An Exploratory Study on Interfacing the Simulation Training Exercise Platform (STEP) with Operational Simulators

Authors

Edward Y. Hua, PhD

Douglas Flournoy

Contributors

Saurabh Mittal, PhD

Anthony Rood

Jacob Richkus

Project No.: 10MSRF18-AC

Document No: MTR-T842-B-3067

McLean, VA

MITRE

Abstract

This report introduces the Simulation Training Exercise Platform (STEP) technology. One of its core capabilities is mapping the effect-impact relationship between the cyber and operational domains within a simulation environment. With this technology we aim to address the problem of understanding precisely how effects in one domain could propagate to the other and manifest into certain impact in a complex simulation environment. STEP could bring benefits to a broad range of sponsors, both military and civilian, who are entrusted with mission-critical responsibilities through analyzing simulation data. We also identify three technical hurdles that could affect sponsor acceptance of STEP and lay out a transition path to the relevant sponsors.

Executive Summary

We introduce the Simulation Training Exercise Platform (STEP), a technology developed by the Carnegie Mellon University's (CMU) Software Engineering Institute (SEI). As a cyber simulator that can be interfaced with a mature operational simulator, one of its core capabilities is to trace the effect-impact relationship between the cyber and operational domains in the simulation environment. STEP has gained traction within the DOD, where it is being applied in several DOD-sponsored cyber exercises.

A long-standing problem in the Modeling & Simulation (M&S) community is the lack of ability to trace and study how effects from one domain would propagate to result in an impact in the other domain. Failure to do so makes it difficult to diagnose the root cause of an adverse impact in the simulation space. In addition, DOD simulations have not kept up with the current reality of more blended missions on the battlefield, which could leave decision makers ill-prepared for real-life crises.

Sponsors, such as the Army Research Lab (ARL) and the Federal Aviation Administration (FAA), have expressed strong interest in adopting STEP in their respective simulation environments. However, there are some technical hurdles that need to be addressed before STEP could find acceptance among a diverse group of sponsors. These include properly evaluating the effectiveness, versatility, and scalability of STEP.

The applicability of STEP to the Army and FAA sponsors requires a well-defined transition path based on studying their respective operational simulators and contextualizing STEP within these two domains.

This page intentionally left blank.

Table of Contents

List of Figures

This page intentionally left blank.

1. Introduction to Simulation Training Exercise Platform

In a simulation environment comprising a cyber domain and an operational domain, the progression of a simulation run is driven by the myriad interactions between the domains. Such interactions are typically initiated by some effect in one domain, which then propagates to the other domain and results in an impact in the target domain, as observed by the simulation operator governing the simulation.

The Simulation Training Exercise Platform (STEP) is a cyber simulator that provides training in various cybersecurity fields, such as Information Assurance (IA), incident response, and computer forensics. First developed at Carnegie Mellon University's (CMU) Software Engineering Institute (SEI) in 2003, STEP has undergone periodic and incremental upgrades. Over the last 15 years of evolutionary development, it has now reached a high level of maturity and stability. One of the key features of STEP is its ability to accurately map out the cross-domain effect-impact relationship; this is achieved through an SEI-defined Application Program Interface (API) called Cyber-Kinetic Effects Integration (CKEI) [2].

STEP traces the inter-domain effect-impact relationship by re-creating the domain space where the impact would be manifested. Figure 1 illustrates this approach, using STEP interfaced with the Army OneSAF simulator as an example. In the operational simulation domain where OneSAF operates, on identifying a target, the Forward Observer (FIS) sends a report to the Battalion (BN), which then relays the information to the Brigade (BDE). BDE issues the Call For Fires (CFF) order, sends it to BN, which forwards this message to the Battery. The Battery then assigns the actual firing to the particular Gun, which executes the CFF order to fire on the target.

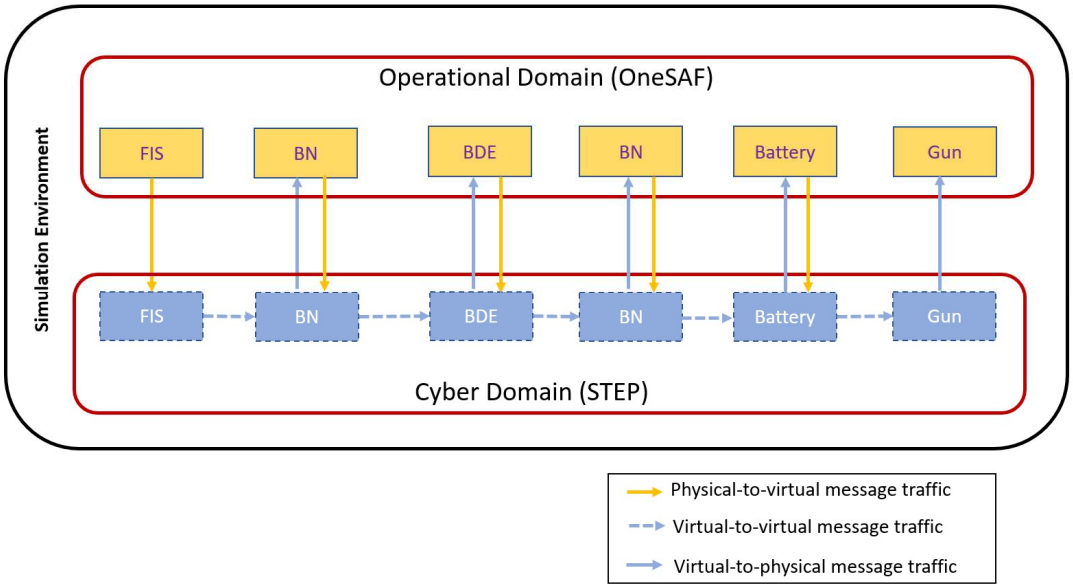

Figure 1. Illustration of how STEP realizes CKEI between the cyber and operational domains.

In the cyber domain, STEP creates a virtual copy of each physical device, as well as the networking that connects these devices, that participates in the CFF order propagation throughout the echelon. The states of these virtual nodes at any given time closely mirror those of their counterparts in the operational domain. Each physical node that receives the CFF message routes it to the next intended recipient via its virtual counterpart, which then forwards it to the virtual counterpart of the intended recipient, who then passes it to the recipient in the operational domain. If the nodes in the operational domain (OneSAF) are compromised on the cyber side, the virtual nodes in STEP update their state and any associated communications message accordingly.

2. Current State-of-the-Art

At the present, STEP is primarily being tested by the DOD, specifically the Army. SEI continues to expand its capability set with new features and enhancements to support ever-increasingly complex simulation scenarios.

2.1 Pairing STEP with Operational Simulators

According to SEI, there are currently two methods of pairing STEP with a mature operational simulator. In the first method, SEI provides an external interface to link STEP with the operational simulator at the customer's site. When a simulation scenario is set up, the customer works closely with SEI to define the detailed requirements on the effects to be introduced into the cyber domain. SEI is then responsible for configuring STEP and implementing these effects. This work is transparent to the customer, who continues to focus on setting up the operational domain for the scenario. The Army is currently testing STEP with two of its simulators, OneSAF and VBS3, via this external-interfacing approach.

In the second method, the customer receives a copy of the STEP software from SEI and installs it at their site. The customer is responsible for configuring the STEP and interfacing it with its operational simulator. To help them do this, the STEP package includes a suite of tutorial videos that train operators how to set up and configure the desired effects. STEP has been used in several DOD-organized exercises such as Cyber Flag and Cyber Guard.

Both methods have been tested in DOD-sponsored exercises.

2.2 Latest STEP Enhancements

Through periodic cycles of development, SEI is constantly expanding STEP's feature set to support cyber training in more complex and diverse simulation environments. The aim is to make STEP more agile and modular. Some of the most recent enhancements added to STEP follow. These features are all optional and their absence from STEP does not affect our study of effect-impact relationship mapping.

- **TopoMojo**: The current STEP contains a rich set of features that may not all be applicable to a particular customer's needs. The set could also create the problem of inflexibility in installation and deployment. In response, TopoMojo was developed as the

lightweight version of STEP. It retains the key features of STEP, such as CKEI, while removing others.

- **WELLE-D**: This is a tool that simulates wireless communications. It can be used to model Open Systems Interconnect (OSI) Layer-2 (MAC-layer) wireless links.
- **SCADASIM**: This feature allows the cyber operator to manipulate SCADA systems (power, lighting, security cameras, etc.) during a simulation run. It contains several components, such as Human-Machine Interface (HMI) and a Historian that archives the log files.
- **GHOSTS**: This application tracks the real-time status (e.g., health check) of all server activities during a simulation run. It uses a PostgreSQL database to archive all data pertaining to activities in the simulation space. Data visualization is achieved through the use of a GUI, which includes a number of more commonly used performance metrics. The user can also write his/her own PostgreSQL script to extract relevant data from the database for more in-depth analysis.
- **GreyBox**: This is a tool that runs on a Virtual Machine (VM) to model the entire Internet ("Internet in a box"). One use case of GreyBox is to study a Local Area Network (LAN) in the context of global Internet. The LAN can be seen as one entity, and the rest of the Internet another entity; the two are connected via a gateway.
- **Cartographer**: This feature is used to validate the network deployed prior to simulation commencement. It is intended to minimize human mistakes when manually entering hundreds of IP addresses for a large simulation scenario. Once launched, Cartographer can identify errors in the IP address space in a matter of minutes. This tool can be used to check for errors from OSI Layer 3 (IP) up to OSI Layer 7 (Application).

3. Applicability to Sponsors

Due to the high volume and complexity of cross-domain interactions, mapping a relationship between the effect in one domain and its impact in the other is a daunting challenge (Figure 2). Failure to accurately capture this effect-to-impact play makes it difficult to investigate the root cause of an adverse impact. Furthermore, current DOD simulation environments are unable to keep up with detailed cross-domain interplay on the battlefield, where cyber operators and kinetic operators work alongside each other in increasingly blended missions. The lack of realism representing blended missions in the simulation space makes the decision makers ill prepared to manage real-life crises.

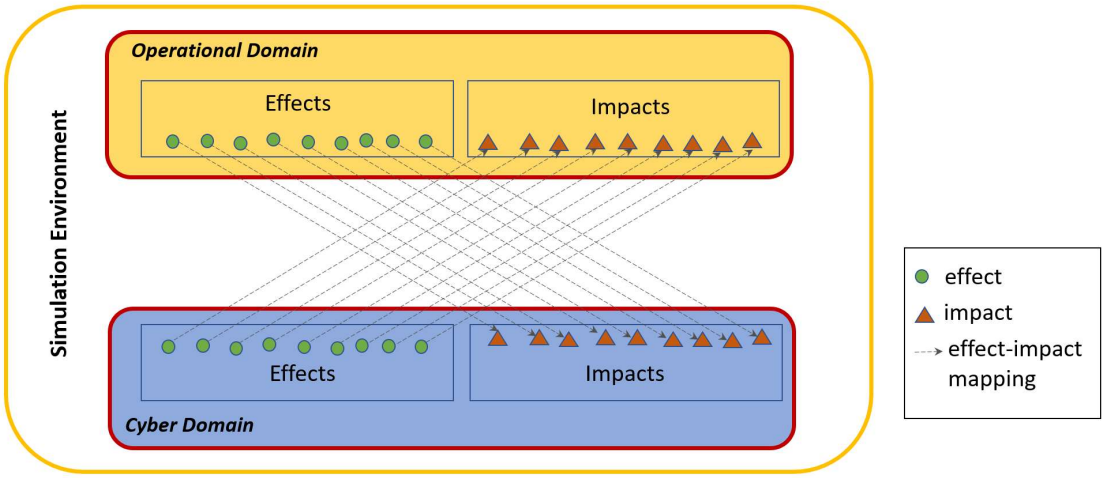

Figure 2. Cross-domain interactions in the simulation space.

3.1 Sponsor Engagement

In this project, we have engaged with three sponsors—the Army, the FAA, and the Air Force—to gauge their interest in STEP and identify suitable operational simulators for study.

The Point-of-Contact (POC) for Army Research Lab (ARL) Survivability Lethality Analysis Directorate (SLAD), who came across a proof-of-concept demonstration of STEP integrated with the OneSAF simulator, expressed a desire to pursue further study of this technology.

The Aviation Cybersecurity group in support of all FAA simulation activities had been conducting their own investigation of effect-impact interactions. On learning of STEP, they were interested in a collaborative study to see how its benefits aligned with the sponsor interests.

We also exchanged communication with the Computing Infrastructure and IT Service Management group, which supports Air Force simulations using the AFSIM simulator. Because integrating STEP with AFSIM would require that STEP be embedded to become part of the AFSIM, this did not fit our original design in which we would maintain two separate domains. Consequently, we decided not to pursue collaboration with them at the present time.

3.2 Benefits to Sponsors

STEP can bring a host of benefits to various sponsors, both military and civilian. It provides a robust platform to evaluate the strengths and weaknesses of new tools and capabilities prior to procurement. It allows stakeholders to design and execute more realistic simulation experiments showing how a cyber component would allow or prohibit information exchange between operational facilities. Furthermore, it gives simulation operators a means to investigate cyber threats as rigorously as other threats that could negatively impact the mission outcome.

For the Army sponsor, STEP could be used to examine, the impacts of cyber effects on the gathered intelligence on the battlefield (whether it is legitimate or compromised) to assist commanders in making more informed decisions. It could also enhance training to study how

cyber effects could maximize operational impact before being applied to real-life missions. Finally, it would enhance training for cyber operators, reflecting the reality of more blended missions.

For the FAA sponsor, STEP would enhance the effectiveness and realism of cybersecurity exercises for the FAA and its aviation sector partners; this in turn would increase the value of such exercises to the stakeholders. It could also improve the effectiveness of air traffic operational incident response during a suspected/confirmed cybersecurity incident.

3.3 Sponsor Acceptance

The Army was the earliest adopter of STEP in several of its simulation exercises. They have shown a strong interest in continuing study on STEP and making it an integral part of its simulation environment.

The FAA sponsor was recently introduced to the capabilities of STEP. It has expressed willingness to partner with us and further explore the potential benefits it may bring to the FAA and its aviation-industry partners. The Integration Experimentation and Demonstration for Aeronautics (IDEA) lab hosts a sophisticated simulation apparatus that could be interfaced with STEP. We expect to produce tangible results in the near future to demonstrate its applicability to this sponsor.

Furthermore, we plan to invite other sponsors to participate in this study, which would allow us to explore the versatility of STEP.

4. Technical Hurdles

STEP promises to bring many benefits. Yet to reach a larger group of sponsors, we need to address the following three considerations that could impede its wider acceptance.

First, there currently is no systematic approach to evaluating the accuracy of STEP in tracing an effect-to-impact relationship. The high volume and complexity of cross-domain interactions in the simulation space could lead to a certain effect manifesting into unintended impacts, as well as impacts of higher orders. How to quantify the impact that deviates from the expected outcome, and how to identify higher-order impacts that may be considered negligible, requires future study and research.

Second, the question remains unanswered as to the versatility of interfacing STEP with a broad range of operational simulators. STEP was designed to be compatible with any mature operational simulator. To the best of our knowledge, currently STEP has only participated in cyber simulations and exercises with the Army and remains untested by other services and agencies. It would be necessary to collaborate with multiple sponsors and interface STEP with their respective simulators to validate its versatility.

Third, the scalability of adopting STEP in a simulation scenario should not be ignored. STEP realizes the CKEI by creating a virtual copy of the domain where the impacts are manifested (as shown in Figure 1). The virtual copy includes each device and networking connection that is involved in manifesting the impacts [3]. As the simulation scenario grows in size and complexity, more computing resources are needed to generate and sustain this virtualization, potentially at the expense of other aspects of the simulation. A careful examination of the

scalability of the use case with a STEP deployment would help define a more robust scope of the simulation in which the capabilities of STEP could be fully and accurately realized.

5. Transition Paths

We have identified two transition paths to move forward with our STEP study with the Army and FAA sponsors:

- For the Army sponsor, interface STEP with OneSAF and develop use cases that examine the impacts that system-level cyber vulnerabilities may have on warfighting missions.
- For the FAA sponsor, leverage the IDEA lab to develop use cases that demonstrate the impact of some operational effects on the underlying communications network during air traffic control operations.

6. Conclusions

This report introduced STEP, a cyber-domain training technology developed at the CMU SEI that can trace inter-domain effect-impact relationships within the simulation environment. We evaluated the feasibility of deploying STEP with two operational simulators utilized by two sponsors: ARL and FAA, one military and one civilian. In our findings, STEP could bring benefits to either sponsor by assisting users to make critical decisions based on high-fidelity, simulation-based analysis. As an initial step, STEP does provide mechanisms to identify and define cross-domain effects and impacts. However, its potential use in an exhaustive simulation exercise needs further evaluation. STEP's versatility and accuracy for mapping out the effect-impact relationship may depend on how it would handle the scalability of the simulation space. Both Army and FAA sponsors are interested in further collaborative study to evaluate STEP in realistic scenarios.

Acknowledgements

The authors gratefully acknowledge the contributions made by Rotem Guttman (Carnegie Mellon University/Software Engineering Institute/CERT).

References

1. Daiello, C., Hancock, K., Surdu, J., and Lacks, D., "Cyber Effects within a Kinetic Model," *Interservice/Industry, Training, Simulation, and Education Conference (I/ITSEC)*, No. 17181, Nov. 2017.
2. Guttman, R., "Combined Arms Cyber-Kinetic Operator Training," SEI Blog, March 2017.
3. Hua, E., and Guttman, R. *Personal Communication,* 2018.

Abbreviations & Acronyms

API	Application Program Interface
ARL	Army Research Laboratory
BDE	Brigade
BN	Battalion
CERT	Computer Emergency Response Team
CFF	Call For Fires
CKEI	Cyber-Kinetic Effects Integration
CMU	Carnegie Mellon University
DOD	Department of Defense
FAA	Federal Aviation Administration
FIS	Forward Observer
HMI	Human-Machine Interface
IDEA	Integration Demonstration & Experimentation for Aeronautics
LAN	Local Area Network
M&S	Modeling and Simulation
MESA	Modeling Environment for Service Oriented Architecture Analysis
OSI	Open Systems Interconnection
POC	Point-of-Contact
SCADA	Supervisory Control and Data Acquisition
SEI	Software Engineering Institute
SLAD	Survivability & Lethality Analysis Directorate
STEP	Simulation Training Exercise Platform
VM	Virtual Machine