Multi Level Security within Collective Mission Simulation Architectures

Cor A.A. Verkoelen
TNO Information and Communication Technology
Brassersplein 2
2612 CT Delft, the Netherlands
+31 (0)15 2857296
cor.verkoelen@tno.nl

Roel R. Wymenga
TNO Defence, Security and Safety
Oude Waalsdorperweg 63
2597 AK the Hague, the Netherlands
+31 (0)70 3740319
roel.wymenga@tno.nl

Keywords:
Multilevel Security, Information leakage, labeling, release

ABSTRACT: *Collective simulation is proving an important driver to establish objectives within application areas such as development, training and exercises. However, the simulation models exist within different security domains and these models need to be protected while information needs to be shared between the different simulators. Therefore there is an increasing need for a multi level security solution that enables the sharing of simulation information across these security domains to establish collective simulations. This paper describes the topic of Multi Level Security (MLS) within a Collective Mission Simulation (CMS) environment. The 'Collective' aspect within CMS means that simulation systems are interconnected to each other and work together to reach a common objective. The main reason to interconnect simulation systems is the complexity of the overall simulation models. This complexity requires multiple organizations to be involved with their own models and simulation systems. For example, the creation of a new airplane requires different commercial companies to interconnect their simulation systems and test the overall performance of the airplane. A second example is Collective Mission Simulations where different simulators from different nations are interconnected, e.g. a Forward Air Controller Simulation (FACSIM) from the Netherlands connected to an US F-16 fighter simulator. In both examples the simulator systems can have their own characteristics and information. By briefly describing the evolution of the simulation systems, from stand-alone to (international) interconnected simulation systems, this paper will explain in more detail the possible conflicting interest of the organizations and security risks that are involved. These conflicting interests, or risks, could result in the limitation of information that is shared between the systems. The paper will describe a security concept that could be applied to prevent leakage of sensitive information. This concept is translated to the High Level Architecture (HLA) and a more detailed description is given of the different security mechanisms "security labeling" and "information release". The Object Model Template (OMT) of HLA is used as the starting point for this security solution. The paper will conclude by describing the current status of the research and will describe future work that is necessary for the implementation of this security concept.*

1. Background

The last several decades Information Technology (IT) systems have a large impact on the way we live. Not only do these systems have an impact in our personal lives by introducing new means of communication such as e-mail, but also in how we do business. The possibility to use IT systems to process our data in a more efficient manner and the capability to exchange information with other partners are just two examples of how our day-to-day business operations is affected. Even more critical is today's fast flow of information that can be processed and shared with others. This has lead to a change in the IT system architecture and IT communication infrastructures. Where traditionally the systems were dedicated systems due to the limited processing power, current processing power is not a constraint anymore and the systems are used for

multiple (parallel) tasks. The same applies for the interconnection of IT systems. Formerly, interconnections of systems were sparse and most systems were stand alone environments. Only very specific interconnections between specific IT systems were realized. Nowadays each IT system is connected to a (international) communication network such as the Internet.

Using systems for multiple tasks and connecting these systems to (international) communication networks causes some points of special interest regarding information security that should be taken into account. One of these points is the possible leakage of (sensitive or classified) information. Traditional IT system architectures do not address this point interest and require an additional security solution to safely share information with other IT systems.

1.1 Simulation system background

As mentioned earlier, original IT systems had limited processing power and were used for dedicated tasks. Information was entered via the human interface and information exchange between systems was not common practice. The result of this was a *stand-alone* IT system used for *dedicated* tasks. The stand-alone and dedicated characteristics are also applicable for early simulation environments. An F-16 simulation system with only pilot interaction is an example of such a simulation environment. These simulation environments are called *dedicated stand alone simulation* systems. Such a system could be seen as a black box containing the appropriate models and information to execute the F-16 simulation. The only interaction that exists is the interaction between the F-16 simulation system and the pilot. No interconnections and interactions with other simulation environments are implemented in these early simulation environments.

When these simulation systems became more mature, partly due to the evolution of IT systems in general, the increase in processing power allowed the simulation system to simulate more complex environments. The added communication capabilities resulted in the interconnection of different simulation systems. For instance, the interconnection between an F-16 simulator and a Forward-Air-Controller simulator (FACSIM), making collective mission simulations became feasible. The interconnection started with only connections between local simulation systems. This means that all simulation systems belong to the same organization and the models and information were kept within the simulation environment and therefore within the organization. These simulation environments are called *dedicated and local/national interconnected* simulation environments.

Because all the simulation systems and the information processed within these systems belong to the same organization and therefore is kept within one security domain information leakage was not identified as an important point of interest. In these local/national environments it is assumed that all information may be shared with all systems and each system is identified as trusted. This does not preclude the existence of classified or sensitive information but it is presumed that all systems and personnel comply with the guidelines that are applicable.

Currently, simulation systems are not only connected locally but also globally where simulation systems of different organization and even nations are connected to each other. This is partially driven by e.g. current military operations where Combined and Joint operation becomes more common practice. Therefore, for an effective and realistic simulation or training the simulation environment should also include this Joint and Combined aspect. This requires simulation systems from different nations. This means that for instance an FAC simulator from the Netherlands will be connected to an F-16 simulator of the United States for Close Air Support (CAS) training. This environment is called the *dedicated and international interconnected* simulation environment.

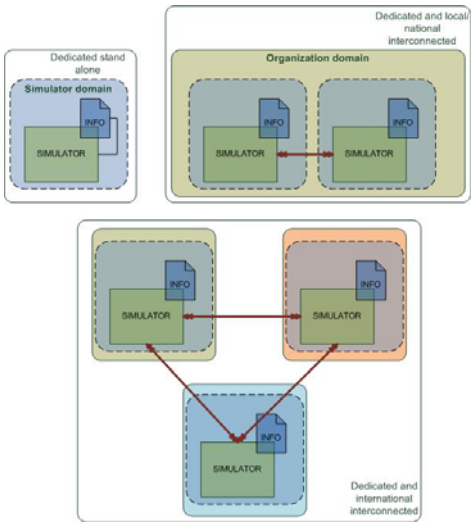


Figure 1. Simulation environment evolution

At this point information is exchanged between different organizations or nations and information is shared across different security domains. From a

functional point of view both simulation systems only exchange the information required for the objective of an accurate and realistic execution of the simulation. In spite of this genuine intent both simulation systems may also contain sensitive or classified information that may not be shared with (international) partners. For instance, the detailed weapon systems and the Electronic Warfare (EW) capabilities of the F-16 may not be 'need-to-know' information for the FAC simulator during the simulation. It is at this point where information leakage to another security domain becomes an important point of interest. The need for the protection of sensitive and classified information from leakage now becomes real and may not be neglected. This recognized risk of *information leakage* is the rationale behind the research on 'Multi Level Security (MLS) within Collective Mission Simulations (CMS)'.

To better understand the influence of storing, processing or sharing classified information on simulation systems a concise overview of *information security* is given. Subsequently the exchange of classified information in current (simulation) environments and the consequences of the interconnection of different environments are described.

1.2 Information security background

This concise overview is divided in three categories. Firstly, the information security ***cornerstones*** category is described; secondly the information security ***views*** category and thirdly the information security ***measure characteristics*** category are described.

The information security ***cornerstones*** category consists of the *Availability*, *Integrity* and *Confidentiality* cornerstone. Availability is defined by the International Organization for Standardization (ISO) [10] as "*the property of being accessible and usable upon demand by an authorized entity*". Integrity is defined as "*the property of safeguarding the accuracy and completeness of assets*" [10]. The assets may vary from physical assets such as computers to non-physical assets such as information. Confidentiality is defined as "*the property that information is not made available or disclosed to unauthorized individuals, entities, or processes*" [10]. The other two categories of information security and additional information security related topics are closely connected with one or more information security cornerstones. The risk of power outage for instance, is closely connected with the availability cornerstone. Username and password combinations are conversely security measures that are closely connected with the confidentiality and integrity cornerstone.

The information security ***views*** category consists of the *Organizational*, *Procedural* and the *Technical* view. The Organizational view contains topics which address information security with a potential organization-wide influence. The appointment of a Chief Information Security Officer (CISO) is just one example that falls within the Organizational view category. Moreover, most of the organizational topics contain a Procedural section. A procedure is an ordered set of tasks for performing a certain action. Usually these procedures are written documents. The procedure describing how to carry out a 'clean desk' inspection is one example that falls within the procedural view. Clean desk means that no classified information may be left behind unattended. The 'clean desk' procedure is a consequence of the information security policy (organizational) describing that loss of classified information is disastrous. The last information security view is the Technical view. The technical view is closely related to information security measures that could be implemented by using available technology. Firewalls, Virus Scanners, or Intrusion Detection Systems (IDS) are just three examples that fall within the technical view category. Besides the technical characteristics these measures also have, as also applied for the organizational view, a procedural section. If for instance the virus scanner is installed there should also be a procedure describing the tasks that should be executed to update the virus scanner regularly with the newest scan engines and virus definition files. In case these updates are not otherwise enforced, the virus scanner will in time only detect old (and possible obsolete) viruses and not the new and currently active viruses.

The final category is the information security ***measure characteristics*** category which consists of the *Prevention*, *Detection*, *Repression*, and *Correction* characteristics. The aim of *Prevention* is to obviate an information security threat from becoming a reality. Within an IT infrastructure the insertion of a firewall falls within this characteristic group. The configuration of the firewall prescribes the information flows that are permitted completed with authorized sources and destinations of the information. This brings the firewall in a position where only authorized information flows are allowed and potential detrimental traffic is ruled out. The Firewall blocks for instance all FTP connections (incoming and outgoing) to rule out information leakage using the FTP protocol. The aim of *Detection* is to identify and take suitable actions on

those information security threats that are not previously prevented. An Intrusion Detection System (IDS) is an example of an IT system that has this characteristic. Information security threats are identified by monitoring network traffic and/or system activity. The operator is then usually alerted by showing the information security incidents on a dashboard. The third information security measure characteristic is *Repression*. The aim of repression is to diminish the effect of an incident if this incident becomes reality. The filtering and/or quarantine competence of a virus scanner is an example of repression. After detection of a virus the virus scanner may decide to remove the virus or place the information including the virus in quarantine. This diminishes the effect of the virus. The last category is *Correction*. The aim of *Correction* is to recover from the damage that is caused by an information security incident. Business Continuance plans, regularly back-ups of critical information, and more in particular restoring the information from these back-ups, are just two examples of the correction characteristic.

Security threats, incidents, measures and other related security topics can always be categorized by information security *Cornerstones, Views* and *Measure characteristics*.

1.3 Exchange of classified information in (current) simulation environments

Currently the whole information security area including the information security cornerstones, views, and measure characteristics are closely related to the physical and/or organizational boundaries. This results in the characteristic of preserving classified or sensitive information within a well defined territory or security domain. At the same time information exchanges across the borders of these territories are only occasional and thoroughly examined. On top of that, the examination functionality is predominantly realized near, or even at, the borders of this well defined territory or security domain. This functionality might be a technical verification process implemented by using various available IT technologies. However, even though technology experienced a mushroom growth over the past several years, some information exchanges still require human mediation. The sensitivity level (classification) of the information and the limited confidence in technology of today are the two main reasons not to rely solely on IT technology.

If for example particular classified information of the Netherlands (security domain A) must be shared with Denmark (security domain B) the information is printed and sent by courier to Denmark. Denmark confirms receiving the document and may thereafter use the particular classified information within its own defined territory. This territory and the treatment of the received information by Denmark must be in accordance with the guidelines that are applicable to the particular classification of the received information. These guidelines describe how to deal with the classified information, see for example [3]. These guidelines entail among others things details on: destruction of the classified information; physical access requirements to IT systems; and even personnel requirements. Entirely automated information exchanges of classified information within IT environments are not common practice and only occasionally available for less sensitive information. The only exceptions are those environments that are connected to each other and both process information with equivalent classifications.

The guideline(s) an organization or nation must comply with is subject to the classification of the information that is processed or received. It is self-evident that guidelines for “NATO Restricted” classified information are dissimilar from guidelines for “NATO SECRET” classified information. The consequences of the requirements that must be met as a result of the “NATO SECRET” guidelines have more impact because these requirements are more stringent compared to the “NATO Restricted” requirements. Within current IT infrastructures various classified information is processed. In spite of the various classified information, if an IT system processes NATO Restricted information the system must comply with NATO Restricted guidelines. However, if the same IT system processes NATO SECRET information the system must comply with the NATO SECRET guidelines and process all information as NATO SECRET even if the information is not classified at all. This property together with the before-mentioned lack of confidence in technology has lead to the “*system high*” theory. The lack of confidence is in this circumstance a result of technology not satisfactorily guaranteeing an effective separation and correct processing of dissimilar classified information. The *system high* theory entails that all IT systems inside the well defined territory must comply with the guidelines belonging to the highest classification that may appear within this territory. All information, even if it is classified at a lower level, should be treated as being of the highest classification.

In explanation of the frequently used term “Classification”, a classification consists of three components. The first component is a “*marking*”; the

second component is the actual "*classification*" and the third component is a "*classification extension*". The marking component is an indicator of the organization or nation that is the original owner or author of the information. Various markings exist such as NATO (NATO organization) and STG (State Secret, the Netherlands). The second component is in fact the actual classification. This is an indicator of the level of sensitivity. Various classifications are SECRET, RESTRICTED, and UNCLASSIFIED. The third component (classification extension) contains additional information. A frequently used extension is the "RELEASABLE TO" extension and influences the distribution of the information. The extension component of the classification is optional and may be omitted. An example classification made up of all components is "NATO SECRET RELEASABLE TO SWE". The classification must be acknowledged by all organizations and nations that have access to the classified information. For example, if STG GEHEIM[1] information is shared with the United States, the United States should recognize this classification and comply with the particular guideline. If classifications are not recognized, security classifications are useless.

1.4 Consequences of interconnecting information systems

The added value of interconnecting various information systems is increasingly recognized. Connecting an F-16 simulator to a FACSIM is just one example. These information systems might process different classified information and may even belong to distinct organization or nation defined territories.

In a well-defined group of information systems connected to each other, supplemented with agreements and trust between organizations and nations, the "system high" theory can be applied. Nevertheless, connecting different information systems always introduces particular information risks. The three predominant information security risks are:

- *Information leakage*;
- *(infrastructure/information) Attacks directed at national system;*
- *Acceptance of information from connected system.*

Information leakage means that (national) information that should be kept within the organizational or national territory is inadvertently shared with connected information system outside this territory. This might be a consequence of a deliberate or accidental activity carried out by own personnel or a consequence of attacks directed against IT systems. The initiator of the second risk is located beyond the national well-defined territory, meaning that the attack is launched from one of the connected IT systems. The third threat is with reference to the acceptance of received information from connected information systems. The connected information systems could (accidentally) send classified information that was not supposed to be shared and is also classified. A consequence of the acceptance of this information would be that additional guidelines may be applicable. Despite the origin is within the connected information system and also the negative consequences will mostly affect the connected information system (information confidentiality breach), processing the received (sensitive) information according to the applicable guideline is seen as a social convention.

The system high theory is also utilizable in the environments where various organizations and nations connect their information security domains. In this particular situation a generic classification must be agreed on by all participating organizations and nations, for instance NATO CONFIDENTIAL RELEASABLE TO SWE. Subsequently all organizations and nations should comply with the guidelines for the chosen classification. This includes the information systems within these security domains. In addition to this, information that is exchanged between the information systems of different organizations or nations is classified as the classification agreed on. Even after system disconnection, the guidelines will still apply to the information systems.

The system high theory has ultimately leaded to multiple information systems and multiple well defined territories and security domains, where each system and territory is available for only one classification.

2. Problem Description

Within present simulation environments the wish to connect various simulators from multiple organizations and nations is emerging. These simulators are in fact just another type of information system and connecting simulators is equal to connecting information systems. Consequently the points of special interest regarding information security are also applicable for a simulation environment.

Currently the system high theory is also used within collective mission simulations and therefore prior to the execution of the collective mission simulation the classification of the CMS is determined and agreed on.

[1] Equivalent to NATO SECRET (Dutch Secret)

Consequently, the classification applies for all information and simulators (and tools) involved in the simulation. All organizations and nations are responsible for adapting the information within their own simulators to comply with the predetermined classification. Equally classified information does not need any modification and may be used, processed and exchanged. Dissimilar classified information requires attention prior to the execution of the collective mission simulation.

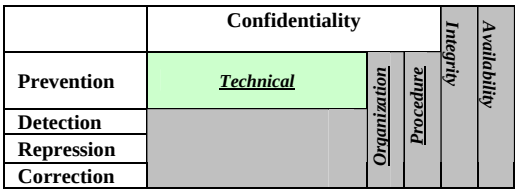
Information classified at lower levels (e.g. CONFIDENTIAL versus SECRET), may be used, processed and exchanged. Information classified above the agreed on classification, SECRET versus CONFIDENTIAL, must be altered or even removed. Information classified equivalently, but with different markings (e.g. NATO versus STG), might possibly be used after small modifications. The decision whether modifications are required and whether or not the applied modifications are sufficient must be made by the National Security Authority (NSA). The NSA of the nation indicated by the marking of the classification must be consulted. An example of altering information is by replacing a classified simulation model by an unclassified model that is less accurate.

After the execution of the collective mission simulation, all simulators must still comply to the guidelines that apply for the predetermined classification. A possible consequence could be that all information carriers (hard disks, USB stick, and memory cards) must be removed from the simulator and stored according to the guidelines. This applies even if the information carriers store only unclassified information and no information is received during the collective mission simulation. The system high approach and a connection of this simulator to the system high infrastructure implies that this unclassified information must now be treated as if it is classified equivalent to the predetermined classification.

Altering information stored on the simulator prior to the execution of a collective mission simulation is not desirable and may be obviated. Altering information adds extra turnaround time before a simulation can be executed and possibly result in needless inaccuracy during simulations. For that, the information exchange should automatically be examined and altered if required before sending this information to connected simulators. For this to take place the simulator must be capable of determining the classification of each information element stored on the simulator. This would results in the protection of the information elements itself instead of protecting the entire simulator and all information elements by applying the system high theory. The information risk of information leakage in this situation may be overcome by adding a filtering mechanism to (all) simulators.

This paper describes a security concept that can be used to identify the classification of an information element and based on that can determine, and carry out, the necessary modifications before sending the information element.

The focus of this research does not include all aspects of information security as described. The primary focus of this research and the remainder of this paper is ***Confidentiality*** on a ***Technical*** level identifying ***Preventive*** information security measures to prevent ***information leakage*** from a simulator environment.



3. Security concept functional building blocks

The above sections described the points of special interest as a result of the interconnections of information systems. At the same time the various properties of information security such as the information security *cornerstones* and *views* were explained. The remainder of this paper describes a security concept that if adopted will potentially allow the interconnection of simulation environments by in essence diminishing the risk of information leakage. First of all, this section describes the functional building blocks that are identified as part of this solution. Subsequently the functional building blocks are translated from conceptual level into an actual simulation environment based on the HLA protocol.

3.1 Building block: Labelling

The first functional building block is ***labelling***. This building block actually consists of two sub components. The first sub component is the *information element identification* and *classification label determination*. The second sub component is the actual placement of a security label on each

information element. This security label is the equivalent of the information *classification.*

Determination of the value of the label can be based on a variety of properties of the identified information elements. The possible, yet not exhaustive enumeration of properties includes 'origin', 'size' and 'sensitivity/ classification' of the information element. From an information security perspective the determination based on the 'sensitivity/classification' is most relevant and is in this paper the basis of the functional building block *labelling*.

Within this security concept the information element could by anything such as HTTP traffic (requests), instant messaging traffic, e-mail messages, electronic documents (word-processor document, spreadsheet document). Depending on the nature of the environment and the objectives of the security concept the type of information elements can be specified. Subsequently the security label must clearly indicate the sensitivity of the information. Classification schemes (national or international) are suitable for this purpose. In the end, the objective of the security label is to give an unambiguous indication of the sensitivity of the information element whereupon a certain decision can be made.

The appearance of the security label may also be subject to the nature of the environment where the security concept is implemented. In a traditional document based world the information elements are the physical documents and the security label is determined by the person who created the document. This label is attached to the document by adding a stamp/hallmark on this document. In this case the information element is the physical document and the functional building block 'labelling' is carried out by a person(s) involving identification, determination and placement of the label. Besides, the label is closely bound to the information element because of the nature of the physical document and the attached label. On each page the label is attached specifying the security label. These labels are hard to tamper with without being detected.

Within an information system environment this label will have the same objective. However, there are some basic differences between the physical environment and the information system environment. One of these differences is the close relation between information element and label. Within an information system environment this close relation is not commonplace. A word-processor document may contain a watermark expressing the security label. However this watermark can be tampered with if an attacker or virus can open this document and change the watermark. Therefore, the implementation of this label should be more closely bound to the document, and after placement as hard to tamper with as within a physical environment.

However, the objective of the label stays the same. *The label indicates the sensitivity of the information*. Based on this label the functional building block *release* can determine whether the information may be shared or whether additional actions must be performed before the information may be shared with other systems.

3.2 Building block: Release

The second functional building block is ***release***. The elementary function of the release building block is to determine whether information elements may be shared with other information systems. The decision to release the information is based on the label which is attached to the information element by the labelling building block. If for instance the label indicates a sensitivity of NATO SECRET, the information element may first of all only be shared with nations that are a member of NATO. Apart from this, the information element may also only be shared with those NATO nations that have a pertinent need-to-know. Non-NATO nations and NATO nations without the need-to-know should not receive this information element. The release building block determines the releasability of the information element based on the label combined with the proposed destinations.

Identical to the labelling building block the implementation of the release building block is subject to the nature of the environment and the objectives of the security concept. Despite of the dissimilarities the fundamental operations of the release building block are the same. Based on the label the release building block resolves whether:

- The information element may be shared without alteration.
- The information element may be shared after alteration.
- The information element may not be shared.

In the first situation the information element label combined with the destination(s) does not raise any objections. Destination(s) are authorized to receive and process the information element. The second situation requires alteration of the information element prior to sharing this information element. This alteration could imply the substitution of the sensitive information element with less sensitive information. If the third option is chosen by the release building block, it is

decided not to share the information element at all, not even when the information element is altered. Possibly due to the perpetual sensitivity of the information element that is independent of the precise values of the information element, or due to the destination(s) of the information element.

4. Security concept within a simulation environment

Before the 'security concept functional building blocks' are translated to a simulation environment a high level introduction of simulation environments is desirable. This introduction includes the communication protocols that are used to share information elements between simulator systems. This section provides this background and elucidates the assumptions made during this research.

4.1 Simulation environment communication protocol

Within the simulation environment there are in essence two main communication protocols in use for the exchange of information elements. These communication protocols are the Distributed Interactive Simulations (DIS) protocol and the High Level Architecture (HLA) protocol. It can be presumed that the HLA protocol is the successor of the DIS protocol. This research has chosen to take the HLA protocol as a starting point for the translation of the security concept. Supplementary information about the DIS protocol can be found in [6] and [7]. In addition, only the basics of the HLA protocol that is used for the realization of the labelling and release building block are briefly described in this paper. Details of the HLA protocol can be found in [8] and [9].

The **High Level Architecture** (**HLA**) protocol is a generic purpose protocol for distributed simulation systems. Using HLA, simulation systems can exchange information with other simulation systems regardless of the different computing platforms (hardware, applications and operating systems) used by each simulation system. Basically HLA consist of three components:

- *HLA Rules.*
- *Interface specification.*
- *Object Model Template (OMT).*

At the highest level, HLA consists of the 10 HLA rules which must be obeyed before a simulator, or set of simulators, is considered HLA-compliant. Five rules are established for an individual simulator (federate), five rules are established for a set of simulators (federation). The federation rules describe the ground rules for creating a federation, including documentation requirements, object representation, data interchange, interfacing requirements, and attribute ownership. These rules have a potential influence on the information elements that are exchanged. Nevertheless they do not describe these information elements in detail. Moreover, this set of rules is not the actual communication protocol used. Despite that, these rules could potentially influence the information elements during the creation of a collective mission simulation environment; this research will not take this specific component of HLA as the starting point.

The Interface Specification defines abstract communication services between HLA compliant simulator systems. These abstract communication services are realized by the Run-Time Infrastructure (RTI) which is a software component implemented in accordance with the interface specifications. Nevertheless the RTI itself is not part of the interface specification. The RTI provides the software services that are essential to support a HLA-compliant simulation system.

As a result of the fact that the RTI provides the communication services, it could be of value for the security concept. The security building blocks *labelling* and *release* operate in the process of the actual exchange of information elements. Owing to this the RTI and interface specification is not affected by the security concept, but may be used by the realization of the labelling to determine the information elements and their precise values.

Finally, the Object Model Template (OMT) specifies information elements within a single simulator (federate) and information elements that exist within a set of simulators (federation). The specification of the information elements within a federation is called Federation Object Model (FOM), specification of information elements for a single simulator is called Simulator Object Model (SOM). The OMT provides a standard for documenting HLA Object Model information. These objects are the information elements that are actually exchanged between the different simulation systems. Capturing traffic leaving a simulation system and resolving this traffic into HLA Objects is the starting point for the labelling building block of the security concept. Based on the captured object the exact information element could be determined after which the sensitivity of the element is determined. Recapitulated, from the three components

of HLA, the OMT seems most suitable for the identification of the information elements exchanged and provides handles for the determination of the sensitivity of the information element.

4.2 Simulation environment information exchange

The actual exchanges of information elements within a HLA compliant simulation environment is realized by using publish and subscribe mechanism and/or a broadcast or multicast mechanism. During publish and subscribe, simulators determine the information elements they are willing to share with other simulators (publish) and determine the information elements of other simulators they are interested in (subscribe). Both are in essence based on the functional operation of the collective mission simulation and not based on security classifications of individual information elements. Thereafter the information elements that are published are broadcasted onto the network and can be interpreted by each simulation system. Due to this fact these present-day environments require the *system high* approach where all information may be shared and all participants are at least authorized to process information elements with the predetermined classification. All participants are also able to treat this information according to the guidelines that belong to the predetermined classification. The downsides of the system high concept are also applicable in these simulation environments.

4.3 Security concept preconditions and assumptions

The exchange of (sensitive) information elements within a simulation environment is a complicated affair with multiple points of departure. Even in the case when the scope is confined to *information leakage* and *preventive security measures* various points of departure can be identified. Adding authentication functionality during publish and subscribe is one of the other points of departure.

The point of departure for this research is to prevent information leakage by observing and influencing the actual information element leaving the simulation system. Other preconditions and assumptions are:

- The security concept is based on HLA; specifically the Object models of HLA.
- The security concept may use the RTI API interface to determine the HLA objects that are intercepted.
- The security concept should be implemented as a black box placed nearby the simulator it protects.
- The security concept affects the exchange of information not the creation of a federation.
- Individual information elements (objects) exchanged within a simulation environment messages can be classified.
- Sensitive/classified information elements will not alter their classification during a simulation.
- Within a collective mission simulation it is acceptable to alter the values of sensitive information elements or to entirely delete information elements.

Whether all these preconditions and assumptions are met and/or accepted by the collective mission simulation community is not clear at this moment.

To go into more detail regarding the ‘classification of individual information elements (5th bullet)’ there exist mainly three categories of information that could be classified.

(1) Individual classified information elements
This means that individual information elements (objects) itself are classified according to the sensitivity of the objects. For instance the GPS coordinates of a command post during a mission.
(2) Classified combined information elements
The second category contains information that could be gained by a combination of information elements. For instance two information elements containing timing and location information could reveal an avoidance manoeuvre of an F-16.
(3) Classified meta-information
The third category contains information that itself is not sensitive but does give away some other sensitive information that can be deduced from the initial information element. For instance, the information element expressing the launch of a missile is not classified by itself. Nevertheless, the launch of this missile from a specific platform reveals information about the capabilities of this platform. These fighting power and fighting capabilities may be classified. This is called meta-information.

The scope for the labelling and release building blocks is the category of *Individual classified information elements*.

Individual classified	Classified combined	Classified meta
		

5. Simulation environments and functional building blocks

The preceding sections elucidated the security concept functional building blocks, the nature of the simulation systems and the preconditions and assumptions made within this research. This section translates the functional building blocks into a labelling and release mechanism that can be used in simulation environments.

Presently it is not expected that the incorporation of a security label capability in the HLA standardization will become available in the not too distant future. Neither is it expected that preventive security measures against information leakage will be included in the simulation systems itself. As a consequence of this the labelling and release building blocks should be effectuated as an additional security gateway placed as close as possible to the simulation system it protects. A high level architecture shows the various functionalities of the security gateway.

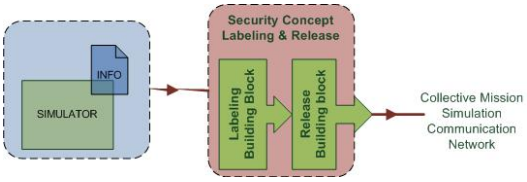


Figure 2. Security concept building blocks

Yet it is foreseen that in the future, parts of these functionalities will be incorporated within other components of the simulator environment such as the simulator itself (labelling), or within crypto devices (distribution).

5.1 Labelling in a simulation environment

The first security building block is the process of labelling individual information elements (objects). As already described the labelling building block is made of two sub-components. These are the *Identification and Determination* sub-component and the actual *labelling* sub-component. Zooming in on these subcomponents the activities are defined as:

- Packet recovery
- Object identification *(Identification)*
- Classification lookup *(Determination)*
- Labelling *(Labelling)*
- Forwarding

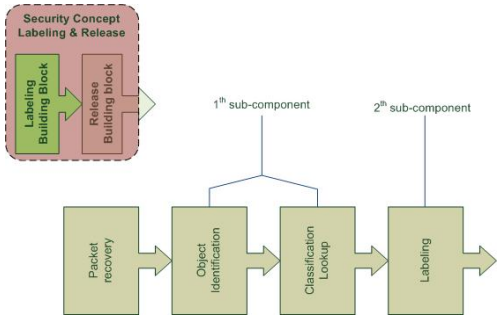


Figure 3. Labelling building block

Packet recovery
The packet recovery is a stipulation for the object identification activity. Within HLA any available link layer or even network layer may be used. The HLA information elements as defined by the Object Model Templates (SOM and FOM) exist on the higher layers of the OSI model. As a consequence, recovering only network traffic such as IP packets or even TCP or UDP traffic is not satisfactory for the object identification activity. The packet recovery activity should recover the actual HLA objects, possibly subdivided over several network packets. For the recovering of the HLA objects the RTI stack can be used. Network traffic is captured and processed by the RTI stack with the result of HLA objects that are reconstructed. Subsequently the HLA objects are forwarded to object identification.

Object identification
When the information elements are resolved the actual HLA object should be identified. This is the responsibility of *object identification*. Object identification deduces the HLA objects using the Simulator Object Model. The SOM enumerates all objects that could be sent by the simulator. Utilizing the SOM the exact HLA object that is transmitted by the simulator is identified. The reconstructed HLA object and the characterization of which HLA object is communicated are forwarded to 'security classification lookup'.

Security classification lookup
Security classification lookup ascertains the sensitivity/classification of the HLA object that is transmitted. For this purpose the security classification lookup utilizes various information sources implemented as databases. Each individual database holds the HLA objects of a particular sensitivity/classification without the actual values of the object. As a result of this multiple databases exist, namely a database for each classification. For instance, a database for NATO SECRET classified HLA objects

and a database for NATO CONFIDENTIAL HLA objects, etcetera.

Note that the database itself does not contain any values that the object may have. For instance the HLA object describing the depth of a submarine may be classified STG CONFIDENTIEEL[2]. Furthermore the missile capabilities of the patrol ship of the navy may be STG GEHEIM. In this case there is a STG CONFIDENTIEEL database containing the '<depth submarine>' object and a STG GEHEIM database containing the '<missile capabilities patrol ship>'. The databases contain no actual values of both HLA objects. Hereafter the HLA object and the label indicating the classification are forwarded to the labeller.

If no database contains the specific HLA object, the object is added to default fall-through database and dropped. This database should be regularly examined and the recorded HLA objects must be classified afterwards. In the end all objects should be classified and the fall-through database will not contain any objects anymore.

Labeller
The second sub-component of the labelling building block is the labeller itself. This sub-component combines the identified HLA object and the security label that is determined. Both parameters are used by the release building block. The security label is used to decide whether the HLA object may be shared in original state, (slightly) altered, or not shared at all. The HLA object itself is used, following the decision made, for distribution towards connected simulation systems.

The label identified will not be shared with other simulation systems because the connected simulation systems are most likely not capable of interpreting the labels at this moment. Therefore the label only exists within the security concept.

[2] Equivalent to NATO CONFIDENTIAL

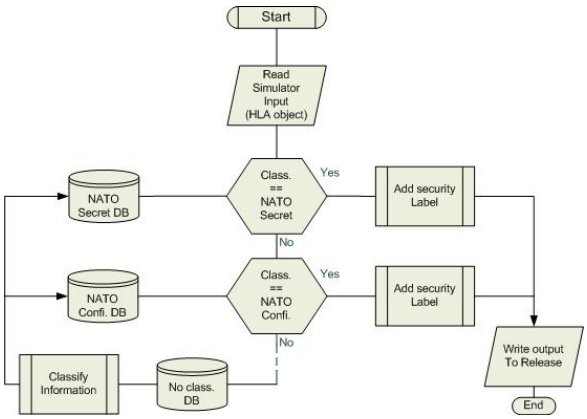


Figure 4. Labelling flow diagram

5.2 Release in a simulation environment

The second building block is release. The release building block decides:

- Whether information elements must be altered
- Whether information elements must be dropped

These decisions are based on the destination(s) of the information elements. In case there are multiple destinations, the release mechanism may decide on the applicable release rule for each individual destination.

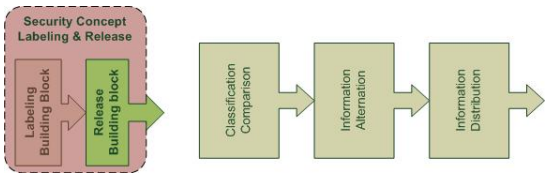


Figure 5. Release building block

Four conceivable situations can appear concerning simulation systems, information classifications and destinations of information elements.
In the first situation the simulation environment consists of one communication network that has only one classification (system high mode). The simulator itself contains only information of one classification. In addition to this both classifications are equal. In this situation the label and release building blocks are actually superfluously.
In the second situation the communication network is similar to the first situation (system high mode). On the other hand, the simulator contains various classified information, not all equal to the classification of the network. In this circumstance there is a possibility that information elements must be altered or dropped to prevent leakage of sensitive information. The destinations of information elements are not taken into

account, principally due to the system high mode of the communication network.
In the third situation, the simulator system still holds various classified information only the simulator system is connected to multiple system high communication networks. Each communication network is individually classified. For instance a communication network classified as NATO SECRET and another communication network classified as NATO CONFIDENTIAL. In this situation the release building block must take destinations into account.

In the fourth situation the simulator system contains various classified information and is connected to one communication network. This communication network is not system high anymore, and information of different classifications (encrypted with different keys for different classifications) may be transported without changing the classification. This fourth situation is the ultimate situation that is aimed for within the communication network working field.

For each situation, apart from the first situation, the release building block is implemented differently. This is the result of taken into account the different destinations and whether the release building block is connected to various communication networks. Common operations are the 'alternation of information elements' and 'writing output to the network'. The release operations executed within situations (2) (3) and (4) are elucidated.

Situation (2)
First of all the HLA object and the label are read. This is received from the labelling building block. The first activity of the release building block is ascertaining the classification of the communication network and equates this classification with the label attached to the HLA object. The information concerning the classification of the communication network is stored separately as a result of changing classification per collective mission simulation. If the classifications are equivalent the HLA object may be shared without being altered. Due to the system high mode of the communication network destinations are not taken into account. If the label and network classification are not equivalent the HLA object, label, and network classification are forwarded to the component responsible of altering the HLA object consistent with the classification of the network. One possible option is to drop the HLA object entirely. The other option is to slightly alter the information contained within the HLA object. Comparison tables may be used to determine the appropriate action. Finally the HLA object is forwarded and sent onto the network. For this purpose the RTI stack may be used again.

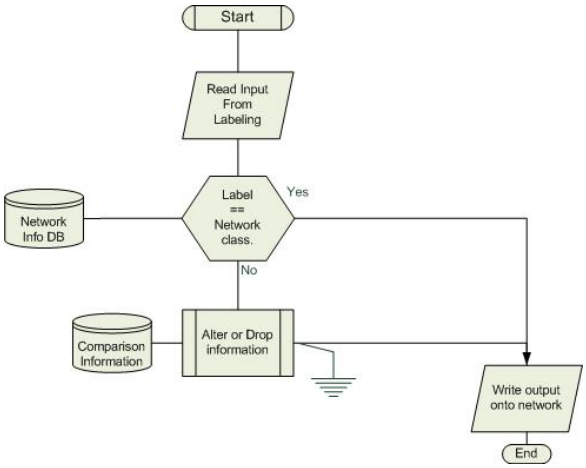


Figure 6. Release flow diagram situation (2)

Situation (3)
Situation 3, and also situation 4, requires knowledge about the different destinations of the HLA object. Initially this is beyond the scope of this research because this required interference with the publish/subscribe mechanism. Nevertheless, a high level description of these situations is provided.
After receiving the HLA object and its label, the first activity is to lookup the various destinations of this HLA object and the appropriate networks the destinations are attached to. This information is retrieved from a database that is filled by the publish/subscribe mechanism. Each time a subscribe message is received, the simulator sending the subscribe request is registered in conjunction with the specific HLA object it is interested in and the network the simulator is attached to. The network the destination simulator is connected to can be deduced from the receiving subscribe message. The RTI stack may be used for this purpose.

The destinations of the HLA object are attached to the HLA object. From this point comparison of network classification and HLA label is performed for each destination. The process of this comparison is actually similar to situation (2). If all the destinations are processed the release building block exits.

Forwarding of the HLA object deviates from situation (2) because the simulator is connected to different communication networks. The 'Write output' block determines the appropriate network using the destination information added previously. Subsequently the HLA object is forwarded on the appropriate network only using the RTI stack.

Situation 4

The difference between situation 3 and 4 is the 'write output' block. Instead of selecting the appropriate communication network onto which the HLA object must be forwarded, this block should now determine the appropriate protection mechanism before sending the HLA object onto the common communication network. This protection could be the selection of the appropriate encryption mechanism using crypto devices. As a result of this encryption the HLA information is 'declassified' and ready to be shared across a non-equivalent classified communication network.

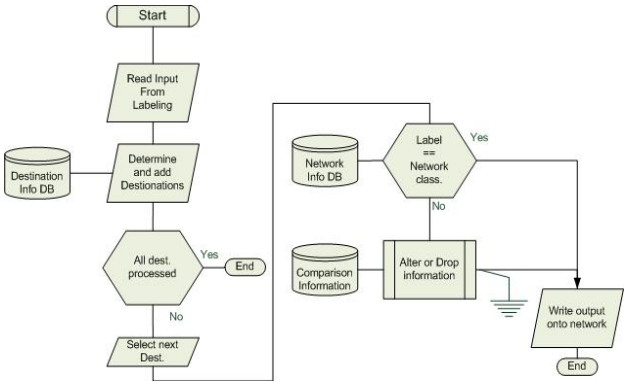


Figure 7. Release flow diagram situation (3) (4)

6. Future research

Currently the different security building blocks and their basic functionality have been identified.

In the near future these security building blocks will be implemented to prevent information leakage for situation (2). This will be a functional Proof-of-Concept. Subsequently the actions required for situation (3) and (4) will be worked out in more detail. The starting point for the demonstrator will be situation (2) based on the HLA protocol.

Additional, common ground related to the information security domain will be identified. It is anticipated that ultimately HLA should provide the mechanisms to label individual HLA object. This entails a standardization of a labelling mechanism within HLA and simulation systems. In addition to this, during the establishment of a collective mission simulation environment a structured step-by-step plan can be followed (FEDEP). In the future security aspects within this FEDEP will be identified. As a result security is taken into account already during the creation of the collective mission simulation environment.

7. References

[1] Defensie Beveiligingsbeleid (DBB) (1999)

[2] Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI) (2004)

[3] NATO infosec and implementation directive for the interconnection of communications and information systems (2003)

[4] Algemene Beveiligingseisen voor Defensieopdrachten 2006 (ABDO)

[5] http://www.sdisac.com/Resources/NatoBrieferInfo.doc

[6] IEEE Std 1278, IEEE standard for distributed interactive simulations – applicationprotocols, march 1996

[7] Standard Agreement 4482, Standardised information technology protocols for Distributed Interactive Simulation (DIS), edition 1

[8] IEEE Std 1516, IEEE Standards for Modelling and Simulation (M&S) High Level Architecture (HLA) – Framework and Rules, September 2000

[9] Standard Agreement 4603, Modelling and Simulation Architecture Standards For Technical Interoperability: High Level Architecture (HLA), edition 1, 2008

[10] ISO/IEC 13335-1:2004, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and Communications technology security management

Author Biographies

COR VERKOELEN is an Information security scientist who graduated in 2000 in the area of 'Telecommunication and Informatics' at the Netherlands. Subsequently he joined TNO Defence and Security specializing in the area of information security. He started his career by doing research on penetration testing and defences against digital attacks by following new emerging technologies. Later he included the architectural and business side of information security and became an all-round security

scientist. Since 2006 Mr. Verkoelen is involved in several research projects (technical as well as at organizational level) that cover the problems around the interconnection of information systems. In line with this background he started the research on possible solutions within the simulation environment which he feels copes with the same problems as other information systems seen from a security point of view.

ROEL WYMENGA graduated from at the polytechnic college Rotterdam and joined TNO Defence, Security and Safety in The Hague, The Netherlands in 2000 as a research engineer. One of his research topics is securing wide area research networks used for simulations and other distributed experiments.