Three Perspectives on DSEEP and Security: Training Goals, Use Cases and the Selection of Security Measures

Björn Möller - Pitch Technologies, Sweden
Stella Croom-Johnson, Dstl, UK
Wim Huiskamp - TNO, The Netherlands

bjorn.moller@pitch.se
scjohnson1@mail.dstl.gov.uk
wim.huiskamp@tno.nl

Keywords:
Simulation, training, NATO, security, requirements, DSEEP, information exchange

ABSTRACT: *As joint, combined and Civil-Military exercises are becoming increasingly common, the need for security in collective mission simulation is growing. SISO has developed the Distributed Simulation Engineering and Execution Process (DSEEP) standard that provides a recommended process for development, integration and execution of federated simulations. Security aspects need to be managed throughout the DSEEP process. This paper offers three perspectives on this, based on the NATO MSG-080 work:*

- *A holistic approach, mapped to DSEEP, is presented. It discusses how training goals and security goals may conflict. It discusses possible resolutions as well as situations where security concerns may limit the training that can be provided.*
- *A real-life use case where a UK integration into the US Joint Training and Experimentation Network (JTEN), including security aspects, is mapped to DSEEP. This provides a deeper insight into the issues real federations may encounter and presents experiences and some advice.*
- *Finally a closer look at security and DSEEP is given. The focus is to support the selection and deployment of security procedures and technical security measures with focus on DSEEP step three and four.*

These perspectives are presented as input to the SISO community in general and the SISO Security in Simulation (SiS) study group in particular.

1 Introduction

The NATO Modelling and Simulation Group (NMSG) promotes co-operation among Alliance bodies, NATO member nations and Partner for Peace (PfP) nations to maximise the effective utilisation of modelling and simulation. The objective of the NMSG task-group MSG-080 is to develop recommendations on how to create a collective mission simulation environment (procedures and processes, organisation and technology) that allows for multiple security domains to participate.

This is the third paper from the NATO MSG-080 group. It builds on the previous two papers:

"Towards Multi-Level Security for NATO Collective Mission Training – a White Paper" [Ref 1] which gives an overview of the problem space, provides rationale for security in collective mission simulation, describes scenarios and use cases and summarizes some common security approaches.

"Security in NATO Collective Mission Training - Problem Analysis and Solutions" [Ref 2] which takes a closer look at what is different with M&S compared to live mission training, describes security concerns within M&S systems and gives an overview of the, potentially sensitive, information that can be found in simulations and federations.

The purpose of this paper is to provide three perspectives on security in simulation based on the DSEEP process for development and execution of simulations. The three perspectives are:

Training versus security goals throughout the DSEEP process. A holistic approach is presented with focus on how to identify and resolve conflicts between these goals.

A **real life use case** from the UK for security in simulation, mapped to the DSEEP steps.

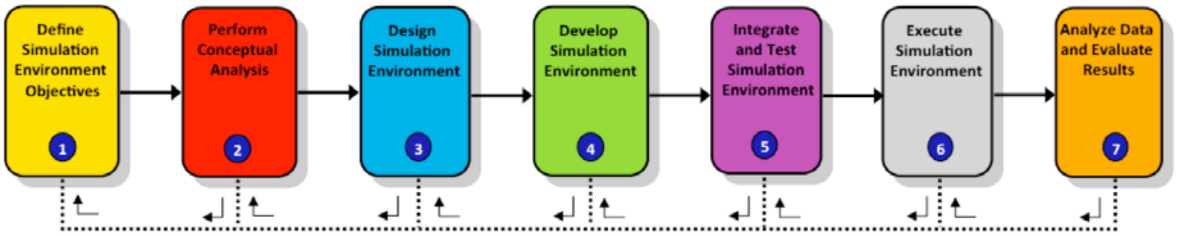
Define Simulation Environment Objectives
1
Perform Conceptual Analysis
2
Design Simulation Environment
3
Develop Simulation Environment
4
Integrate and Test Simulation Environment
5
Execute Simulation Environment
6
Analyze Data and Evaluate Results
7

Figure 1 DSEEP overview

The **selection and deployment of security measures** throughout the DSEEP process with focus on step three and four.

2 Short DSEEP Overview

The Distributed Simulation Engineering and Execution Process (DSEEP) has been developed by SISO and is formally standardized through IEEE 1730-2010. DSEEP is a 'seven step' process that starts with the need for interoperable simulation systems together with a clearly stated goal for the federation. The process consists of seven steps, ending with executing the interoperable set of systems and evaluating/assessing the outcome of the simulation. It can be used to develop distributed simulations systems based on architectures like HLA [Ref 3] and supports most types of development methodologies (e.g. waterfall or more iterative approaches).

As can be understood from the feedback arrows, DSEEP is not necessarily a linear or waterfall process. Each step or series of steps can be revisited, enabling for example spiral or incremental development. The process is usually combined with other processes, typically development processes for participating simulations. The process may also be tailored to fit smaller or larger projects or projects with special requirements. The steps are as follows:

Define Simulation Environment Objectives
In this step the goals and requirements of the sponsor (typically customer) for this simulation are established, for example training certain staff to carry out a particular mission under certain constraints. In addition to the goals the constraints shall be specified, typically including budget, deadlines and use of particular simulators or resources. Initial planning documents are a key part of the outputs.

Perform Conceptual Analysis
In this step a scenario for the simulation is developed. Based on the scenario a conceptual model is developed, for example what physical entities and interactions will need to be simulated. The requirements for the federation are designed, such as what needs to be simulated at what level. Hardware and networking requirements are also developed.

Design Simulation Environment
In this step the federation is designed, starting with the selection of which federates to use. The responsibility for simulating different entities in the scenario is allocated to the chosen federates and any gaps are identified. For missing federates a design is developed. Finally a detailed plan is prepared.

Develop Simulation Environment
In this step the Federation Object Model (FOM) is developed together with the Federation Agreement. Existing federates are adapted to these and any new federate is implemented. Finally the simulation infrastructure, like networking and middleware is set up.

Integrate and Test Simulation Environment
In this step the execution is planned. The federates are also integrated and tested.

Execute Simulation
This step includes execution of the federation as well as preparation of the outputs.

Analyze Data and Evaluate Results
In this step the simulation output data is analysed and evaluated. In practice this may mean providing feedback to staff that were trained or reducing data in analysis simulations to a limited number of diagrams and measurements. Data storage and reuse is also considered.

3 A Holistic Approach

The major security risk addressed by MSG-080 is unintended disclosure or leakage of information in collective mission simulation. In the training case and even more so in the mission rehearsal case, this could relate to the planned mission, the performance or capability of systems (sensor, weapon, etc) or the location of facilities. The leakage of task force composition, tactics and doctrines are other types of sensitive information.

In some cases of hostile code intrusion or information obscuration there may be a risk of negative training, if inappropriate or misleading information is provided. Hostile overload attacks (“Denial of Service”) may result in lost access to training facilities or analysis capabilities.

On the analysis side a simulation system that has been manipulated may provide misleading or corrupt tactical and strategic analyses, possibly leading to suboptimal or even harmful decisions.

In order to address the issue of Information Security in Collective Mission Simulation (CMS) and work on solutions, we need to understand what the problem space is and what makes ‘Security in CMS’ different when compared to other information security questions that have been around since the 1970s and that have not been solved for the general case.

The CMS requirements and security issues have been identified and discussed during the MSG-080 workshops and resulted in the following two questions and categorizations:

1. What differentiates information security in CMS from information security in other domains (e.g. office automation)
2. What is the impact of meeting security goals on the training goals that are to be addressed by CMS.

The next sections first describe some of the differences between information exchange needs using CMS compared to those in real world operations and exercises. Secondly they describe some of the differences between security needs in CMS and other domains. Finally, we discuss how CMS may be affected by security measures. The implications of this when using the DSEEP process are then examined by mapping a live use case to DSEEP.

3.1 Differences between CMS and Live Training

CMS has several distinct characteristics in comparison to Live Mission Training. These characteristics have an impact on the security issues which are present within CMS.

- Information value

  One of the main differences between CMS and other domains is that in distributed simulations the receivers need to use ‘exact’ or ‘ground truth’ information in order to function efficiently. Since simulators are often equipped with operational software and highly accurate models all their output is ‘ground truth’. The term *ground truth* information is used to describe exact information concerning the simulated objects; e.g. the exact impact of weapons or the exact positions of simulated objects in time. 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 classified system performance from ‘ground truth’ data and from combining ‘ground truth’ and ‘perceived truth’ data. When we compare this to the ‘real-world’ situation the information which can be gained there is only ‘perceived’ truth, and depends on the participant’s ability to perceive events and on the accuracy with which those events can be perceived.

- Visibility / Radius

  In addition to being able to receive the exact value of a piece of information, the exposure radius of that information is larger in CMS. Ground truth data includes detailed interactions of sensors and weapon systems and is potentially visible to all participating entities in the CMS. In the ‘real-world’ and in live exercises this is not the case; unless coalition forces operate in the immediate vicinity of each other, it will be impossible to collect detailed information. E.g. the only ‘visible’ data for outsiders is the outcome of an engagement.

- Sample size

  CMS offers the possibility to execute the same operation(s) over and over again. This may be under identical or slightly different circumstances (e.g. weather conditions). This allows for analysis of ‘big sample size’ and thus deduction of information that is otherwise hard to obtain.

3.2 Security differences between CMS and other domains

CMS are interactive simulations with a ‘man-in-the-loop’ in which information exchange with low latency is essential. When we compare CMS to other domains in which information security plays an important role, e.g. an office environment, we can identity several specific characteristics of CMS which are of less interest in these other domains.

- Dependency on machine interpretable information exchange

  The (manned) simulators that compose a CMS system need to exchange digital information in order to operate. Their behavior and actions are directly dependent on *machine interpretable information exchange*. A lack of information exchange has a direct impact on the execution of the CMS. In office environments this effect is less strong and direct. Verbal exchange or printed data may be used as alternatives. General background knowledge of recipients may fill in the 'gaps'.

- Time critical

In addition to the high dependancy on information exchange in CMS, the information exchange itself is also highly time critical. When the latency becomes too high it will have an impact on the operator experience in the CMS. In office environments where personnel send and receive digital information this effect is less strong and direct.

- Coarse-grained information exchange

Current technology used within CMS is based on publish and subscribe mechanisms which lack fine-grained distribution mechanisms w.r.t. the intended recipients. This means that published information is publicly available to all participants within the CMS. In office environments we are used to more fine-grained information exchange where the sender can select a group of recipients and where in addition the information itself can be protected (through encryption) against unauthorized disclosure.

- More information types

CMS explicitly exchange information about things that are implicit in the live world. Effects, terrain and detailed technical status of platforms and weapons are some examples. Security policies that are sufficient for the live situation may need to be extended when applied to a corresponding CMS system in order to limit the visibility of such information.

- Many systems and people are simulated

In operations and in live exercises security rules apply to real people and real systems. In CMS many of the systems and people may not exist for real, not even as individual network nodes. Instead they exist as simulated entities in a scenario executed by software. This may fundamentally change how security principles are applied. Still, since the purpose of CMS is to replicate operational situations, it is crucial that the policies applied in the CMS are identical to the operational policies. Otherwise there is a risk of negative training.

- Multiple entities in the same simulation

In CMS it is common to simulate a large number of entities in one simulation. When information is released to entities in an operational situation, the corresponding action in CMS may introduce challenges. If one simulation contains simulated entities that, from a scenario perspective, are cleared for different security levels, the release policy becomes unclear. One solution for this is to only allow entities cleared for the same highest security level within the same simulator. This is actually a mix of a security problem and a challenge in creating a valid simulation. This also means that a simulation may need to be validated with the appropriate security policy in place.

3.3 Impact of Security on CMS

Security solutions and processes will inevitably have an impact on CMS applications. The issues identified are described in this section. Typical security mechanisms include:

- Filtering on information level (what do you want to share and what should not be shared in pure form)
- Filtering on communication level (what do you want to share with whom)

These security approaches need to be controlled in order to minimize the impact on the execution of CMS. Obviously, solutions will often have impact on different levels. The main concerns are:

Impact on training value (realism)

Security approaches often work by limiting the information that can be seen and produced from some or all trainees. It is important to verify that the training is still both valuable and valid with these limitations. Another challenge is to perform (plenary) debriefing using systems with different classification levels. In this case it is also necessary to prevent leakage of classified information.

The need to exchange classified data can be minimised to some extent by designing the training and the scenario in a certain way. However, in some cases the classified data is essential for providing trainingvalue. An important consideration here is whether the data is sufficiently important to the objectives of the exercise to warrant the measures that need to be put in place to obtain accreditation. The impact of those measures on factors such as latency, bandwidth etc must also be taken into account. The requirements for designing and developing simulation models can also be affected by security concerns. Simulation models may have to become more easily tailored to address different classification levels. For example parameters and settings should be configurable. This can however have an impact on the credibility of the simulation if the new parameters are less realistic. It could also be possible to alter information before sharing with other simulators, making it seem to operators that the systems behave in unexpected ways and thus it can compromise the credibility of the exercise. E.g. the entity ID and visual model of the F-117 (Stealth) may be changed into that of an F-16. However, the F-16 will then show a strange behaviour in the eyes of an observer by flying slower and at low altitudes near air-defence installations.

The ability to share information between simulations has consequences for the CMS goals. Some participants may even have training goals which need to be debriefed, but which may not be disclosed to other participants.

If there are training goals specific to one party, these may be compromised when information is required for the correct operation of the CMS. This could mean that CMS training cannot always have the same training goals as real exercises.

Timing

Performance is another issue where it is necessary to verify that the introduction of security solutions does not have an adverse effect on the training goals. Security solutions often impose latency and reduce available bandwidth. Interactive simulations that have man-in-the-loop operators need low latency and high bandwidth data exchange. This may add performance requirements to interoperability middleware.

Possibility for accreditation

Modern simulators often run ‘operational software’ as part of the simulator. This development is the result of the desire to keep simulators up-to-date with the actual platforms (e.g. F16 flight management software) and at the same time reduce maintenance costs for the simulator. This software is usually highly classified. Modifications to this software to address classification and CMS concerns are difficult or impossible. A second consequence is that after updating the operational software package a re-accreditation may be needed. That process can take 18 months, whereas flight-management software updates may have cycle times of 6 months. Security requirements impact the simulation federation development process e.g. when using DSEEP. This may also mean that security accreditation has to be partially repeated when the same simulation is re-used with different players and or different scenarios.

Feasibility of the solution

The feasibility of a solution may be limited by the fact that the user does not have the possibility to modify the simulator due to closed vendor software or hardware.

Simulation infrastructures are often reused in differently classified exercises to reduce costs. In many cases, data may not cross the border between two different exercises. Alternatively, there may be the need to run an exercise and a during action review (DAR) session in parallel on the same infrastructure, with the DAR having a different classification.

Cost and Resources for implementation

Adaptations and modifications required to address security concerns need to be minimised to reduce costs in time and resources. Overly complex configurations and accreditation efforts will limit the usability of CMS and fail to meet the need for effective training.

4 Use case: UK Integration into JTEN

4.1 Use case Description

As part of a task to gain a better understanding of the potential utility of using the US Joint Training and Experimentation Network (JTEN) to link a simulation based in the US to one based in the UK a series of trials – known as the ‘JTEN’ trials – took place in 2008.

The first of the series used the JTEN network to link JFCOM in the US to Westdown Camp in the UK allowing UK and US participants to communicate over a JTEN remote node.

The aim of the trial was to allow a ‘live’ Forward Air Controller (FAC), out on the range at Westdown Camp, to direct a pilot in the US flying a simulated aircraft and for the resulting ground truth effects of any munitions dropped by that aircraft to be made visible – via Synthetic Wrap[1] - to the FAC on the ground using an AR monocular to view the effects.

A live exercise on Salisbury Plain (at Restricted) ran concurrently with JTEN Trial 1. The AWES[2] system generated a feed from the exercise on Salisbury Plain into a Synthetic Wrap, allowing the simulated entities on both sides of the Atlantic to interact with the live entities on Salisbury Plain.

JSAF was used as the simulation in both countries and data was exchanged over the JTEN network by the transmission of DIS PDUs. The US simulation and the simulated part of the UK event ran at Secret, but the live exercise, the AWES system and the FAC had a Protective Marking of Restricted. A data diode permitted data to pass from Restricted to Secret, but no data could be passed down.

As a result of this, the AWES system did not receive detonation PDUs direct from the DIS

[1] a data bridge between the ‘virtual’ simulation network & the ‘live’ tactical engagement simulation (TES)

[2] Area Weapons Effects System, provided by Cubic.

network and the FAC was unable to receive information about weapon effects originating from the Secret US simulation. To handle this, a terminal in the Restricted domain (showing the AWES 'ground truth' & which enabled the operator to manually inject detonation events into the AWES simulation) was located near to an equivalent terminal in the Secret domain. The 'air-gap' between the two systems was managed by a 'man in a swivel chair', who monitored the events in the Secret domain (i.e. location of detonation events) and manually replicated the ground effects through the manual triggering of detonation events within the AWES system, triggering the appropriate interactions (validating the detonation point location through the Secret system, as both (the original detonation point & the manual inject) where visible on the Secret system. Through the interface to AWES the information was sent to an Augmented Reality (AR) monocular to allow the FAC to visualise the detonation event. The FAC was then able to communicate the results of the strike to the pilot in the US simulation.

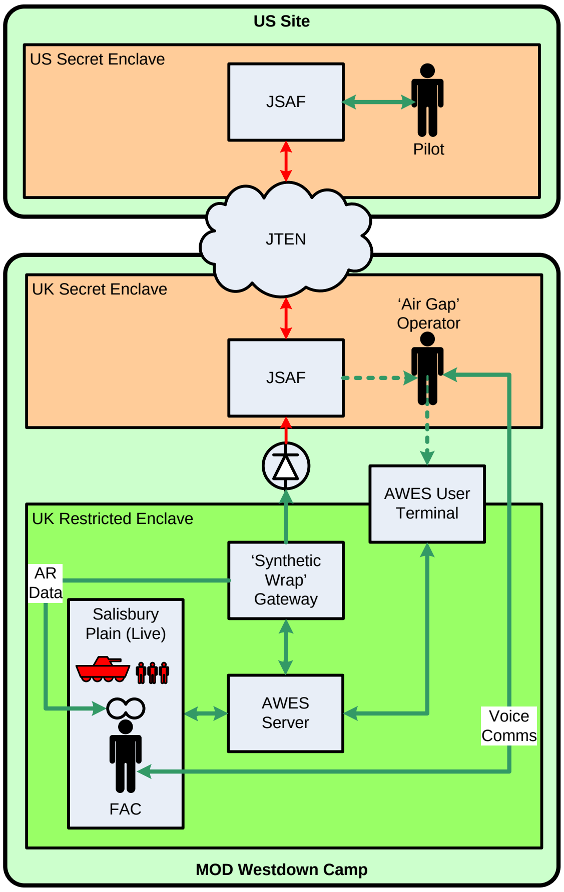

Figure 2 Architecture for JTEN Trial 1

The flow of events was as follows:

- UK FAC guides US pilot to target.
- The US JSAF pilot released a munition.
- UK JSAF in the Secret domain received a DIS PDU from the US JSAF providing information about the detonation, displayed to the 'air gap' operator on the UK JSAF graphical map display. The Live entities on Salisbury Plain, and the FAC were outside the Secret enclave, so did not have visibility of this.
- A Restricted terminal, located adjacent to the Secret enclave, displayed events from within the Restricted domain as they occurred.
- A 'man on a swivel chair' manually replicated the detonations events into AWES: this generated feeds into the Synthetic Wrap and the AR monocular.
  - The SW allowed the AWES system to calculate the outcome of the detonation event on the live players – i.e. whether they were 'killed' or 'damaged' or not effected.
  - The AR monocular allowed the FAC to visualise the outcome of the detonation, which then he could inform the US pilot of the result using his radio.

As part of the After Action Review it was agreed that whilst this was a workable solution it was far from ideal. Inevitably, inaccuracies were introduced, delays were experienced and there was a noticeable delta between the simulations running at Secret, and the entities relying on manual injects.

One example of potential issues experienced relate to the targeting of a live vehicle. The delta between events in a simulation and manually replicated events are likely to mean that by the time a vehicle became aware of a detonation it could have travelled some distance from the point of impact. As it would no longer be at the point of detonation it would not realise it had been destroyed, so would continue to execute its mission. On the other hand, the co-ordinates from the simulation would show that the vehicle was hit – and destroyed – by the munition. This situation was avoided in the JTEN trials by keeping the enemy target vehicle static; obviously an artificiality for the trials which would not be acceptable for real training.

As part of the post-exercise discussions with the accreditors it was agreed that this situation could be improved. The DIS munitions PDU contains descriptors of the location and magnitude of a detonation, but no weapon or performance parameters are passed – neither data on the type of munition nor when it was released. On these grounds, the event accreditors gave a verbal indication that for future exercises of this type the detonation PDU might be transmitted into the Restricted enclave, but this has not yet taken place. It is also possible that a similar arrangement might be allowable for other PDU types provided they do not contain sensitive information but this would be subject to further discussion with the accreditors.

4.2 Use case mapping on DSEEP

The following paragraph demonstrates how this use case might be mapped against DSEEP – the DSEEP steps are given in normal font, the mapping in *italics*:

<u>Step 1: Define Simulation Environment Objectives</u>

- A) Identify user/sponsor needs:
  The standard mentions the need to identify security constraints.
    - *A good understanding of the user and sponsor needs – which are not necessarily the same – is needed to ensure any issues are identified at the earliest possible stage.*

B) Develop objectives

- *<u>JTEN objectives</u>*
    - *Overarching: To gain a better understanding of the potential utility of using the US Joint Training and Experimentation Network (JTEN) to link a simulation based in the US to one based in the UK.*
    - *Detailed: To allow a 'live' Forward Air Controller (FAC), out on the range at Westdown Camp, to direct a pilot in the US flying a simulated aircraft and for the resulting ground truth effects of any munitions dropped by that aircraft to be made visible – via Synthetic Wrap - to the FAC on the ground using an AR monocular to view the effects.*

This section mentions the need to identify:

- Security needs
    - *More than one level of security being used*
    - *Need to ensure no unauthorised release of data*
    - *How data and outputs will need to be stored – short term and long term*
- Potential security risks,
    - *Identify by carrying out a risk assessment*
        - *Multiple nations participating*
        - *Possibility of unauthorised release of data (static and kinetic) to either users or networks*
            - *Data leakage e.g. parameters for weapon or performance data*
        - *By an aggregation of data raising the classification levels*
        - *By deduction from the actions/reactions of participants*
- Probable security level
    - *A combination of Secret (US/UK) and Restricted (UK)*
- Possible designated approval authority (or authorities, if a single individual is not possible)
    - *US and UK accreditation authorities:*
        - *Hardware*
        - *Software and data (e,g, terrain databases and 3D models)*
        - *Networks*
        - *Sites*
        - *People – although the individuals may not be known at this stage*

C) Conduct initial planning

- As a potential outcome DSEEP lists:
    - Security plan
- Sections where security is implicit:
- DSEEP recommends defining a high-level schedule of key development and execution events in section 4.1.3. This may include planning of security

<u>Step1 MSG-080 comments</u>:

- *Get accreditors involved!*
- *Handling of collective simulation between nations: Establish controlled processes and formal agreements (e.g. memorandum of understanding, MOU). These need to cover everything from the design phase to the data protection of after the exercise has finished.*

Step 2: Perform conceptual analysis

- Develop simulation environment requirements
- This section lists the tasks:
- Define security requirements for hardware, network, data, and software.
  - *Networks must be accredited for the intended use*
  - *Software and data must be accredited for the intended use*
  - *Hardware must have passed evaluation to an agreed appropriate level*
  - *Measures are likely to be needed to manage the flow of data*
  - *Need to decide who we will allow to see what*

Step 2 MSG-080 Suggestions:

- *Add – we need an understanding of the impact on the training objectives of the security measures proposed. At this stage it may be necessary to review the training objectives and/or the security measures.*
- *Also need to understand the financial burden of implementing the security measures.*

Step 3: Design Simulation Environment

- DSEEP Section 4.3.4 Prepare detailed plan:
- The following activity is suggested:
  - Define security plan identifying needed simulation environment agreements and plans for securing these agreements.
    - *The live exercise, the AWES system and the FAC could not receive data from the simulations in the Secret enclave due to the use of an approved data diode; all data from the AWES live tracking system and simulation was passed into the Secret enclave*
    - *JTEN used 'man on a swivel chair'/'air gap' (controlled information flow) to transfer pre-agreed information from the Secret enclave to the Restricted enclave.*
- *Potential for latency leading to discrepancies between the participating simulations*
  - *Potential for the introduction of errors by the 'Man-In-The-Loop'*
- The following outcome is also suggested:
  - Security plan

Step 3 MSG-080 Suggestions:

Consider selecting federates that minimizes the impact by the security classification.
Review again the impact on the training objectives of the proposed security measures
Each participant needs to identify the information security issues that are relevant to their assets: which type of information is releasable in what form or way and to which other participant.
Decide in which ways the information will be released or could be released either intentionally (e.g. data exchange during runtime) or unintentionally (voice or data exchange during execution or debriefing).

Step 4: Develop Simulation

DSEEP Section 4.4.2 - Establish simulation environment agreements – mentions:

• Agreements on … and security procedures are all desirable to facilitate proper operation of the simulation environment.
• Additionally, simulation environments requiring the processing of classified data will generally require the establishment of a security agreement between the appropriate security authorities.

It also lists the tasks:

• Review security agreements, and establish security procedures.
• Perform required system administration functions (establish user accounts, establish procedures for file backups, etc.).

Step 4 MSG-080 Suggestions:

Design the simulation to maximise the training value that can be obtained within the security constraints. In the case of JTEN an example of this was a decision for the enemy target vehicle to remain static in an attempt to mitigate the *discrepancies caused by the different classification levels of the simulations.*

Check the security measures will not have any hitherto unforeseen impact on the training objectives.

DSEEP lists the outcome

- Established security procedures

Section 4.4.4 Implement simulation environment infrastructure mentions

- Confirm that the infrastructure adheres to the security plan.

Step 5: Integrate and Test Sim. Environment

This section mentions accreditation, probably related to VV&A rather than security.

Carry out a final check on the impact of the security measures on the training objectives.

Check that compliance with the security requirements has not invalidated the V&V of the event – will the training goals still be met? Is it a realistic environment?

Step 6: Execute simulation

Section 4.6.1 Execute simulation mentions

- "When security restrictions apply, strict attention must be given to maintaining the security posture of the simulation environment during execution. A clear concept of operations, properly applied security measures, and strict configuration management will all facilitate this process. It is important to remember that authorization to operate is usually granted for a specific configuration of member applications. Any change to the member applications or composition of the simulation environment will certainly require a security review and may require some or all of the security certification tests to be redone."

The following task is mentioned:

- Confirm secure operation in accordance with certification and accreditation decisions and requirements.

Step 7: Analyze Data and Evaluate Results

Manage the risk for information leakage during AAR for example the risk that comments by participants or instructors on the exercise events lead to unwanted information disclosure.

Handle security considerations w.r.t. logged data that is not releasable.

Handle security considerations w.r.t. archiving of relevant engineering and exercise data for possible future use or re-use.

Review impact of security measures on

a) The security requirements – were they maintained?

b) The success of the training objectives – how well were they achieved?

Possible changes identified for future events:

In JTEN the DIS munitions PDU contains descriptors of the location and magnitude of a detonation, but no weapon or performance parameters are passed – neither data on the type of munition nor when it was released. On these grounds, the event accreditors gave a verbal indication that for future exercises of this type the detonation PDU might be transmitted into the Restricted enclave.

Other comments:

There appears to be no mention made regarding the archiving of information. We have added this to step 1 as if this is going to cause major issues, early identification of them is essential.

5 Selection of Security Measures

A distributed simulation event, with different security levels, may require many types of security measures. These may be both technical and organizational. This section focuses on technical security measures and the process of selecting and deploying them. The description is based on the DSEEP process. Typical technical security measures that are common today are cross-domain gateways [Ref 4, 5] and data diodes. Note that the "system high" approach is not a main focus here, since it actually eliminates different security levels.

Step 1 Define federation objectives

In this step it is necessary to understand the need for different organizations with different requirements to train together. It is usually possible to get an overview of the degree that different security levels need to be handled already at this stage. This is usually based on the purpose of the training, the training facilities that will need to interoperate, the use of classified data and the tasks that are simulated. Limitations in time and funding will usually also affect the degree to which multiple security levels can be handled. It is strongly recommended to try to resolve as many conflicts as possible at this early stage. Can selecting other training facilities or models decrease the difference in classification levels? Is there time enough to get the required accreditations, given the expected setup? Will the technical and organizational security measures fit within the budget? Will a "system-high" or other reclassification approaches be a cheaper approach in the short run? All of the above needs to be documented in a preliminary security plan.

Step 2 Perform conceptual analysis

In this step it is necessary to understand to what degree simulations of entities and processes, that may have a classification, need to be used to meet the requirements of the scenario. What is the expected classification level of the scenario (for example in mission rehearsal), terrain data, models of platforms, sensors and weapons? To what degree is the fidelity of models allowed to vary, which may give room for replacement of models with different classification levels? A tentative selection of security measures may be made at this stage. Some, but not all security requirements on hardware, software and networks may be specified at this stage.

Step 3 Design federation

In this step it is necessary to understand what systems and facilities that are selected. Understand the deployment plan. In this step the architecture is planned. In most cases the simulation needs to be partitioned based upon the different security levels handled. It is now time to make a decision on the technical security measures and to prepare and submit a security plan for approval by accreditors. It is also necessary to create detailed requirements for the technical security measures. This includes both security aspects as well as technical aspects like performance and reliability. If the fidelity and classification level for some simulations is allowed to vary, as analyzed in step 2, some simulations may be replaced. Some technical security measures may only be approved for certain classification levels.

The proposed design needs to be analyzed with the training goals in mind. This will be a key decision point since it may call for a need to iterate through step 1 and 2 again.

Step 4 Develop federation

At this stage the federation is developed. Policies for information gateways as well as other technical components need to be developed and adapted. Security equipment needs to be configured and other preparations for deployment needs to be done. Accreditors will be involved regarding the permitted type of crypto, gateways and other equipment.

Step 5 Integrate and test

The technical security measures now need to be integrated in the target environment. Test and verification needs to be done in two respects. Do the security measures provide the required security? Do they work correctly and perform well enough for effective simulation? Accreditors will be involved regarding verification of equipment and rulesets.

Step 6 Execute simulation

During the execution the security of the simulation must be monitored and managed in an effective way. Any deviations from the planned security measures must be handled and the effect analyzed.

Step 7 Analyze data and evaluate result

When the execution is over there is still security questions that needs to be handled. The output from the simulation needs to be handled with the different security classifications in mind. The simulation equipment may also contain sensitive data that must be taken care of.

6 Discussion

Security measures must always be related to risks and threats and usually also to the benefits of a training event. Getting security accreditations and introducing the required measures will always take time, costs and introduce more complexity. For some urgent missions this may be unacceptable, given the military threat or risk of losing strategic advantages. In this case high command levels may choose to reclassify the entire training event to become unclassified, or to mandate special security measures.

It makes no sense to protect data that is widely known: the colour of a vehicle or its dimensions may be easily available to anyone that can use the Internet. The exact position of an aircraft may need protection during a critical part of a mission, but it can be shared with all participants and at high accuracy when the aircraft is parked on the runway.

Better approaches and methodology are needed to define and identify risk (Risk Management).

Defining, verifying and maintaining proper security policies, in particular for guards, may not be trivial for many of the above solutions.

When most of the previously mentioned security approaches are introduced in CMS this will limit the information that can be seen and produced from some or all trainees. It is important to verify that the training is still both valuable and valid with these limitations.

Performance is another issue where it is necessary to verify that the introduction of security solutions don’t have an adverse effect on the training goals.

Another challenge is to perform debriefing using systems with different classification levels. In this case it is necessary to prevent leakage of classified information. Some participants may even have training goals, that need to be debriefed, that may not be disclosed to other participants.

In some cases there may be a requirement to obscure data, for example by replacing one aircraft type with another (static obscuration) or by altering the acceleration of a vehicle (dynamic obscuration). Whilst it is possible to sanitize data for transmission from a 'high classification' simulation to one of lower classification, this does entail the risk of negative training.

For technical reasons there may also be a requirement to provide "dummy" values for data that has been removed, in order to prevent simulators that require these from crashing. If, for example, the nationality attribute of an aircraft is filtered out by a guard it may useful to automatically insert a value representing "unknown" instead of transferring no data at all.

A related approach is to use multi-resolution modeling and only provide aggregated information or information for selected entities to some participants. In addition to the above obscuration of digital information it may also be necessary, during an exercise, to restrict the information exchange carried out through other channels, like voice communication.

7 Conclusion

This paper has provided some insight on how security can be applied throughout DSEEP, including some lessons learned and common challenges. Some notable observations are:

Security in CMS is not a new challenge, but with increasing amounts of joint collective training being carried out its profile has been raised significantly in recent years. However it is not realistic to expect a 'one size fits all' security solution in the near future. This study has looked at a number of steps that could be taken to improve the situation in the short term. Security, in CMS and elsewhere, can only be addressed by a mix of organisational, procedural and technical measures. A balance, between these measures, needs to be achieved for acceptable training value and manageable security concerns.

MSG-080 has been working on improving the conceptual model of how to classify and structure security related issues in M&S. This is a starting point for evaluating technical solutions. The conceptual model is also a possible starting point for integrating security issues in the development process and may lead to a DSEEP 'overlay' regarding security aspects.

Risk Management, instead of risk avoidance or risk acceptance, must be implemented in the M&S security lifecycle.

The need for acceptance of new risk management based security measures, from accreditation offices and officers, may be a particular challenge. This needs to be addressed by involving accreditation specialists early on in the future experimentation activities of MSG-080.

We hope that this is useful in the continued efforts of the SISO Security in Simulation study group as well as for individuals and organisations active in the SISO community.

References

[1] B. Möller, et al, *Towards Multi-Level Security for NATO Collective Mission Training – a White Paper*, 11S-SIW-069, 2011

[2] B. Möller, et. al, Security in NATO Collective Mission Training - Problem Analysis and Solutions, 12S-SIW-032, 2012

[3] IEEE: "IEEE 1516, High Level Architecture (HLA)", www.ieee.org, August 2010.

[4] C. Verkoelen, et all, *Security within Collective Mission Simulation Architectures*, 09S-SIW-035, 2010

[5] B.J. te Paske, et all, *Information Labelling – Cross-Domain Solutions*, Intercom Vereniging Officieren Verbindingsdienst, 38th volume, nr. 2, June 2009

Acknowledgements

The authors would like to acknowledge the contributions of the other members of the MSG-080 Taskgroup to the ideas and results presented in this paper.

Author Biographies

BJÖRN MÖLLER is the vice president and co-founder of Pitch Technologies, the leading supplier of tools for HLA Evolved, 1516-2000 and HLA 1.3. He leads the strategic development of Pitch HLA products. He serves on several HLA standards and working groups and has a wide international contact network in simulation interoperability. He has twenty years of experience in high-tech R&D companies, with an international profile in areas such as modelling and simulation, artificial intelligence and Web-based collaboration. He is currently serving as the vice chairman of the SISO HLA Evolved Product Support Group.

STELLA CROOM-JOHNSON is a Principal Analyst in the Analysis, Experimentation and Simulation Group in the UK Defence Science and Technology Laboratory (Dstl). Before she joined Dstl in 2003 she worked as a computer scientist outside the defence industry. Since then she has worked on a variety of projects (including managing the DIAMOND Peace Support simulation model) and is the technical lead on a project looking at options for achieving a persistent Multi Level Security solution across standards and domains.

WIM HUISKAMP is Chief Scientist Modelling, Simulation and Gaming in the M&S department at TNO Defence, Security and Safety in the Netherlands. Wim leads TNO's research programme on Live, Virtual and Constructive Simulation, which is carried out on behalf of the Dutch MOD. Wim is a member of the NATO Modelling and Simulation Group (NMSG) and acted as member and chairman in several NMSG Technical Working groups. He is co-chair of MSG-080, Chairman of the NMSG M&S Standards Subgroup (MS3) and he is the liaison of the NMSG to the Simulation Interoperability Standards Organization SISO.