Booz | Allen | Hamilton®

DIGITAL SIMULATIONS

MODEL, TEST AND SCALE VIRTUAL SYSTEMS

Digital Simulations use Model Based Systems Engineering (MBSE) to create a Digital Twin of a weapon system, improving design, testing, integration and cybersecurity posture.

MODELING COMPLEXITY

As weapon systems become ever more complex, agencies within the Department of Defense must find new methods to manage complexity while reducing program cost and acquisition time. Transforming engineering practices is key to addressing this trend by streamlining design, delivery and sustainment. Digital simulations, or digital twins, represent such a transformation, bridging the gap between design and reality.

A 'Digital Twin' is a reference digital simulation that recreates the internal state and behavior of a component to seamlessly interact with real-world systems. These simulations reduce risk and cost across the weapon lifecycle by validating requirements, benchmarking performance, evaluating cyber risk, and testing upgrades.

OUR ISSUE: 1647 REPORT FOR GPS

Booz Allen was called upon to perform a vulnerability analysis for GPS Block IIR satellites. However, the risk to critical infrastructure prohibited the use of on-orbit or test assets. While a traditional paper-based assessment was available, it would be unable to directly demonstrate vulnerabilities and could not react to 'what if' scenarios.

OUR APPROACH: MODEL AND DEVELOP A DIGITAL SIMULATION

Booz Allen developed a better methodology - applicable to complex weapon systems - that fills the gap between paper assessments and full-scale replicas:

This digital simulation approach addresses the task of the 1647 report by replicating the ground, space and attack segments of the system with lightweight applications that could run on a single PC.

After reviewing thousands of pages of design documents, Booz Allen used MBSE to create a model of GPS Block IIR to characterize the system, identify potential vulnerabilities, and inform the simulation architecture.

This model was then transformed into a suite of scalable software applications which could run on one or more PCs to demonstrate and validate cyber vulnerabilities.

This solution performed as a flexible cyber test bed which allowed us to go beyond validation and propose strategies for detection and mitigation.

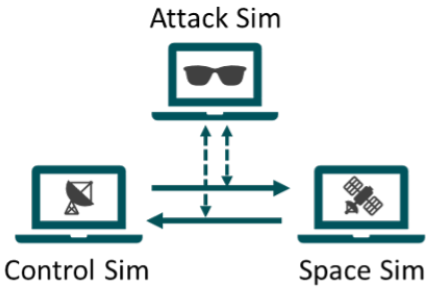
OUR APPROACH: A FLEXIBLE CYBER TEST BID

The cyber test bed comprised three applications: a control segment simulator, a space vehicle simulator, and a Man-in-the-Middle (MITM) attacker.

Running on either a single system or connected by software-defined radios (SDRs) as a local network, they form an end-to-end representation of the GPS IIR command and control system.

Beyond an isolated network, this test bed can connect with 'real' test assets to generate data, provide wargaming support, or explore attack scenarios.

In addition to a flexible architecture, the system provides a public API which provides developers a means to extend the capability through new applications built on top of the base simulation.



THE RESULTS

Creating an effective, scalable digital simulation and implementing it in a cyber test bed is not a slow, costly proposition.

Booz Allen's small team of engineers reproduced the command and control elements of the Block IIR GPS satellite and ground command system in less than 6 months, using only existing program documentation.

This test bed was then used to evaluate cybersecurity without ever risking an operational system or conducting expensive on-site tests.

BEYOND CYBER – APPLYING SIMULATIONS

The skill to comprehend complex systems, evaluate and synthesize documentation and produce a functional simulation represents the complete integration of requirements modeling, model-based systems engineering, software development and cyber security.

We see this cross-domain approach as a valuable blueprint for further efforts in design validation, testing, and security.

Digital simulations can be applied beyond cyber risk analysis to improve systems acquisition and support:

- **Requirements and requirements allocation:** Build models to ensure OEMs know what is needed.
- **Acquisition and proposal support:** Build test assets to clarify requirements.
- **Integration:** Create virtual units to test interface design and specifications.
- **Training:** Simulate threats and anomalies without risking critical infrastructure.
- **Cyber-security:** Examine security while a system is under development. Test potential mitigations.
- **Obsolescence and vendor lock:** Build reference systems to validate OEM solutions.

About Booz Allen

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems.

One of the world's largest cybersecurity providers, we solve the most consequential problems for our clients.

Unparalleled technical expertise and cyber-focused management consultants, our experts are the experts.

On the forefront of cyber innovation, we integrate intelligence-grade tradecraft with the most advanced cybersecurity solutions.

Using expert tradecraft to combat the most advanced adversaries, we are often the first company to work on really hard problems.

To learn more, visit BoozAllen.com.

For more information, please contact:

Randy Yamada
Principal
Yamada_Randy@bah.com

Sarah Olsen
Senior Associate
Olsen_Sarah@bah.com