Certification for Simulation Interoperability: Where we are and where could we go?

Tom Gray, Jonathan Denny, Suranga Wickramasekera, Pitch Technologies Ltd
5 Upper Montagu Street
London W1H 2AG
tom.gray@pitchtechnologies.com

Björn Löfstrand, Pitch Technologies AB
Repslagaregatan 25
582 22 Linköping
Sweden
bjorn.lofstrand@pitchtechnologies.com

Keywords:
Interoperability, Certification, Re-use, Standards

ABSTRACT: *The current "language" used for describing simulation interoperability, for example DIS, HLA and RPR FOM, has provided a good base of understanding between simulations, but it does not always achieve the desired outcomes. For example, an HLA Evolved federate that is "RPR FOM v2.0 compliant" does not necessarily mean it is fully interoperable with another "RPR FOM v2.0 compliant" federate if they are providing simulations for different parts of the object model, or interpret the information within the objects differently.*

To achieve meaningful interoperability and develop a market of truly reusable simulation components, this "language" needs to evolve to a next level. In many other domains, this evolution is often achieved through the usage of a concept such as "capability certification". This paper will explore why this evolution in interoperability language is required in the simulation domain, what we can learn from other industries, the current state of play around simulation use cases - such as NATO's HLA Certification process and the associated Integration, Verification and Certification Tool, and SISO's Simulation Interoperability Readiness Levels concept - and how they could be taken further by standards groups, industry and governments.

Getting interoperability right through the usage of de-facto standards certification will further increase the opportunities to re-use simulation components. This could open the door to more advanced federations of simulations by allowing developers to concentrate on how they can best exploit models from other best of breed simulation components, rather than continuously adapting or integrating their applications to work with different interpretations of standards. Certification offers improved reuse and savings for the developer, integrator and ultimately the end user both in the short term and the long term evolution of capabilities.

1. Introduction

More and more we see "Standards Profiles" are being introduced within defense departments to mandate the use of standards for simulation systems. The profiles are intended, in the short term, to aid the development of simulation systems and in the long term to promote greater re-use of simulation components. Thinking towards the future as larger or more sophisticated simulation systems are required, it won't be feasible (or optimal) for one vendor to create and own the entire system. Instead specialist vendors will produce specialist simulation components that must be able to interoperate with others in a large system. Due to these demands of modern simulation systems, defining a set of standards is an important first step to allow the components to talk to each other. However, these profiles often still contain ambiguity, such as the exact standard to use where multiple applicable standards exist and have been included, or how exactly to apply them. This results in a market where simulation systems and components can adhere to standards, but are not always interoperable, meaning the benefits of standardization are not fully realized. Through research and development activities, both at national and international levels, a number of concepts have been proposed to address some of these challenges, such as the standardized Interoperability Requirements and Capability Badges concept for simulation interoperability. Recently, NATO activities have resulted in the establishment of a certification process for verifying simulation component compliance with the HLA interoperability standard.

This paper presents knowledge and experiences gained from testing some of the theorized processes and applications for simulation certification. This is followed by proposals for how these concepts should be taken further if interoperability and re-use are to be maximized.

1.1 HLA and Federation Object Models

For the purpose of discussion within this paper, the HLA (High Level Architecture) standard for modelling and simulation interoperability was chosen**.** HLA is a generic and domain independent standard for simulation interoperability. It provides a standardized set of services through a Run Time Infrastructure (RTI), including information exchange, data distribution management, ownership, synchronization and federation management. One prominent feature of HLA is that it facilitates the development of information models, called Federation Object Models (FOM), for any simulation domain. A FOM describes the shared objects and interactions that are exchanged in a distributed simulation. A FOM can be provided as modules for better separation of concern, and to better support development by different teams. There are standardized FOMs, often known as reference FOMs, that can be extended using project specific FOM modules. Two examples of prominent reference FOMs within defense training and simulation are SISO's Real-time Platform Reference FOM (RPR FOM) and NATO's Education and Training Network FOM (NETN-FOM).

2. Current state of interoperability certification in simulation

2.1 What are the challenges?

Interoperability can be defined at several levels, as described in the Levels of Conceptual Interoperability Model (LCIM) [1]:

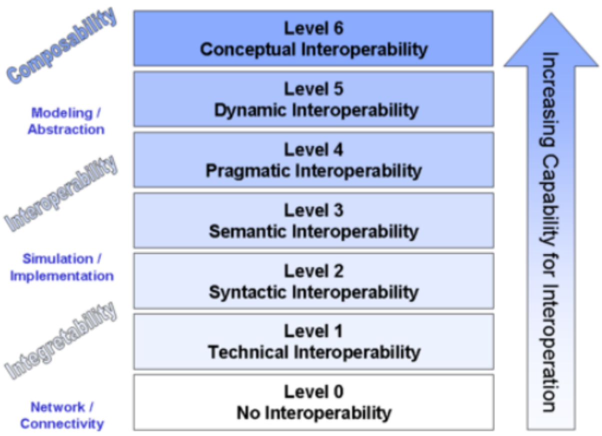

Figure 1 - Interoperability classification models

It is generally accepted that Technical Interoperability (Level 1) is no longer a fundamental problem as standards for communication infrastructures – that allow components to exchange the basic bits and bytes - are widely adopted and stable. However, higher level interoperability is still considered a major challenge in establishing reliable and trusted federations of simulations.

Syntactic Interoperability challenges can arise when components do not agree a common structure to exchange information. While interoperability standards exist within defense to alleviate these challenges, such as SISO's HLA / RPR-FOM standards and NATO's NETN FOM, mismatches in FOM definitions due to custom vendor-specific implementations or use of different versions still occur, and are often not fully identified until integration stages of the program lifecycle when the disparate components are brought together for the first time.

Similarly, issues associated with Semantic Interoperability are usually encountered during the integration stages, where it is discovered that components are able to exchange information effectively, but have derived different meanings of the data. For example, a common issue occurs when exchanging entity type identifiers in RPR FOM. One component may publish the identifier believing an entity to be a main battle tank, while another may receive the same identifier and understand it to be a civilian car. Again, there are interoperability standards to address these issues, but the compliance to these standards is left to the component developer and only manually verified by their own test tools. The result is that the developers and the integrator spending valuable time configuring (or worse, fixing) simulation components during system integration.

While the Levels of Conceptual Interoperability Model has been widely spread and used in the modelling and simulation community to express simulation interoperability, it has not been used to classify individual simulation components and/or systems. In fact, a simulation often exhibits several different levels of interoperability at the same time, as well as in different contexts. A component may be highly interoperable in one federation but much less interoperable in another, depending on the federation requirements. Making a homogenous system interoperable is much easier than integrating heterogeneous components. Defining interoperability requirements related to interacting with an existing system is much easier than defining interoperability requirements for a conceptual federation design, which in turn can be more concrete than general architecture requirements.

Interoperability requirements are defined all the time when designing and developing distributed simulation systems, but very rarely are they written in a way that they can fully achieve the actual intentions behind the requirement, or can be effectively re-used between systems. For example, an interoperability requirement will state that "a component needs to be HLA 1516-2010 compliant", but in reality what does this actually mean? Does the component need to implement and support all of the HLA services, even if they are not applicable to the federation being designed? What information model should be used? A further requirement could state that the RPR-FOM information model must be used, but again further questions arise. Should the component support the entire RPR-FOM, and if not, which parts should be used? What semantic information is required? For example, how should damage state be calculated or which entity type identifiers are used? Often these requirements are resolved based on a simulation component vendor's interpretation of the requirement, leading to potential disagreements with customers on whether the requirement has been met or not – which usually occur late into the development lifecycle, perhaps the reasons why are the subject of a different paper! - or by using project-specific decisions resulting in a system of components that are interoperable for the individual federation being put together, but each component may not be interoperable on another and require additional integration effort.

In order to design and build interoperable systems with truly re-usable components, specifying a component's role in a design and their specific interoperability requirements is key. Alongside the definition of interoperability requirements is the ability to identify components that are achieving those requirements. As explored above, a component may state that it is "HLA compliant", but what does that actually mean within the context of the federation being designed? Mechanisms for discovery and identification of reusable simulation components for federations require them to be characterized not only in terms of function, but also in terms of their capability of being interoperable.

Finally, verification of interoperability requirements is often performed in isolation by each simulation component vendor, according to their own interpretations, and then again later during system integration activities by the integrator. Performing verification in this way, as explored previously, usually results in issues being discovered during the later integration stages, and as most systems engineers and project managers would attest, are more expensive to resolve. Generally, each system development and component developer will generate their own test tools or framework for verifying requirements, which may or may not include interoperability testing. The main reason for this is that standardized and trusted verification tools or processes are still lacking within the defense simulation domain.

While developing interoperable simulation components and connecting them together in federated simulation systems is now much less complex due to the wide spread adoption of modern open international interoperability standards, meaningful integration and re-use is still challenging. Standards profiles for Modeling and Simulation systems, such as the UK's Defense Modeling and Simulation Coherence (DMaSC) Modeling and Simulation Profile (DMSP) [2] and NATO's Allied Modeling and Simulation Publication (AMSP) 01 [3], have specified the basic common "language" to describe interoperability, however an evolution of the "language", through the use of standardized interoperability requirements, capability badges and certification tools / processes, is required to start fully reaping the benefits of standardization.

2.2 Known research and activities

Over the last decade there has been active research on solutions to above challenges. Firstly, the concept of Capability Badges started in the UK through the DSTL CDE and SE Tower research programs and was later taken on and developed further by NATO MSGs 134, 163 and currently 191.

Capability Badges

The Capability Badge approach is based on the verification of compliance to predefined sets of Interoperability Requirements. A component that completes successful verification testing against a set of Interoperability Requirements achieves a Capability Badge as a token of compliance.

The general approach for Capability Badges is analogous to other interoperability approaches within the technology industry, such as: "HD Ready", "Works with Alexa". Organizations that perform and maintain interoperability certification activities in consumer markets advertise the key benefits of "Capability Badges" as:

- Shows customers that your product will work
- Clear & independent proof of interoperability
- Lowers barriers to market entry by providing access to the vast technology ecosystem
- Confirm product's interoperability via testing from experienced professionals

Capability Badges can also be found in other areas of society to express achievements, levels of knowledge, experience and skills. The scouts have badges to indicate abilities related to hiking and camping e.g. making fires and building shelters. Most online computer games have reward and capability badges to express skill and level of gameplay. Military service stripes and medal ribbons express grade, corps, function and experience. The use of these "badges" varies but includes specification of required capabilities, identification of suitable candidates and marketing. They are often presented as tokens of achievement that individuals or organizations strive to obtain.

Capability badges are primarily intended to support system design, test and integration but are also proven to be useful when defining system interoperability requirements.

When compared to existing Standards Profiles, the concept of Capability Badges is designed to provide a more fine-grained description of a system or component's capabilities to be interoperable in a given context. For example, there may be a Capability Badge that describes a component adheres to a set of standardized Entity Type Identifiers (i.e. derived from the SISO-REF-010 standard). Components with this badge are instantly identifiable as compliant and interoperable in that context, and would not require further integration or testing i.e. plug and play.

NATO MSG-134 developed 11 Capability Badges, which encapsulated 146 Interoperability Requirements. The interoperability requirements were mainly focused around the idea of ensuring interoperability against the HLA standard. MSG-134 also initiated work on developing tools to support the integration, verification and compliance testing of simulation systems against common interoperability requirements.

MSG-163 continued the work by refining how the Interoperability Requirements could be verified, and culminated in developing tooling (IVCT) and processes around HLA component certification (NATO HLA Certification Service).

NATO Integration, Verification and Certification Tool (IVCT)

The IVCT is designed to test an individual simulation component's interoperability capabilities, as well as support integration activities of distributed simulations. The IVCT is currently focused on testing and verification of simulation components / systems using HLA. This paper will not provide a detailed overview of the tool, however, extensive resources on the tool are available [4][5][6].

The IVCT is a framework for running Executable Test Cases to verify interoperability requirements. It is Open Source, maintained on GitHub and specific versions of the tool are accredited for use in NATO's HLA Certification Service together with accredited Executable Test Cases. It is currently provided with a small number of Executable Test Suites (collections of Executable Test Cases) that can be used to test and verify HLA federates. As indicated by the IVCT documentation, there is also a number of planned and under development test suites, however it is understood that progress on these is slow or has been paused, while work on better interoperability requirements is continued in MSG-191.

NATO HLA Certification Service

One of the main objectives of NATO's MSG-163 was to develop the NATO HLA Certification Service. The service is a solution that NATO identified to overcome the challenges faced when establishing a reliable and trusted federations of distributed interoperable simulations.

The following figure illustrates the key roles and the most relevant information they exchange:

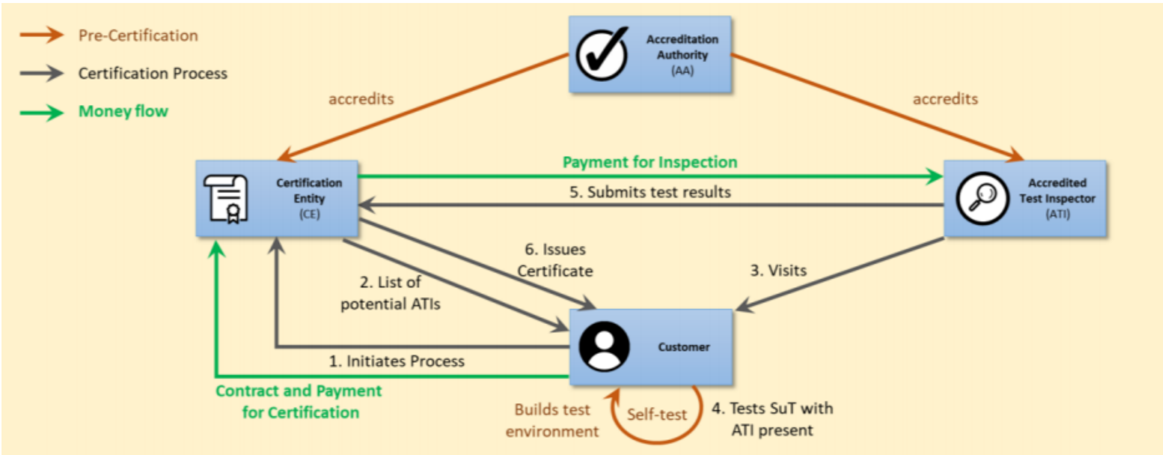

Figure 2 – Key roles of the NATO Test and Certification Service [4]

A brief description of the process is as follows: Before initiating the process of certification, the customer should perform a self-test of its System Under Test (SuT). The customer can download (or access an instance of) the IVCT and executable tests cases for interoperability requirements relevant to the Capability Badges to be certified. After being satisfied that the system can successfully be verified, the customer contacts the Certification Entity to initiate the certification process. As part of the initiation, the customer provides information about the system to be tested and which Capability Badges to verify in the form of a Conformance Statement. The Certification Entity provides a list of available accredited test inspectors to the customer and a visit is planned between the customer and the selected Accredited Test Inspector. During the visit the Accredited Test Inspector together with the customer performs tests using accredited versions of IVCT and executable test cases. The result of testing is forwarded by the Accredited Test Inspector to the Certification Entity. If testing is successful and accepted by the Certification Entity, a certificate is issued to the customer.

In the proposed business model, the customer establishes a contract with the Certification Entity for the payment of the certification. The Accredited Test Inspector is tasked and paid by the Certification Entity for work related to the certification. This means the Accredited Test Inspector is acting as an agent for the Certification Entity and not for the customer.

NATO MSG-191

While the IVCT and HLA Certification process are two key elements, what is ultimately lacking currently are good interoperability requirements. As such, NATO MSG-191 will undertake this task to develop interoperability requirements than can be used as the basis for design and acceptance across training systems. At the time of writing, the group is in early planning stages, but it is believed both functional and non-functional requirements could be considered – for example, requirements to support composition, start-up or containerization in methodologies such as Modelling and Simulation as a Service (MSaaS).

SISO Simulation Interoperability Readiness Levels (SIRL)

The SISO Product Development Group has been developing a methodology to objectively measure interoperability between two simulations using engineering artefacts [7]. These metrics would contribute to easing the integration of a distributed simulation and can make the integration more mechanical and less prone to error-based discovery. In general, it builds upon existing standard processes (Distributed Simulation Engineering and Execution Process (DSEEP)) and artefacts (Federation Engineering Agreements Template (FEAT)) to identify and reduce integration issues as early as possible into the development process.

At the time of writing this paper, the group is in the process of producing a draft standard before making a decision on balloting.

One observation is that Interoperability Requirements and Capability Badges would be a prime input into the SIRL process, as they would provide clear evidence of whether a simulation component is meeting the engineering evidence criteria for a particular level - and could drive the creation of further criteria. This would be particularly applicable for the “modeling” and “simulation control” levels.

3. Certification in other industries

Certification for interoperability is not a concept unique to modeling and simulation. There are many examples of the process applied across the technology sector, addressing interoperability at different levels. As part of writing this paper, we researched a number of certification processes and have highlighted a sample of certification processes including their key features, the model they use and the benefits to their stakeholders.

3.1 Premium HDMI Cable Certification

Premium HDMI Cable Certification [8] addresses interoperability at the Technical Level. All manufacturers that want to provide Premium High Speed HDMI® cables must have them tested to ensure quality for feature-rich 4K/Ultra-HD content. The program is designed to give end users confidence when purchasing new HDMI® cables for their 4K/UltraHD products.

Cables / connectors tested at HDMI Authorized test centers and regular audits of already certified manufacturers are also required.

3.2 Kubernetes Certification

Certification of the Kubernetes System / API [9] addresses interoperability at the Syntactic Level. Kubernetes is an open-source container orchestration system for automating software deployment, scaling, and management, providing a number of services and APIs to do so. This allows many vendors to implement their own Kubernetes-based offering, while allowing consumers the flexibility to choose and move between them. Most of the world’s leading enterprise software vendors and cloud computing providers (e.g. AWS, Azure, Google) have Certified Kubernetes offerings.

The Cloud Native Computing Foundation (CNCF) maintains the standard and provides the free online certification service. All major providers of Kubernetes installations are represented within the CNCF, both as part of the standards working group and on the governing body.

The certification service is comprised of automated conformance tests that vendor Kubernetes applications can be tested and verified against. Upon being conformant, a Kubernetes installation is provided permission to display the

"Certified Kubernetes" logo (or badge) and is listed on the CNCF website. A certified Kubernetes installation provides consumers with confidence that their chosen vendor will work as intended, but the certification process also provides a known playing field for vendors, where they can innovate within the standard and confidently test their solutions against.

3.3 Matter Smart Home Connectivity Certification

Matter is an emerging standard for smart home devices and hubs, led by Connectivity Standards Alliance. Again, the working group is represented by all major players in the smart home market (e.g. Amazon, Google, Apple, Huawei, Signify) and more, with the goal of creating a standard that provides confidence and flexibility to consumers of smart home devices, while allowing vendors to compete and innovate within an agreed set of rules. The Matter standard will provide interoperability between smart home devices and hubs at the Technical, Syntactic and Semantic level.

While the standard is yet to be finalized, a certification program is also being developed in parallel. This demonstrates that reference implementations, testing tools and certification tools are thought about at the standards development stage, by the experts: the standard developers, and not as an afterthought. This process appears to be common across other standards development in technology as well.

3.4 Comparisons with development of interoperability standards for modeling and simulation

One observation when comparing the researched certification processes and modeling and simulation community is the size of the end user base. Each of the technologies highlighted above are used (or will be used) in millions of instances across the world. Therefore, they inherently contain a lot of value, and it is in the best interest of the vendors to have access to as much of the market as possible. It is clear that vendors have identified that attempting to lock customers into their eco-system is not always in their best interest, as it could end up freezing out a large portion of the market. In all cases a very well represented industry consortium has come together to invest not only in the development of the standard, but also the certification and tooling around it.

The modeling and simulation user base is (currently) a lot smaller than the technologies identified above, however the costs of solutions are often much greater than in the consumer markets. Arguably, this makes it even more important that vendors have access to the widest market possible. Also the exploitation of modeling and simulation is on a growth trend with the advent of the "Metaverse" and sharp increase in interest in Digital Twins. Therefore, involvement and investment in standards and certification is very much worthwhile for the industry and the defense customer.

4. What could be done?

While the concept of certification for simulation interoperability may have grand aims, the initial recommendation would be to start small and achieve something meaningful.

NATO's work on simulation interoperability requirements is an excellent starting point for future training system requirements. For customers, using standardized interoperability requirements will give confidence that they will receive what they are asking for and will improve the extensibility of their system. The concept of Capability Badges would extend this further by making it easier to identify and compare products that meet certain interoperability requirements. For vendors, adhering to the requirements will mean a common interoperability implementation for their products across project deployments, allowing them to concentrate on their true value differentiators – innovation within the product itself.

As the adoption of interoperability requirements becomes more widespread, not only would it improve the design and specification of the training systems and their components, it would also provide opportunity to tools vendors to develop standards-based applications for test and verification.

Ideally interoperability requirements would be written when a standard is created, or new features are added to an existing standard, as per the examples in the wider technology industry. At the very least, a suggestion is that existing standards groups, for example RPR FOM, could write interoperability requirements – using the examples development by NATO so far - for key features to ensure they will be implemented as intended. Within SISO, this activity could form part of a Product Support Group's role.

When looking at certification models that could be adopted within modeling and simulation, it is likely that meaningful results would be achieved by first starting at the national or project level where interoperability is key (for example, large scale national distributed training simulations). Concepts could then be shared between nations or organizations before looking towards an international approach (if required). Investment into the certification process and tooling would indicate a level of buy-in and credibility that will help adoption. Investment could either be driven directly from national authorities themselves, or as is the case in other sectors, come from industry collaborating in a consortium with the goal to create a known playing field that all can access.

A further concept that fits loosely around the verification of interoperability requirements is the idea of a “trusted federate”. Very often during development of a distributed simulation component, a developer will want to test whether the data they are sending or can receive and process is correct. This would usually be performed by developing their own tool, or testing against “some other” federate. Instead, a number of simple federates could be implemented that adhere to standards that perform simple verification tasks, for example: publish a RPR FOM Aircraft entity with pre-defined spatial information that includes all appearance, capabilities and articulations, or a federate that receives RPR FOM entities are displays their values. Again, to improve credibility and adoption these federates should be made freely available and authorized by the relevant standards organization (and could even be developed as part of standards organizations).

5. Conclusions

It has been proven in other industries that the certification approach reduces barriers to achieving interoperability between systems. While vast steps to increase simulation interoperability have been made in the last two decades by using established open standards, higher level interoperability is not always achieved and often still involves high costs and risks during integration. As explored in this paper, simulation component certification will have a big impact in improving interoperability between and within training systems, reducing risks and providing highly advanced cost effective solutions to customers.

The use of standardized interoperability requirements will allow simulation component providers to know exactly what needs to be developed. A certified tool (or number of tools) that verify requirements could also be provided to suppliers as a mechanism to increase confidence before integration activities. Looking out to the wider technology industry, there is an argument to suggest that these tools should be created and maintained by our standards organizations, through the mechanism of an industry consortium, to provide trust and validation that interoperability is the primary goal.

Using verified capability badges, that group interoperability requirements, as part of the design process will have the benefit that future simulation systems will be designed with interoperability in mind. This would lead to cheaper system upgrades, a competitive marketplace (leading to more innovation), and could reduce the amount of discarded effort when systems have not been sufficiently designed to be extensible or interoperable.

System Integrators would easily be able to identify candidate simulation components for their systems by analyzing standardized interoperability requirements and identifying simulations components that have been awarded the relevant badge. Targeted introduction of new Capability Badges at an international or national level could also focus the simulation market on desirable interoperability requirements, for example adoption of a new standards such as UCATT FOM or a technique such as aggregation / de-aggregation of units for modelling.

Certification would also offer a number of benefits to the industry. Having access to standardized interoperability requirements and trusted verification tools will improve product interoperability, performance and reliability when operating in different federations. Once interoperability requirements have been satisfied (and certified) once for a product, there will be lower test and integration costs going forward. This means more time can be spent on the real value drivers for products. As identified when researching certification use cases in the wider technology industry, a known playing field that all industry has collaborated to construct will offer access to a wider market, both within the defense enterprise and potentially worldwide. As well as providing components, the use of certified interoperability requirements will also allow vendors to easily identify other complimentary 3rd party products and services to supplement their offering, while at the same time improving relations with other suppliers. Finally, it is not coincidence that technology’s biggest companies are actively involved in standardization and certification across their relevant domains. They are therefore seen as collaborative, open and forward thinking. Smaller vendors involved in the same process have the opportunity to improve their brand recognition by being involved in de-facto standards.

Ultimately, an important first step has been taken by many nations to reap the benefits of standardization in modelling and simulation, by creating modelling and simulation standards profiles. This has enabled a basic common "language" to be understood when describing interoperability requirements in systems, but significant effort is still required to achieve the intended goal. An evolution of the "language of interoperability" is required to provide higher level, reusable interoperability in simulation systems, and it is strongly believed that certification for simulation interoperability will provide it. Capability cadges and interoperability requirements would be an important tool for assuring interoperability standards during capability design, development and delivery so that the long-term goals of enterprise-wide coherence, reuse and value for money for training and simulation systems are realized.

References

[1] Tolk, A. and Muguira, J.A. (2003). The Levels of Conceptual Interoperability Model (LCIM). Proceedings IEEE Fall Simulation Interoperability Workshop, IEEE CS Press
[2] UK DMaSC Modelling and simulation standards profile (DMSP) (https://www.gov.uk/government/publications/modelling-and-simulation-standards-profile)
[3] NATO Allied Modelling and Simulation Profile 01 (AMSP-01) (https://nmsg.sto.nato.int/amsp/amsp01)
[4] NATO Modelling and Simulation Centre of Excellence Page (https://www.mscoe.org/nato-hla-certification-home/)
[5] IVCT Video introduction / tutorial (https://www.youtube.com/watch?v=FfBW5oVnYv0)
[6] IVCT Source code on GitHub (https://github.com/IVCTool)
[7] SISO-REF-076-2020-draft Reference for FEAT PSG Simulation Interoperability Readiness Levels – 22nd September 2020
[8] Premium HDMI® Cable Certification Program (https://www.hdmi.org/spec/premiumcable)
[9] Kubernetes Certification by CNCF (Cloud Native Computing Foundation) (https://www.cncf.io/certification/software-conformance/)

Author Biographies

TOM GRAY is a Senior Software Developer at Pitch with more than ten years of experience in design, development, integration and acceptance of simulation systems for UK and international customers. Tom is currently an active member of SISO's RPR FOM Product Development Group. He studied B.Eng. Electrical and Electronics Engineering at the University of Surrey, England.

JONATHAN DENNY is a Software Developer at Pitch Technologies UK with eight years of experience in the simulation industry. Jonathan has worked with CGF and Link 16 applications and has an interest in enabling simulation connectivity. Jonathan has a B.Sc (Hons) Computer Science at the University of the West of England.

SURANGA WICKRAMASEKERA is a Business Development Manager at Pitch Technologies UK. Suranga has 20 plus years of experience within the aerospace and defense industry in developing modelling and simulation solutions, initially for commercial aviation training, and now specializing in distributed simulation systems for Defense, Space and other sectors. Suranga studied Linux based Software Engineering for Flight Simulation for his MSc at University of Brighton, and Aerospace Technology for his BEng at Kingston University in the UK.

BJÖRN LÖFSTRAND is a senior systems architect and vice president at Pitch Technologies. Mr. Löfstrand provide support to various organizations in their transformation of simulation-based training systems to meet current and future interoperability requirements. Mr. Löfstrand also engage in NATO and international M&S standards development activities to evolve and develop standards that allow smart design of simulation systems. He has been engaged in M&S standardization activities for over 20 years participating in the development of standards like High-Level Architecture and engaging in NATO S&T projects including MSG-134, MSG-163 and MSG-191. Mr. Löfstrand has a M.Sc. in Computer Science from the University of Linköping Sweden.