DMT for US and coalition team training as discussed below.

3.1 Permanent Solutions

3.1.1 Navy Continuous Training Environment

Navy Continuous Training Environment (NCTE) is a US program and platform used to support Fleet Synthetic Training (FST). NCTE combines shore-based and ship-embedded simulation and stimulation systems into a single, distributed simulation network and includes voice and data communication systems and infrastructure required to

support training and Fleet trainers [10]. NCTE enables Navy warfighting readiness by providing a tailored, realistic, environment networked to Fleet/Joint/Coalition FST exercises and other distributed training events. NCTE maintains a permanent link to the Joint Training and Experimentation Network (JTEN).

3.1.2 Distributed Mission Operations Network

The Distributed Mission Operations Network (DMON) is a training network primarily for US pilots and aircrew [11]. DMON operates as a Virtual Private Network and is not connected to the US secret operational network. While the NCTE focus is on team skills, the DMON focus is on aircrew training with simulators that maintain concurrency with the real aircraft. Connectivity to JTEN and NCTE is only performed under exacting control conditions.

3.1.3 Nevada Test and Training Range

The Nevada Test and Training Range (NTTR) is an environment used for air and ground military exercise, including pilot and crew training, combat exercises and testing new aircraft and weapons systems. Exercise operators employ the Digital Integrated Air Defense System (DIADS) to provide C2 data to threat simulators [39]. DIADS operates at Secret but is required to communicate with other unclassified systems and NTTR assets. Radiant Mercury Guard is used to separate the red (high classification) and black (low classification) systems with filtering rules to determine what can be sent between high/low and low/high. The Radiant Mercury system was first deployed in 2009 hosted on a Trusted Solaris Sun workstation and approval granted for operation in 2010.

3.1.4 Joint Pacific Alaska Range Complex

The Joint Pacific Alaska Range Complex (JPARC) comprises the air, land, and sea training areas used by the US DoD and military services in Alaska. All US services conduct training and testing in the JPARC. JPARC is the largest US DoD training area with over 5 times the airspace of the Nellis range in Nevada and is the largest instrumented air, ground, and electronic combat training range in the world [12].

3.1.5 Republic of Korea - US Combined Battle Simulation Center

The Republic of Korea and the US operate a Combined battle Simulation Center that uses 'Rialto' [13]. Rialto is a guard interface that is one component of a CDS with Radiant Mercury Guard (RADMERC) in an HLA distributed simulation environment [45]. The Rialto-RADMERC configuration prevents unauthorised data crossing the federation barrier. An interesting observation is that HLA's publish/subscribe mechanism implies that a subscriber can receive all information a federate publishes leading to potential security issues.

3.2 Temporary CDS

Temporary CDS have been developed for specific exercises or exercise series as discussed below.

3.2.1 USN Broad Area Maritime Surveillance LVC Distributed Environment

The USN developed a persistent LVC distributed simulation environment designated LVC-DE to support its Broad Area Maritime Surveillance (BAMS) program [14]. LVC-DE linked 4 facilities through the secure Joint Mission Environment Test Capability (JMETC) network, 3 military training sites and also the NASA AMES non-DoD laboratory. DIS, HLA, and TENA protocols were deployed for interoperability with TENA used for WAN traffic and local gateways converting between DIS/HLA and TENA as required. The unclassified assets representing civil air traffic and air traffic control at NASA AMES were hosted on the DREN. The LVC-DE was required to simulate how the BAMS Unmanned Aerial Systems (UAS) will operate in the civilian environment with civil air traffic in the US National Airspace System.

3.2.2 US Army Vengeance Program

The US Army Redstone Test Center and US Army Aviation and Missile Research Development and Engineering Center developed a CDS to connect an unclassified cockpit simulator with a classified laboratory for testing under the Army Vengeance program [15].

The unclassified helicopter simulator uses DIS and employs a DIS-TENA gateway to communicate with the TENA-enabled human-in-the-loop gunnery simulators, constructive simulations (OneSAF) and live systems. The underlying architecture is TENA; however some systems also require further DIS-TENA gateways to interoperate. A real-time SimShield CDS, certified and accredited using TENA 5.2.2, transfers data between the unclassified and classified network security domains. The high side systems use TENA 6.0.1 which is not backward compatible with TENA 5.22 necessitating additional gateways between TENA versions. Latencies of less than 1 ms were achieved for the CDS and less than 8.5 ms for the combined network and CDS.

3.2.3 Fleet Battle Experiment KILO

The US Seventh Fleet training exercise Fleet Battle Experiment Kilo (FBE-K) was a large sea strike training exercise run in 2003 that included a coalition partner (Australia) [16]. The core simulation employed was Joint Semi-Automated Forces (JSAF) run from the US. Australia participated via the Virtual Maritime System representing an ANZAC ship that was federated with JSAF. RADMERC provided multilevel and multinational information transfer for structured messages while chat, email, internet and VoIP were used to send unstructured messages. The RADMERC bridged the security boundary between the SECRET US NOFORN and SECRET AUSCANUKUS releasable networks.

3.2.4 LVC Bold Quest Series

Bold Quest 15.2 was an LVC coalition (US, Canada, France) demonstration and assessment event run in 2015 [17]. CDS was recognised as a critical enabler for achieving interoperability across nations, service, and programs but no details were provided. Bold Quest 16.2 was run in 2016 and anticipated expansion of coalition participation from European nation; again CDS was cited as critical to success but few details were provided.

3.2.5 Cyber Operational Architecture Training System

The Cyber Operational Architecture Training System (COATS) is a US Defense Modeling and Simulation Coordination Office (DMSCO) initiative that integrates cyber range environments, simulation architectures, operational networks, and cyber emulations to deliver realistic cyber effects to the battle staff [18]. COATS aims to improve integrated cyber operations during DoD exercises.

COATS employs a network guard to protect data flow across disparate networks. This comprises a Radiant Mercury device in conjunction with the USAF's Air, Space and Cyberspace Constructive Environment - Information Operations Suite (ACE-IOS) Joint Information Operations Range (JIOR) Broker application. ACE-IOS is the simulation tool used to create the cyber range environment. COATS has been incorporated into trials including Operation Blended Warrior (OBW) 2015, OBW 2016 and USN Fleet Synthetic Training (FST) exercises.

3.2.6 UK MOD Niteworks

The UK Ministry Of Defence (MOD) Network Integration Test and Experimentation Works (Niteworks) is a partnership between industry and government that provides support to military operations, capability development and acquisition practices. The UK MOD Defence Operational Training Capability (Air) (DOTC(A)) tasked Niteworks to develop an understanding of risk associated with cross domain training [19].

3.2.7 NextGen Interagency Experimentation Hub

MITRE established an innovation program called 'NextGen Interagency Experimentation Hub' to explore how different US federal agencies and industries would share information in times of aviation crisis under the US Next Generation Air Transportation System. A paper-based study of cross domain solutions was undertaken and specifically examined the RADMERC and SimShield systems [20]. Since RADMERC cannot process HLA or TENA natively the Rialto system is required for these protocols whereas SimShield can process DIS, HLA, and TENA. The proposed system involved an unclassified node at MITRE's Experimentation for Aeronautics (IDEA) Lab, reuse of the SimShield at the Redstone Test Center (reported in[15]) and an unnamed classified US research facility.

4. Technology Survey

A survey of CDS systems was categorised using the 9-level NASA Technology Readiness Level (TRL) system. These TRLs run through 1 (basic principles observed and reported) to 9 (actual system proven through successful mission operations).

4.1 Technology Readiness Level 1-3

TRL 1-3 systems are generally laboratory experimental systems or even theoretical designs. TRL 1 specifies basic principles identified, TRL 2 technology concepts, TRL 3 proof of concept. These are discussed in the following subsections.

4.1.1 French Aerospace Office System – CERTI

ONERA[1] developed CERTI, a prototype RTI that includes security extensions [21]. This is implemented using an RTI gateway (RTIG) that transfers information among federates and adds security domain filters to the publication and subscription services. Each class, attribute, and federate is associated with a security domain and the RTIG filters messages according to their security domains. Updated attributes are only sent to authorised and authenticated federates.

4.1.2 SecProxy

Andrews et al proposed a novel CDS for HLA simulations that installs a guard component between each federate and the RTI [22]. This differs from other guard-based solutions that use trusted bridge federates for transferring data between different federations at different security domains. The main advantage of the SecProxy approach is that it results in a single federation. By locating the guard between the federate and RTI, its rule engine can access more information from which to base downgrade or sensitisation decisions.

The paper presented a design and hypothetical use case but did not provide evidence of a working prototype or results. The authors also discussed potential weaknesses with their approach including concern for the traffic required to synchronise SecProxy servers and vulnerability to Denial of Service attacks.

4.1.3 HLA Security Guard

Filsinger described a HLA Security Guard approach to meet multilevel security simulation requirements [23]. The security guard acts as a gateway between federations and downgrades or sanitises formatted data from a high security domain to a low one. A design was discussed but there was no implementation or results presented.

4.1.4 Sensitive Simulation (SENSIM)

Sensitive Simulation (SENSIM) was a joint US Army Simulation and Training Command (STRICOM) and Royal Netherlands Army (RNlA) research project to incorporate multi-level security into military simulations [24]. The use case was multi-nation simulation exercises where not all participants shared the same security domain. It was proposed as an alternative to the system-high approach using bulk-network encryptors.

NSA certified encryption hardware (Fortezza) was integrated with the ModSAF[2] constructive simulation. The ModSAF DIS interface library used the standard Berkley sockets interfaces. The DIS interface was modified to use the Fortezza Cryptologic Interface Library instead. This device supported eight encryption keys enabling PDUs to be selectively encrypted based on exercise security policy. The modified ModSAF was installed in STRICOM and RNlA laboratories, and both laboratories were linked using ISDN. In the experiments, PDUs associated with stealth entities were encrypted while all other entities were unencrypted. Only instances of ModSAF loaded with the appropriate keys could therefore interact with the stealth entities.

Much of the research was concerned with throughput and latency added by the network encryption hardware. However,

1 Office National d'Etudes et de Recherches Aerospatiales (French National Office of Aerospace Research Centre)
[2] ModSAF (Modular Semi-Automated Forces) was a predecessor to OneSAF and JSAF

the encryption and decryption processing for each message was found to take 1200 ms in total, and this was deemed inadequate for DIS exercises.

4.1.5 HLA RTI IPsec

Elkins et al proposed a public-key encryption approach to enable multi-level security HLA exercises [25]. Their proposal is conceptually similar to that for SENSIM. HLA objects and interactions are encrypted using different public keys for each security domain, and then public on network. For example, aircraft positional information is encrypted with an unclassified public key, and weapons information is encrypted with a secret public key. Only federates with access to the appropriate private keys are able to decode the information. Extensions are required to the HLA Federation Object Model (FOM) to support this approach.

Results were presented on how public-key encrypted affects simulation performance, demonstrating a 10% increase in simulation execution time when encryption is used.

4.1.6 Non-hierarchical Cross Domain Solution

Valle and Djahandari described existing CDS approaches used in DMON as hierarchical, whereby Mission Training Centres are each fitted with a CDS, and connected together on the low side [26]. The authors suggested that this low side may be too limiting, and there is a need for some participants, namely white cell, to have access to the information present across all security domains. They proposed a non-hierarchical solution, where each MTC connects independently to a central site at the security domain of the MTC. The central site functions as the CDS for all participants. The paper presents a design and hypothetical use case, but gives no evidence of a working prototype or field results.

4.1.7 Generic HLA Solution

Verkoelen et al proposed a generic HLA solution comprising two building security building blocks [27]:

- A labeller block, that attaches a security label to each HLA object. This is achieved by inspecting the content and metadata of each object.
- A release block that determines whether the HLA object can be immediately written to the network, or must be altered or dropped.

In the long term these blocks would be incorporated into simulators, but the authors acknowledged that in the short term, an external solution is required. This paper did not provide any substantive use cases using this approach, or provide experimental results.

4.2 Technology Readiness Levels 4-5

TRL 4-5 systems are generally prototypes. TRL 4 specifies laboratory validation while TRL 5 specifies validation in a relevant environment. Sample TRL 4-5 implementations are discussed in the following subsections.

4.2.1 DIS Deep Packet Inspection

A prototype DIS network guard was built by the Australian Defence Department based on Field Programmable Gate Array (FPGA) architecture [28]. In contrast to normal firewalls, this included a deep packet inspection that could read and analyse the entire content of the messages being filtered (in this case DIS PDUs). The prototype system was written in a hardware description language to run on a FPGA. The software compromised roughly 4000 lines of code that is owned by the Commonwealth of Australia. A set of generic rules was developed for blanking fields in specific PDU types: Electromagnetic Emission, Designator, Transmitter, Receiver, and IFF. It was acknowledged that this approach cannot be applied to the Entity State, Fire and Detonation PDUs or exercise fidelity would be compromised. For EE PDUs, processing delay was of order 50 µs, much faster than equivalent software filters.

4.2.2 Patented System from L3

US Patent 9760731 (proposed by L3) describes a method for developing a configurable data guard based on a hardware programmable logic device using the DIS protocol [29]. A hardware approach was recommended to achieve low-latency data throughput similar to the system described in the previous section. Existing software-based CDS were considered to have difficulty scaling to future requirements with 100 Gb/s data rates. The system was envisaged to comprise several integrated circuits and a microprocessor configured to receive a data guard configuration.

4.3 Technology Readiness Level 6-7

TRL 6-7 systems can be considered as mature prototypes. TRL 6 specifies a prototype demonstration in a relevant environment whereas TRL 7 specifies a prototype demonstration in an operational environment.

4.3.1 AIME Secure

Khetia el al described the AIME Secure simulation firewall developed at the UK Defence Science and Technology Laboratory (Dstl) [30] that employs the SyBard data diode developed by QinetiQ [31]. This system controls the flow of DIS PDUs from a high security domain to a lower security domain through a set of rules and can also modify fields within the PDUs.

AIME Secure is also covered by a patent that specifically mentions DIS rules, and gives examples [32]. Four types of rules can be implemented:

a. Block: prevents data being passed to another domain
b. Set: overrides some data fields to mask original values
c. Allow: passes data if conditions are satisfied; includes option to modify some data fields
d. Throttle: restricts the data rate being passed to the second domain

The rules can modify or obfuscate PDU fields to enable transfer to lower fidelity domains, block data, or limit the data rate being sent to a second domain. While any protocol for data messages could be employed, DIS PDUs are preferred. A flow chart schema is provided that shows how the system invokes these 4 rule types.

4.3.2 NAWCTSD Distributed Training Network Guard and Enterprise Network Guard

The US Naval Air Warfare Center Training Systems Division (NAWCTSD) developed a Distributed Training Network Guard (DTNG) that can label, segregate, protect, and exchange data between simulation networks that operate at the same classification level [33]. The system can work with multiple LVC protocols including DIS and HLA. DIS v6 is supported natively while the Joint Simulation Bus (JBUS) gateway is required to support HLA. DTNG was developed to facilitate USN training in LVC environments with coalition partners. Future work is planned for the Joint Strike Fighter (JSF, F-35) with native HLA 1.3 and HLA 1516 interfaces under development.

The Enterprise Network Guard (ENG) is another related NAWCTSD initiative [34]. ENG will provide a CDS for both data and voice. ENG employs DIS and HLA for simulation data and uses the P5 Combat Training System. It will also include Link-16 and Air Tasking Orders. Certification and testing should be complete by 2020 when the USN plans to field the system.

4.3.3 AFRL Distributed Training Network Guard (DTNG)

Distributed Training Network Guard (DTNG) was an AFRL advanced research project [35]. It was implemented on Sun Trusted Solaris V8.0 operating system and used HLA. Six sample vignettes were described. The DTNG comprised the Trusted Bridge Federate (TBF) and the Security Reclassification Rule Set Intelligent Assistant Tool (SRRSIAT) where the TBF “is the physical real-time automated network guard component that supports two-way data transfer between simulation federations operating at different security levels”, and the SRRSIAT “is a stand-alone interactive GUI that provides the federation security classification/domain expert the capability to develop and review classification rules that govern the transfer of objects, attributes, interactions, parameters, and the execution of cross-security level run-time infrastructure (RTI) operations for cross-federation object models”

The application of DTNG to the DMO was described in [36]. It was noted that use of HLA created complexity since the DMO uses mainly DIS and that the DIS-HLA gateways were unreliable. Three possible architectures were discussed.

More evaluation and testing were required before the USAF could implement the system.

4.4 Technology Readiness Level 8-9

TRL 8-9 refers to systems that have been deployed and are operational. TRL 8 describes a system that has been qualified and tested while TRL 9 describes a system that has been proven in operations. The only systems reported at this level are RADMERC and SimShield.

4.4.1 Radiant Mercury (RADMERC)

RADMERC, also known as RM Guard or RMG, is a USN-developed TRL 9 system. The earliest report (1994) of RADMERC was implemented using a Hewlett Packard 750 workstation running HP-UX BLS operating system [37]. It is an NSA-accredited system. The system has been further evolved over the past 25 years at the Space and Naval Warfare Systems Command (SPAWAR[3]) by Lockheed Martin [38]. In 2009, there were at least 483 instances world wide [39], while by 2018 there were over 800 [40].

RADMERC is composed of baseline software that is reliant on Lockheed Martin Rotary and Mission Systems (LMRMS) proprietary Message Analysis and Generation (MAG) software code, which is required to make RADMERC fully functional [41]. MAG is software that provides parser/formatter capabilities to break messages into specified fields [42]. There are at least three US patents describing inventions concerning MAG [43-45].

The current operational baseline is version v5.1.1 running on Trusted Solaris 10 [40]. This version has been deployed on a wide range of platforms including HP, Dell, IBM, Crystal Computers, and Oracle/Sun. Version 6 was proposed to migrate to Red Hat Enterprise Linux 6 [42]. This baseline comprises a core server computer and a separate software loader computer [46]. Specification of the server is an Intel Xeon-based computer.

RADMERC is natively DIS enabled [38] and is reported to be capable of processing 1000s of DIS Protocol Data Unit (PDU) messages per second.[42]. RADMERC can also operate with HLA via gateways: Mitre developed the Rialto translation system that can be used with RADMERC to process HLA messages as XML messages [20]. This approach could be used for the TENA protocol. Pollock also discussed HLA implementation with RADMERC but only for a data diode configuration that transfers one way low to high [38]. This HLA implementation required MAGs for over 300 objects and 800 interactions leading to a total of more than 26000. There were plans to enable RADMERC to operate directly with the Run-time infrastructure (RTI).

4.4.2 SimShield and High Speed Guard

SimShield is another accredited security guard system that can be employed for cross domain simulation. It is developed by Forcepoint[4] [47]. According to the datasheet, it supports DIS, HLA, TENA, Real Time Transport Protocol, and several MPEG-related protocols as well as Key Length Value Metadata.

Lesuer measured packet delay across SimShield operating on an IBM System x3650 server [48]. Interestingly he found that latency through the CDS was much smaller than the Wide Area Network (WAN) latency for US continental exercises with a maximum value of 2.5 ms compared to WAN latencies of up to 37 ms. Later testing measured latency and throughput for TENA data with latencies observed to be less than 1 ms average and throughput up to 300 MB/s [15].

Raytheon also offers the High Speed Guard [49]. This was first made commercially available in 2011[5]. High Speed Guard is included on the UCDSMO Baseline list as an accredited and operational transfer solution. This system supports MPEG video format, Ground Moving Target Indicator (GMTI) data and several proprietary formats. It appears to be more suited for streaming video and file transfer across security domains rather than exchange of real-time simulation protocols. The fact sheet does not mention DIS, HLA, or TENA explicitly.

[3] renamed to Naval Information Warfare Center in 2019
[4] part of Raytheon
[5] https://www.prnewswire.com/news-releases/raytheon-announces-commercial-availability-of-high-speed-guard-135573558.html

5. Discussion and Conclusions

This report surveyed the state-of-the-art of CDS for DMT using only open-literature sources with the potential of informing the development and deployment of CDS for Distributed Mission Training in Australia. Not surprisingly the US was the major source of literature on CDS with only a few papers cited from Europe and other areas. Interestingly few of the papers cited were themselves referenced by other authors perhaps because the entire unclassified CDS literature is sparse and there are intellectual property and patent considerations.

Various technical solutions are available with RADMERC and SimShield the main commercial products from Lockheed Martin and Raytheon respectively. RADMERC appears to be the more widely adopted system with applications dating back to the mid 1990s and over 800 installations globally. RADMERC is also protected by US patents. SimShield is a newer, seemingly more capable system with support for more protocol types but there is little information on its performance reported in the literature.

6. References

1. Australian Cyber Security Centre (2019). *Australian Government Information Security Manual*. Canberra, Australia,
2. Australian Defence Signals Directorate (2012). *Guide to the secure conguration of cross domain solutions*. Canberra, Australia, Department of Defence
3. Ross, P., Oliver, W. and Ryan, P. (2019). *A Survey of Cross Domain Solutions (CDS) for Distributed Mission Training (DMT) (in progress)*. DST Group
4. National Security Agency. *Committee on National Security Systems (CNSS) Glossary*.
5. Australian Cyber Security Centre. (2019). *Introduction to Cross Domain Solutions*.
6. Croom-Johnson, S., Huiskamp, W. and Moller, B. (2013). Security in Simulation - A Step in the Right Direction (13F-SIW-009). In: *Fall 2013 Simulation Interoperability Workshop* Orlando, Florida, US.: 16 - 20 September, 2013, SISO
7. Chapman, R. and Valle, T. (2012). Training Credibility in Cross Domain Events. In: *Interservice/Industry Training, Simulation and Education Conference (I/ITSEC) 2012,* Orlando, Florida, US
8. Warmbrod, K. (1995). Architecture and Security Implications of the DoD M&S Master Plan for DIS Architectures. In: *13th Distributed Interactive Simulation Workshop,* Orlando, Florida, US
9. McGowan, G. and Raney, C. (2005). Integrating Multi-Level Security into the Joint Warfighter Training Environment. In: *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2005,* Orlando, Florida, US
10. *Navy Continuous Training Environment (NCTE).* [Accessed 2019 23 October]; Available from: https://www.nwdc.navy.mil/site/ncte.html.
11. Djahandari, K., Archer, J. and Danner, B. (2009). Cross Domain Solution Challenges Transitioning From Concept to Operations. In: *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2009,* Orlando, Florida, US
12. Gruber, T. (2011). Radiant Mercury Usage at the Nevada Test and Training Range. In: *International Test and Evaluation Association (ITEA) Test Instrumentation Work- shop Conference,*
13. Kim, Y.-H., Lee, Y.-J. and Lee, C.-H. (2008). Advanced Simulation Architecture as a ROK-US OPCON Transformation Enabler. In: *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2008,* Orlando, Florida, US
14. Lutz, R., LeSueur, K., Fast, P., Graeff, T., Simlote, A., Rutledge, J. and Mottl, R. (2010). A Persistent LVC Simulation Environment for UAS Airspace Integration. In: *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2010,* Oralndo, Florida, US
15. LeSueur, K. G., Elbert, J. M. and Millich, S. (2013). Distributed Testing using a Real-Time TENA-based Cross Domain Solution (12S-SIW-013). In: *2013 Spring Simulation Interoperability Workshop,*
16. Schacher, G., Pilnick, S., Irvine, N. and Gallup, S. (2003). *Seventh Fleet Field Training Exercise Fleet Battle Experiment Kilo Fires Initiatives Final Report*. NPS-97-03-006, Monterey, Californina, US, Naval Postgraduate School
17. Seavey, K., Reitz, E., Lagrange, P., Gorham, W., Biran, H. and Whelan, D. (2016). Bold Quest 15.2: A Case Study in Establishing Multinational Simulator Interoperability. In: *MODSIM World 2016,* Virginia Beach

Convention Center, 1000 19th Street Virginia Beach, VA 2345, US: 26 - 28 April 2016
18. Wells, D. and Bryan, D. (2015). Cyber Operational Architecture Training System – Cyber for All. In: *2015 Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC),* Orlando, Florida, US
19. Hughes, K. (2014). *Niteworks DOTC(A) Cross Domain Security Task - Final Report*. NW/PR/0645/008, UK MOD Niteworks.
20. Flournoy, R. D. and Schlipper, L. M. (2013) Cross-domain information sharing for next generation interagency experimentation: possibilities and challenges. *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* **10** (3) 297-312
21. Breholee, B. and Siron, P. (2002). CERTI: Evolutions of the ONERA RTI Prototype (02F-SIW-018). In: *2002 Fall Simulation Interoperability Workshop,* Orlando, Florida, US: 10 - 15 March 2002
22. Andrews, D., Wharington, J. M. and Stratton, D. (2008). SecProxy - A Proposed Security Architecture for the HLA. In: *SimTecT 2008,* Melbourne, Victoria, Australia: 12 - 15 May 2008
23. Filsinger, J. (1997). HLA Security Guard Federate (97S-SIW-163). In: *1997 Spring Simulation Interoperability Workshop,* Orlando, Florida, US, SISO
24. Luiijf, E. A., Dey, A., Watson, J., Muckenhirn, C. and Garnsey, M. (1998). Fortezza-enabled Multi-level Sensitive Simulations (98S-SIW-020). In: *1998 Spring Simulation Interoperability Workshop.,* Orlando, Florida, US, Simulation Interoperability Standards Organization
25. Elkins, A., Wilson, J. W. and Gracanin, D. (2991). Security Issues in High Level Arcgitecture based Distributed Simulation. In: *2001 Winter Simulation Conference,* Arlington, Virginia, US: 9 - 12 Dec 2001
26. Valle, T. and Djahandari, K. (2010). Implications of Interoperating with Non-Hierarchical Security Domains In: *2010 Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC),* Orlando, Florida, US
27. Verkoelen, C. A. and Wymenga, R. R. (2009). Multi Level Security within Collective Mission Simulation Architectures (09S-SIW-035). In: *2009 Spring Simulation Interoperability Workshop,* San Diego, California, US: 23 - 27 March 2009
28. Robbie, A. and Ackland, H. (2019). Implementation of IEEE DIS deep packet inspection firewall in FPGA hardware (10E-SIW-020). In: *2010 European Simulation Interoperability Workshop,* Ottawa, Canada: 12 - 14 July 2010
29. Winslow, R. N., Costantini, F. A., Devlin, S. D. and Smith, R. M. (2017) *Configurable cross-domain information assurance.* US-9760731 B2
30. Khetia, S. and Crush, D. (2013). Secure Cross Domain Operation. In: *2013 Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC),* Orlando, Florida, US: 2 - 5 Dec 2013
31. QinetiQ. *SyBard Diode V3*. (2012) [Accessed 30 October 2019]; Available from: https://www.qinetiq.com/what-we-do/cyber/sybard-diode.
32. Jobson, M. I. (2017) *A data hub for a cross-domain communication system.* QinetiQ Ltd
33. Naval Air Warfare Centre Training Systems Division. *2019 Research Compendium*. (2019) [Accessed 30 Oct 2019]; Available from: https://www.navair.navy.mil/nawctsd/sites/g/files/jejdrs596/files/2019-02/2019-ResearchCompendium_0.pdf.
34. Gritton, K. (2019). Live Virtual Constructive for Training (LVCT). In: *Simulation Innovation Workshop (019-SIW-044),* Orlando, Florida, US: 11 - 15 Feb 2019
35. Martinez, R. G., Polliard, S. and Flo, R. (2002). *Distributed Training Network Guard Trusted Bridge Federate Initial Capabilities Demonstration: After Action Report*. FRL-HE-AZ-TP-2002-0012, US Air Force Research Laboratory
36. Danner, B., Valle, C. T. and Sparta, N. G. (2002). Multilevel Security Assessment for the Distributed Mission Operations Network (DMON). In: *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC).* Orlando, Florida, US
37. Hahn, R. and Tretick, B. (1994). Multilevel security guards: controlling data flow. In: *16th Department of Energy Computer Security Group Training Conference,* Denver Colorado 3-5 May 1994
38. Pollock, R. E. (2003). Radiant Mercury Simulation Capabilities. In: *2003 Spring Simulation Interoperability Workshop,* Kissimmee, Florida, US: 30 Mar - 4 Apr 2003
39. Lockheed Martin. *US Navy Selects Lockheed Martin To Continue Development Of Secure Information Sharing System*. (2019) [Accessed 30 Oct 2019]; Available from: https://news.lockheedmartin.com/2009-07-14-U-S-Navy-Selects-Lockheed-Martin-to-Continue-Development-of-Secure-Information-Sharing-System.
40. SPAWAR. *The SPAWAR List*. (2018) [Accessed 30 Oct 2019]; Available from: https://www.public.navy.mil/spawar/Documents/List.pdf.
41. SPAWAR. *Notice of Intent to Award a Sole Source Contract for {General Service (GENSER) Cross Domain*

Solution (CDS), Radiant Mercury (RADMERC). Solicitation Number: N00039-19-D-0006. (2018) [Accessed 18 Nov 2019]; Available from: https://www.fbo.gov/index.php?s=opportunity&mode=form&id=58ece63ae750ad6157d887fa4c816a15&tab=core&_cview=1.

42. Gunter, D. and Bowden, W. E. (2016). Radiant Mercury Update to {CDSE} Workshop. In: *Cross Domain Support Element (CDSE) Summer Workshop 2016,* Hyattsville, Maryland, US: 19 - 20 Jul 2016
43. Marso, T. and Hawkins, R. (2007) *Message parser and formatter.* Lockheed Martin US-7293175
44. Brown, L., Marso, T. and Savage, R. (2007) *Automatic information sanitizer.* Lockheed Martin Corporation US7293175
45. Schwartz, M. I., Tolley, R. G., Flesher, K. E., Franklin, K. B., Scott, W. D. and Auten, C. W. (2010) *Information aggregation, processing and distribution system.* Lockheed Martin Corporation US7809791
46. NAVAIR. *P-8A Cross Domain Solution - Radiant Mercury (Contract Award Number: N00019-18-C-0057).* (2018) [Accessed 30 Oct 2019]; Contract Award Number: N00019-18-C-0057]. Available from: https://www.fbo.gov/index?s=opportunity&mode=form&id=54b81ab1a68a6ae27d48c38bd0fe3171&tab=core&_cview=1.
47. Forcepoint Federal LLC (2015) *SimShield: BI-DIRECTIONAL FIXED-FORMAT DATA FILTERING AND DISGUISE.*
48. LeSueur, K. G. (2010). Future Trends and Needs for Distributed T&E Infrastructure. In: *International Test and Evaluation Association (ITEA) Live-Virtual-Constructive Conference 2010,* El Paso, Texas: 11 - 14 Jan 2010
49. Raytheon. *Raytheon High Speed Guard.* (2014) [Accessed 30 Oct 2019]; Available from: https://www.raytheon.com/sites/default/files/capabilities/rtnwcm/groups/gallery/documents/digitalasset/rtn_216064.pdf.

7. Author Biographies

PETER ROSS graduated from RMIT University in 2001 with a Bachelor of Applied Science, majoring in computer science. He joined DST's Aerospace Division in 2003, where he has undertaken a role in evaluating the use of advanced distributed simulation for collective training.

WILL OLIVER holds degrees in Aerospace Engineering and Mathematics. Will joined Defence Science & Technology (DST) Group's Aerospace Division in 2006 and works in the Air Operations Simulation Centre; researching interoperability issues and analysis techniques for advanced distributed simulation. Prior to joining DST, he developed software for flight simulators and simulated maintenance trainers.

DR. PETER RYAN is an Honorary Research Fellow in Defence Science & Technology Group's Aerospace Division. He has a 35 year background in the modelling and simulation of military operations. His main research interests include Advanced Distributed Simulation, real time simulation, synthetic environments, and their potential to provide enhanced training solutions for the Australian Defence Force.