Booz Allen®

NATIONAL CYBER

CYBER DIGITAL TWIN FRAMEWORK

SOLUTIONS OVERVIEW

The Booz Allen Hamilton Cyber Digital Twin Framework (CDTF) is a technology platform that utilizes advanced and secure software tools to provide a high fidelity all-in-one testbed for Cyber-Physical Systems. The platform provides functionality to emulate hardware in a virtual environment, integrate the hardware for hardware-in-the-loop (HWIL) testing, rapidly network physical and simulated assets, record data flow at the software level for security analysis, and consume test plans and requirements. The adaptability of the CDTF provides rapid configuration of hardware emulations and physical components, supporting the ability to mirror the behavior of an asset-under-test.

HOW IS CYBER DIGITAL TWIN DIFFERENT THAN DIGITAL TWINS?

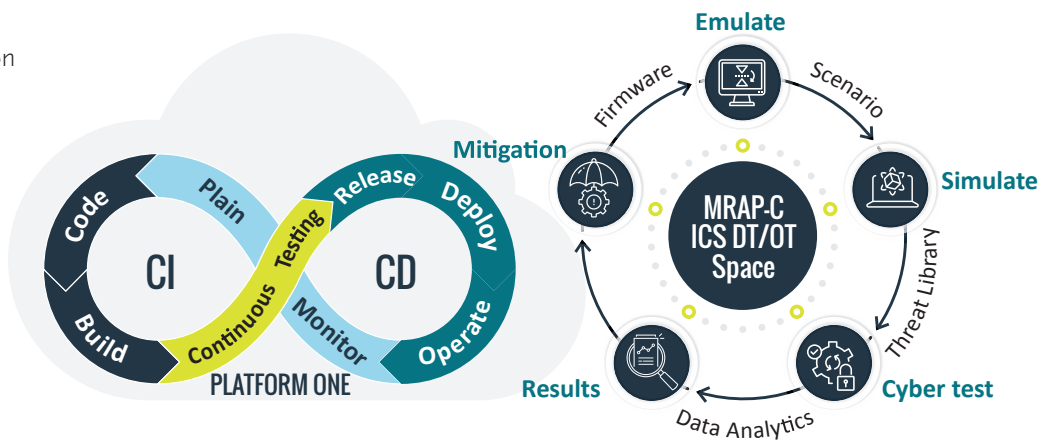
The CDTF can comprise an infinite number of Cyber Digital Twins (CDTs) running the same binary and configurations as their real-world counterparts. This supports creating twins of assets that may be too costly or restricted to acquire when conducting modeling and simulation (M&S) exercises. With the CDTF, it is possible to include these hard-to-acquire assets in larger, system-of-systems simulations—where they can interact with other simulated or real systems. Use cases include offensive and defensive cyber activities against fixed operational technology (OT) systems, vehicle systems, and weapons systems. It also allows cyber-physical testing of physical sensors like radar arrays during simulated combat activities. It can be used to scale up the number of evaluated assets to a level greater than can be achieved via traditional HWIL testing. The CDTF can also enable non-sensitive proxies for classified systems for development of novel security controls in non-sensitive lab spaces.

OUTCOMES DELIVERED

- **Emulate:** Accurately virtualize physical components
- **Simulate:** Containerize their instance and integrate into testing environment/scenario
- **Optimize:** Design system-of systems to best meet requirements at minimum risk and cost
- **Cyber Test:** Conduct testing and collect data
- **Data Analysis:** Analyze data and determine any mitigations needed
- **Mitigations:** Develop and implement mitigations into original models
- **Rerun:** Rerun your testing simulation with mitigations to determine impact

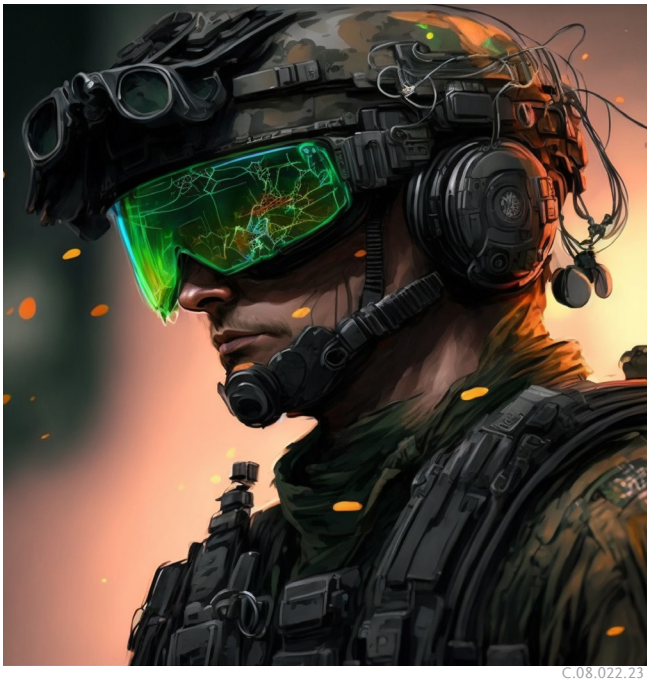
CDT CORE CAPABILITIES

- Hardware/firmware emulation
- Virtualization
- Full system images
- Hardware-in-the-loop
- Behavioral modeling
- Geospatial applications
- On-premises or in the cloud
- Pipeline integration



THE FRAMEWORK CAN BE IMPLEMENTED TO SUPPORT THE FOLLOWING TYPES OF ACTIVITIES:

- Mission-based cyber risk assessments (MBCRAs)
- Physical security assessments
- Mission exercise events
- Developmental/operational testing
- Training (offensive and defensive)
- Support cyber risk management decisions
- Cyber testing at all classification enclaves



C.08.022.23

WEAPON SYSTEM USE CASE

Department of Defense (DOD) 5000.89 requires DOD systems to have MBCRAs conducted in development. Cost of spares or the physical size of the hardware often precludes bench testing. The CDTF provides engineers with reliable results nearly identical to the actual hardware by using a CDT capable of responding to simulated inputs just as the physical piece of hardware, and then connecting that CDT to a larger simulation or HWIL environment to conduct cyber tests. The CDTF allows for rapid prototyping at different levels of fidelity, as required by the system and its test plan. Test data is automatically cataloged, and simulations can be repeated or adjusted as needed to validate or test risk mitigations. The CDTF also allows for the incorporation of the continuous integration/continuous delivery pipeline to push code under development/test into the environment to enable cyber testing within a mission-based scenario that device is required to meet.

INDUSTRIAL CONTROL SYSTEM USE CASE

Many digital twins of facilities, utilities, or port infrastructure are only 3D visualizations of static design drawings. The CDTF goes beyond that—providing the fidelity needed to test system interaction and enabling offensive or defensive cyber testing or training—what we call "bringing the model to life." An example is a building design, where the various automated systems interact physically, creating cyber and/or physical vulnerabilities to the safety and operations of the building, even when the subsystems aren't integrated electronically into a Building Automation System. In the CDTF, the system-of-systems can be tested with a wide variety of cyber effects to find any system vulnerabilities or limitations that could lead to failure. The CDTF allows for the incorporation of one or more systems such as fire alarm and suppression, electrical, heating/ventilation/air conditioning, security and access control, or telecom. The ability to conduct ad hoc and complex cyber testing now can become a common everyday activity versus an intense, time-consuming, and costly approach many clients are faced with today.

ABOUT BOOZ ALLEN

Trusted to transform missions with the power of tomorrow's technologies, Booz Allen Hamilton advances the nation's most critical civil, defense, and national security priorities. We lead, invest, and invent where it's needed most—at the forefront of complex missions, using innovation to define the future. We combine our in-depth expertise in AI and cybersecurity with leading-edge technology and engineering practices to deliver impactful solutions. Combining more than 100 years of strategic consulting expertise with the perspectives of diverse talent, we ensure results by integrating technology with an enduring focus on our clients. We're first to the future—moving missions forward to realize our purpose: **Empower People to Change the World®**.

CONTACT INFORMATION

CyberDigitalTwin@bah.com