Cross Domain Security in Airpower Mission Training through Distributed Simulation

Dr. Manfred Roza, Arjan Lemmers M.Sc., Capt. James Quarmyne & Lt.Col. Peter van Onzenoort

Royal Netherlands Aerospace Centre NLR

Amsterdam, The Netherlands

manfred.roza@nlr.nl, arjan.lemmers@nlr.nl, james.quarmyne@nlr.nl, phgj.v.onzenoort@mindef.nl

ABSTRACT

Airpower Mission Training through Distributed Simulation (MTDS) is becoming a crucial capability for Air Forces to satisfy their collective training needs. In these MTDS exercises simulation assets from different (inter)national security domains must be able to interoperate effectively and efficiently within a single training environment. Meanwhile, air forces want to protect their most sensitive or classified assets, underlying data and information, against exposure to (cyber)security threats that could result from joining such MTDS exercises. Implementing secure connectivity and interoperability between simulation assets of different sensitivity, trust or security classification level is essential for the successful implementation of MTDS capabilities and exercises. This is even more so in an international coalition context within NATO.

The paper describes a conceptual framework with fundamental cross domain security terminology, concepts and principles pertaining to the secure interoperability of simulation assets from different security domains within joint Airpower MTDS exercises. The framework aims to facilitate the communication, understanding and implementation of cross domain security (CDS) solutions within the modeling and simulation (M&S) domain. In here also the distinctive M&S cross domain security aspects are identified that impose unique challenges and requirements on CDS appliances and services for MTDS not seen in other domains such as C4ISR. The framework served as one of the foundations for the NATO MTDS reference architecture - M&S cross domain security services – which are highlighted in the paper. Both the CDS conceptual framework and reference architecture served as the baseline for NLR's secure airpower simulation interoperability testbed. This is discussed in the remainder of the paper along with some possible CDS implementation designs and the lessons learned from an initial experimentational evaluation.

ABOUT THE AUTHORS

Dr. Manfred Roza is Senior Scientist at the Royal Netherlands Aerospace Centre NLR. He holds a Ph.D. in aerospace engineering from Delft University of Technology and has more than 25 years of experience in simulation and training, in the academic world, simulator industry, and governmental organizations. His current activities focus on AR/VR/MR, distributed cloud-based simulation, cross domain security, training eco-systems, and cost-optimization.

Arjan Lemmers is Senior R&D Engineer at the Royal Netherlands Aerospace Centre NLR. He holds a M.Sc. in aerospace engineering from Delft University of Technology and has more than 30 years of experience in the M&S technology applications in the military domain and governmental organizations. He has led many NATO MSG task groups and currently chairs the NATO MSG-165 on the incremental implementation of MTDS.

Capt. James Quarmyne is a graduate of the US Air Force Institute of Technology at Wright-Patterson Air Force Base. He has been involved in multiple USAF LVC simulation efforts and electronic warfare system developments. Currently he is a USAF exchange research fellow at NLR focusing on MTDS, LVC and AirC2 simulations.

Lt.Col. Peter van Onzenoort is the modelling and simulation group coordinator of the Air & Space Warfare Centre of the Royal Netherlands Air Force (RNLAF). His group is responsible for the development and operation of the RNLAF Airpower Battle Lab, and involved in many (inter)national airpower CD&E activities and events.

Cross Domain Security in Airpower Mission Training through Distributed Simulation

Dr. Manfred Roza, Arjan Lemmers M.Sc., Capt. James Quarmyne & Lt.Col. Peter van Onzenoort

Royal Netherlands Aerospace Centre NLR

Amsterdam, The Netherlands

manfred.roza@nlr.nl, arjan.lemmers@nlr.nl, james.quarmyne@nlr.nl, phgj.v.onzenoort@mindef.nl

INTRODUCTION

Air forces are faced with challenges regarding 5th generation airpower training and exercises. While current and future operations are becoming joint, combined arms and multinational in nature, the missions and the systems are becoming more complex and need detailed preparation and rapid adaptation to changing circumstances. Therefore, the Royal Netherlands Air-Forces (RNLAF) and its coalition partners have a common need for training of air combined and joint collective tactical training. MTDS is crucial in satisfying these training needs and as to assure RNLAF and NATO's readiness at an appropriate level. Like many other air forces, the RNLAF is moving towards a persistent national MTDS capability to integrate, interoperate and leverage its national simulation assets as well as with NATO coalition partners within a single collective mission training environment. This means that the RNLAF MTDS capability must be able to interconnect with the NATO MTDS architecture, which is currently under development within the NATO MSG-165 task group (Lemmers et. al 2020).

Both on a national and coalition MTDS level, one of the biggest challenges is to interoperate different nationally (sovereign) classified simulation assets within a single collective training exercise. This is a balance between protecting sensitive simulation assets, their underlying data and information, against exposure to (cyber)security threats on one side and on the other side enabling simulation data sharing between these assets in such a manner that the collective training objectives are achievable. However, these goals are usually in competition with each other. A cross domain security (CDS) solution, is a common means used to securely connect discrete military systems or networks, such as C4ISR systems (Norbotten et. al 2015, NATO IAG 2018). These separate military systems or networks, referred to as security domains, usually have different security policies to address their exposure to different types of threats and levels of risk, and therefore hold differing levels of trust. Simply stated, a CDS is an assured system which performs the security functions necessary to control the flow of information and data between security domains. However, common knowledge and experience of CDS application in distributed simulation is scarce and specifically designed CDS solutions by industry for simulation assets are rare (NATO MSG 2015, NATO IAFG 2012). MTDS capabilities in this regard imposes unique challenges and requirements on such solutions not seen in other military application domains, that directly relate to the real-time simulation performance (e.g. latencies and throughput), simulation realism (e.g. fair-fight) and training effectiveness. Though a M&S specific CDS appliance is the key building block to facilitate effective cross domain security for MTDS, a thorough approach should consider more than a single technical solution in isolation. Additionally, not all cross domain issues can be solved with technical solutions alone. Human factors, information management practices, personnel security clearances and other security measures must be considered to ensure an accredited solution is established that also meets the training objective. This requires a risk-based approach to cross domain security to properly balance the level of simulation training objectives that are achievable against the level of acceptable residual security risks from deploying M&S CDS appliances.

The paper describes a conceptual framework with fundamental cross domain security terminology, concepts and principles pertaining to the secure interoperability of simulation assets from different security domains within joint Airpower MTDS exercises. This framework has been developed by The Royal Netherlands Aerospace Centre NLR as part of the joint RNLAF and Dutch Defense Material Organization (DMO) national research program into MTDS. The framework was also used as input for the NATO MTDS reference architecture security component, an effort led by NLR, and which describes a set of M&S cross domain security services and a baseline deployment topology. NLR's secure airpower simulation interoperability testbed is discussed in the remainder of the paper along with several possible CDS implementation designs and the lessons learned from the initial experimentational evaluation.

COMMON CROSS DOMAIN SECURITY TERMINOLOGY AND CONCEPTS

This section defines the common cross domain security terminology and concepts, which are part of the conceptual framework for M&S CDS. Its purpose is to facilitate the communication, understanding and implementation of actual CDS solutions within the modeling and simulation domain. Though more references have been used, the most important ones and recommended reading are the NATO MSG (2015), Industrial Internet Consortium (2016), Curran (2017), Australia Cyber Security Centre (2019 and 2020) and National Security Agency (2018).

Security Domains – Some Definitions

A security domain in a M&S context is defined as a simulation asset or a federation of simulation assets in a network, within a defined boundary operating under a consistent security policy and the ownership of one organization, nation and/or security authority (SA). A security policy in this regard defines key elements such as the security classification, releasability rules, community of interest, and any other special handling caveats for the data and information of the actual military systems and doctrines contained and processed within the simulation asset(s). The security policy will also specify the physical and personnel security controls needed to protect the security domain. Security domains can be (hierarchically) organized to form larger domains. For example, a security domain can comprise one or more network enclaves, which are sections of an internal network that are subdivided from the rest of the network by a single and commonly shared boundary protection security measure. In other words, an enclave is a security domain within a security domain, under control of a single SA. Here, a boundary is a logical delineation around a security domain wherever simulation assets that are contained within that security domain can interface externally, such as with simulation assets within other security domains. If there is no such external interface, there will still be a physical separation and boundary with the rest of the outside world, which is known as an air gap.

The security policy defines the level of protection (e.g. security measures), referred here as a security level classification, with which a security domain is protected against (cyber)security threats. The classification of an information or data item's sensitivity (e.g. unclassified confidential, secret and top secret) that is stored and handled within a security domain is expressed by means of a security label that is associated or bonded to such item. This means for instance that a simulation facility (i.e. security domain) with a security level of NLD-secret may store and handle NLD military sensitive data items that ranges from unclassified up to data classified as NLR-secret.

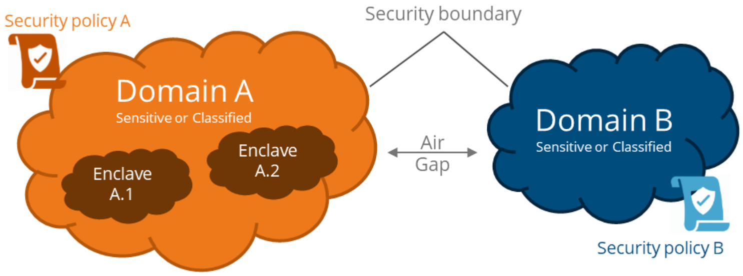

Figure 1. Security Domain, Enclave, Boundary and Policy

In the context of security domains also the terms Multiple Independent Levels of Security (MILS) and Multi-Level of Security (MLS) are often used. MILS is a standard security model where typically one security domain per security classification or sensitivity level per organization exists. For instance, an air-force can have multiple separated network such as unclassified network and a secret network. The MLS security model is the opposite of MILS. Instead of working with independent environments, under the MLS model there only exist one encompassing environment (i.e. security domain) that holds all the organizational information and data tagged at all sensitivity, security levels and enforces access rules accordingly. Due to the complexity and high cost of managing or accrediting the MLS model and the simplicity and the ease of achieving segregation of the MILS model, the MILS model is almost always the de-facto standard within the military domain. Therefore, it is also the common underlying model for most CDS solutions.

Cross Domain Security – Connecting Security Domains

Cross domain security is defined as a comprehensive approach to defending against both known and unknown threats to data connections and interoperability at the boundaries between two or more security domains. It comprises secure CDS technology in combination with organizational or national security policies, processes, procedures and additional controls to provide sufficiently strong cyber security protection for high risk use-cases. Key is to understand the security risks inherent to interconnecting and exchanging data between simulation assets in the target security domains for a specific M&S application use-case, and ensuring policy enforcement to reduce security risks to an acceptable level of the responsible security domain owner and/or authority. In here, a CDS is the actual technological solution that implements the necessary security functionality to securely connect, and control the access and transfer of data between two or more differing security domains (e.g. isolated classified or sensitive simulation networks and assets). As such, a CDS embodies the physical enforcement of the cross-domain security policies to mitigate the security risks of the threat environment and warrant the confidentiality, integrity and availability of the simulation system, information and data (Figure 2), where:

- *Confidentiality* – the assurance that data or information is not made available or disclosed to unauthorized persons, entities or processes
- *Integrity* – the assurance that data, information and systems are not modified or destructed without authorization
- *Availability* – the assurance that on-demand, timely and reliable access to the required data, information or data by an authorized user is guaranteed
- *Authenticity* - the assurance that the identity of a user, process or system is known and verified, as a prerequisite to allowing authorized access
- *Accountability* - the assurance that the origin and integrity of data has been proven, or that an authentication can be asserted to be genuine and any subsequent actions cannot be denied (also known as non-repudiation)

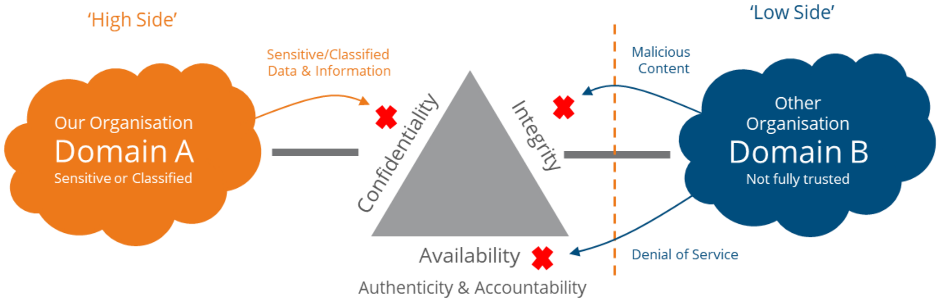

Figure 2. Data and Information Cross Domain Security Objectives

When security domains are considered together, one security domain will be more trusted than the others (Figure 2). The more trusted security domain, typically with a higher security classification or caveat, is commonly referred as the high side or domain high. The high side security domain usually has more restrictive security policies, and provides higher levels of confidentiality, integrity and availability. The less trusted security domain is referred as the low side or low domain. It will be considered to have less restrictive security policies and hold lower levels of confidentiality, integrity and availability. Between different organizations or in a multinational context, such as in combined or joint military operations and collective training, it is hard to make a distinction between high side and low side security domains. In these cases, each security domain owner from its perspective will usually consider its own security domain as the high side security domain and take the responsibility for its own CDS implementation, while all other connected security domains are considered to be the low side.

Cross Domain Solutions – Basic Functions and Principles

In essence a CDS is simply a technical means that enforces a certain security policy by explicitly controlling the flow of data exchanged between security domains. Different (sub)types of CDS solutions can be defined, such as transfer, access, cross domain guards, MLS system and combinations thereof. Given the scope of this paper and the relevance for air-power MTDS context, only transfer CDS types will be considered here. A transfer CDS facilitates the transfer of data that moves between two or more independent security domains (i.e. applying a MILS model). Transfer CDS could be either uni- or bi-directional. Given the fact that distributed simulation interoperability requires bi-directional simulation data exchange bi-directional transfer CDS are the only effective types for airpower MTDS application purposes. A bi-directional transfer CDS consists of a physically separate low side to high side and high side to low side data flows paths to enforce separation of data flows through one-way flow control mechanisms (Figure 3). From the perspective of the high side, data transfer through the CDS from the low side to the high side, is described as data import or inbound data, whilst a data transfer from the high side to low side is described as data export or outbound data. In this regard a CDS is an assured and controlled gateway environment that connects two security domains (i.e. isolated classified or sensitive simulation networks and assets). It provides interfaces on both sides that serve as network proxies to accept data from authenticated and authorized simulation assets in one security domain for inspection and treatment. And after the treatment by security-enforcement points inside the CDS, the other interface presents this data in a usable form to the destination simulation assets in the approved security domain.

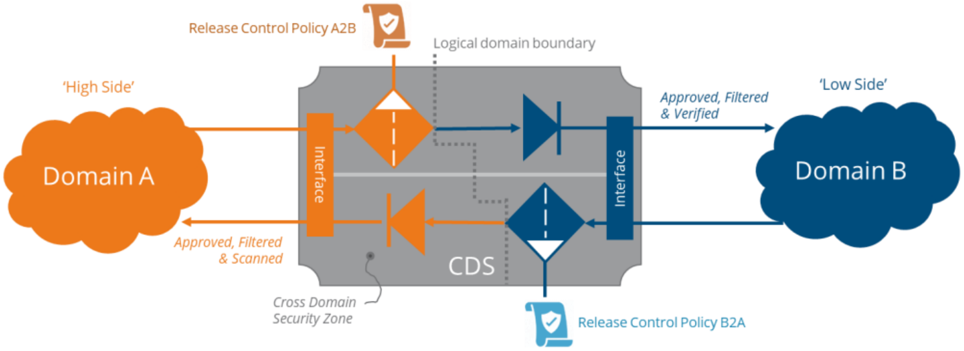

Figure 3. Bi-Directional Transfer CDS – Abstract Architectural View

This security enforcement in a CDS commonly comprise two major buildings blocks. The first are typically one-way security controls (e.g. data diodes) that enforce the paths that simulation data can transverse through the CDS. The second are typically guard security controls that filter, normalize, transform and/or sanitize the data to avoid import of undesired malicious content, and prevent uncontrolled export of sensitive or classified data (i.e. information leakage). The key principle of this guard security controls is by default blocking all data, and only permitting data to pass based on pre-determined security policy rulesets and release approval. The internal architecture of a real CDS may differ from the abstracted model as depicted in Figure 3. Moreover, an actual CDS could be an integrated appliance or, more commonly, be composed of a combination of general purpose security hard- and software components and dedicated security-enforcing technologies.

DISTINCTIVE M&S CROSS DOMAIN SECURITY ASPECTS

Cross domain security and transfer CDS types are commonplace in the C4ISR application domain to manage the controlled information and data exchange between military systems that operate on different security levels and which are used in joint live training exercises (e.g. red flags and Frisian flags). The application of any type of CDS in airpower MTDS exercises are scarce. The rationale for this is that although CDS in both domains serve the same core function, distributed simulation environments for training purposes impose unique challenges and requirements on CDS devices and services not seen in the other application domains (NATO 2015, Möller et al. 2015, Lippe and Odermatt 2019):

a. Simulation assets require **'exact'** or **'ground truth' information** concerning simulation objects and interactions to allow their underlying models to function properly. This ground truth is established through a common information exchange data model (e.g. FOM and DIS PDU) that is shared between all simulation assets participating in a MTDS exercise to allow consistency between federates. Due to simulation data filtering, normalization, transformation and/or sanitization by guard security controls, the local simulation asset ground truth may deviate too much, from this common shared ground truth (i.e. disjoint or uncorrelated fidelity levels), that this negatively impact the simulation realism (e.g. fair-fight) and training effectiveness.

b. The simulation data exchange in MTDS exercises is highly **time critical** requiring low latency and high data throughput rates. When the CDS interfaces, one-way security controls and guard security controls introduce high latencies, and largely varying update rates in the simulation data flow in or out the simulation asset. This could cause human observable time-related anomalies that negatively impact the immersion and learning experience.

c. Direct and full **observability** of the detailed quantified ground truth information, including sensors and weapon system behavior, through the common information exchange data model used in MTDS exercises. In live training exercises such data is most often not directly or fully observable, and therefore one has primarily access to 'perceived truth' data. This poses a challenge with respect to unintended information leakage that gives direct insight into the simulated system's capabilities and the ability to extrapolate (sovereign) classified system information from 'ground truth' simulation data and from combining simulated 'ground truth' and 'perceived truth' data from reality.

d. Simulation training environments are highly **controllable** and offer the possibility to **repeat** the same operation(s) over and over again, within a single MTDS exercise or even over multiple MTDS exercises. This can be done systematically under similar or slightly different conditions and with different inputs. This allows for analysis of 'big' sample sizes and thus deduction of information that is otherwise hard to obtain, using todays modern data-science methods (e.g. data re-identification techniques).

The elements above refer to assuring the confidentiality of the simulation asset and its underlying data and information (Figure 2). The simulation data flow is composed on a combination of structured data (e.g. DIS PDU or HLA objects) but also unstructured data, as for instance audio, video or tactical data link flow based on raw/unpredictable content. This unstructured data may also be an opportunity for malicious content that may compromise a simulation asset, hence may set up covert channels for uncontrolled data leakage, and impair the integrity and availability of MTDS capabilities.

All these together makes CDS solutions for MTDS exercises more complex and challenging to design, implement and deployed compared to the C4ISR application domain. It requires a constant trade-off of assuring that classified information and simulation data shared between participating (inter)national simulation assets in a MTDS exercise is sufficiently protected and regulated with the proper privileges (i.e. security policies), without negatively impacting the real-time simulation performance (e.g. latencies and throughput), simulation realism (e.g. fair-fight), and training effectiveness. Therefore, as an alternative sometimes the lower security domains is reclassified to the security level of the high domain it needs to interoperate with, by imposing the high domain security policies and measures onto the lower security domain. This is known as the "system high" security model. The major drawbacks of this approach are that these additional security measures come at a significant extra development and operational costs, and more importantly simulation assets in these reclassified domains are no longer available outside the security domain for other purposes. Within an international joint collective training context, even in NATO coalitions, this is practically not feasible for two reasons. First, there is no common shared simulation data security policy or classification. Second, such state seems unattainable since each NATO nation is owning and protecting its sovereign simulation assets and underlying data or information under its own nationally governed security policies.

CROSS DOMAIN SECURITY APPLICATION IN MTDS – A REFERENCE BASE

In this section the reference topology for deploying M&S CDS solutions within the MTDS exercises, the reference architecture building block for such M&S CDS solutions and their underlying services will be outlined.

M&S CDS Reference Topologies

In essence there are two topologies in which a CDS solution can be deployed in an M&S context (Figure 4).

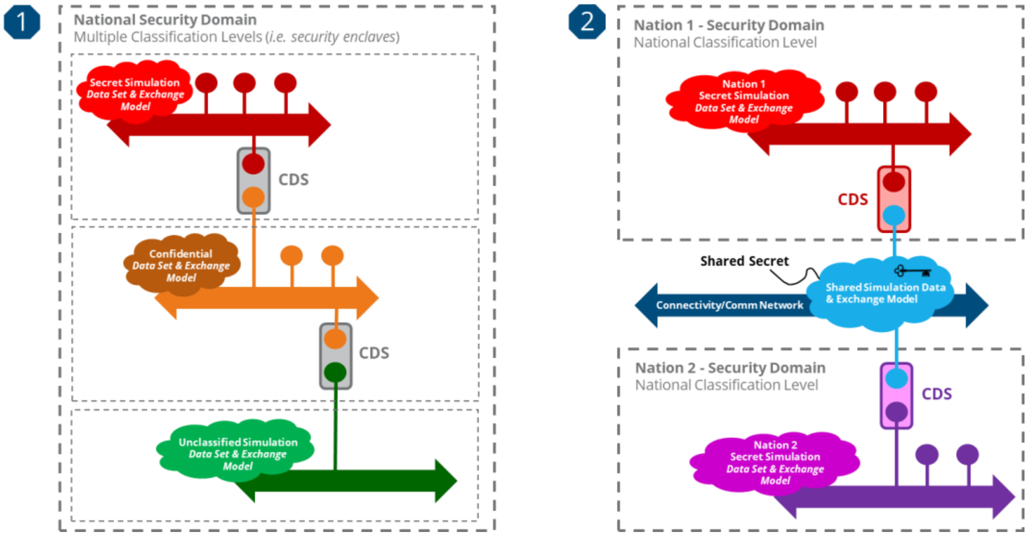
1
National Security Domain
Multiple Classification Levels (i.e. security enclaves)
Secret Simulation Data Set & Exchange Model
CDS
Confidential Data Set & Exchange Model
CDS
Unclassified Simulation Data Set & Exchange Model
2
Nation 1 - Security Domain
National Classification Level
Nation 1 Secret Simulation Data Set & Exchange Model
CDS
Shared Secret
Connectivity/Comm Network
Shared Simulation Data & Exchange Model
Nation 2 - Security Domain
National Classification Level
CDS
Nation 2 Secret Simulation Data Set & Exchange Model

Figure 4. Basic Reference Topologies for M&S CDS Deployment

Deployment topology 1 comprises the situation where the simulation assets and M&S CDS solutions in a distributed simulation environment are owned by one armed force, nation or governed by single security authority. In here a single CDS solution can directly be used to bridge and control the simulation data exchange between simulation assets that operate in different security enclaves each with a specific classification level. This is typically realized through a layered network architecture approach, where each security enclave is hierarchically stacked on top of each other and connected through a CDS solution that resides in the higher classified enclave.

Deployment topology 2 comprises the situation where simulation assets in a distributed simulation environment are owned by different armed forces or nations, and thus belong to security domains that are governed by different security authorities. To ensure that each nation has the full control of its nationally owned classified simulation data and how this is shared with other nations, each nation shall typically use its own M&S CDS solution. In here each nation's CDS first transforms and maps its own sovereign classified simulation data set into a releasable data set (e.g. SOM), and then publishes it into the collective shared simulation data set on a joint simulation backbone (e.g. HLA or DIS network) according to the agreed simulation information exchange model (e.g. FOM). This collective simulation data set is a "shared secret" of all participating nations (i.e. security domains) in the distributed simulation environment. This shared data needs to be collectively protected with common agreed security measures such as data encryption to assure confidential information exchange over third party military network infrastructure (e.g. NATO CFBL Network) and security measures imposed on each nation's participating simulation facility. Deployment pattern 2 is the reference deployment topology of M&S CDS solutions in combined and joint collective airpower MTDS exercises in general and NATO MTDS exercises in specific.

M&S CDS Solution Architectural Pattern

Figure 5 shows the NATO M&S CDS solution reference architecture for the secure simulation data exchange in NATO MTDS exercises between simulation assets that reside in different national security domains.

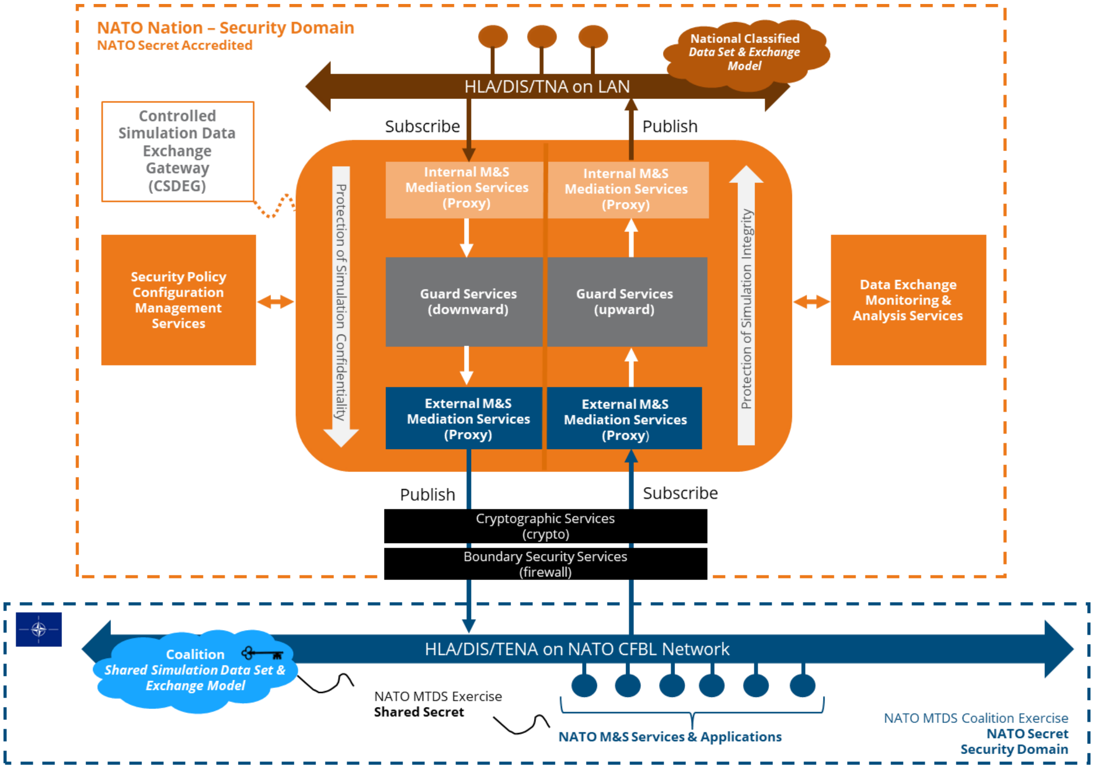
NATO Nation – Security Domain
NATO Secret Accredited
National Classified
Data Set & Exchange
Model
HLA/DIS/TNA on LAN
Subscribe
Publish
Controlled Simulation Data Exchange Gateway (CSDEG)
Internal M&S Mediation Services (Proxy)
Internal M&S Mediation Services (Proxy)
Protection of Simulation Confidentiality
Protection of Simulation Integrity
Security Policy Configuration Management Services
Guard Services (downward)
Guard Services (upward)
Data Exchange Monitoring & Analysis Services
External M&S Mediation Services (Proxy)
External M&S Mediation Services (Proxy)
Publish
Subscribe
Cryptographic Services (crypto)
Boundary Security Services (firewall)
HLA/DIS/TENA on NATO CFBL Network
Coalition
Shared Simulation Data Set & Exchange Model
NATO MTDS Exercise
Shared Secret
NATO M&S Services & Applications
NATO MTDS Coalition Exercise
NATO Secret
Security Domain

Figure 5. M&S CDS Solution Architectural Pattern and Building Blocks Overview

A clear distinction in the architectural pattern is made between the specific M&S CDS solution building blocks (orange) and the additional common cyber security building blocks (black) that collectively provide the full security solution to securely connect a national security domain to the distributed simulation backbone (e.g. HLA, DIS or TENA) running on the NATO CFBL network infrastructure.

The core of a M&S CDS solution is a Controlled Simulation Data Exchange Gateway (CSDEG). This CSDEG is configured with the national security policy. Among other security-enforcement functionalities, this security policy defines a release rule set based upon which the CSDEG makes context dependent decisions about what and how simulation data is bidirectionally exchanged and as such prevents unauthorized data exchange between the national and NATO MTDS security domain. In here the M&S mediation services are proxy components (i.e. federates) that manage the connections of the CSDEG to local national simulation assets on the high side and to the MTDS simulation environment (e.g. federation) on the low side with a limited publish/subscribe subset interface (e.g. public SOM) that implements a release control mechanism.

The CSDEG is organized as separated upward and downward paths to provide the ability to enforce uni-directional data flow separation. This not only improves the reliability and robustness of the M&S CDS solution, it also facilitates the optimization of the data flow paths to address the specific threats to each nation's simulation assets (i.e. high side) confidentiality and integrity. Generally, simulation data moving from low side to high side security domains will be channeled through a different arrangement of security-enforcing mechanisms compared to data moving from high side to low side (See Figure 3):

- **High to Low Security Domain Flow Channel**: Simulation data flowing from the national domain (high side) simulation assets to the NATO domain (low side) must be protected against unintentional sovereign classified information disclosure or leakage, hence the CSDEG services should assure their confidentiality. In here an internal M&S Mediation Service subscribes to a limited subset of the classified simulation data exchange model, according to the national security policy. This M&S Mediation Service terminates the simulation interoperability middleware service protocols (e.g. DIS PDU, HLA Objects and Interactions), serializes (i.e. transforms) the simulation data by means of an object serialization protocol (OSP), and transmits it to the downward Guard Services. These Guard Services provide the ability to first apply data filter (e.g. suppressing, modifying and replacement) and release control mechanisms (i.e. block or pass), which ensure that only permitted simulation data transfers from the national security domain to the NATO domain. Secondly, the downward Guard Services provide the ability to enforce one-way data flow control on the releasable simulation data through appliances such as data-diodes. Hereby blocking any network traffic on the CFBL Network that attempts to flow from the low side back into the high side, which may compromise the integrity of the high side filter and control mechanisms. Finally, the serialized releasable simulation data is deserialized by an external M&S Mediation Service into the simulation interoperability protocol (e.g. DIS PDU, HLA Objects and Interactions) that runs on the NATO CFBL network.

- **Low to High Security Domain Flow Channel**: National simulation assets must be protected against simulation data with malicious content flowing from the NATO domain (low side) to the national domain (high side) and that may intrude national simulation assets, hence the CSDEG services should assure their integrity. In here an external M&S Mediation Service subscribes to the shared NATO simulation data exchange model. This M&S Mediation Service terminate the NATO MTDS coalition simulation interoperability middleware service protocols, serializes the simulation data by means of an object serialization protocol (OSP), and transmits it to the upward Guard Services. These Guard Services provide the ability to first enforce one-way data flow control on the releasable simulation data through appliances such as data-diodes. Hereby blocking any network traffic on the nation's network that attempts to flow from upstream on the high side into the low side, which may compromise the confidentiality of the national simulation assets and sovereign information. Secondly, the upward Guard Services provide the ability to apply data filter (e.g. checking, inspecting and scanning) and release control mechanisms (i.e. block or pass), which ensures that only permitted simulation data transfers from the national security domain to the NATO domain. Aside additional traditional high-assurance malware detection not covered by the firewall protection services, this process may comprise advanced content filtering to detect possible attacks that try probing/stimulating national simulation assets with dedicated simulation data signals. Finally, the serialized approved upward simulation data is deserialized by an internal M&S Mediation Service into the simulation interoperability middleware service protocol that runs on the nation's local network.

The CSDEG mediation and Guard Services are configured by means of a security policy file(s), which comprises the definition of the simulation data release control and filtering rules. These rules are established and accredited prior to each MTDS exercise and remain fixed during the exercise execution. For this purpose, release policy configuration management services are provided within the national security domain. These services enable authorized national simulation asset owner personnel, together with the security authority, to design, create, modify, maintain, verify and accredit release policy files and securely load these into the CSDEG.

Simulation Data Exchange Monitoring and Analysis services shall be provided within the national security domain and attached to the CSDEG. These services monitor, analyze and log the simulation data exchange across the CSDEG to identify security breaches as well as report, alert and take appropriate (automatic) countermeasures (e.g. disconnect or shutdown simulation assets) in (near) real-time. Exhaustive post-analysis of logged simulation data exchange during a MTDS exercise, even in combination with other logged historic data of other MTDS exercises, should also be conducted with machine learning and other AI intensive analysis to detect more advanced security intrusions, to compromise simulation assets and stealing national classified information. If such security incidents are found and reported, additional offline countermeasures could be taken such as updates to CSDEG hard- and software hardness, Guard Services filtering mechanisms and security policies for joining future MTDS exercises.

The common cyber security building blocks in Figure 5 comprise (additional) boundary security and cryptographic services. Boundary security services, typically implemented by firewalls, should be used to protect the national security domain from being compromised or against other possible cyber-attacks from malicious or compromised insiders that may try to intrude the domain from the external network. Cryptographic services should be applied to ensure the confidentiality of the simulation data in transit and shared across the external network between simulation assets inside each participating national security domain. The required type, hard- and software set-up, robustness and hardiness of such firewalls and cryptos depends on the security risks anticipated by the national security authority from participating nations in a combined and joint collective airpower MTDS exercise and NATO in specific.

M&S CROSS DOMAIN SECURITY FOR AIRPOWER MTDS IN ACTION

In this section NLR's secure airpower simulation interoperability testbed for the RNLAF is introduced along with several possible actual, but conceptual, M&S CDS implementation and data filtering designs. These M&S CDS conceptual designs are currently undergoing a series of experimental evaluation trials in NLR testbed to proof their capabilities and limitations. The section presents several initial lessons learned from the first experimental evaluation trials regarding their feasibility and utility in airpower MTDS exercise.

Secure Airpower Simulation Interoperability Testbed

NLR's secure airpower simulation interoperability testbed has been established in support of the joint RNLAF and DMO national research program into MTDS. The objective of this capability is to provide a low-barrier testbed to experimentally evaluate the feasibility and impact of various CDS solutions for MTDS but also for M&S applications in general such M&S as a Service and LVC simulation. The need for such capability is eminent due to the many unknowns pertaining to cross domain security in the M&S domain, practical restrictions of experimenting with real classified simulation assets, high costs and very limited access to actual industrial GOTS/MOTS CDS solutions from large vendors such as Boeing, Lockheed-Martin, Raytheon and Collins Aerospace. Therefore, the core of NLR's testbed is based on open simulation standards. COTS and unclassified simulation hardware, assets (e.g. Prepar3D), M&S applications (e.g. STAGE and VR Forces) and tools (e.g. VR Exchange), which are complemented with NLR's natively developed simulation models and software for various RNLAF platforms and operational environments. This allows for low TRL research and development to cross domain security with emulated security domains and sensitivity levels, while the modularity of the test-bed provides the ability to mature promising CDS solutions towards actual implementations, with or without dedicated assured GOTS/MOTS CDS components, for real classified simulation assets by isolating such solutions in dedicated security enclaves. The latter is a specific requirement since long-term R&D objective set by the RNLAF for this testbed is to develop, assess the value and residual security risks of actual CDS solutions to enable RNLAF NLD secret classified mission simulation training capabilities (e.g. F16 ULT, F35 CDEF, NH-90 FMFT and AH64-E/CH-47F MSMT) to participate in (inter)national Airpower MTDS exercises.

M&S CDS Implementation Designs

As discussed in the beginning of this paper CDS solutions are always tailor made and accredited for each individual M&S use-case and threat environment. In other words, CDS solutions are developed for each individual MTDS exercise. Therefore, to cost-effectively and timely deploy classified simulations assets requires CDS solutions that are designed with known ‘pre-approved’ architectural design patterns and reusable components, when available. This ensures (residual) risks related to common cross domain security threats and M&S training impact are more easily understood and addressed. To satisfy these operational requirements and meet the RNLAF long term objective for CDS, the NLR testbed adopted a modular toolbox approach to deliver M&S CDS solutions that can be composed by means of patterns, reusable and reconfigurable components. This approach centers around NATO MTDS reference architecture for M&S CDS (Figure 5). As depicted in Figure 6, in this CDS toolbox a global division is made in (*A*) assured hard- and software security components (e.g. data-diodes, secure OS, hardware gateways, identity management and anti-malware software) and (*B*) guard security algorithms to orchestrate filters that block, normalize, transform, sanitize, verify and release simulation data between the connected security domains.

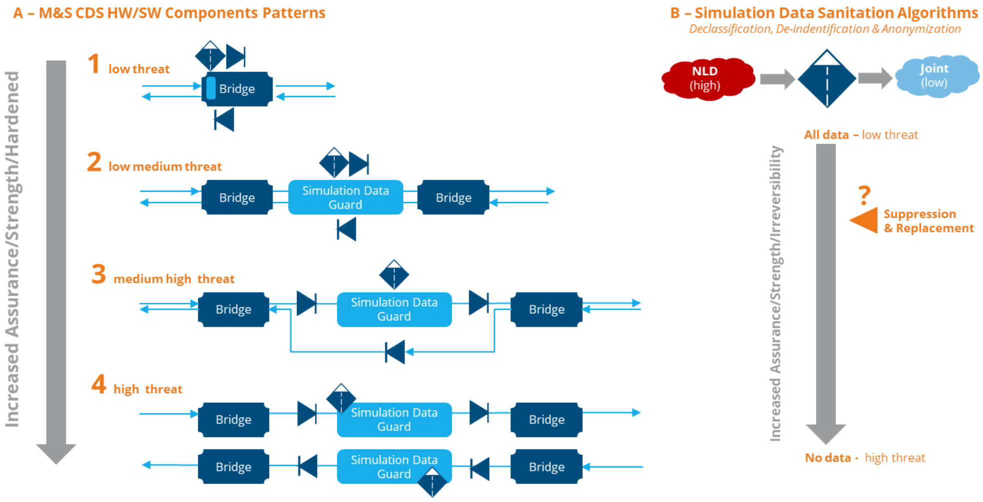

Figure 6. Pattern-based Modular Toolbox Approach to M&S CDS

The secure M&S bridge component, utilizing standard VR-Exchange gateway/bridge software and plug-in interfaces, implements the internal/external M&S mediation services for multiple simulation protocols including DIS, HLA, TENA and DDS. Depending on the threat level this bridge component can run on a single host and directly filter and control the direction of the simulation data-flows for very low threat environments up to running on different hosts, perform filtering and release control on separate appliance, and deploy fully physically separate flow channels and data-diodes for very high threat environments. In the latter case the secure M&S bridge component acts primarily as a network proxy that (de)serializes simulation data protocols to, for instance JSON, WebLVC or ProtoBuffer, to realise the protocol break security measure. The secure M&S bridge component by default publishes no simulation data to and subscribes to all available simulation data from the low side domain (e.g. NATO MTDS collation shared secret data-set). Based on the security release policy the bridge component publishes only the minimal necessary set of data to reduce the simulation data attack surface to a bare minimum, and internally only feeds forward the actual required simulation data to obfuscate the real data and data-regions of interest (e.g. SOM) for the national simulation assets.

M&S CDS Simulation Data Filtering Taxonomy

A M&S CDS should deploy different guard security control mechanism (i.e. Guard Services in Figure 5) for the combination of all structured and unstructured data that is exchanged between security domains in a MTDS exercise. However, the present and key focus is on simulation data guards or filter mechanisms for DIS, HLA, TENA and DDS protocols since these comprise the distinctive M&S cross domain security aspects as outlined in the beginning of this paper. By default, a simulation data guard blocks or suppresses all bi-directional data and based on the security release policy configures and applies the appropriate release rules, conditions and filtering mechanisms for the simulation data that is transferred between the security domains. To facilitate the development of reusable and standard filtering mechanisms along with understandable/auditable machine-readable release policy configuration files a first simulation data filtering taxonomy has been defined for NLR's testbed (Figure 7).

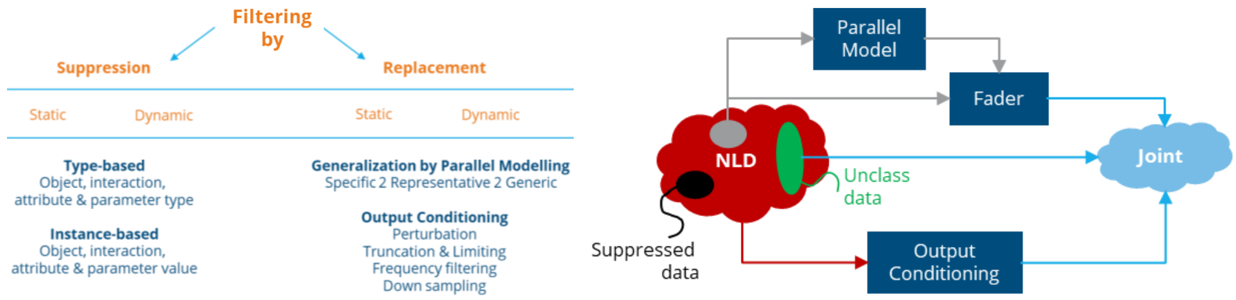

Figure 7. Simulation Data Filtering Methods & Techniques Taxonomy

In essence there are two ways to filter: either suppress the simulation data (e.g. HLA objects and interactions) or replace the actual simulation data with a modified version. This can be done either statically and pre-scripted, or more dynamically based on the simulation data items values changes over time using more complex algorithms. Suppression can be done based on the simulation data item type, simply by not publishing specific simulation data. Or it can be done instance-based where a data item value is used to decide whether or not to suppress a simulation data item completely or partially. Replacement involves value-based filter algorithms that replace actual simulation data items or attributes values by a modified value. As depicted in Figure 7, this modification (red line) can be done directly on the simulation output data with stateless (e.g. truncation) and stateful algorithms (e.g. low pass filtering). The other option is to operate "lower" classified parallel simulation models (grey lines), whose output values can be fed in/out to replace actual simulation data items or attributes based on certain rules or conditions. Unclassified simulation data that doesn't pose any security risks, even not by any indirect cascading or propagation effects, can be directly transferred to the lower domain (i.e. joint domain in the case of MTDS exercises). Filtering by suppression is in theory relatively the easiest to implement and understand, while replacement done by output conditioning and parallel models become rapidly more complex.

M&S Cross Domain Security Experimentation - Experimental Set-Up & Execution

Currently a series of experimental evaluation trials in NLR testbed are planned to evaluate various M&S CDS implementation and data filtering designs, for different use-cases and threat environments. These start from simple lab experiments to more complex and operational oriented use-cases and threat environments. In here the M&S CDS designs start from low threat M&S CDS components patterns and suppressing filter algorithms, and evolutionary develop these into more complex and high assurance M&S CDS solution based on lessons-learned. The focus of these series of experiments is to gain insight in the impact of CDS solutions on the real-time simulation performance, level of collective training fidelity and value, and residual risks of unwanted classified information leakage in MTDS exercises.

As the initial lab experiment use-case for the implementation of M&S CDS solutions, a fictitious scenario was designed which included multiple vignettes, each with a set of events and behaviours. The set-up included a DIS network connecting two emulated "classified" simulation environments, referred as a high side and a low side, in a joint distributed simulation environment. The deployment topology pattern 2 of Figure 4 was used as the basis for this joint environment in combination with two M&S CDS solutions (i.e. hosts Alien 1 and Alien 4) according to the low security threat pattern 1 (Figure 6) and applying basic suppressing filter algorithms. The idea here is that the high side is privy to all data from the low side, whilst the low side is privy to only access a subset of data from the high side as shared on the DIS backbone. Filtered data from the high side, not shared with the low side are emulated to be secret for experimental reasons. The scenario is a classic Blue Forces against Red Forces, where Red Force assets are considered ordinary/unclassified, whereas some Blue Force assets, in this case F-35s and some of their missiles and radar emission beams, are considered secret as deemed so by some security policy. On the low side, only pre-approved outbound data from the high side published via CDS to the DIS backbone can be viewed (Figure 8). On the other hand, all outbound simulation data from the low side is directly published onto the DIS backbone and thus subscribed to by the high side.

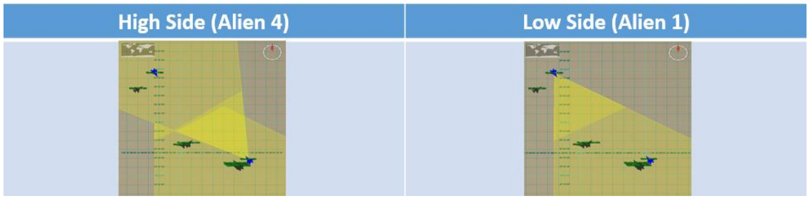

Figure 8. God's Eye View of High and Low Sides DIS entity states and radar emissions

In the first vignette, all missiles fired from Blue Forces on Red Force assets can only be seen on the high side and not the low side (Figure 9). This includes both air-to-ground and air-to-air engagements for scripted and unscripted simulations. The rationale is that Blue Force weapons are state of the art, thus appropriate measures must be taken to prevent reverse engineering by unauthorized parties. The aftermath of the missile flyouts, which is destroyed Red Force assets, can be seen on both sides. During the simulation, fire PDUs effects can only be observed on the high side whereas detonation PDUs effects can be observed on both the high and low sides.

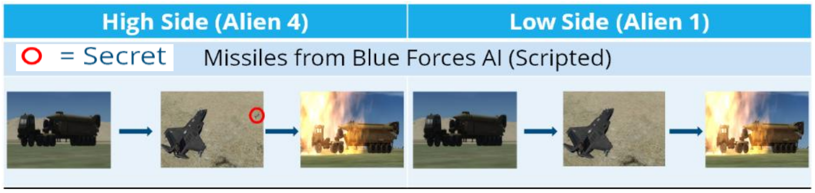

Figure 9. CDS Suppressing of Missile Fire Events and Flyouts from Blue Forces

In the second vignette, one of five F-35s in a simulated air pack is considered to have additional capabilities which are deemed secret and can only be viewed on the high side (Figure 10). This application, although not realistic in the context of military exercises, is a proof of concept that an entire entity can be suppressed just as well as one or more articulated parts and emitter devices (e.g. radar and designator lasers) of an entity as previously seen in Figure 8.

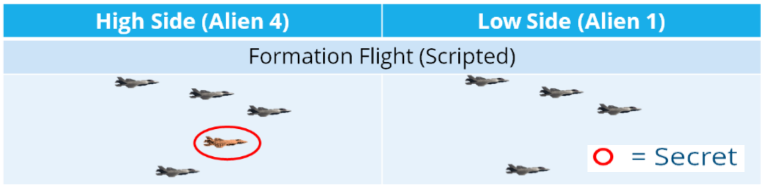

Figure 10. CDS Suppressing of Full Secret F35 from Blue Forces

The third vignette, shows all Red Force events on Blue Forces used in the set-up (Figure 11). These engagements include Red Force attacks from both a SAM site and an air asset against Blue Force assets. As stated before, all Red Force assets are considered unclassified and thus engagements can be seen on both the high and low side. Likewise, both fire and detonation PDUs are seen on both high and low sides.

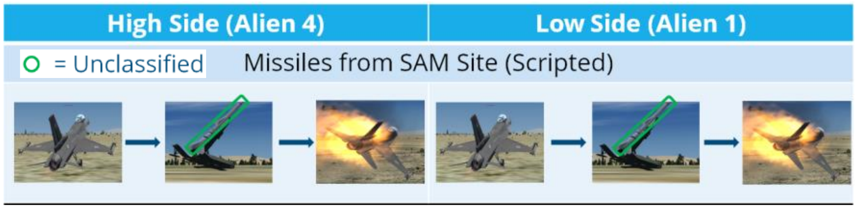

Figure 11. Unfiltered Unclassified Missiles from Red Forces

M&S Cross Domain Security Experimentation – Initial Lessons Learned

A small group of RNLAF operational users and DMO M&S subject matter experts were invited to observe and review this initial lab experiment use-case outcomes in the context of future MTDS exercise, as well as participate as a human role player operating one of the F-35 aircraft (Blue Forces) and one of the F-16 aircraft (Red Forces) in these vignettes. Based on a follow-on group discussion moderated by the NLR testbed team, the following initial lessons-learned were captured:

- No human observable latencies effects due to simple simulation data suppressing filter algorithms that could hamper pilot training effectiveness or immersion were experienced.
- Fidelity correlation anomalies between high and low side due to suppression of entities and events by a M&S CDS are in some case directly noticed by human role-play while others require more effort or may be entirely missed due to difference in situational awareness, workload or location of the aircraft. Proper scenario design in combination with tailored training objectives for a specific MTDS exercise may compensate for such anomalies and maintain the collective training effectiveness to an acceptable level.
- One should be aware of various propagation channels and combinatory (high-order) effects where simply suppressing a specific simulation data item or attribute is not sufficient to protect confidential information. For instance, suppression of a fire PDU and removal of the articulated part (e.g. missile) of the DIS entity still provides a means to reconstruct the time to target of the missile if the exact detonation DIS PDU is available to the low side. Another more advanced example of information disclosure could occur if multiple samples of similar tactical turn-breaks after a missile fire are observable during simulation execution(s) in combination with detonation DIS PDU and location of the target, it may then be possible to statistically estimate effective missile ranges with more advanced (big) data analytics methods.
- Estimating and analysing the impact of M&S CDSE filter algorithms and residual security risks is easier in a national MTDS exercise (i.e. can be done within the highest classified security domain) than in a NATO coalition MTDS exercise due to the fact that only sovereign simulation data of the own nation is fully known. This also make it more difficult in NATO Airpower MTDS to design scenarios to compensate for M&S CDS induced fidelity correlation anomalies.
- An important insight but unconventional approach that was tossed by several participants, was that striving for absolute or strongly enforcing fair-fight (i.e. fidelity correlation) in large scale mission training simulations is not the ultimate goal but gaining training value is. Hence, introducing additional fair-fight violations of fidelity correlation mismatches due to simulation data filtering may not be bad at all and acceptable. According to these participants who have been involved in actual combat missions, they claimed that war by itself is never a fair fight and always involves uncertainties and surprises regarding capabilities of your allies and enemies in large complex combat situations. It is particular these kinds of aspects and related competencies that one wants to train for. In live multinational flag exercises this is also commonly encountered and recognized, and still a lot of training value is gained from this with known but acceptable residual security risks.

CONCLUSIONS AND FUTURE WORK

Based on our initial experimental use-case, the effective application of M&S CDS for Airpower MTDS exercises seems to be feasible but not straightforward to implement and requires considerable effort. Though challenging, the key challenge of M&S CDS does not lay in the area of technical feasibility of assured security hard- and software appliance for M&S CDS, but in the design and application of appropriate simulation data filtering methods and techniques (Figure 6 and Figure 7). Successful application of M&S CDS for Airpower MTDS exercise requires simulation data filtering methods and techniques that balance training effectiveness against residual security risks. Finding this right balance and providing guidance to help design MTDS exercise require significant experimentation. And with an experimental design where collective training objectives, filtering methods and techniques and counter attacks & model stealing methods to these filtering methods are systematically varied. This is the core objective of NLR's secure airpower simulation interoperability testbed future research for the next 2-3 years, aside bringing M&S CDS solution concept to full maturity in all other aspects for dedicated RNLAF NLD secret simulation assets. The first step in this experimentation process is directly mapping the live flag exercise approach and way of execution one to one onto a MTDS environment, since this seems the most feasible manner to implement M&S CDS solution on a short term. Even though, it may introduce fair-fight/fidelity correlation issues its hypothesis is that it provides a level of training value that is equivalent to today's live flag exercises, but then at lesser training life-cycle costs (e.g. fuel consumption and material wear and tear) and in a better controlled and richer training environment.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the staff members of the RNLAF, the Dutch DMO Joint IV Command and the NATO MSG-165 members, we have worked with on this topic. In particular, we would like to thank Michael Jabautzke (Collins Aerospace), Jean-Louis Gougeat (Sogitec) and Sqn Ldr. Mike Hasbrig-Hartley (RAF-DOTC(A)) for their pragmatic and critical contributions. Furthermore, thanks to MAK Technologies for sharing their views, experience and technical support, as well as Pitch Technologies for their insights and reflections on this subject.

REFERENCES

Lemmers A. et. Al. (2020), Mission Training through Distributed Simulation for Joint and Combined Air Operations, *Proceedings of Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC), Paper No.20343. Orlando 2020 (to be published)*

Nordbotten N. et. Al. (2015), *Information sharing across security domains*, Norwegian Defence Research Establishment (FFI)FFI-rapport 2015/00456, August 2015

P. Curran (2017), *DOTC(A) Candidate CDS Architecture*, UK-MoD NITEWORKS, November 2017

Industrial Internet Consortium (2016), *Industrial Internet of Things Volume G4: Security Framework*, IIC:PUB: G4:V1.0, September 2016

Australia Cyber Security Centre (2019), Fundamentals *of Cross Domain Solutions*, Australian Government, December 2019

Australia Cyber Security Centre (2020), *Guidelines for Data Transfers and Content Filtering*, Australian Government January 2020

National Security Agency (2018), *Cyber Security Solutions – Multi-Site Connectivity Capability Package V1.1.*, June 2018

Lippe von der, S.R., A. Odermatt (2019), Distributed Data Service for Secure Cloud Simulations, *Proceedings of Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC), Paper No.19288. Orlando 2019*

Möller B. et. Al. (2015), Using HLA Object Models for the Analysis of Cross Domain Security Policies, *SISO SIW Fall2015, Paper 15F-SIW-038, Orlando, September 2015*

Ceranowicz A., et. Al. (2013), An Alternative Approach for Distributed Cross Domain Simulation, *SISO SIW Spring 2013, Paper 13S-SIW-08, San-Diego, April 2013*

NATO MSG-080 (2015), *Security in Collective Mission Simulation*, STO TR-MSG-080, April 2015

NATO IAG-162 (2012), *Study on Distributed Simulation for Air and Joint Mission Training*, NIAG-D (2012)0022, October 2012

NATO IAG-221 (2018), *Study on Industrial Contribution of ISR Information Exchange*, NIAG-D (2018)0011, April 2018