Security in Simulation – A Step in the Right Direction

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

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

Keywords:
Security in simulation, simulation, training, NATO, security, requirements, DSEEP, information exchange, multi-level security, cross-domain solutions, accreditation

ABSTRACT: *A number of approaches are currently in use to allow limited sharing of data between simulations running at different native classification levels, but each have their associated issues which prevent full interoperability. This presents users and accreditors alike with a unique set of challenges. Building on the work presented to recent SIWs by NATO MSG 080 (Security in Collective Mission Simulation) the Security in Simulation Standing Study Group has been considering the role standards might play in making progress towards a Cross Domain Solution.*

This presentation summarises the work of the SSG showing how it has built on past papers and the work of NATO MSG-080 to identify where standards might contribute to – if not a full Cross Domain Solution – at least to making progress in this area.

The SSG members propose to draw on national use cases to create a set of guidelines for best practice, to create a taxonomy of terms commonly in use and to create a Security overlay for DSEEP. The paper will examine some of the use cases to consider how they might be applied across the various approaches, where they highlight common challenges and what this might mean for the proposed product nomination.

SISO cannot expect to influence the policies and processes of individual nations, but engagement with their accreditors is an important factor and it is hoped this paper will provide sufficient material to stimulate engagement and obtain their buy-in.

1. Introduction

In Joint Collective Training there is an increasing need to achieve simultaneous, multi-way interoperability between simulations operating at different native classification levels.

Interoperability standards (DIS, HLA, TENA, etc.) are already in place to connect the simulations based on 'ground truth' exchange of all relevant data, but to create an accurate representation of operational issues there is also a need to share certain information in accordance with the classification levels that are in place to protect that data.

A significant and growing percentage of training in the foreseeable future will be with coalition partners: this means that participating simulations need to be connected across not only domain boundaries, but also across national boundaries. To enable this, internationally agreed standards are needed to support a flexible and adaptable security architecture, which ensures that the appropriate interactions take place between the participating simulations without violating security classifications.

The problem space is now reasonably well understood, and the next step is to consider how to take things further using a combination of existing and novel processes and technologies.

2. Background

This is not a new challenge and as long ago as 1997 a paper to the SISO Fall SIW [1] mentioned the issues arising from the need to exchange data between systems operating at different security levels. In more recent years the topic was revisited in a presentation to the 2009 Spring SIW [2] which looked at the limitations arising from the conflict between the need to share data and the need to protect that same data, and outlined the concept of a labelling and release mechanism that could be applied to prevent leakage of sensitive information.

.

This paper takes a brief look at three subsequent papers [3] [4] [5] presented by members of NATO Modelling and Simulation Group MSG-080 to SISO in recent SIWs and shows how the SISO Security in Simulation Standing Study Group (SiS SG) has built on these to determine the role standards could play in making progress towards a Cross Domain Solution.

The MSG-080 papers (from which Figures 1-5 are reproduced) looked at a number of scenarios and use cases with typical solutions. Five possible approaches were outlined, four of which are in current use: the other is a vision of how a true Cross Domain solution might operate. These are covered in some detail in the papers so the summary given below is intentionally very brief.

2.1 System High

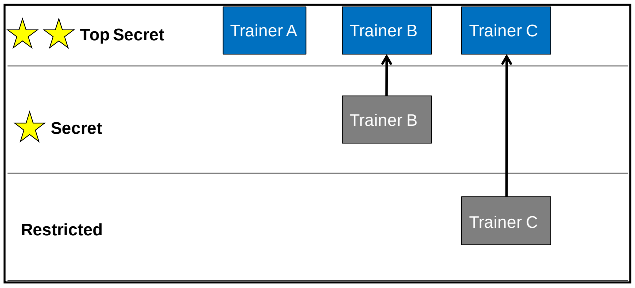

Figure 1: All systems and participants reclassified to highest level

Everything – including data and (potentially) facilities is reclassified to the highest level. This effectively means that each participant agrees to expose all data that is exchanged with all other participants. This may result in unacceptable risk for some participants leading to withdrawal from the exercise or significant rework to ‘dumb-down’ a classified simulation with possible loss of training value.

2.2 Multiple Single Levels of Security

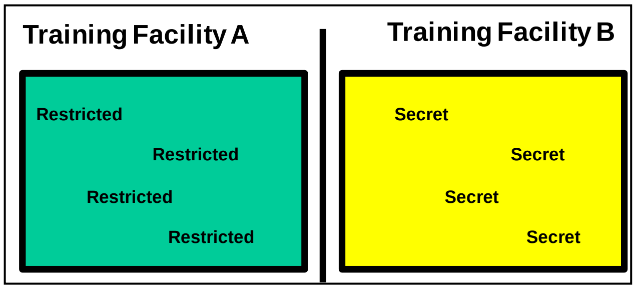

Figure 2: Physically separate domains

The security domains are physically separate, although limited data exchange can be achieved via manual intervention. Interactive response time will be limited and the burden of guarding against information leaks will fall on a human operator.

2.3 Multiple Independent Levels of Security

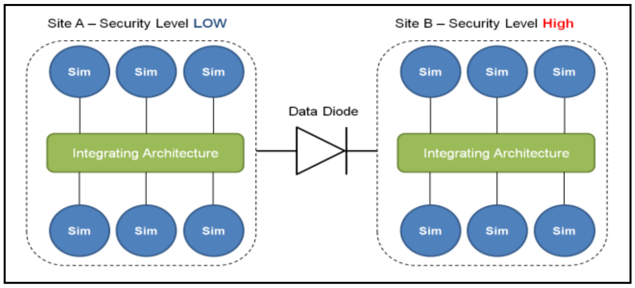

Figure 3: One way flow using a data diode

A data diode permits a unidirectional data flow from (in this case) Low to High, but there are no true two-way interactions between the domains. This may severely limit the training value. The approach is also rather blunt: there is no inspection or decision at the information level. All data is either passed or blocked based on source and destination.

2.4 Information Exchange Gateway

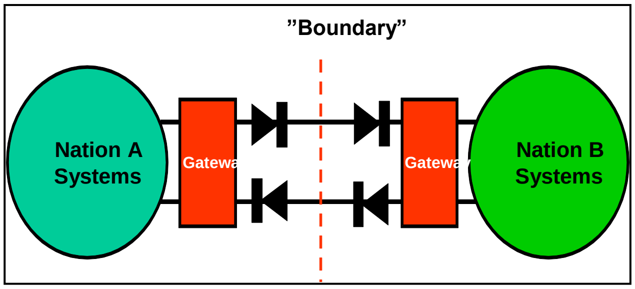

Figure 4: Limited 2-way data exchange across security boundaries

This is useful when multiple security authorities are involved who do not necessarily trust each other. Data is sanitized by using a combination of devices such as Data Guards and Data Diodes. This achieves a limited form of two-way interaction between simulations, but has the disadvantage that data discrepancies arise from the use of accurate data in some federates and sanitized data in others.

2.5 Trusted System (vision)

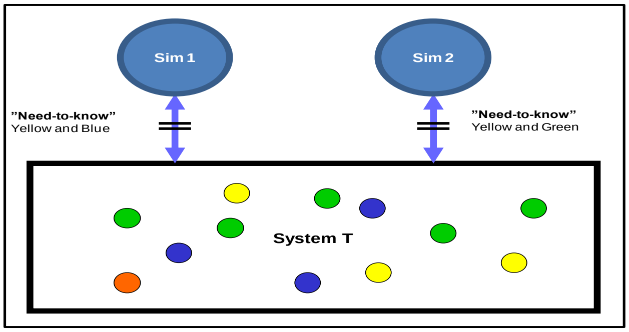

Figure 5: Data released on 'need-to-know' basis

In this approach data from systems of different classifications would be permitted to mix freely, using devices such as Data Diodes and Data Guards to release data to participants on a ‘need-to-know’ basis.

2.6 Context

A number of use cases around typical scenarios and solutions and early experiments were identified and analysed to show where issues might arise on the exchange of data within a simulation, where the sensitivities lie, and how this highlighted the main concerns, issues and threats.

Each of the approaches has their own strengths and weaknesses, but no formal guidelines exist to indicate under which circumstances one approach might work better than another.

The MSG-080 papers also identify where security for Collective Mission Simulations differs from that for other domains and concluded that the main areas are:

- Federates exchange accurate data (ground truth), which means it can – potentially – be accessed by all participants. In the real world the data released to a given individual depends on what can be directly observed, or is specifically released to that individual.
- In simulation a given scenario can be replayed, giving rise to a larger sample size than would be available in real life, with the opportunity to examine the simulation ‘ground truth’ data in slower time.
- Simulations require truly interactive, low latency levels of data exchange.
- The need to meet the goals of the simulation (e.g. effective training) may cause conflict with the security goals.

The papers concluded that a holistic approach is necessary, with a focus on risk management rather than risk avoidance or risk acceptance and with an overarching need to obtain early engagement from the accreditation communities involved in any given event.

A number of isolated strands of work are ongoing in various organizations/nations and the importance of ensuring coherency both between proposed solutions as the problem space evolves and with existing simulation standards forms part of the objectives of the Security in Simulation SSG.

3. SISO and Security in Simulation

The approaches outlined earlier are already well understood by both the simulation and accreditation communities, but they do highlight a number of issues:

- Each use case is very different from the next one: what constitutes an acceptable solution will vary from case to case and there is no ‘one size fits all’ solution.
- Local Subject Matter Experts (SMEs) often understand what works well in their own context, but this may not be transferrable to a distributed federation involving disparate players. Although individual organisations might have something written down this is not always the case at national or international levels.
- Any implementation will depend on what an accreditor is willing to approve – and each nation’s accreditors have different perspectives.

The current process is designed to ensure compliance with national accreditation requirements. Whilst this manages the security issues (e.g. avoidance of data leakage) the implementation of it can create simulation related issues (e.g. how to achieve meaningful data exchange between simulations). The SiS SSG concluded that whilst new/amended standards would be of limited utility in this context other SISO products do have the potential to yield significant benefit during the development of a simulation, and to facilitate engagement with the accreditation community. The recommendations were:

a) The creation of a security overlay to DSEEP to help users consider the implications of security in simulation at each of the 7 DSEEP stages. This would highlight what is important to a given simulation and show where the challenges are likely to arise.

b) The creation of a ‘Best Practice’ Guide to provide a baseline from which to work when setting up a simulation: what has worked in the past, and – perhaps as importantly – pitfalls to avoid.

c) To create an agreed, common glossary for Security in Simulation to ensure all participants have a common understanding of the terms used. To ensure coherence with existing glossaries and ontologies these would be used as a starting point.

4. Two use cases: (JTEN and MTMD)

4.1 UK – mapping JTEN to DSEEP

4.1.1 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.

In order to provide a useful training environment the trials 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 node on the JTEN network.

The aim of the first trial was to allow a 'live' Forward Air Controller (FAC) on the range at Westdown Camp to direct a pilot in the US flying a simulated aircraft in a Close Air Support (CAS) role and for the resulting ground truth effects of any munitions dropped by that aircraft to be made visible – via Synthetic Wrap[1] (SW) - to the FAC on the ground using an Augmented Reality (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 a 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 the other way.

As a result of this, the AWES system did not receive detonation PDUs direct from the DIS network and the FAC was unable to receive information automatically 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 an air gap operator (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) were visible on the Secret system. Through the interface to AWES the information was sent to an 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.

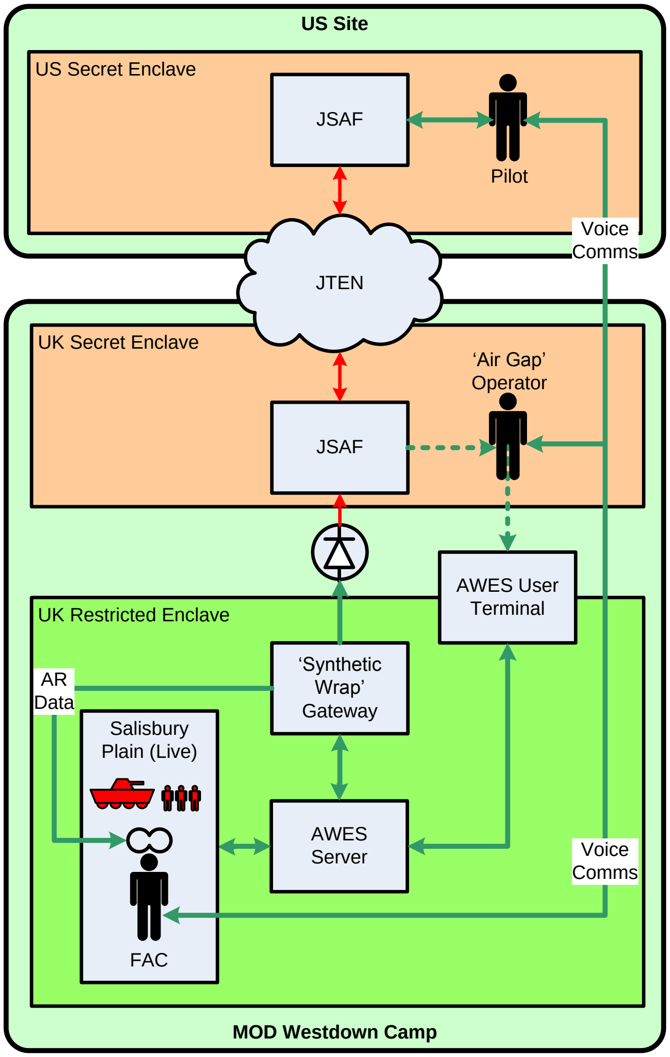

Figure 6: Architecture for JTEN Trial 1

[1] a data bridge between the 'virtual' simulation network & the 'live' tactical engagement simulation (TES)
[2] Area Weapons Effects System, provided by Cubic.

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.
- The air gap operator manually replicated the detonation events into AWES: this generated feeds into the SW 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 affected.
    - The AR monocular allowed the FAC to visualise the outcome of the detonation, which meant 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 were noticeable discrepancies 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.

An alternative approach might have been to permit the vehicle to move and for the air gap operator to be responsible for keeping the domains in step. He would have been aware that the vehicle was shown as disabled in the Secret enclave, but not in the Restricted enclave. Manual intervention in the Restricted enclave would have then brought the two representations back into line with each other.

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.

4.1.2 Use case mapping on DSEEP

The following paragraphs demonstrate 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>

- 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.*
- 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 and constraints
    - *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*
    - *Risk of data leakage e.g. parameters for weapon or performance data*
    - *An aggregation of data may raise the classification levels*
    - *Deduction from the actions/reactions of participants may reveal classified information*
- Probable security level
  - *A combination of Secret (US), Secret (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*
- 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>Step 1 MSG-080 Suggestions</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.*

<u>Step 2: Perform conceptual analysis</u>

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 will be allowed to see what

<u>Step 2 MSG-080 Suggestions:</u>

- *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.*

<u>Step 3: Design Simulation Environment</u>

DSEEP Section 4.3.4 – Prepare detailed plan – suggests the following activity:

- 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 an air gap operator (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

<u>Step 3 MSG-080 Suggestions:</u>

- *Consider selecting federates in a way that minimizes the impact of 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(s).*
- *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.).

<u>Step 4 MSG-080 Suggestions:</u>

- *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
- DSEEP 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 Verification, Validation and Accreditation (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

DSEEP 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 After Action Review for example the risk that comments by participants or instructors on the exercise events lead to unwanted information disclosure.
- Handle security considerations with regard to 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:*
  - *The security requirements – were they maintained?*
  - *The success of the training objectives – how well were they achieved?*
- *Possible changes identified for future events:*
  - *The DIS detonation PDU (as used in the JTEN trials) 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. This has been added to Step 1 since early identification of any major issues arising is essential.

4.2 NLD – mapping MTMD (Maritime Theatre Missile Defence) to DSEEP

4.2.1 Use case Description

The Maritime Theatre Missile Defence (MTMD) Forum consists of nine nations (the United States, Canada, Australia, Germany, The Netherlands, United Kingdom, France, Spain and Italy), with the key focus on improving maritime coalition interoperability and capability in the area of missile defence - for example, improvements in the area of command and control, and tactical data links (TDL). Modelling and Simulation is used for testing, evaluating and assessing the performance of proposed interoperability improvements in an early stage of development. National simulation assets are connected in a (distributed) simulation environment to support this.

4.2.2 Use case mapping on MTMD

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

Step 1: Define Simulation Environment Objectives

- The objective of the simulation environment is to determine (through simulation) the performance of interoperability improvements, by making use of available national simulation models of the maritime platforms in the coalition force. The simulation models need to be representative for the national platforms. This almost automatically leads to the use of classified sensor, effector and TDL models. This need was recognized from the beginning and is reflected in the objectives of the analysis.
- *The required classification level needs to be stated from the beginning. Participants need to start preparations to work at this level (specifically lab accreditation and secure network communication).*

Step 2: Perform conceptual analysis

- *Although the information that is used in this step is partly classified, none of the results are classified. By keeping results unclassified the project team was able to perform their work in an unclassified working environment (e.g. using regular phones, mail exchange and collaboration sites). MOEs and MOPs are formulated in a generic way, the scenario does not hold any details on the national platforms or threats, and the simulation environment requirements are also stated in a generic way. Where specifics are needed, this is done via an anonymous reference to a classified document.*
- *For distributed teams, try to work in an unclassified environment for as long as possible e.g. stating scenarios and simulation environment requirements in an unclassified way, and only using classified data by anonymous reference.*

Step 3: Design Simulation Environment

This step involves the design and development of the simulation environment based on the requirements from the previous steps.

- *A similar approach is followed as in step 2. By keeping the component configuration separate from the component logic, it is possible the maintain components at a lower classification level. This approach enables the project team to do integration and test in an environment with a lower classification level, using unclassified component configurations. The design of the simulation environment itself is unclassified, by using available (open) standards for connecting simulation models, like RPR-FOM and L16 BOM. All models in the simulation environment are at an equal playing level, i.e. there is no information filtering between models.*

Step 4: Develop Simulation Environment

- Development or modification of components.
- *A similar approach is followed as in step 2. By keeping the component configuration separate from the component logic, it is possible the maintain components at a lower classification level. This approach enables the project team to do integration and test in an environment with a lower classification level, using unclassified component configurations. The design of the simulation environment itself is unclassified, by using available (open) standards for connecting simulation models, like RPR-FOM and L16 BOM. All models in the simulation environment are at an equal playing level, i.e. there is no information filtering between models.*

Step 5: Integrate and Test Sim. Environment

- For this step a process had to be devised to overcome several constraints and limitations such as:
- The federation contains sensitive information and as such classified data.
- The participating partners are located far from each other, in different time zones, making co-ordination of the federation members difficult.
- *All tasks are performed in an unclassified (co-located or VPN) environment, with the purpose to switch to a classified (co-located) environment for the final test event.*
- *With these constraints shown above and past experiences on (classified) network setup and performance, the following decisions were made at that beginning of simulation environment development:*
    - *A test federate shall be used to support local component interface and behaviour testing as much as possible.*
    - *The final simulation environment shall execute at one location to overcome distributed network delays and security issues.*
    - *In order to increase efficiency during co-located integration and test, existing (classified) components shall be modified or re-developed as configurable (unclassified) components.*
- *Another advantage of the introduction of unclassified components is the ability to conduct geographically distributed testing via an unclassified VPN connection between the project members.*

Step 6: Execute Simulation

- *The final test event is performed in a classified environment, where each of the models can be configured with classified data.*

Step 7: Analyze data and evaluate results

- *The data is collected and stored on removable hard disks, for analysis and evaluation in a classified environment.*

5. Way Forward

The JTEN use case shows how a security overlay to DSEEP would assist with the integration of security into the development process. Whilst a complete solution to all the issues is unlikely in the foreseeable future this does not mean no progress can be made. Raising the issue to the user and accreditor communities and providing a framework to adopt would be a step in the right direction.

At the Spring 2013 meeting of the SiS SSG a decision was made to draw up a Product Nomination for the creation of a security overlay to DSEEP, a Best Practice Guide to act as a reference point and for a glossary to ensure a common understanding of the terms used. As well as creating coherence in the development of an exercise, the intent is that these products will serve as a starting point for enterprise level engagement with the accreditation community, with the hope that this will lead to a better understanding of the issues and their impact on both sides.

This is a challenging topic and all SISO members are invited to join the SiS SSG and provide input to the product nomination.

The NATO Modelling and Simulation Group community will continue to support this activity and its members will be able to provide operational and technical experience with this problem. Experiments or exercises undertaken by NMSG task groups may serve as test cases for the proposed security overlay standard.

6. References

[1] J. A. Tufarolo, L. Suprise, M Raker, *International Interoperability for Simulation-based Training,* 97F-SIW-140, 1997

[2] C. A. A. Verkoelen, R. Wymenga, *Multi Level Security within Collective Mission Simulation Architectures,* 09S-SIW-035, 2009

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

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

[5] B. Möller, S. Croom-Johnson, Wim Huiskamp, *Three Perspectives on DSEEP and Security: Training Goals, Use Cases and the Selection of Security Measures*, 13S-SIW-005, 2013

7. Acknowledgements

The authors would like to thank Ian Grieg of UK Defence Science and Technology Laboratory (Dstl) for his advice and review of the document and Tom van den Berg of TNO (NLD) for supplying the MTMD use case.

Author Biographies

STELLA CROOM-JOHNSON is a Principal Analyst in the Analysis, Experimentation and Simulation Group in the UK Defence Science and Technology Laboratory (Dstl). For the past few years she has acted as the technical lead on a UK MoD project looking at options for achieving a persistent Cross Domain Solution across standards and domains and has been a member of NATO Modelling and Simulation Group-080 (Security in Collective Mission Simulation). She is currently chair of the SISO Security in Simulation Standing Study Group.

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 Organisation.

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.