Design & Process

eGuide

SECURING DEFENSE ENGINEERING DATA

From Compliance to Strategic Advantage

Executive Summary

In today's defense engineering landscape, data isn't just a byproduct of operations — it's a strategic asset that can drive competitive advantage, enhance security, and accelerate innovation. For defense contractors, integrators, and suppliers, mastering engineering data isn’t optional — it’s mission-critical. Yet many organizations struggle to transform their engineering data management from a compliance requirement into a strategic capability.

"The Department of Defense has elevated transformation to Digital Engineering as a core mission objective... Continuous insight/oversight via digital collaborative environment and interaction with the Single Source of Truth is essential." [5]

Steve Ruffin
Chief Executive Officer
Design & Process

TABLE OF CONTENTS

The Evolution of Engineering Data Management

From File Systems to Integrated Ecosystems

The defense industry's approach to engineering data has undergone a dramatic transformation. What began as basic file management has evolved into a complex ecosystem of interconnected information that drives decision-making, ensures compliance, and enables innovation.

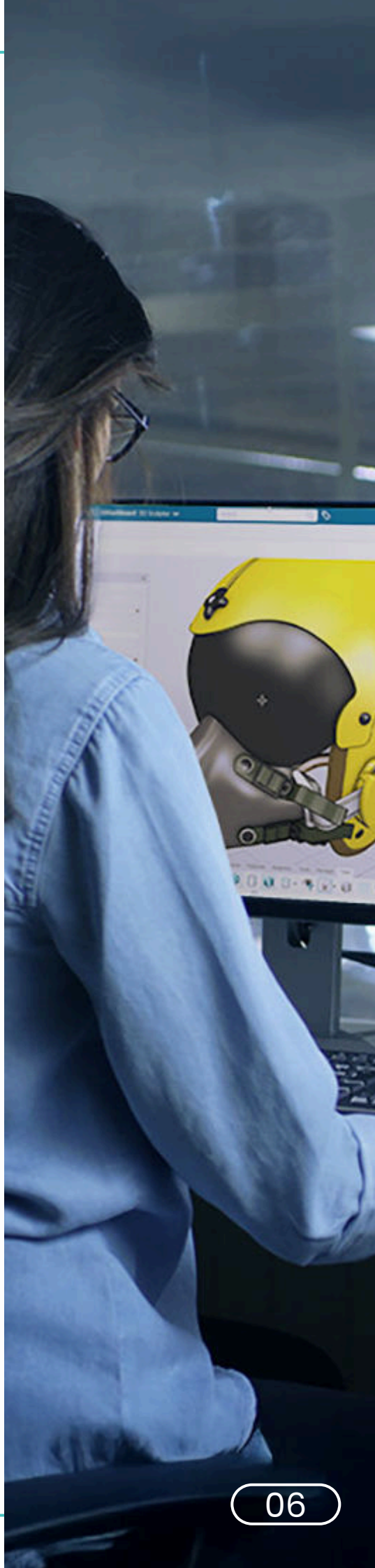
According to Department of Defense statistics, the commitment to digital transformation is clear:

- RDT&E funding has surged more than 86% in the past seven years [2]
- Funding accounts for 17.5% of the entire defense budget [3]
- FY 2025 requested funding reached $145.7 billion [4]

Current Challenges in Defense Engineering Data Management

The complexity of defense engineering data management creates unique challenges that impact efficiency, security, and innovation. We see firsthand how these barriers affect programs across the lifecycle of design and product. These challenges are best illustrated through real-world scenarios we encounter.

During an engagement with a federal RDT&E facility, the Design & Process team witnessed two engineers in the same cubicle exchange design data via DVD despite having networked computers. This seemingly simple data transfer underscores deeper systemic issues in digital infrastructure and policy within the defense sector.



Fragmented Data Storage & Security Protocol Conflicts

The facility lacked a centralized repository for storing designs. The base IT group, unable to guarantee data security within specific Program groups, defaulted to preventing shared locations entirely. This common scenario forces engineers to resort to manual data transfer methods, significantly impacting productivity while potentially compromising security.

Version Control & Data Integrity

After the senior engineer completed simulation work and made design changes, there were now two disconnected versions of the model with no clear way to determine the correct iteration. This version control challenge is amplified in defense environments where multiple teams may be working on different aspects of the same project, each requiring accurate, up-to-date design data.

Data Accessibility & Continuity

When the engineer later transferred to another base, the local IT group wiped their workstation as part of standard security protocols. Without proper data management systems in place, all 3D data was lost. At best, this meant reverting to 2D PDFs provided to the acquisition group. At worst, it meant complete data loss requiring expensive and time-consuming recreation of models.

Loss of Institutional Knowledge

Beyond just losing files, the lack of proper data management means losing valuable context:

- Design intent and engineering decisions
- Historical revision data
- Project-specific requirements and constraints
- Cross-team collaboration insights
- Compliance and certification documentation

These challenges compound over time, creating inefficiencies that impact project timelines, increase costs, and potentially compromise security protocols. This knowledge — once lost — is nearly impossible to recover, especially in organizations where workforce churn or contractor transitions are common.

The Cost of Ineffective Data Management

In the complex world of defense engineering, ineffective data management can create a cascade of costly and operationally critical challenges that extend far beyond simple file storage:

- Duplicate work requiring complete vehicle disassembly
- Lost engineering hours scanning existing parts
- Inaccessible data stored on contractor systems
- Risk of future data loss
- Delayed equipment upgrades and repairs

CASE STUDY

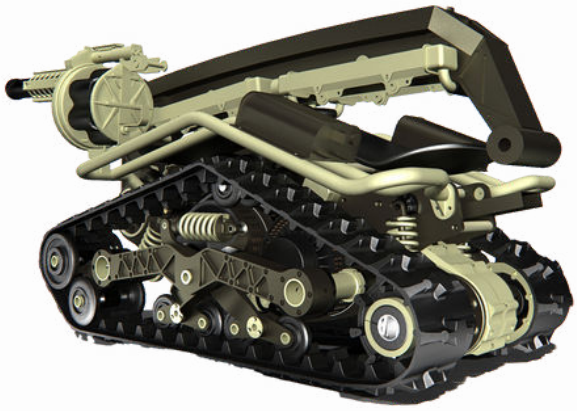
MRAP Vehicle Data Loss

I witnessed the complete disassembly of several $500K Oshkosh Cougar MRAP vehicles so they could scan all the parts into 3D models. The Military needed these models to aid the interfacing of new equipment and the repair or replacement of parts. What happened after they scanned all this data? They kept it on the contractor's system since they didn't have a place to store it!

Steve Ruffin
Chief Executive Officer
Design & Process

The case of the MRAP vehicles illustrates the profound inefficiencies that can emerge when digital engineering practices fall short. This scenario is not unique. Across multiple programs, we've seen the consequences of fragmented design ecosystems, outdated PDM practices, and poorly defined data ownership.

Consider the extraordinary lengths the Military was forced to go to in order to create 3D models of these $500,000 vehicles. Rather than accessing existing documentation or digital designs, engineers were compelled to completely disassemble multiple vehicles — a process that represents a staggering waste of resources. Each disassembly not only consumed significant labor hours but also potentially compromised the structural integrity of expensive military assets. Highly skilled engineers, whose expertise is both rare and valuable, were reduced to performing what essentially amounted to mechanical archaeology, meticulously scanning and documenting parts that should have been readily available in a well-managed digital repository.



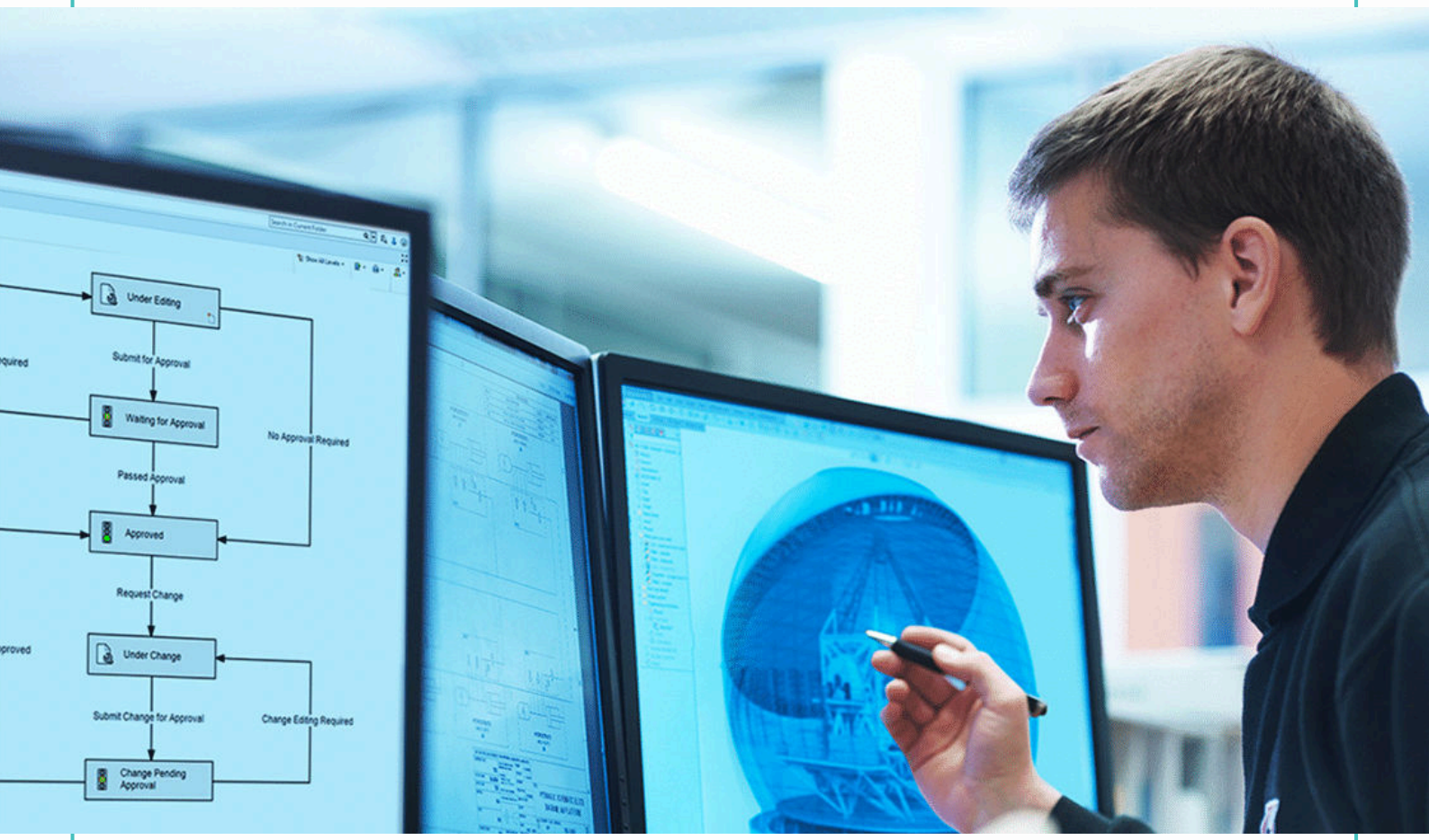
The ripple effects of this data mismanagement extend far beyond the immediate project. By storing critical design information on disparate contractor systems, the military creates multiple points of vulnerability. Data becomes isolated, making collaborative efforts nearly impossible and creating significant risks for future maintenance, upgrades, and institutional knowledge preservation.

Imagine the scenario where a critical piece of military equipment needs urgent repair, but the original design specifications have been lost or are trapped in an inaccessible system. The potential consequences range from operational delays to compromised national security.

These inefficiencies directly impact military readiness and technological adaptation. Equipment upgrades are delayed, maintenance becomes more complicated, and the ability to quickly respond to changing strategic needs is severely hampered. The cost is not just monetary — though the financial implications are substantial — but also operational and strategic.

For organizations like Design & Process, these challenges represent more than just technical problems — they're opportunities to fundamentally reimagine how engineering data is captured, stored, shared, and leveraged.

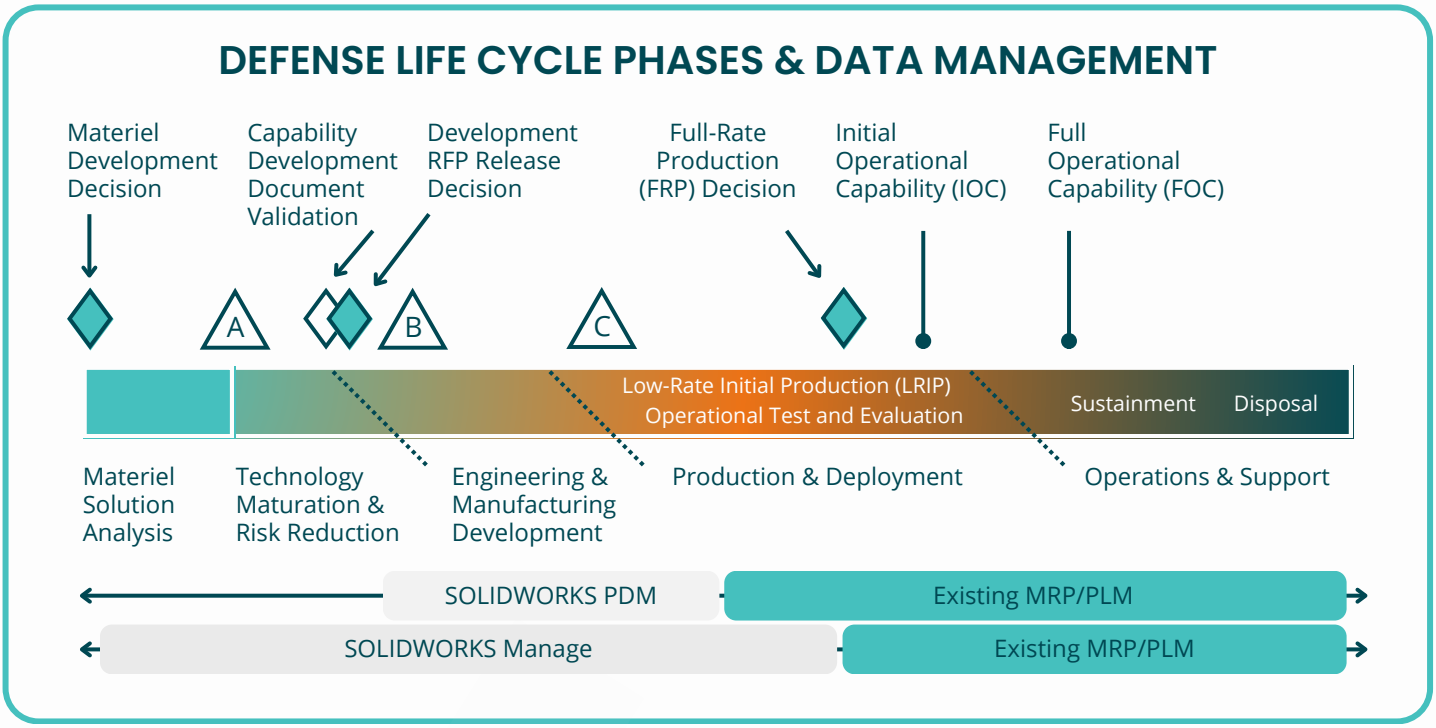
By implementing comprehensive digital engineering strategies, it becomes possible to transform these inefficiencies into competitive advantages, ensuring that every piece of engineering knowledge is not just preserved, but actively contributes to innovation and operational excellence.



The future of defense engineering lies not in manually scanning disassembled vehicles, but in creating robust, secure, and interconnected digital ecosystems that allow instant access to critical design information, enable rapid iteration, and support the mission-critical work of keeping nations secure.

A Comprehensive Data Governance Framework

Beyond Technical Implementation



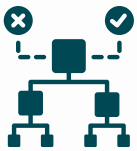
Organizations must view data governance as a cross-functional initiative that blends IT, engineering, manufacturing, and compliance. Some of our recent implementations demonstrate the importance of a comprehensive approach that addresses:

Organizational Structure

Successful data governance begins with a clear organizational structure that defines precise roles and responsibilities for data management. This isn't about creating bureaucratic layers, but about ensuring that every team member understands their critical role in maintaining, protecting, and leveraging engineering data.

Security Protocols

Security protocols are critical in defense environments where ITAR compliance and national security demand strict control over engineering data. Meeting standards like CMMC and NIST 800-171 requires solutions that offer role-based access, multi-factor authentication, FIPS-compliant encryption, and full auditability. We deliver purpose-built, defense-ready engineering data management systems that are easier to secure, faster to deploy, and tailored for compliance—ensuring every interaction with sensitive data is controlled, tracked, and protected.



Workflow Optimization

Workflow optimization represents the practical implementation of these strategic considerations. By streamlining processes for data access and sharing, organizations can break down silos that traditionally impede collaboration. This means creating systems that allow the right people to access the right information at the right time, without compromising security or creating unnecessary friction.

Training & Adoption

The most sophisticated systems are meaningless without user adoption. Effective digital transformation programs build training into every phase — from pilot deployment to sustainment — ensuring high utilization and confidence among users from junior engineers to senior managers. This cultural component transforms technical solutions from mere software into strategic assets.

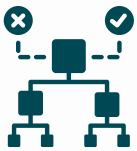
Compliance Management

Compliance management serves as the ongoing backbone of this approach. It's not a one-time effort, but a continuous process of monitoring, documenting, and refining how engineering data is created, stored, shared, and ultimately utilized. In the defense sector, where precision and accountability are paramount, this ongoing vigilance isn't just good practice — it's essential.

Ultimately, effective data governance in defense engineering is about creating an integrated ecosystem where technology, process, and people work in harmony. It's a strategic approach that transforms data from a potential liability into a powerful competitive advantage

Cultural Considerations

Program managers and directors are key to transforming into a Digital Engineering environment. Key cultural changes needed to ensure successful implementation include:

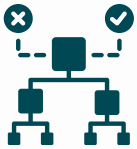


Shifting from 2D PDF deliverables to full 3D model-based definitions

This critical transformation isn't merely a technical upgrade, but a philosophical change in how engineering data is conceived, shared, and utilized. Three-dimensional models provide rich, contextual information that flat PDFs can never capture, enabling more precise communication, better decision-making, and enhanced collaborative potential.

Establishing processes for securing sensitive data while maintaining accessibility

In the defense sector, this balancing act is particularly challenging — protecting classified information while ensuring that necessary personnel can access vital engineering insights. It requires a nuanced approach that combines robust security protocols with intelligent, flexible information management.

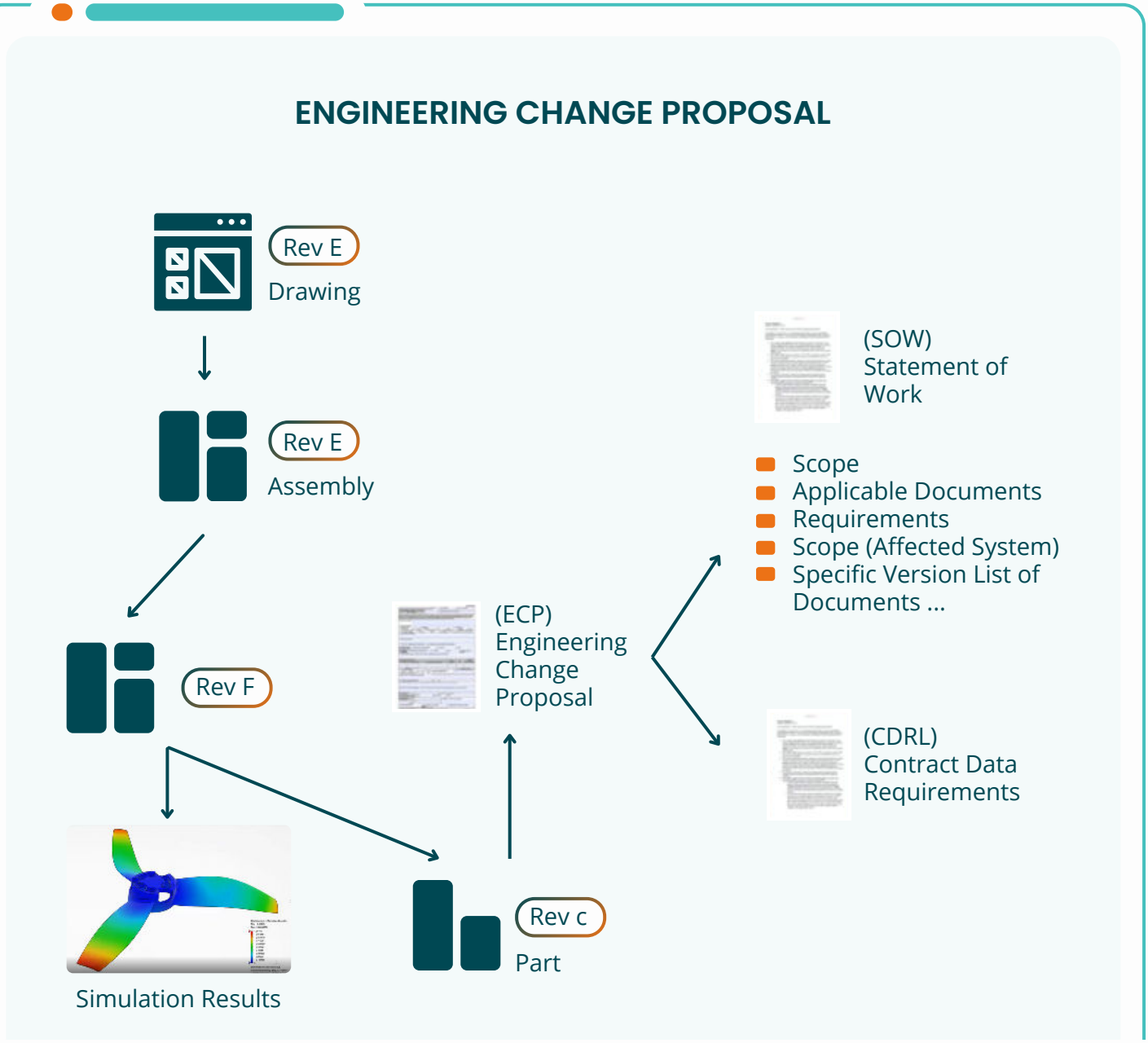


Creating centralized repositories for storing engineering data

Centralized data repositories emerge as a key strategic infrastructure, replacing the fragmented, siloed approach that has historically plagued defense engineering. By creating a single source of truth, organizations can dramatically improve data integrity, reduce redundancy, and create a more collaborative engineering environment.

Implementing standardized revision control practices

Underpinning these efforts must be standardized revision control practices. In an industry where precision can mean the difference between mission success and failure, tracking every modification, understanding design evolution, and maintaining a clear historical record becomes paramount.



These cultural changes represent more than technological implementation — they're a fundamental reimagining of how engineering knowledge is created, preserved, and leveraged.

CASE STUDY

Air Force Equipment Documentation

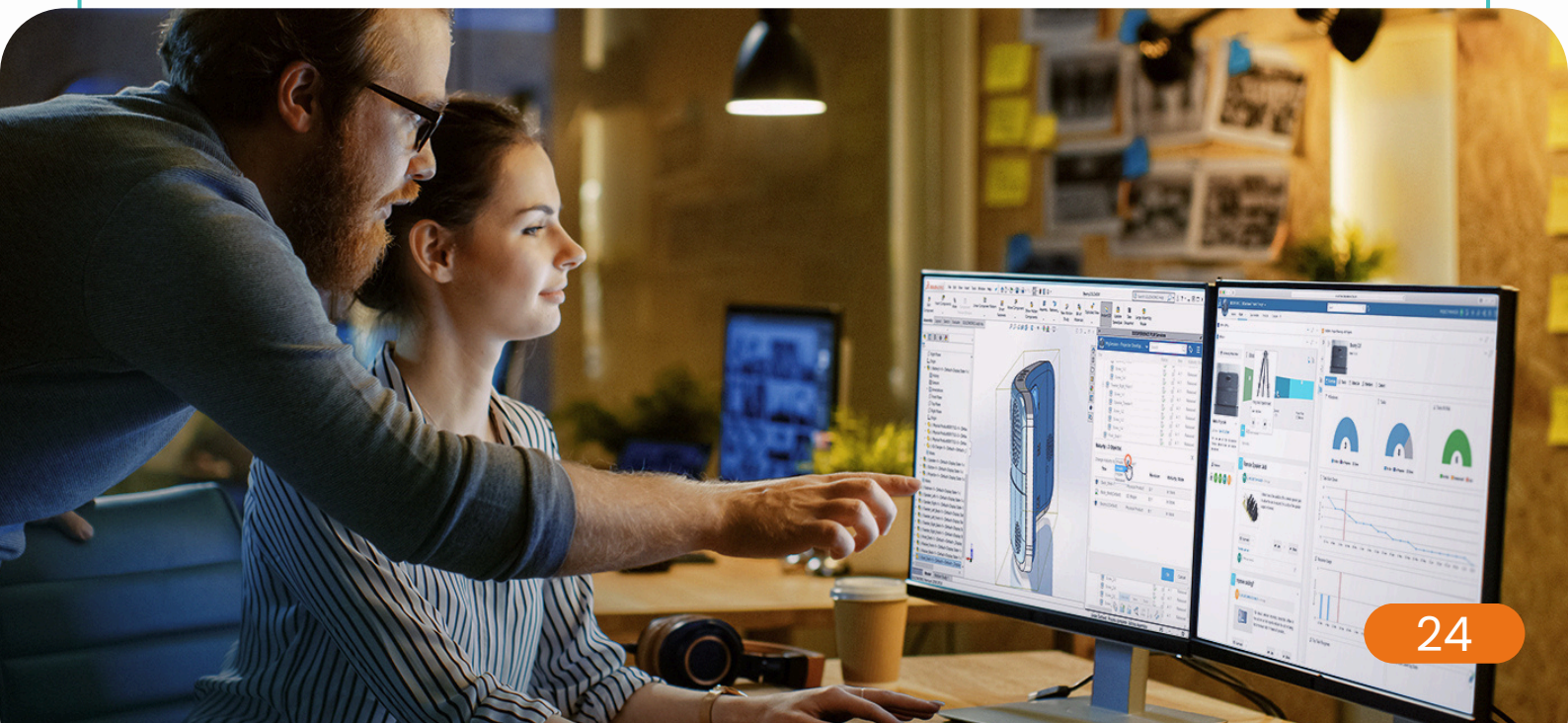
A group at an Air Force base that developed weapons loading equipment for aircraft illustrates common cultural challenges. Once equipment is designed and tested, they need to provide information so other military bases can create it locally. However, they only provide 2D information, forcing bases to recreate complicated parts in 3D - despite having the original 3D SOLIDWORKS designs available. The lack of proper data management processes means valuable 3D engineering data can't be reliably distributed.

Technology-Enabled Governance

A comprehensive data governance strategy requires more than just basic file management. Today's defense engineering challenges demand a fully integrated suite of tools that work together seamlessly. SOLIDWORKS offers a complete ecosystem designed specifically for these complex needs, where mechanical design integrates naturally with electrical systems, simulation validates designs before production, and product data management ensures every stakeholder has access to the right information at the right time.

The true power lies in how these tools work together. For instance, while SOLIDWORKS PDM serves as the backbone for data management, it becomes exponentially more valuable when integrated with tools like SOLIDWORKS Composer for technical documentation and SOLIDWORKS Inspection for quality control. This integration ensures that when an engineer updates a design, all downstream documentation and inspection requirements automatically reflect those changes.

For defense contractors dealing with complex assemblies, the combination of SOLIDWORKS Mechanical and Electrical capabilities enables true concurrent engineering. Teams can work simultaneously on mechanical components and electrical systems, with changes in one domain automatically reflected in the other. This level of integration is particularly crucial in defense projects where electrical and mechanical systems must work in perfect harmony.



CASE STUDY

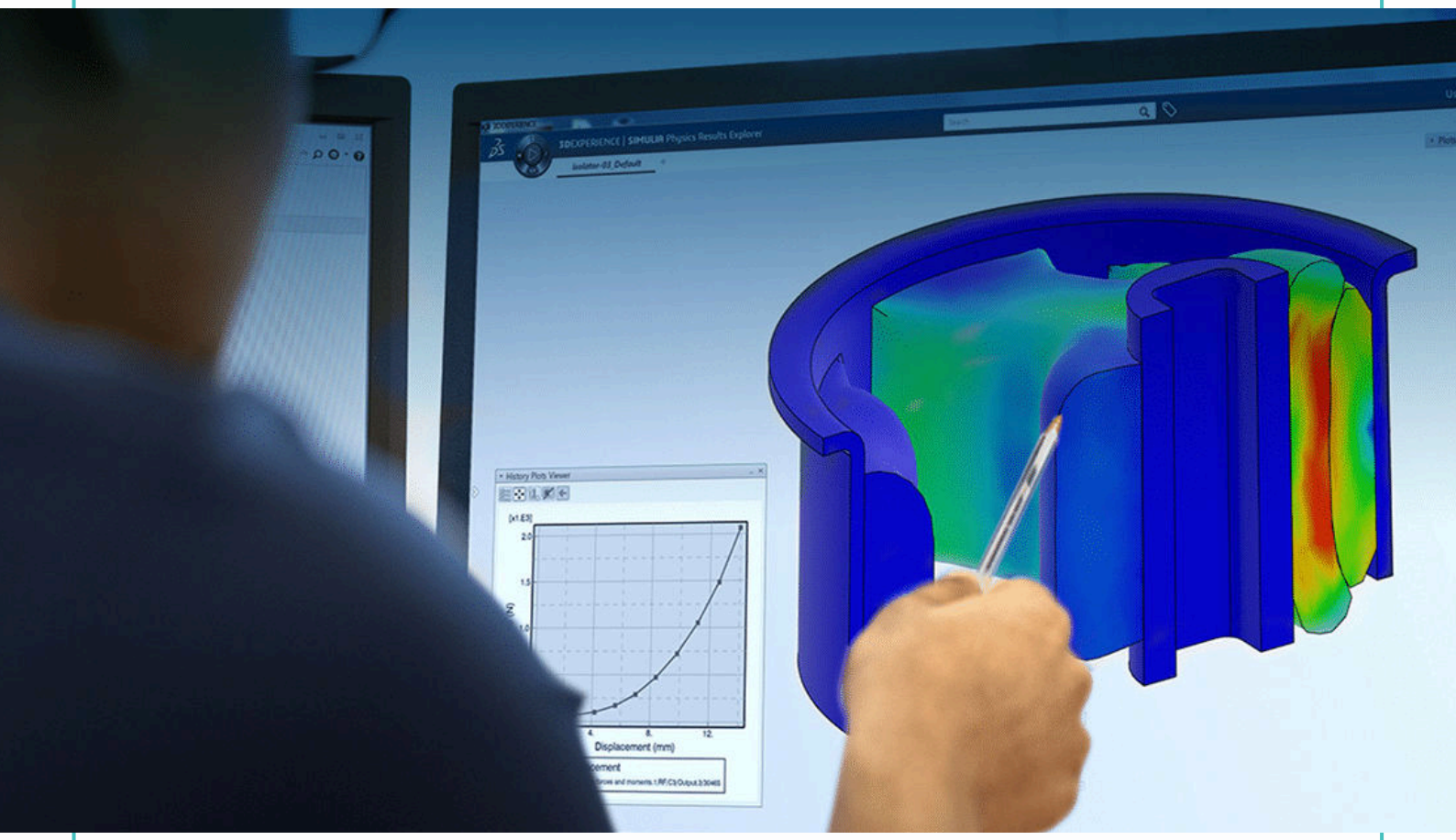
A Large Arms Manufacturing Company's PDM Implementation

In a recent implementation, the client repeatedly noted how smooth their PDM system upgrade went compared to past experiences. For a system supporting 50 daily users, the client emphasized two key factors in the success:

1. The IT team's confidence in Design & Process's understanding of both software and server/security requirements

2. The focus on maintaining data integrity throughout the migration process

The addition of manufacturing-focused tools like SOLIDWORKS CAM means that production considerations can be evaluated early in the design process, reducing costly late-stage changes.



Meanwhile, SOLIDWORKS MBD (Model Based Definition) supports the defense industry's move toward complete digital engineering by enabling the creation of comprehensive 3D data packages that include not just geometry, but also manufacturing and inspection requirements.

Ready to transform your engineering data management from a compliance requirement to a strategic advantage?

Design & Process offers:

- Complete SOLIDWORKS Platform Implementation & Integration
- Secure Engineering Data Management for DoD Environments
- Engineering Data Governance Assessments & Strategic Planning
- End-to-end product development process assessment & gap analysis
- Model-Based Enterprise (MBE) Strategy & Deployment Comprehensive Technical Support

Contact Design & Process today to begin your digital engineering transformation.

Sources

1. Naval Air Systems Command Digital Engineering Initiative Report
2. Department of Defense Research, Development, Test, and Evaluation (RDT&E): Appropriations Structure
3. FY2025 Defense Appropriations: Summary of Funding
4. Department of Defense Fiscal Year (FY) 2025 Budget Estimates
5. Department of Defense Digital Engineering Strategy


Design
&
Process