Using HLA Object Models for the Analysis of Cross Domain Security Policies

Björn Möller - Pitch Technologies, Sweden
Stella Croom-Johnson, Dstl, UK
Åsa Falkenjack – Pitch Technologies, Sweden
Kester Hughes – Niteworks, UK

bjorn.moller@pitch.se
scjohnson1@mail.dstl.gov.uk
asa.falkenjack@pitch.se
kester.hughes2@niteworks.net

Keywords:
Simulation, training, security, accreditation, guard, HLA, FOM, SOM

ABSTRACT: *Across defence, training equipment, data and scenarios are likely to have different classification levels. Thus it is sometimes necessary for training to be carried out using a federation of participating systems running at different classification levels, but without compromising security rules. This is usually done using guards and filters to limit the data that may be released from the higher security domain to the lower security domain. In some cases, limiting the data may negatively impact the training and make it impossible to meet all the training goals. When following the process from design to security accreditation it is crucial to understand how to meet security requirements while also understanding the impact this will have on the training.*

This paper suggests an approach based on a description of the data exchange using the object models of the High Level Architecture. One type of object model is the Federation Object Model (FOM). It specifies the type and format of any data exchanged in the federation. This includes descriptions of objects (such as aircraft, soldiers and weapons) and interactions (such as orders, fire and detonation). Another type of object model is the Simulation Object Model (SOM). This is used to describe which objects and interactions are published (produced) and subscribed (consumed) by any one simulation system.

The proposed method uses the SOMs to analyse the data flow within and between the different security domains. It allows the user to suggest different security policies. It then provides an automatic analysis that can be used to analyse the effect from both training and security perspective. This analysis can be performed for standard FOMs, like RPR FOM and NATO NETN FOM as well as extensions of these and project specific FOMs.

The proposed method can be used as a basis for a dialog between accreditors and developers of training federations. This can help to avoid security issues, to understand the impact of training goals and also to detect any technical issues that may be introduced by the presence of a guard.

1. Introduction

In order to provide effective training for military personnel, information exchanges must be effected between simulations running at different levels of protective marking. This generates a need to reconcile the demands of security requirements to protect information with those of the training requirements, which need information to be shared: this is a key constraint in achieving interoperability between these systems.

1.1 Information Leakage in Simulations

There are three main ways in which information leakage from a simulation might occur:

- Inappropriate transmission of data items;
- Information that can be derived from actions taken by entities which unintentionally reveal capabilities at a higher classification level;
- Information that can be derived from an aggregation of individual unclassified data items which, when taken together reveal classified information;

The first of these is the focus of this paper and builds on previous research [1] [2] [3] [4] [5] [6] [7], which compared the advantages and disadvantages of the various approaches and technologies available to prevent the inappropriate transmission of data. These allow the flow of data to be controlled by suppressing or sanitizing data that cannot be transmitted due to its protective marking.

Whilst this meets the security requirements and allows a simulation to be accredited, the process can lead to material differences between simulations in a federation and can have a detrimental effect on the training objectives. Whilst the risks can never be eliminated

completely, there is a need here to balance the risk of leakage of classified information against the risk inherent in failing to provide military personnel with effective training. Revealing classified data could compromise operations but – equally – compromised training might compromise operations.

1.2 Equipment versus process

The first reaction, within a project that needs to approach the cross-domain security problem, may be to try to find a piece of equipment that provides security at some generic level. This is usually an over-simplification of the problem. The project actually needs to work together with accreditors to properly address the problem. A common understanding of security risks needs to be developed. Solutions need to be proposed and assessed. The implications of security solutions for the training goals need to be understood. When filtering out, or obscuring data, technical problems may also occur, since certain data may not be delivered to all federates.

This means that it may be just as important to focus on the process, as the equipment, when developing cross-domain training. Tools that enable developers and accreditors to get an in-depth understanding of the information handled in the training system, and how it may flow across the security domain borders can facilitate this. It is useful to be able to evaluate the impact on security and training.

1.3 The Niteworks task

Niteworks is a partnership between the UK Ministry of Defence (MOD), including the Defence Science & Technology Laboratory (Dstl), and industry. Niteworks aspires to be the definitive partnership to provide decision support to enhance current and future capability in the UK. A Niteworks team, together with Pitch Technologies was funded and tasked by UK MoD Flight Simulation and Synthetic Trainers (FsAST)[1]project team to develop an initial understanding of the risks associated with cross domain training, identify potential technical solutions and determine the accreditation challenges in establishing the capability. Part of this work involved experimentation using content inspection. A key challenge identified by this work was "the complexity of understanding the information flows between the systems in different domains." [4]. Using a set of scenarios drawn up in earlier stages of the task, experimentation was carried out to gain a better understanding of which data items could be suppressed or sanitized without detrimental impact on the event, and which ones were essential to meet the training objectives.

The particular question addressed in this paper is: how can we use the HLA object models to facilitate the design and analysis of cross-domain policies as well as to support collaborative process.

2. HLA Object Models and Security

The High Level Architecture (HLA) [8] is an open international IEEE standard (IEEE1516-2010) for simulation interoperability, i.e. making training systems work together. HLA provides a services bus whereby simulations can exchange information, synchronize and more. A group of connected simulations is called an HLA Federation. Figure 1 shows the components of a federation.

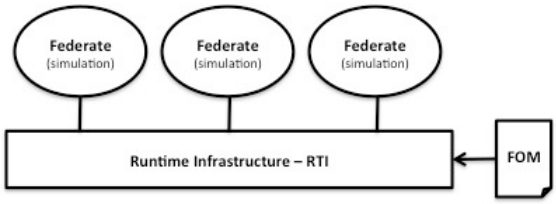

Figure 1: HLA Federation

Each participating system is called a Federate. It connects to the Runtime Infrastructure (RTI) to exchange information and other services. The data exchange format is specified using a Federation Object Model (FOM). The FOM is the language of the federation and is different, for example between a defence training simulation and a railroad simulation. The FOM is stored as an XML file.

The earlier standard for simulation interoperability, Distributed Interactive Simulation (DIS) [9], provides a fixed information model. The exact data to be exchanged are specified in the standard. Since the requirements, equipment, resolution, doctrines and scenarios have developed over time, this lack of flexibility has limited the usefulness of pure standardized DIS, and nearly all DIS simulation systems are typified by non-standard solutions. This greatly inhibits interoperability between different systems.

One of the main advantages of HLA is that it provides the information flexibility required to meet training needs, while still providing well-documented information models using the FOM.

2.1 HLA Object Models: FOM and SOM

The FOM describes the information exchange in detail. It describes object classes, like 'aircraft', that exist over time. Such objects have attributes, such as 'marking', 'type of aircraft', 'nationality' and 'position'. The values of these attributes can be updated over time.

The FOM also describes interactions, which are instantaneous events, like a 'radio message', a 'firing of a weapon' or a 'signal to start' a simulation exercise. An interaction has a number of parameters that describe the interaction in detail.

[1] The FsAST remit is to deliver the right air synthetic training, in the joint environment, to support the front line now and in the future.

The exact data format used, for example to specify the type of aircraft and the positions are described in detail using standardised HLA data types. This makes it possible to inspect and interpret all data that is exchanged down to the bit level.

There is another type of HLA model called the Simulation Object Model (SOM). It describes the information that one particular simulation publishes (sends) and subscribes (receives). A 3D viewer may for example subscribe to all simulated objects (including aircraft) and their positions, whereas a particular flight simulator may both publish its own aircraft attributes and subscribe to attributes of other aircraft.

2.2 HLA federations with High and Low Domains

In order to create a training system with high and low security domains, the federation can be partitioned into two separate federations, as shown in Figure 2.

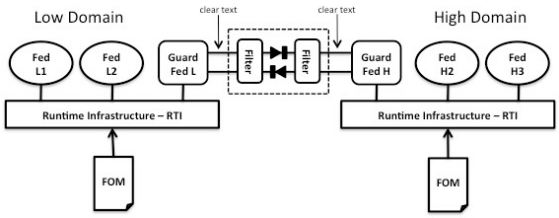

Figure 2: Partitioned Federation

A guard connects the high and low domain and enforces a security policy. The implementation of any specific guard solution is not discussed in this report, but it may consist of software components such as protocol filters and hardware components like data diodes.

3. A Sample Cross-Domain Federation

The sample scenario is as follows:

A Forward Air Controller (FAC) is to provide guidance by voice radio together with laser designation to a strike aircraft, the target being a ship. The FAC and the pilot need to communicate via well-defined procedures. The pilot fires a munition at the ship, which detonates when hitting the target. The entire exercises is started, stopped and monitored from an instructor station.

The following federates are involved:

Aircraft Federate. This is a virtual flight simulator manned by a (trainee) pilot. It publishes information about the aircraft and the munition, including the firing and detonation. The pilot can also communicate by radio with the forward air controller.

FAC Federate. This is a virtual simulator manned by a human (trainee) forward air controller. It publishes information about the forward air controller and the laser guided designation that he provides. The forward air controller communicates with the pilot by radio.

Ship Federate. This is a small constructive simulator that provides a target to the exercise. It publishes information about the ship. It also receives detonation information to properly represent damage when the ship is hit.

IOS Federate. The 'Instructor Operator Station' provides monitoring and visualization of the entire demonstration. It also controls the start and stop of the scenario.

The aircraft federate has a High security classification. The FAC federate and Ship federate have Low security classifications. In order for the instructor to be able to monitor the entire exercise, including detailed information about the aircraft, the IOS federate is placed on the High side. Figure 3 illustrates the federation:

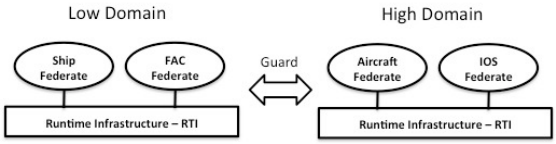

Figure 3: The Sample Federation

In this case the SISO Real-time Platform Reference FOM (RPR FOM) [10] is used. The "Publish/Subscribe" table in Figure 4 shows the SOMs of the federates, i.e. what they publish (P) and subscribe (S) from the RPR FOM.

	Ship Federate	FAC Federate	Aircraft Federate	IOS Federate
Aircraft		S	P	S
Surface vessel	P	S	S	S
Forward air controller		P		S
Designator		P	S	S
Munition			P	S
RadioTransmitter		PS	PS	S
RadioTransceiver		PS	PS	S
StartResume	S	S	S	P
StopFreeze	S	S	S	P
WeaponFire			P	S
MunitionDetonation	S	S	P	S
EncodedAudioRadioSignal		PS	PS	S

Figure 4: Publish/Subscribe Table

As can be seen from this table, the constructive Ship federate mainly knows only of itself. The FAC and the Aircraft have an extensive interplay. The IOS subscribes and visualizes all information.

The reader is encouraged to spend some time inspecting this table, to better understand the following sections.

4. A Cross-Domain Analysis Prototype

The concept demonstrator is a computer program that loads a set of SOMs (XML files) for the Low and High security domain, as shown in Figure 5. It presents the SOMs in a graphical user interface. It then enables the user to experiment interactively with different 'policy rules' for the Guard.

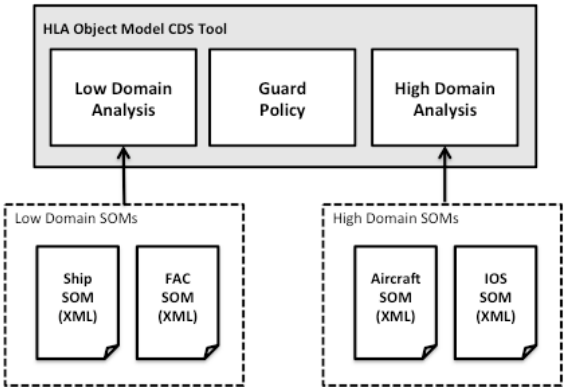

Figure 5: Policy analysis tool

As these rules are designed, the tool calculates and displays the effect on the information flow and how different federates are impacted. This can then be used to assess the impact on training goals. It is also possible to try out different federation designs, for example by moving federates between the Low and High domain or to adjust the filters in the Guard.

The tool uses the following icons:

	The information is published by the federate.
	The information is subscribed to by the federate. All subscribed information in the federation will be delivered.
	The information is subscribed to by the federate, but the information from the high domain **will not** be delivered, due to the security policy.
	The information is subscribed to by the federate, **but only some** of the information from the high domain will be delivered, due to the release criteria.

A similar approach is used to visualize guard rules:

	**All information** is allowed to pass through.
	**No information** is allowed to pass through.
	**Selected information** is allowed to pass through, based on certain release criteria.

As policy rules are designed, and conditions for information release are specified, the icons change accordingly. The user interface initially provides an aggregated overview. The user can then drill down to more and more detailed views.

Figure 6 shows an aggregate level overview of the information flow between the high and low side. A security policy has been specified in the tool, as described by the arrows. Some interesting observations in this case are:

- Information published in the low domain is usually allowed to be released into the high domain, for example the Surface Vessel information.
- The Aircraft information published in the high domain is only released to the low side under certain conditions. This means that subscribers in the low domain may be impacted.
- The Munition Detonation information published in the high domain is not released to the low domain. This will impact subscribers in the low domain.

In Figure 7 we have further expanded the view. We can now see the particular federates that publish and subscribes. We can also look at the information at the attribute level for object classes. Further observations can be made, for example:

- It is only the FAC federate that is affected by the policy rules for the aircraft, since the Ship Federate does not subscribe to it.
- The subscribed attributes affected for the FAC are Spatial and Damage State.

It is possible to define policies interactively and study the result on an aggregated level, for individual federates, or for object class attributes. It is also possible to update the SOMs, or move federates between the high and low domain, which may sometimes be an option. The analysis will be updated and the effect of policy rules can be analysed interactively.

4.1 Testing the prototype

This tool has been presented to simulation developers, training staff as well as accreditors, using SOMs that have similarity with, but are not identical, to a real world application. The following observations were made.

- The use of publish/subscribe tables was new to almost all users. Everyone seemed to understand it immediately and some users expressed their appreciation of the condensed overview that they were now given.
- The interactive specification of policy rules, together with the presentation of the results, in particular in the low domain, triggered a well-structured discussion of how the impact (loss of information) should be handled, as well as a discussion on impact on training goals.

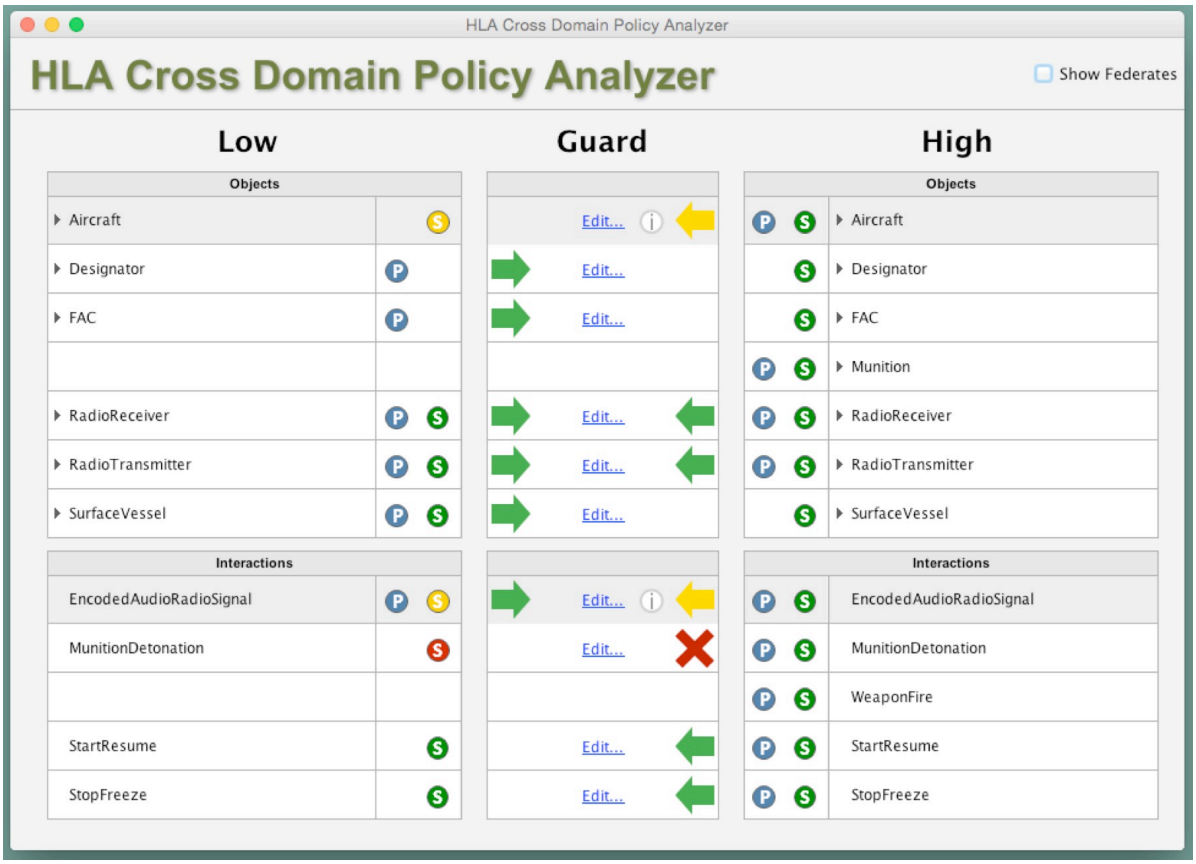

Figure 6: Aggregated View

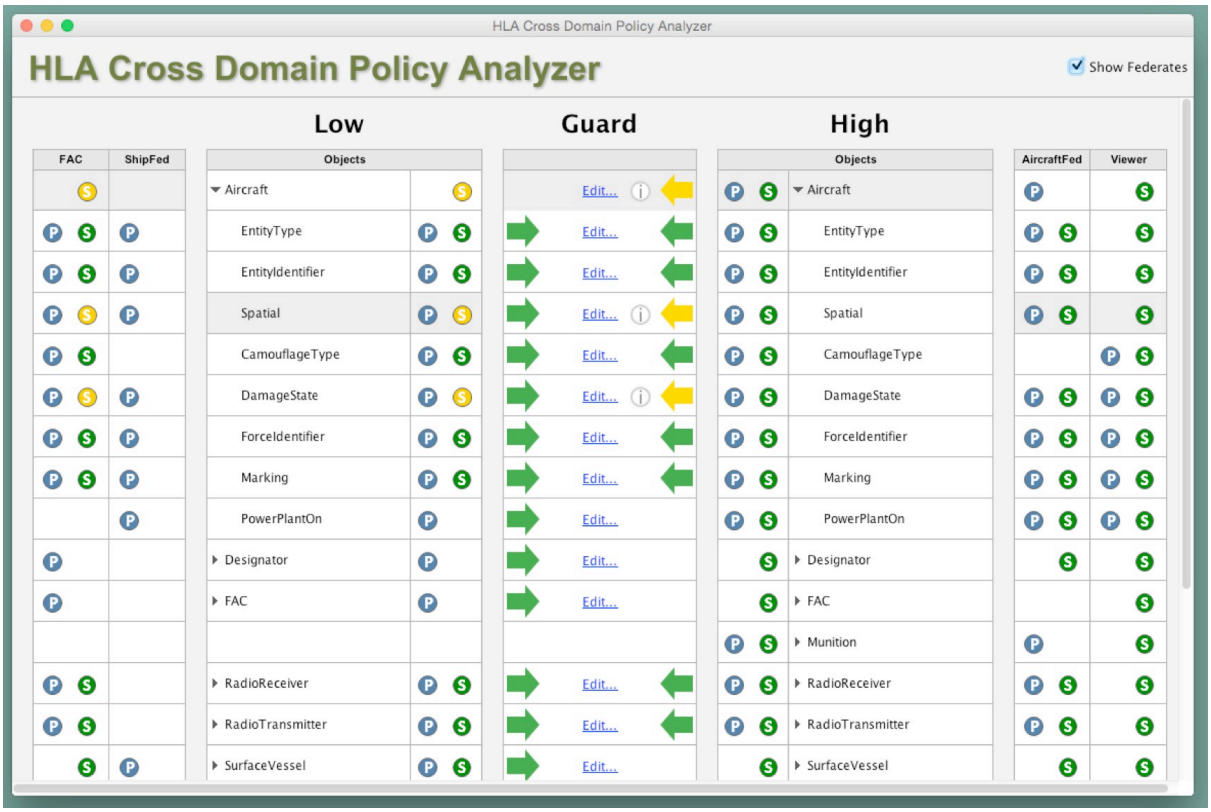

Figure 7: Expanded View

5. Conclusion

There are circumstances in collaborative training under which participating personnel, equipment and information will be classified at different levels. Exchange of data in these situations must be controlled. To support this control of data exchange, a detailed understanding of data flowing between systems at the different classification levels must be achieved to:

- Support a risk assessment of the data exchanged
- Allow a "what-if" analysis of the impact of data exchange controls
- Support the configuration of control mechanisms

This analysis required to achieve this detailed understanding can be very complex and prone to error. HLA has models in the FOM and SOM that can support this analysis. The analysis would benefit from tools that could facilitate the semi-automation of the process.

Such a tool has been prototyped to show the feasibility of such an approach. Initial feedback on the prototype has been promising. Areas for further work could include:

- Adding rules based on instances of objects in the analysis
- Support for automating the construction of guard rules

Acknowledgements

The authors would like to acknowledge UK MoD FsAST that funded some of the work presented in this paper through Niteworks.

References

[1] Anderson R; 'An Overview of Multi Level Security', Dstl/CR39492, 11 December 2009

[2] Croom-Johnson S; 'From Multi Level Security to Cross Domain Solutions', CR69986, 31 March 2013

[3] NATO MSG-080 (2013) Security in Collective Mission Simulation STO-TR-MSG-080.

[4] Hughes K; 'Niteworks DOTC(A) Cross Domain Security Task - Final Report', NW/PR/0645/008, 25 March 2014

[5] B. Möller, et al, Towards Multi-Level Security for NATO Collective Mission Training – a White Paper, SISO paper 11S-SIW-069, www.sisostds.org, September 2011

[6] B.Möller, et. al, Security in NATO Collective Mission Training - Problem Analysis and Solutions, SISO paper 12S-SIW-032, www.sisostds.org, September 2012

[7] B.Möller, et. al., Three Perspectives on DSEEP and Security: Training Goals, Use Cases and the Selection of Security Measures, SISO paper 13S-SIW-005, www.sisostds.org, September 2013

[8] IEEE: "IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA)", IEEE Std 1516-2010, IEEE Std 1516.1-2010, and IEEE Std 1516.2-2010, www.ieee.org, August 2010

[9] IEEE: "IEEE standard for, Distributed Interactive Simulation – Application Protocols", IEEE Std 1278.1-1995 and IEEE Std 1278.1a-1998, www.ieee.org, September 1995 and March 1998.

[10] SISO: "Real-time Platform Reference Federation Object Model (RPR FOM) Version 2.0D17", www.sisostds.org, September/October 2003.

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 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 currently serves as the vice chairman of the SISO HLA Evolved Product Support Group and the chairman of the SISO Real-time Platform Reference FOM (RPR FOM) Product Development Group.

STELLA CROOM-JOHNSON is a Principal Analyst in the Analysis, Experimentation and Simulation Group in the UK Defence Science and Technology Laboratory (Dstl). She has worked on a wide variety of simulation-related projects, and was the technical lead within Dstl on a project looking at options for achieving a persistent Cross Domain Security (CDS) solution across standards and domains. More recently she has been the International Comparators and CDS lead on the UK MOD Defence Operational Training Capability (Air) Niteworks project. She is also currently co-chair of NATO Modelling and Simulation Group 117 M&S to support Cyber Defence.

ÅSA FALKENJACK is a Systems Developer at Pitch Technologies and a major contributor to several commercial HLA products. She holds an M.Sc. in Computer Science from Linköping University, Sweden.

KESTER HUGHES is an experienced team leader and technical lead with QinetiQ. He has experience in defining, managing and delivering complex technical programmes, and has broad experience of a wide variety of communications systems and technologies including military specific systems, communications technologies for sensor networks, IP and the Internet, cellular networks and wireless LAN technology. He has also gained significant experience in simulation and modelling, both for communications systems and, more recently, for flight simulation systems. In over twenty years, he has contributed and led many applied research tasks, technology development tasks and provided advice and consultancy to MOD's procurement teams and industry.