Mission Possible

Enabling Joint Force System Interoperability

Since its establishment — and even before — the United States has relied on alliances to unite against shared enemies and bolster its military strength. The roots of these formidable relationships extend deep into military history and provide a cornerstone from which allied nations can rally to defend common interests and values against new threats. It follows logically, therefore, that maintaining military advantage through a resilient and adaptable Joint Force is a key element of the National Defense Strategy.

The imperative to strengthen partnerships among US Forces, partners, and allies has driven the Joint Force to adopt a multi-domain approach as its central operational concept. Multi-Domain Operations (MDO) depend on alignment and coordination – and U.S. leaders have committed to it as a way to continually out-match and out-pace adversaries.

But coming together demands more than agreements and changes in bureaucratic structure. It also requires changing the ways we build and maintain the mission-critical systems on which our forces rely. MDO will rely heavily on system integration.

Interoperability — the ability of components and systems to be integrated with one another — is both a priority and a prerequisite for the success of an MDO approach. **Our ability to merge the capabilities of our combined forces is the only truly sustainable and achievable route to ongoing competitive advantage.** Yet it remains a challenge. Patchworking conventional hardware engineering processes and hacking workarounds together to fit a software-driven world has become our “good enough” solution. But, as General Brown wrote in 2020, good enough today will fail tomorrow.

Barriers to integrating new capabilities, improving cyber security, and adapting to constantly changing military landscapes are becoming more apparent each day. As technical leaders, we must change the way we build and deliver software components to allow the integration of systems from multiple teams using unique tools and processes — all while continuing to meet cost, schedule, and performance demands. It’s a lot, but it’s not impossible.

“Accelerate, Change, or Lose”

Gaps between designing, developing, and fielding of new system capabilities aren’t new. Even hardware designs need to be translated between teams and forces, and the methods used to bolt everything together depended on the cultures and toolboxes of the teams building them. They worked through it, so the tools and processes we have traditionally relied on work fairly well for things you can see, but software changes the game.

The sheer complexity and nuance of software has made the disparities between our forces, allies, and teams far more treacherous. Each military branch, contractor, and ally has its own preferred standards and coding languages. The lack of standardization and limited interoperability is a recipe for “mission impossible” The trifecta of rising DoD demand for modernized systems, increasingly complex software and security environments, and rapid technological change have made it more necessary and more challenging than ever before to keep up.

Sharing technology and integrating systems in an MDO environment challenges even the most advanced engineering teams. A great deal of tedious, manual coding is required to connect disparate systems and components together — a problem that is not exclusive to DoD systems, but one that is made more severe by long-standing policy and acquisition processes that exacerbate vendor lock and prevent the sharing of systems, tools, and processes.

> **3-5 Years:** The typical time to deploy a new software functionality using currently available systems engineering processes (Defense Innovation Board May 2019)

> **70%:** The percentage of software errors introduced during requirements and design phases that aren’t realized until after implementation, where they cost up to 100x more to resolve

We cannot achieve interoperability and deliver at the speed of relevance without changing the way DoD systems are maintained. Today’s missions demand access to proprietary and off-the-shelf software components from large primes, commercial industry, and non-traditional companies to keep pace with our adversaries– and we need them quickly. This is a need the DoD understands and a heavily publicized strategic goal, but the path to true interoperability and consistent upgrades has not been clearly laid out.

> *Without sustained and predictable investment to restore readiness and modernize our military to make it fit for our time, we will rapidly lose our military advantage, resulting in a Joint Force that has legacy systems irrelevant to the defense of our people.”*
>
> - 2018 National Defense Strategy

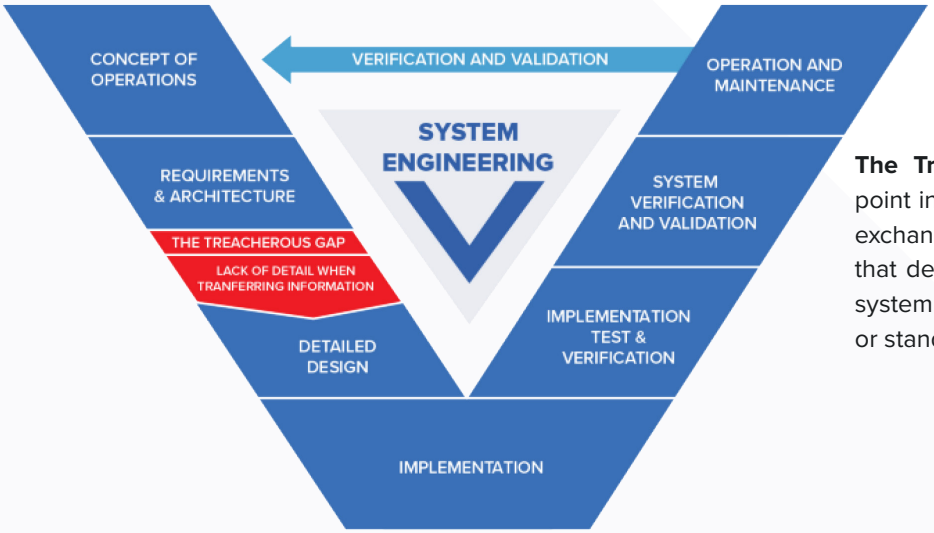
Standards Aren't Standard

The commercial world has made huge strides in adopting state-of-the-art technologies and integration between platforms. In the past five years alone, backup cameras and adaptive cruise control technologies have transitioned from high-priced luxury option packages to being standard features in almost every car– and the same technology you see in a Honda CR-V is used in a Jeep Cherokee. The advent of open source software and cooperation among industries has allowed commercial system manufacturers to quickly adapt to changing markets and advancements in technology as they arise. Consumers have come to expect easy and affordable access to the latest capabilities and, in most cases, it is widely available on demand.

These same innovations are available to the DoD, but delivering them to the systems warfighters have at hand is much slower than what we see in the open market.

Defense systems are lagging in modernization, and programs are struggling to repurpose technologies the way commercial industry has. This is not due to differences in engineering skill or funding. It's an issue of highly specialized standards and disconnection across teams on the engineering lifecycle. The lifecycle gaps between requirements, system design, software development, and implementation slow down component software integration across the board in DoD systems. It's difficult to keep pace even if the same standards apply for every team in a program– and this problem compounds when you need to work with partners who have different standards. Program leaders are challenged to deliver more capability on a shorter schedule while meeting high quality benchmarks, but introducing new technologies is slow and painful with the disjointed tools with which their teams are required to work.

Moving along the engineering V is troublesome for many large DoD projects– especially those that include software. A single miscommunication or design error can cascade into miswritten code and deep errors which escape detection until after integration, or worse, make it all the way to the field and lead to failure when the system is needed most. Joint interoperability increases the complexity of requirements, designs, and implementation, and in turn the risk to mission success.



The Treacherous Gap in the Engineering V: Any point in the engineering lifecycle where information is exchanged between those who write the requirements that define the system and those who implement the system requirements using disparate tools, processes, or standards.

Bridge The Gap

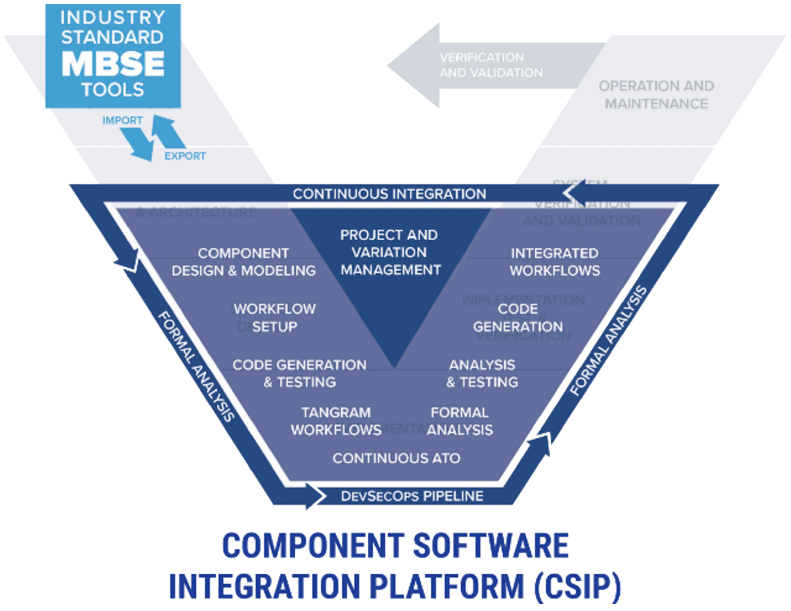
We can't just throw in the towel on MDO because it's difficult. The government needs to adopt solutions that reduce barriers to joint interoperability in mission-critical systems. Our systems can be developed, tested, and maintained more effectively and made interoperable when we are able to:

- Define system components
- Constrain software interfaces between components
- Apply focused, integrated testing and analysis
- Embrace approaches to system safety
- Share models, code, and requirements between teams.

Model-based engineering is the perfect place to start, but it doesn't solve disparities between tools, software languages, standards, and cultures that block interoperability. Component Software Integration Platforms (CSIP), however, are built to mitigate these differences.

CSIPs are centralized toolkits that connect and unify tools and processes across the engineering V. They provide a shared interface that narrows the gaps between system design and implementation by bringing together requirements, system models, and software code. Whether you're integrating Silicon Valley software into the next gen UAV or scaling a training environment to simulate MDO, a CSIP enables you to build rapidly reconfigurable, interoperable systems.

A CSIP also provides a single place where every team member can trace their work from the system's design to its code. A good CSIP integrates with system design tools like Cameo, includes a library of verified components that can be reused by software designers, and can integrate with the organization's existing deployment processes.



Improvements to the Engineering V with a CSIP: *Integrating the full system implementation lifecycle to support rapid development and deployment goals.*

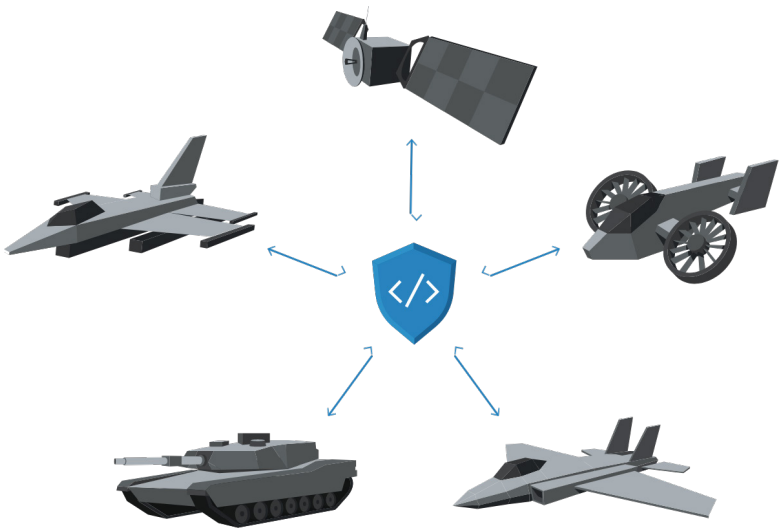
CSIP AT WORK: Training and Simulation in the DOD

Joint force collaboration and coordination is critical in modern military exercises. DoD modeling and simulation organizations are invested in developing wargames and training environments that can be accessed from multiple locations, updated to show new scenarios, and able to integrate with simulations and systems between military branches.

CSIPs help teams break complex systems down into a set of components, define how each one works on its own, and how they work together when connected. This visibility greatly improves adaptability and enables component swapability, making it feasible to quickly change training and simulation scenarios. CSIPs also generate secure code for adding or changing components, even providing translations between systems that were previously incompatible– a huge win for interoperability.

With the proper CSIP and deployment support, geographically distributed joint-force training becomes a reality.

Formula One training shows us how powerful the ability to quickly and accurately integrate seemingly unrelated systems can be. Training for races used to require drivers to be in a car that wasn't quite finished on a track that wasn't representative of where they would actually be competing. Now a driver sits in a race car seat at home and practices races in simulation using the same gaming systems they use to play Call of Duty. This is possible because the car manufacturers and game system developers can work together to quickly create and change simulations to provide distributed and realistic training through interoperable systems.



With dynamic understanding of the properties of each software component, a CSIP can allow for new breakthroughs of functionality to the warfighter, repurposing systems that have yet to be integrated or even envisioned.

Interoperability at Speed

Unifying the goals of each force, ally, and partner is the only way to deliver new capabilities at the speed our missions demand without increasing risks to safety and performance. The CSIP approach to engineering integrates the entire system implementation lifecycle, enabling teams to get better capabilities to the field faster.

This is something we spend a lot of time thinking about at Tangram Flex. A core part of the technology in our CSIP, Tangram Pro™, is our interface generation software. True interoperability magic is unlocked by automatically generated interface code that components use to send and receive data – including translations and transformations between software languages and standards.

> *We can build the best airplanes and satellites, but we will lose if we can't update the software at the speed of relevance in this century."*
>
> - Dr. Will Roper, former assistant secretary of the Air Force

TANGRAM PRO™ IN ACTION - Integrating Autonomous Systems

Each military branch uses a unique architecture and standard for its autonomous systems, presenting an obstacle to joint interoperability. This creates a burden for companies who wish to provide technology to the DoD and contractors who are tasked with integrating these systems. In support of a government prime customer, Tangram Flex uses its CSIP to generate interfaces that translate between US Air Force OMS and US Navy FACE standards. The Tangram Pro™-generated interfaces include transforms between standards, allowing our customer to focus on product development, refinement, and capability enhancements instead of writing integration code by hand.

CSIPs streamline joint force efforts and provide more control and insight into the engineering lifecycle. Rather than manually handing off design and code between teams and tools, features like the component library and shared workspaces seen in Tangram Pro™ enable a culture of sharing that's critical to joint interoperability. Bringing components, tools, and people together bridges disparate tools and processes for your technical teams and promotes reuse of components across systems and programs.

The result? Greater alignment among partners and reduced time to identify threats, deliver capabilities to the field, an d meet the needs of today's missions.

The call for joint force interoperability today is important and challenging, but we can continue to address lifecycle gaps and meet our needs where they arise by remaining adaptable and adopting the right tools for today's unique and changing systems.

Visit tangramflex.com/technology to find out how to solve the interoperability problem with Tangram Pro™.

TANGRAMFLEX

At Tangram Flex, we understand the challenges of security, speed, and safety. That's why we are dedicated to simplifying software integration for mission-critical defense systems. Our team combines engineering expertise with our core product, Tangram Pro™ to arm customers with customized toolkits for meeting mission needs. Tangram Flex is headquartered in Dayton, Ohio, the home of Wilbur and Orville Wright and a hub of defense innovation. Get in touch: hello@tangramflex.com