171-183

UTILIZATION OF SYNTHETIC ENVIRONMENT FOR DEFENCE EXPERIMENTATION IN PLANNING, EVALUATION AND ACQUISITION OF C4ISR SYSTEMS

Mr Manoj Tyagi et al.*

Abstract

Response to contemporary threats require defence forces to strategize its war fighting capabilities through adapting newer command and control structures, planning for sensors, weapons and communication systems. There is a need to quickly assess the aptness of a selected capability against the threat, through Operational Analyses (OA) tools and techniques. The measure of effectiveness and merits are to be arrived to prove a hypothesis of success of such concepts, systems, in a particular threat-scenario.

A readily configurable framework to test and prove the conceptual manifestations is need of the hour. A contemporary approach to capability development is required-one that uses experimentation, rapid concept exploration, and prototyping to integrate materiel and non-materiel solutions in ways that most effectively address war-fighter capability gaps. This paper proposes such a framework which maximizes effectiveness through continuous and iterative experimentation to bring alignment, rigour, efficiency and faster insertion of new capability. This ecosystem aims to provision analytics-based development, tactical planning and acquisitions in Command, Control, Communications,

Computers, Intelligence, Security, and Reconnaissance (C4ISR) systems.

Introduction

"*Anything we use today arrives through a process of organized experimentation; over time, improved tools, new processes, and alternative technologies all have arisen because they have been worked out in various structured ways*".[1]

Lack of such an approach can lead to undesired consequences [2]. On the contrary, utilization of the approach can be advantageous [3].

Modelling and simulation is the technique of representing and virtually executing complex systems, processes, system of systems. A 'System of Systems (SoS)' is a concept where various heterogeneous systems become participants in a scenario and the conduct of scenario itself is treated like a system. Essentially, SOS is made up of components, which are systems, interactions & events, processes & activities, resources, assumptions & constraints and operating environment. The aim of such a representation and virtual execution can be to educate / train people on skill, tactics, decision making, or to analyse various typical-to-futuristic scenarios. To enable smooth design, development and execution of such a training or analysis exercises requires an infrastructure, referred to as Synthetic Environment (SE).

SE includes computing hardware, networks, software tools, models, simulations, people, and real equipments like sensors, weapons, or platforms; to form a common representation of a realistic typical / futuristic scenario in virtual or synthetic world. SE is typically used for simulating a wide range of highly interactive activities, including the human, to enable generation of 'enough data' for the purpose of analysis. SE can also be utilised for research, training and evaluation. Figure 1 shows the purpose of models, simulations and synthetic environment.

Figure 1: Purpose of Combat Models

The proposed facility would be basically a synthetic environment (SE), and will be exploited for operational analysis (OA) using defence experimentation (DE) approach. “Defence experimentation is the application of the experimental method to the solution of complex defense capability development problems, potentially across the full spectrum of conflict types, such as war-fighting, peace-enforcement, humanitarian relief and peace-keeping” [4].

Operational Analyses (OA)[5]

Operational Analysis (OA) is concerned with the study of complex decision-making problem often characterised by incomplete and uncertain information on various aspects of problem space. Typical decision-making problems involve the allocation of scarce resources

in the systems where effectiveness is measured against an array of multiple, and usually conflicting, objectives. Following is a listing of typical OA scopes for defence industry analysis:-

- Force Structuring
- Military task evaluation
- Capability gap analysis
- New capability Requirements
- RFP / RFI / Requirement document generation support
- Logistics / Through life
- Cost Effectiveness
- Campaign planning and mission rehearsal / training
- Operational support
- Doctrine / Concept proving and development

The OA process through defence experimentation brings together the assumptions, options, data and expert judgement relevant to the operation of a particular system in a particular context and examines their implications in a structured, explicit and auditable way using models and simulations. As a first step, OA approach identifies the alternatives between which a decision is to be made. Secondly, the criteria against which these alternatives are to be judged are defined (measure of performance and effectiveness). Thereafter, a synthetic environment is configured to carry out defence experiments, to generate 'enough' data for statistical insights and analysis.

Capitalization of commercial information technologies for C4ISR systems are proving a game changer and essential step for development of interoperable and flexible systems to support joint operations

and leveraging of inter service military assets. Similar approach for commercially viable ecosystem for Advanced Modelling & Simulation and Experimentation (AMSE) is necessary for viable and effective Operational analysis (OA) using defence experimentation.

Defence Experimentation

In general terms, experimentation answers the question, “If I do this, what will happen?” *Defense experimentation*[6] extends that question to the military domain, providing decision makers with information they need to make good decisions. Defense experiments provide opportunities for technologists and warfighters to evaluate potential solutions to existing or emerging warfighter capability gaps and probe the integration of technology development and concept exploration in order to maximize synergies that exist. Experimentation also enables rapid evaluation of a military problem, increasing the speed by which knowledge and understanding is gained and decisions can be made. Experimentation fuels the discovery and creation of knowledge and leads to the development and improvement of products, processes, systems, and organizations.

Development of Tactics, Techniques, and Procedures (TTP); development of CON-OPS, Planning and Rehearsal of complex missions and Joint Operations, Simulation Based Acquisition (SBA); Course of Action Development and Analysis; and Execution Monitoring are some of the challenges in development of C4ISR systems that can be addressed through analytics-based Defence experimentation.

Necessity of commercial Synthetic Environment (SE) ecosystem

An Advance M&S and Experimentation facility requires state-of-the-art modelling & simulation and analysis suits and excellent 2D / 3D visualisation software. It requires high-end presentation facilities for

internal as well as strategic decision makers, including well designed conference, exercise control and experimentation area / labs. Typical tool suit available in such a facility are: Terrain Visualization Tools, Platform/Weapon/Sensor Models (Virtual as well as Simulation), 3D Model Development Tools, Aggregated Force Models, Civilian

Figure 2: Synthetic Environment

Behaviour Models, Sensor detection, identification and tracking models and Communication Models as pictorially depicted as in Figure 2.

Defence Experimentation (DE) through Synthetic Environments (SE) is the key to success in maintaining lead in defence markets in India and abroad. It's all about how fast and credibly we can predict and satisfy our customers' needs. Inherent concepts for defence experimentation are:

- Capability gap analysis
- Technology planning
- Military requirement analysis
- Verify concept of operations (CONOPS): Experiment

before building system/sub-system to arrive for “optimal” specifications / intended operational purpose

- Test the system deployment, virtually, for “best-plan” in an operational environment

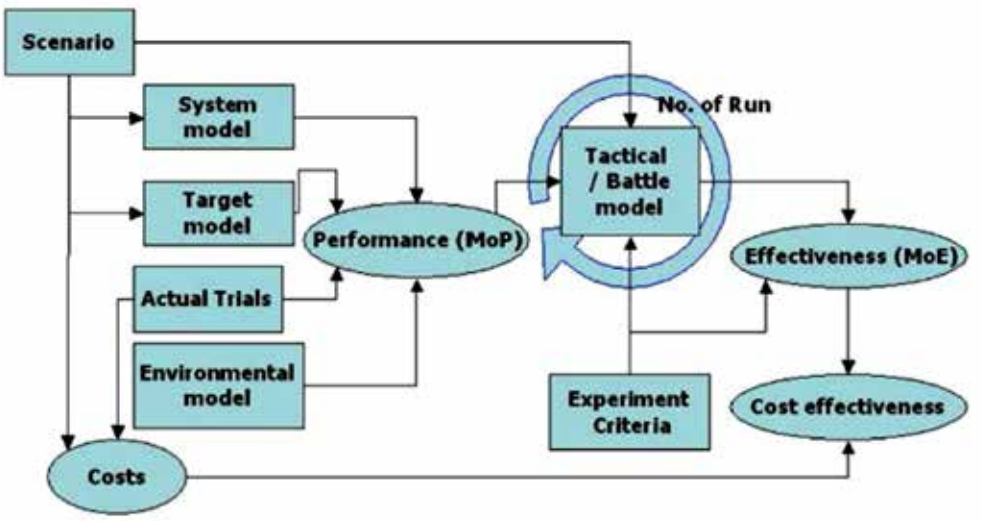

Figure 3: OA through DE framework

- Cost effectiveness studies
- Evaluation and What if analysis.

Lets us consider an exemplary framework given in Figure 3, for operational analysis of a system. Such a framework provisions, tools and processes to carry out studies as listed in ‘Inherent concepts for defence experimentation’ above. Clearly, it would be required to iteratively change experiment criteria and re-configure models and simulation. User participation is a must in such experiments. The scenario executions (scenario stage through to obtaining measures of effectiveness) often involve user inputs and user decisions in the tactical battle area. We also

require subject matter experts (SMEs) to validate fitness for purpose of models and simulations.

Benefits of Defence Experimentation (DE)

Defence experimentation provides important insights and understanding of the operation of the system. It leads to quantification of the comparative performance of the systems operating under different conditions. Finally, Operational Analysis (OA) using Defence Experimentation (DE) becomes a more objective and justifiable basis for management decisions on the operation of the system. Other advantages as compared with other alternative like field trials, development of and thereafter experimentation on prototypes and live exercises like war games are[5]:

- Cost effectiveness
- Time can be compressed
- Control is easier
- Safety is not a problem
- Applicability is very wide
- Visualisation aids understanding

However, care must be taken to define 'achievable goal' and ample level of 'actual' user participation must be ensured for defence experimentation. Additionally, the model / simulations used in the SE should be verified / validated by subject matter experts (SME).

Experiment Development Process

Experiment process starts with seeking and establishing a hypothesis like, "If Air Command and Control System is to be inducted by Defence Forces[7], then they would be better in terms of identifying and neutralizing threats". What is actually meant by "better", can be defined in measures

to be captured or derived during and after experiment runs. Experiment Development Life Cycle (EDLC) can at least be divided into two logical parts, Development & Usage. Development part phases and activities require technical expertise in modelling & simulation and software design & development. Engineer is expected to learn, configure, script, program, interface, interoperate[8] and manage bespoke & COTS software. Usage part phases and activities require expert level knowledge of conduct of wargames and operational analysis to conduct of experiment runs, collect relevant data, quantify, analyse in details all measurements and portray consolidated results supporting or rejecting the hypothesis.

Following are concise activities under experiment phases:

- Preliminary: Identify experimentation opportunity and develop concepts.
- Problem Formulation: Formulate crisp problem & proposed solutions
- Experiment Design: Design scenarios, define MOPs / MOEs, plan experiment, technical and participants, generate event and feature list for proposed solutions.
- Experiment Development-Capability: Develop required features, solve issues, conduct trials, refining scenarios, and training.
- Experiment Execution: Conduct, control, monitor and log runs
- Analysis: Consolidate results, derive and analysis measures.
- Report: Producing conduct and run reports, analysis on MOE report.

Defence Experimentation Case[9]

The Command, Control, Communications, Computers and Intelligence (C4I) Systems provide situational awareness about operational

environment and supported in decision making and directed to operative environment. These systems had been used by various agencies like defense, police, investigation, road, rail, airports, oil and gas related department. The increased use of C4I system had made it more important and attractive. Consequently effectiveness of such systems needs to be established.

A scenario encompassing major aspects of C4I system is formulated. Objective from utilization of C4I system in this scenario is defined, e.g. “Monitor, identify and neutralize threats”. Measurable parameters to indicate effectiveness of C4I system in the scenario are listed. Parameters in this scenario can be: threats in the scenario, threats identified confirmation to threats neutralization, time to react, damage to own resources etc.

The scenario is executed and values of various parameters are noted.

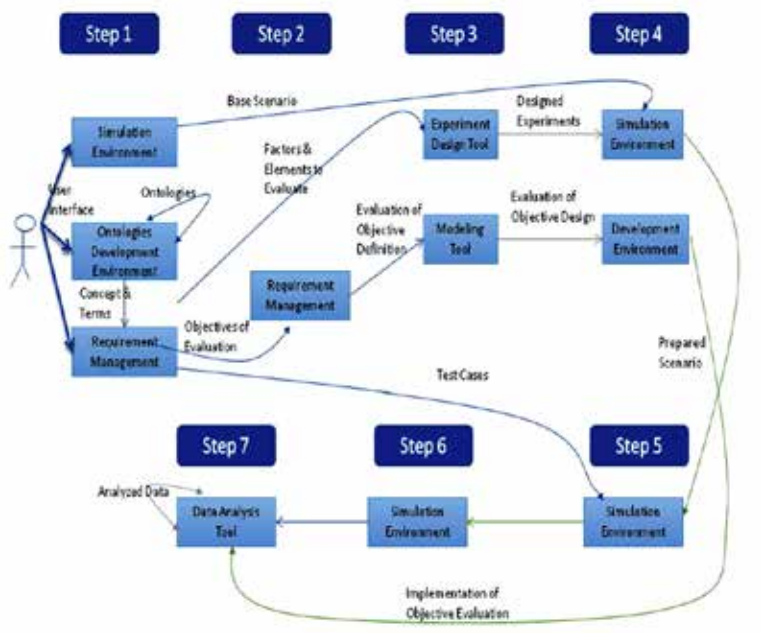

Figure 4: Methodology

Methodology

As shown in Figure 4, Using *Synthetic Environment* as a Tool, *Defence Experimentation* Method is applied in a scenario to describe Hypothesis (e.g. *Force Multiplier Effect of C4I systems)*.

It shows variety of external environment requirements that can act as input to Simulation Environment, thus moving closer to the real external environment. Combination of some real inputs with Simulation tools can result in another Simulation Environment. Development Environment, which represents inner capabilities, is catering to variety of capability requirements and can be changed by adding / removing / editing capabilities.

The plan is to baseline the measured parameters, by having some “as it is” runs, and then one by one introducing capabilities and observing the effect in measured parameters across multiple runs (four to five runs per capability). Graphs to show the different stage outputs of the data are collected, analysed and presented in form of bar charts and increase / decrease of measured values in percentage when a capability is introduced and what can be said about its hypothesis. Data would also indicate if more number of runs is required. Also, comparison of various capabilities can be derived from the data output.

Thus, from outputs analysis, capabilities (e.g. of C4I systems/sub-systems) conforming to hypothesis can be added and others can be removed.

The decision maker now has the understanding of the scenario and data support for decision making. Important point to note here is that these capabilities may be at production state or at design or even conceptual level for the company. The requirement for defence experimentation is that only equipment’s / capabilities’ basic characteristics/ features should be known, for proving / supporting a hypothesis. This brings out that

the field of defence experimentation can be utilized at various stages of product/capability development cycle.

Conclusion

Constitution of Centre of excellence for Defence Experimentation using Synthetic Environment is need of the hour. Such a rapidly configurable CONOPS experimentation laboratory has credible potential to be utilized across joint defence programmes to:-

- Reduce time of prototyping / concept proving and supporting
- Moving beyond measures of performance, to measures of effectiveness/merits for quantifying force-multiplier effect of produced equipments.
- Increase cost-effectiveness by reducing field trials

The facility and method described in the paper would prove to be a contemporary approach to capability development — one that uses experimentation, rapid concept exploration, and prototyping to integrate materiel and non-materiel solutions in ways that most effectively address war-fighter capability gaps.

*__Mr Manoj Tyagi__, currently working as DGM, Network Centric Systems, Bharat Electronics Ltd, Ghaziabad has done Masters in DSM (RMCS, Cranfield University, UK) and is a former Scientist at Institute of Systems Studies and Analyses, DRDO

Co-authors:

Mr Varun Gupta, Manager, Bharat Electronics Ltd, Ghaziabad

Mr Sandeep Kumar, Manager, Bharat Electronics Ltd, Ghaziabad

Mr Amit Gupta, Sr DGM, Bharat Electronics Ltd, Ghaziabad

Endnotes:

1. Thomke Stephan H., “Experimentation Matters; Unlocking the Potential of New Technologies for Innovation”, Boston: Harvard Business School Press, 2003, p. 307
2. Seth G. Jones, “Russia’s Ill-Fated Invasion of Ukraine: Lessons in Modern Warfare”, CSIS Briefs, https://www.csis.org/analysis/russias-ill-fated-invasion- ukraine-lessons-modern-warfare, June 1, 2022
3. Ralph D. Thiele, “Over five years of Russian hybrid warfare against Ukraine provide lessons how to make Ukraine stronger”, ISPDW Strategy Series: Focus on Defense and International Security, https://www.ispsw.com/wp-content/ uploads/2020/01/662_Thiele.pdf, Issue No 662, January 2020
4. “Understanding and Implementing Defense Experimentation (GUIDEx)”, NAMRAD- TTCP-JSA WF Experimentation Group,Version 1.1,March 2006
5. Searle, Jonathan R. (Manager SSEL), “Course notes and Handouts for Networked & Distributed Simulation module of MSc course in DSM”, ESD- RMCS, Cranfield University, April 2005
6. “Department of Defense Experimentation Guidebook”, https://www.dau.edu/tools/Lists/DAUTools/Attachments/381/DoD%20Experimentation%20Guidebook%20 v2.0%202021.pdf, Nov 18, 2021, p. 2
7. Karyn Matthews, Mike Davies, John Dunn, Carsten Gabrisch (1997), “Synthetic Environments for C3I Experimentation”, Information Technology Division, Defence Science and Technology Division, Salisbury
8. LTC Robert L. Bethea (Jr. U.S. Army) (2003), “Joint C4I Interoperability– A Look At The Process For Army Transformation”, USAWC Strategy Research Project, https://apps.dtic.mil/sti/pdfs/ADA414829.pdf
9. Michael R. Hieb, Lieutenant Colonel Donald H. Timian (1999), “Using Army Force-on- Force Simulations to Stimulate C4I Systems for Testing and Experimentation”, https://apps.dtic.mil/sti/pdfs/ADA461500.pdf