# PULSEbox: A High Fidelity, Integrated, GFI-Based Threat Scene Generator

**Peter Grossman, Julien Pierru**
**Systems Engineering Group, Inc.**
**Columbia, MD**
**Peter.grossman@segmail.com, Julien.pierru@segmail.com**

## ABSTRACT

All aspects of threat mitigation defense systems engineering rely on simulated scenes that influence the overall design, details, and performance evaluation of algorithms, hardware, and system doctrine. Systems developed using simplified design data that does not include real-world observables risk brittle performance in the real world; however, the acquisition and integration of complete and accurate threat data and simulations can be cost-prohibitive and error-prone. A solution has been developed that hosts a wide range of high-fidelity government-furnished scene-generation software into a network-based scene generator called PULSEbox that produces government-certified scene data. PULSEbox is a groundbreaking tool with applications across the entire defense community from threat characterization, to weapon system design, to weapon system performance testing and evaluation, and warfighter training.

This document will summarize the underlying Government Furnished Information (GFI) threat data and Modeling and Simulation (M&S) software suite that is provided to the Missile Defense Agency (MDA) elements and their contractors to support development of defensive systems. The document will detail the complexities of integrating the entire GFI threat scene into user simulation and Hardware-in-the-Loop (HWIL) environments and demonstrate the efficiencies gained through the use of an integrated Hardware/Software solution, followed by a discussion of PULSEbox which is designed to simplify these complexities by taking on most of the software integration and configuration management of the threat data in a way that is transparent to the user. The document will then discuss the operation of PULSEbox showing the user interface and highlighting its flexibility. The final section will discuss future PULSEbox capabilities.

## ABOUT THE AUTHORS

**Peter Grossman** is an aerospace engineer with 12 years of experience supporting the Navy and Missile Defense agency performing threat missile modeling and analysis of various types including trajectory modeling and debris and reentry phenomenology. Peter obtained his B.S. and M.S. in aerospace engineering from Virginia Tech in May 2005 and December 2006 respectively where he conducted graduate research on wind tunnel testing of scramjet fuel injectors. He has also consulted with a Major League Baseball team to perform modeling and simulation of baseball pitch dynamics.

**Julien Pierru** is an aerospace and software engineer with 10 years of experience developing high fidelity simulations for the Navy and the Missile Defense Agency. Julien Pierru is a member of the National Training and Simulation Association (NTSA) as well as Simulation Interoperability Standards Organization (SISO). Julien obtained his B.S. and M.S. in aerospace engineering from Virginia Tech in June 2003 and May 2005 respectively where he conducted graduate research on spacecraft electric propulsion with particle in cell plasma electrostatic simulation on high performance clusters. Julien is the manager of the Modeling and Simulation Development Branch at SEG.

# PULSEbox: A High Fidelity, Integrated, GFI-Based Threat Scene Generator

**Peter Grossman, Julien Pierru**
**Systems Engineering Group, Inc.**
**Columbia, MD**
**Peter.grossman@segmail.com, Julien.pierru@segmail.com**

## THREAT SCENE MODELING AND SIMULATION

The Integrated Air and Missile Defense (IAMD) environment (Figure 1) is a highly complex scene that can be difficult to model efficiently and accurately. In addition to continuously evolving threat capabilities, there is also a wide range of phenomena that all must be represented accurately to provide a complete representation to sensors with evolving capabilities. Due to the cost prohibitive nature of live fire testing, the defense community relies heavily on simulated threat data for weapon system design, validation and testing. Thus, the quality and accuracy and completeness of these threat representations has a direct impact on the overall effectiveness and robustness of weapon system hardware, algorithms and doctrine.

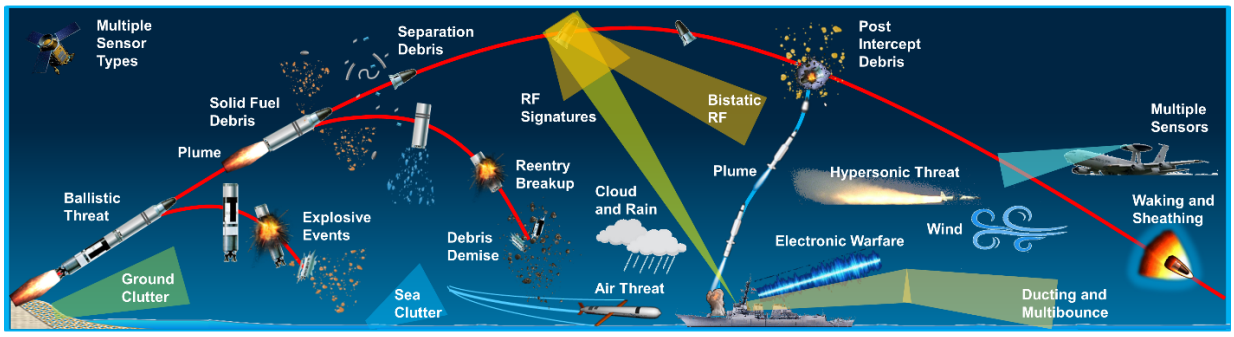


**Figure 1: The IAMD Threat Scene**

### GFI Modeling Tools and Techniques

Using MDA Aegis Ballistic Missile Defense (BMD) as an example, Figure 2 illustrates the legacy approach to Government Furnished Information (GFI) threat data and Modeling and Simulations (M&S) used in the development of weapon system baselines. The threat scene represented by the M&S suite includes: Principal Object (PO) trajectories (Systems Engineering Group, Inc., 2017), Radar Frequency (RF) signature (Systems Engineering Group, Inc., 2015), and Infrared (IR) signature data (Johns Hopkins Applied Physics Lab, 2010), as well as Frame Correlation information (Systems Engineering Group, Inc., 2010) which align the signatures to the trajectory data; Debris representations which are provided as inputs to an M&S tool called DebrisSim (Systems Engineering Group, Inc., 2015) which produces real-time correlated RF, IR, and trajectory data; and other phenomenology such as Corporate Clutter (Systems Engineering Group, Inc., 2017), Wake (Systems Engineering Group, Inc., 2015), and Plume Signatures. This process can be cost-prohibitive and error-prone because each organization making use of the threat data and/or M&S suite has to go through their own process of integration and configuration management. Not only does this result in additional cost due to the redundancy of potentially dozens of organizations all performing the same task as each other multiple times, but it also introduces risk of inconsistencies across a program resulting from different organizations implementing the GFI scene differently. The results of inconsistencies across a user base can be devastating to the success of a program. Additionally, each time any component of the GFI M&S suite is updated, each user organization must go through an integration process again for the updated software which adds unnecessary additional cost and scope to a program.

In addition to the technical risk incurred during weapon system design and development, the approach to testing and certifying a weapon system introduces even more technical risk as lower-fidelity faster-running threat-scene tools and

data are used during hardware in the loop (HWIL), digital tests (DT), operation tests (OT) and certification. The risk using data with little relation (pedigree) with the high fidelity design data has two impacts. First, the real system is not being tested in an operationally-representative scenario reducing overall confidence; second, any reproducing deficiencies in the high fidelity models can be problematic as the underlying scene data is different.

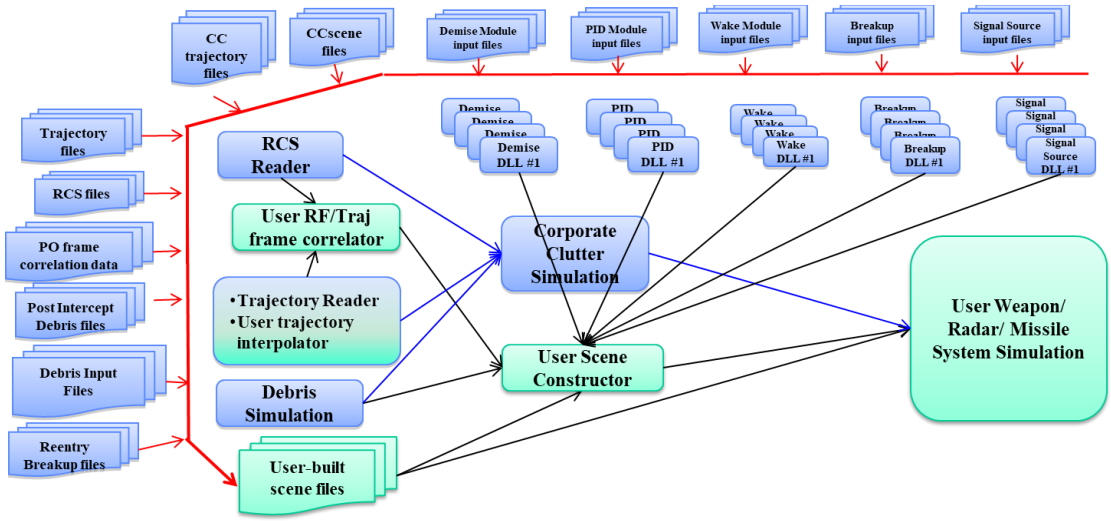


**Figure 2: The Complex GFI M&S Environment**

Over the last several years, a new software architecture has been developed (Figure 3) that integrates the disparate parts of the M&S tool suite into a framework called PULSE (Systems Engineering Group, Inc., 2017) with a single stable interface. Each facet of the IAMD threat scene is modeled by a module within the PULSE architecture and all of the integration and interaction between the modules is performed once at SEG by the Subject Matter Experts (SME) and software developers of the M&S tools mitigating the risk and cost associated with the legacy approach. PULSE is also designed with an open architecture which allows third party developers to create their own modules that can be integrated into the PULSE framework to better support the wide range of applications across the defense community. Because the PULSE input files (Systems Engineering Group, Inc., 2017) explicitly define the correlation between all of the threat data and inputs to the PULSE modules, there is also significantly less burden on the users of the GFI threat representations to configuration manage the file systems that contain the threat data.

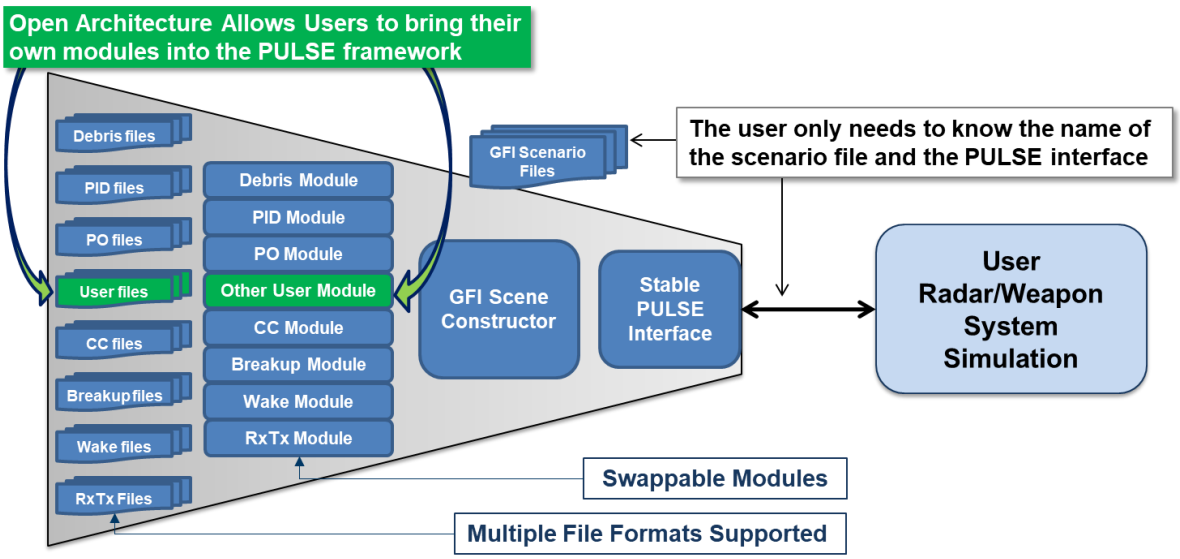


**Figure 3: Integrated M&S Software**

## INTEGRATED SCENE GENERATION SYSTEM

While the integrated M&S tool suite solves some of the complications associated with comprehensive high-fidelity threat scene models, there still remain the problems of configuration management and ease of access to the underlying threat data and M&S inputs that define each threat, as well as problems of barrier to entry, computing hardware uncertainty, and threat representation consistency due to different performance requirements at different stages of the systems engineering life cycle. Finally, the integrated tools suite does not, by itself, solve the problem of testing and certifying weapon systems with high fidelity data.

In addition to the complexity of the tools, the vastness of complete threat ecosystem represents a large barrier to entry for small businesses and other organizations with limited resources and infrastructure. For example, the full threat space that represent the design requirements for the Aegis BMD Build 6 (Systems Engineering Group, Inc., 2017) cover 15 years of data development and are represented by more than 400,000 individual data files comprising more than 1 TB of data. Additionally, supporting a broad set of users' computing infrastructures requires sub-optimizing the simulation to run on any operating system (Windows, Linux, etc.) with any hardware configuration (single core/multi-core CPUs, GPUs, FPGAs, etc.). Thus, the M&S tools will never run at optimal speed or efficiency.

### Efficiencies and Advantages Gained Through Tool Suite Integration

An integrated hardware/software solution presents a solution to the above challenges by allowing the software to be optimized to the exact hardware and operating systems that will host them. This solution also allows the threat scene and M&S suite to be hosted centrally while granting access remotely to a large group of user organizations. Software integration and upgrading are additionally simplified through the use of an integrated hardware solution by eliminating the need for each user organization to integrate new software and regression-test their simulation each time any component is updated because in an integrated system, the external interface remains the same even when underlying components are upgraded or added. By taking on the integration and configuration management in the development of PULSEbox, only one organization is performing the integration and configuration management step a single time which significantly reduces the cost of redundancy and eliminates the risk of multiple organizations implementing the threat scene differently resulting in errors. Thus, while there is still a small amount of work to be done due to the need for performance impacts resulting from an upgrade to one of the underlying M&S tools, the majority of the cost and schedule impact resulting from software integration/recompile and version management is eliminated through this type of deployment.

The efficiency of the integrated threat scene generator can still be realized without the hardware optimization component through the use of a virtual or installation deployment of the fully integrated tool-set for users who cannot accept third party hardware into their infrastructure. The virtual or software only deployment will still provide all the same advantages other than some of the performance improvements associated with a full hardware optimization. Because Virtual and Software Only deployments use the same web-based interface, the need for integration into the user simulations or re-compile is still eliminated even though the tools are residing on the users' hardware infrastructure.

Finally, a fully integrated M&S tool suite is required to support fully on-the-fly threat simulation. Because many of the phenomena associated with the representation of the threat system are highly interdependent (e.g. RF signatures, kinematic state, and debris generation), a disparate set of M&S tools requires much of the data to be generated a priori and then correlated. In order for these interdependent phenomena to be modeled live, the various M&S tools must be fully integrated and able to communicate information across each other. Without the ability to generate on-the-fly threat simulation, there can be no capability to represent reactive threats or coordination of threats. Additionally, if all threat data is characterized offline and distributed to users, there is no opportunity to perform a blind test in simulation because the test material is all available from the start.

**Threat Data Accessibility and Resources**

PULSEbox (Figure 4) represents this fully integrated GFI threat scene solution. PULSEbox can be integrated with multiple simulations in an interoperable test and analysis ecosystem and provides a simple "one-stop" solution to threat scene integration which takes the onus off of the user organizations of the complex process of integration and configuration management by providing a pre-integrated piece of hardware or virtualized software that contains a database of all threat data and fully integrated M&S suite. Additionally, PULSEbox contains pre- and post-simulation analysis tools further increasing the usability of the threat models and increasing the potential user base.

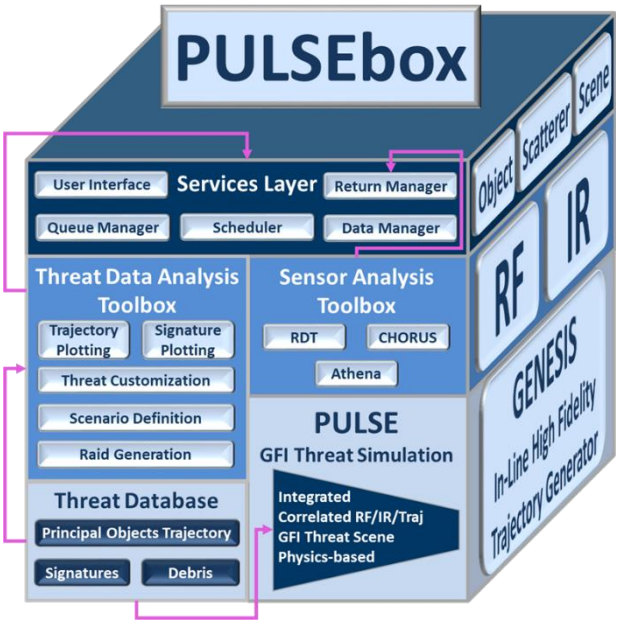


**Figure 4: PULSEbox Integrated Scene Generator**

The PULSEbox threat database is accessed through a Graphical User Interface (GUI) which allows users to browse all available threat models and create a scenario at instantiation (Figure 5). The GUI interface and database also allow users to create Raid scenarios directly by selecting multiple instantiations of the same or diverse threats and even apply launch timing offsets. PULSEbox supports pre-scenario visualization of the trajectories as well as analysis of the debris scene and RF signature representations. The scope of the scenarios can be tuned up or down to support different analysis/performance requirements through the GUI. For example, principal objects can be excluded from the scene, and individual pieces or entire groups of debris can be excluded in order to reduce the total number of objects the simulation propagates. These user modified scenarios are saved and configuration managed separately from the official GFI that comes pre-loaded on the database to avoid unintentional corruption of the official threat representations.

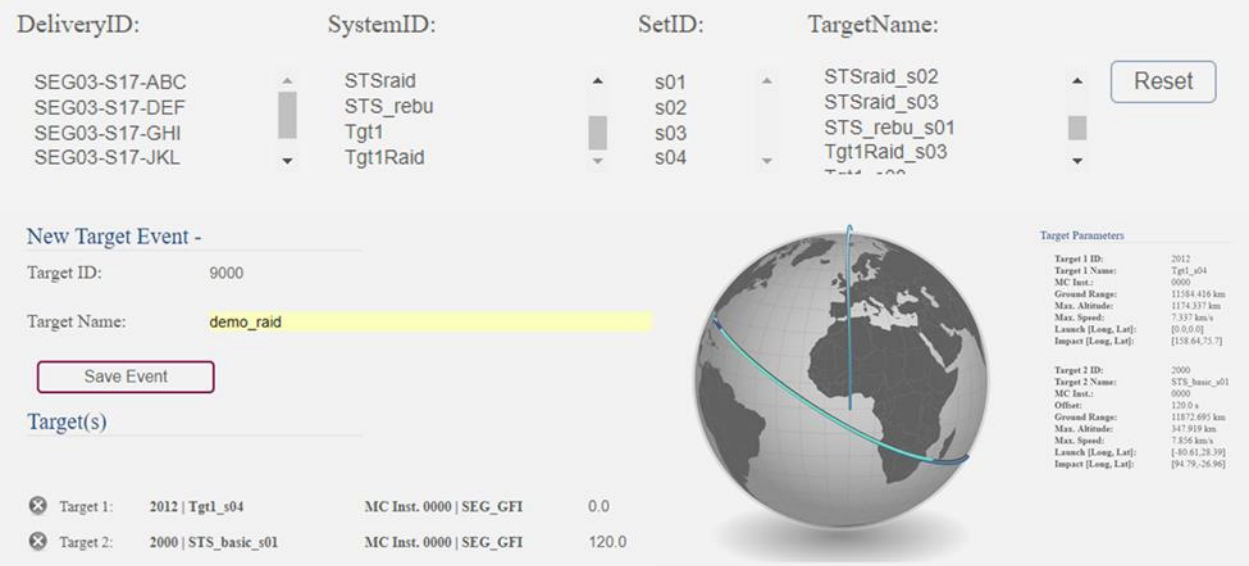


**Figure 5: Threat Database User Interface**

The PULSEbox post-scenario analysis tools (also accessed through the GUI) are intended to improve the usability of the underlying threat data by providing visualization data to users who do not have the expertise or infrastructure required to interact with high fidelity threat data. Current analysis tools include kinematic state plots and Range Time Intensity (RTI) plots showing an RF sensor's point of view of threat scene (Figure 6). These analysis tools are

developed using python and the GUI is designed to allow additional python analysis tools to be incorporated as they are developed.

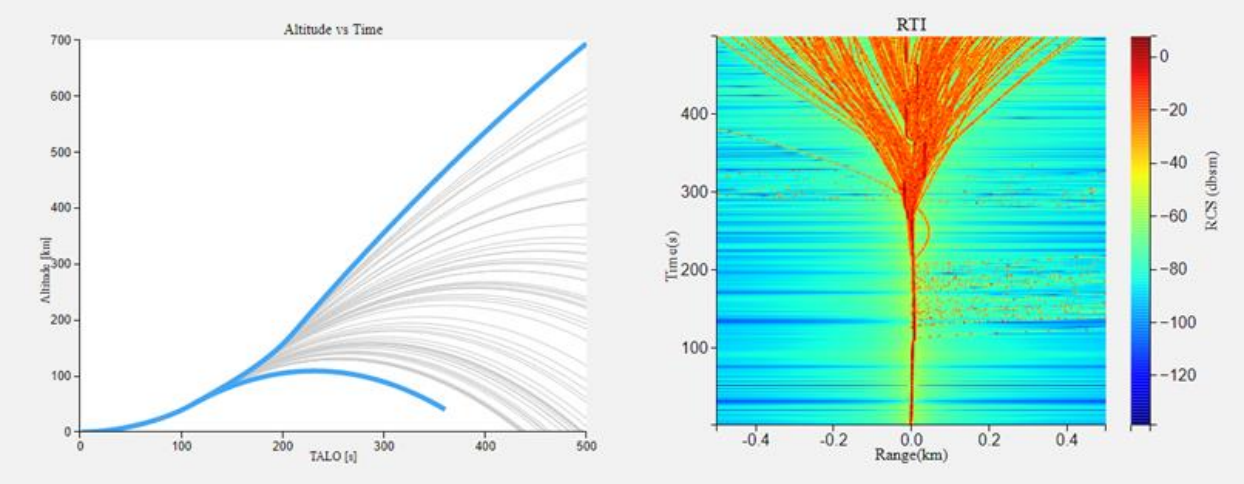


**Figure 6: Post-Process Analysis Capability**

In-line Sensor representations are also available for PULSEbox through the GUI scenario generator allowing users who do not have access to the validated sensor models to conduct threat data analysis enabling a wider array of users to access the GFI threat data for various purposes such as algorithm development.

**Future Capability**

PULSEbox will continue to evolve to support a wider array of users with additions of new phenomenology and support to different types of simulations. Different users will eventually be able to leverage PULSEbox at different levels of the weapon system design such as at the signature return level, at the detection and track level, at the discrimination level, at a full sensor model level, or at the full weapon system simulation level. The fully integrated M&S suite in PULSEbox will also allow for the development of coordinated and reactive threats in the future.

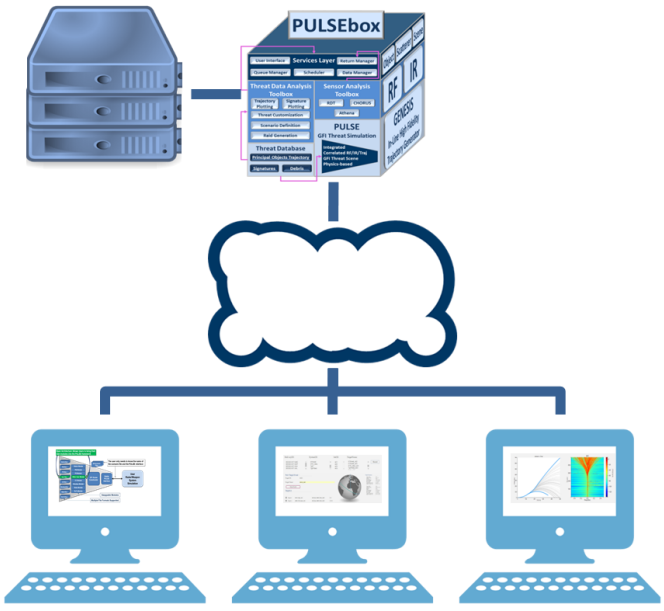


**Figure 7: PULSEbox Cloud Deployment**

There are four main growth and development areas for PULSEbox which build upon each other to bring increased capability. These areas are grouped as follows: "Cloud Computing / Modeling and Simulation as a Service (MSaaS) / High Performance Computing (HPC)", "Distributed Simulation / Simulation Interoperability", "Hardware in the Loop (HWIL) / Real Time Simulation", and finally "Field / Range Deployment".

A fast growing area in Simulation is Cloud Computing where simulations are run on a remote publicly available server. Users also have the ability to analyze the data in-situ using a wide range of web data analytic tools. Cloud computing is a perfect fit for PULSEbox particularly in its virtual form. A cloud capable PULSEbox will make it straightforward for any users regardless of their physical location to access the latest data and simulations available in PULSEbox. In this capacity, cloud based simulations are referred to as Modeling and Simulation as a Service (MSaaS). The attraction from a user/customer perspective is that they

would not need to cover the cost of developing and maintaining an IT infrastructure capable of running the wide range of simulations provided by PULSE. Furthermore the adoption and use threshold has been lowered tremendously since there is no need to develop a driver or an interface between user tools and environment and the simulation provided in PULSEbox. A user would simply select the scenario of interest and start a simulation with the click of a button. The Department of Defense also has several High Performance Computing (HPC) centers that could eventually be leveraged to dispatch a large number of runs, such as a Monte Carlo analysis, and make use of the hardware available on such systems such as multi-core and GPGPUs (General Purpose Graphic Processing Units) (Kewley, et al., 2018).

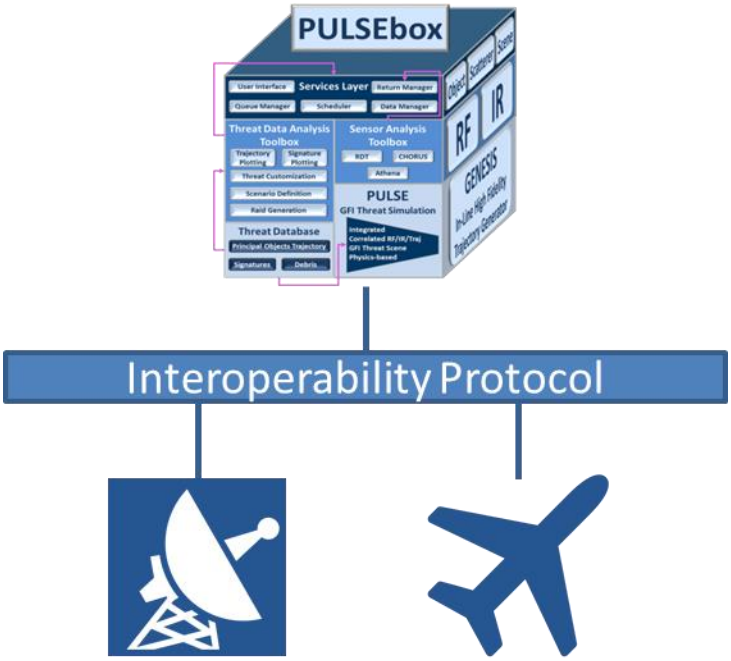


**Figure 8: PULSEbox in an LVC event**

Beyond the deployment of PULSEbox in a cloud environment, PULSEbox is being expanded to provide Threat Scene as a Service. In this use case PULSEbox will be part of a distributed simulation which typically leverages standard interoperability protocols such as Data Distribution Service (DDS), Distributed Interactive Simulation (DIS), High Level Architecture (HLA) and Test and Training Enabling Architecture (TENA). One can imagine several distributed RF sensors in a simulation federation where PULSEbox plays the role of the threats and RF signatures provider. Adding a simulation interoperability capability to PULSEbox opens the doors for integration into large Live Virtual Constructive (LVC) events.

The main advantage of hosting PULSEbox in a specific piece of computer hardware is that the configuration is locked and known to the developers. As a result many of the simulations modules present within PULSE can be optimized to this hardware whether it would be by CPU vectorization with SSE and AVX, or by leveraging all the CPU cores available as well as the GPGPUs and FPGAs present in the PULSEbox configuration. This level of optimization will allow for a real time capability in PULSEbox. Such a capability is absolutely necessary for PULSEbox to be brought into a Hardware In The Loop (HWIL) simulation.

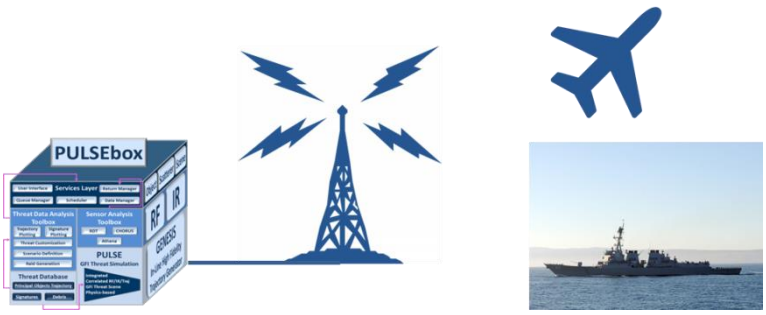


**Figure 9: PULSEbox deployed on a range**

Finally once PULSEbox has successfully achieved hard real time processing and demonstrated that capability in an HWIL environment its next logical step is to be running in a Software In the Loop (SIL) environment. At that point PULSEbox can be deployed in live tests as a provider of synthetic threats into a real live environment. PULSEbox can be deployed on board a ship to augment the real live environment with synthetic threats injected directly into the radar weapon system feed. This virtual over live could be useful for shipboard system testing as well as providing realistic training to the sailors while on deployment.
Similarly a real time capable PULSEbox matted with an RF emitter frontend could be deployed on a live testing range to inject synthetic threats into a live test of radar systems or into an LVC test or training event.

**REFERENCES**

Johns Hopkins Applied Physics Lab. (2010, December 20). MSLRAD 6.07. Laurel, MD, USA.

Kewley, R., McDonnell, J., Snively, K., Diemunsch, J., McGroarty, C., & Gallant, S. (2018). Cloud-based Modeling and Simulation Study Group. *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC).* Orlando, FL.

Systems Engineering Group, Inc. (2010, March 05). ASC Angles Version 2.0. *CA58-U10-0007*. Columbia, MD, USA.

Systems Engineering Group, Inc. (2015, March 20). ASC v3.4.0. *SEG02-U15-051*. Columbia, MD, USA.

Systems Engineering Group, Inc. (2015, August 07). DebrisSim v6.6.1. *SEG02-U15-241*. Columbia, MD, USA.

Systems Engineering Group, Inc. (2015, July 16). WakeSim v0.2.0. *SEG02-U15-220*. Columbia, MD, USA.

Systems Engineering Group, Inc. (2017, December 19). Darwin v4.1.0. *SEG03-U17-713*. Columbia, MD, USA.

Systems Engineering Group, Inc. (2017, August 31). MDA/AB ES PULSE Inputs Compilation 2017 Volume 1 Version 2. *SEG03-S17-513*. Columbia, MD, USA.

Systems Engineering Group, Inc. (2017, July 07). MDA/AB ES Threat Data Compilation 2017 Version 1 Volume 1 BETA. *SEG03-S17-216*. Columbia, MD, USA.

Systems Engineering Group, Inc. (2017, October 12). PULSE: Physics Unlimited Scalable Simulation Environment Software, Version v1.3.0. *SEG03-U17-543*. Columbia, MD, USA.

Systems Engineering Group, Inc. (2017, February 20). Threat Model Clutter Assessment Tool (TMCAT) Version 3.0.0. *SEG03-S16-199*. Columbia, MD, USA.