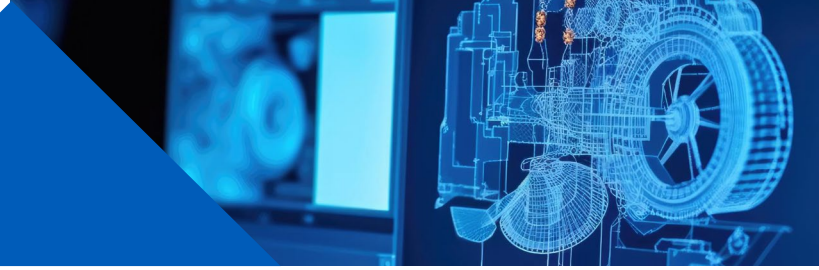


TRADEOFFS FOR FEDERAL GOVERNMENT USE OF DIGITAL TWINS

WHAT IS A DIGITAL TWIN?

A digital twin is a digital representation of a physical object, system, or process that provides **feedback** and/or **control** to the physical system using simulation, artificial intelligence/machine learning (AI/ML), and optimization. It is designed to replicate real-world conditions and behaviors and is continuously updated with data from sensors on its physical counterpart.

While both a digital twin and a model can represent real-world entities, a model is typically a static or predefined representation of a system that does not provide direct feedback and control. In contrast, a digital twin is dynamic, continuously evolving based on real-time data feeds from its physical counterpart. It therefore offers a more holistic and up-to-date representation of its state and performance, enabling real-time feedback and control.

VALUE PROPOSITION

Digital twins can bring **business impact** through long-term cost savings and improvement of processes and efficiency. Realization of value depends on the **technical feasibility** of the twinning effort, which is a function of available infrastructure, connectivity, data access, and design maturity. Use cases should consider both of these factors before proceeding with design.

Overall, applications that can maximize economies of scale tend to be best suited to maximizing digital twin benefits. Similarly, twins of costly systems (e.g., an aircraft) can draw substantial benefit when simulating failure modes. A digital twin should be geared at the failure points, production losses, or downtime situations. Improving an asset's performance, reducing downtime, and increasing production or throughput, in alignment with an organization's objectives and business cases is appropriate.

WHAT SHOULD FEDERAL AGENCIES CONSIDER?

Limited budgets for technology investment mean that the cost-benefit balance must be carefully understood. While digital twins provide opportunity to improve aviation systems, they also pose a risk in making changes to the operational environment. The federal government must also consider protection of sensitive data from release, to maintain safety and security, and to meet certain regulatory responsibilities, which could be affected by using digital twins.

HOW CAN AVIATION BENEFIT FROM DIGITAL TWINS?

For the aviation industry, digital twin technology has the capability to enable maintenance automation, efficiency improvements, and analytics of aircraft, navigational aids, and aviation systems. To realize these improvements, a considerable amount of data must be collected, and a suite of complex models and simulations of physical systems must be created and maintained. Comprehensive insights into real-time behaviors support making better decisions with less lead time. However, the desire to increase aviation efficiency must be balanced with the need to maintain safety.

SYSTEMS ENGINEERING OF A DIGITAL TWIN

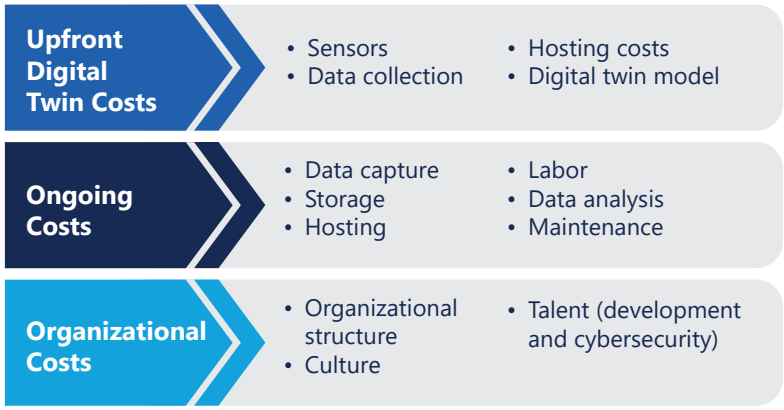
In order to produce a digital twin, planning and design need to consider multiple factors: the way in which the digital twin will operate and how the model will be built; the costs that will be associated both upfront and in the longer term; risks of the twin to the physical system; and cybersecurity concerns and impacts to the entire enterprise.

USE OF MODEL-BASED SYSTEMS ENGINEERING

Model-based systems engineering (MBSE) is a methodology that involves a complete model of a system's requirements, design, verification, and validation. MBSE allows digital twin developers to build and maintain the twin and ensure that the system requirements, architectures, interfaces, and data flows are accurately identified and managed throughout the system lifecycle. Models for digital twins can be very complex, and MBSE can model the system and subsystems, factoring in the physical architecture, operating environment, and sensor and interface data feeds. Building and maintaining an MBSE model can add to the costs associated with designing a digital twin system but could save ongoing documentation costs.

FACTORS OF COST

Digital twins are a significant investment, and only cases with high business impact, economies of scale, or significant long-term cost savings are typically worthwhile. Both technical costs and organizational costs must be considered and assessed with the value of the digital twin application. The **upfront technical costs** include developing algorithms, building the model, instituting data collection from the physical system, data analysis, physical assets, and long-term server or cloud hosting costs. **Ongoing** technical costs include data capture and storage, compute costs, and labor. **Organizational** costs involve obtaining and retaining talent, such as developers and cybersecurity personnel, and the overall organizational structure and culture to extract value from a digital twin while balancing the risks.



RISKS

Because digital twins can be used as feedback mechanisms to make operational changes, the risks introduced must be evaluated. Erroneous changes caused by inaccuracies in the model, sensor failure or degradation, and delays in the data feed could introduce faulty changes leading to severe damage or safety risk. To prevent incorrect feedback delivered to the physical systems, additional controls, such as human-in-the-loop decision-making may need to be implemented or a more rigorous review of processes, error code mitigation, and planning conducted.

CYBERSECURITY

Digital twins enable real-time monitoring and control of their physical counterpart, making them attractive targets for malicious and unauthorized users. Prior to investing, the organization should develop an in-depth understanding of how digital twins are accessed and monitored, as well as how quickly the organization can detect suspicious activities to scope security concerns of security. Implementing robust cybersecurity practices to digital twins (e.g., firewalls and intrusion detection systems, data encryption, strong authentication and access controls, and a Zero Trust network architecture) ensures that the protection of an organization's sensitive data endures even after deployment.

ABOUT CNA

CNA is a nonprofit research and analysis organization dedicated to the safety and security of the nation. It operates the Institute for Public Research—which serves civilian government agencies—and the Center for Naval Analyses, the Department of the Navy's federally funded research and development center (FFRDC). CNA develops actionable solutions to complex problems of national importance. With nearly 700 scientists, analysts, and professional staff, CNA takes a real-world approach to gathering data, working side by side with operators and decision-makers around the world. CNA's research portfolio includes global security and strategic competition, homeland security, emergency management, criminal justice, public health, data management, systems analysis, naval operations, and fleet and operational readiness.

CNA's report *Federal Government Decision-Making for Digital Twins in Aviation* details both the benefits and the risks, costs, and impacts of using digital twins. To learn more, discuss the viability of potential digital twin applications, or request a copy of CNA's report, contact:

Halleh Seyson, Vice President, Enterprise Systems and Data Analysis | hallehs@cna.org
Shaelynn Hales, Director, Center for Data Management and Analytics | hales@cna.org
Marina Rozenblat, Chief Scientist, Center for Data Management and Analytics | rozenblatm@cna.org

IMM-2024-U-040137-Final