PROSTEP GROUP

WHITEPAPER

# DIGITALISIERUNG IN DER VERTEIDIGUNGSINDUSTRIE

Digitale Kollaboration, regulatorische Compliance
und der Weg zu Software-Defined Defense


# Inhaltsverzeichnis

# Einleitung

Die Verteidigungsindustrie befindet sich in einer Phase tiefgreifender Transformation. Internationale Kooperationsprogramme, steigende Softwareanteile und eine volatile sicherheitspolitische Lage erfordern Entwicklungsansätze, die deutlich schneller, transparenter und resilienter sind als bisher. Klassische, isolierte Entwicklungs- und IT-Strukturen stoßen dabei zunehmend an ihre Grenzen. Gefragt sind integrierte digitale Architekturen, die eine sichere Zusammenarbeit über Organisations und Ländergrenzen hinweg ermöglichen und gleichzeitig regulatorische Anforderungen konsequent berücksichtigen.

Zentrale Bedeutung kommt dabei der durchgängigen Verknüpfung von Daten über den gesamten Lebenszyklus militärischer Systeme zu. Digitale Ansätze wie Digital Thread und Digital Twin schaffen die Grundlage für vollständige Nachvollziehbarkeit von Anforderungen, Architekturen, Software, Tests, Produktion und Betrieb. Sie ermöglichen simulationsbasierte Entwicklung, virtuelle Validierung sowie eine kontinuierliche Weiterentwicklung bestehender Waffensysteme über Jahrzehnte hinweg. Modellbasiertes Systems Engineering (MBSE) und modulare, offene Systemarchitekturen unterstützen diesen Ansatz, indem sie Komplexität beherrschbar machen und Änderungen frühzeitig bewertbar halten.

Engineering-Daten, Systemmodelle und Softwareartefakte müssen über Unternehmens- und Ländergrenzen hinweg ausgetauscht werden. Gleichzeitig müssen Sicherheitsanforderungen, Exportkontrollvorschriften und unterschiedliche IT-Infrastrukturen berücksichtigt werden. Die Fähigkeit, solche kollaborativen Entwicklungsprozesse effizient zu unterstützen, wird damit zu einem entscheidenden Erfolgsfaktor. Dabei sieht sich die Verteidigungsindustrie mit Architekturvorgaben wie der Modular Open Systems Approach (MOSA), Cybersecurity-Standards oder der DoDI 5000.97 Engineering Richtlinie NATO-Interoperabilitätsanforderungen sowie Exportkontrollregularien konfrontiert, die zusätzliche Anforderungen an die Gestaltung digitaler Entwicklungs- und Kollaborationslösungen stellen.

Für Unternehmen der Verteidigungsindustrie ergibt sich daraus eine klare strategische Leitlinie: Digitalisierung darf nicht isoliert betrachtet werden, sondern muss Technik, Prozesse, Organisation und Regulierung ganzheitlich verbinden. Wer integrierte Engineering Architekturen, sichere Kollaboration und softwaredefinierte Ansätze konsequent umsetzt, schafft die Basis für effizientere Entwicklungsprogramme, höhere Systemtransparenz und eine langfristig tragfähige Transformation hin zu Software-Defined Defense und erhöht damit letztendlich seine Wettbewerbsfähigkeit.

# Herausforderungen der Digitalisierung in kollaborativen Verteidigungsprogrammen

Die Digitalisierung in der Verteidigungsindustrie ist aufgrund der Besonderheiten der Branchen und der Kollaboration-Anforderungen besonders komplex. Mehrere Faktoren verstärken sich gegenseitig:

- **Lange Lebenszyklen:** Plattformen wie Kampfflugzeuge, Schiffe oder gepanzerte Fahrzeuge bleiben oft 30–50 Jahre im Einsatz. Hardware-Upgrades, Softwaremodernisierungen und neue Missionsfunktionen müssen kontinuierlich integriert werden.
- **Softwarekomplexität:** Moderne Plattformen enthalten Millionen von Softwarezeilen und zahlreiche miteinander vernetzte Subsysteme. Änderungen an einer Komponente haben systemweite Auswirkungen.
- **Internationale Programme:** Multinationale Joint-Venture-Strukturen erfordern Abstimmungen zwischen Partnern mit unterschiedlichen IT-Systemen, Prozessen und Sicherheitsanforderungen.
- **Regulatorische Anforderungen:** Architekturvorgaben wie MOSA, US-DoD-Richtlinien (DoDI 5000.97), Cybersecurity-Standards (RMF, NIST SP 800-53), Geheimschutz, NATO-Interoperabilität und Exportkontrollen (ITAR, EAR) müssen beachtet werden.
- **Fragmentierte IT-Landschaften:** Historisch gewachsene Systemlandschaften erschweren den unternehmensinternen und - externen Austausch von Informationen zwischen Engineering-, Produktions- und Wartungssystemen.

Um diese Herausforderungen bewältigen und komplexe Entwicklungsprogramme effizient steuern zu können, benötigen die Unternehmen der Verteidigungsindustrie integrierte Daten-Architekturen, modellbasierte Entwicklungswerkzeuge, leistungsfähige Digital Thread-Plattformen und sichere Kollaborationslösungen.

# Regulatorische Compliance und MOSA als Treiber der Digitalisierung

Die Digitalisierung der Verteidigungsindustrie findet in einem stark regulierten Umfeld statt. Neben technologischen Herausforderungen müssen Unternehmen eine Vielzahl von Vorgaben in punkto Architektur, Cybersecurity, Geheimschutz, Exportkontrolle und Interoperabilität erfüllen. Diese Anforderungen beeinflussen zunehmend auch die Gestaltung ihrer digitalen Engineering-Architekturen. Regulatorische Compliance wird damit zu einem zentralen Faktor für die Architektur moderner Entwicklungsumgebungen.

Eine wichtige Rolle spielen in diesem Kontext insbesondere Vorgaben des US-Verteidigungsministeriums, die aufgrund der internationalen Vernetzung der Verteidigungsindustrie weit über die USA hinaus Wirkung entfalten. Richtlinien wie **DoDI 5000.97** fordern unter anderem eine stärkere Nutzung digitaler Engineering-Methoden, modulare Systemarchitekturen, die Nutzung von **Digital Thread**- und **Digital Twin**-Lösungen, den Einsatz von Standards und die Fähigkeit, Softwarefunktionen schneller in bestehende Waffensysteme zu integrieren.

Ein **zentrales Architekturprinzip** ist der Modular Open Systems Approach (**MOSA**). Dieser Ansatz verlangt, dass militärische Systeme modular aufgebaut sind und auf offenen, standardisierten Schnittstellen basieren. Ziel ist es, Abhängigkeiten von einzelnen Herstellern zu reduzieren und gleichzeitig Innovationen schneller in bestehende Systeme integrieren zu können. Auch die NATO Industrial Advisary Group empfiehlt den Einsatz von MOSA. Für die Industrie bedeutet dies, dass Systemarchitekturen von Beginn an auf Erweiterbarkeit und Austauschbarkeit von Komponenten ausgelegt sein müssen. MOSA schreibt allerdings nicht vor, wie diese Architektur aufgebaut sein soll, sondern überlässt es den beteiligten Partnern zu entscheiden, welche Standards sie für ihr Programm nutzen wollen. **MOSA verlagert die implizite Gesamtintegration hin zu einer expliziten Architektur-, Schnittstellen-, Konfigurations- und Nachweisbeherrschung.** Genau deshalb ist Systems-Engineering-Fähigkeit der eigentliche Kern des Ansatzes.

Neben Architekturvorgaben spielen Cybersecurity-Anforderungen eine zentrale Rolle. Militärische Systeme sind zunehmend digital vernetzt und müssen entsprechend gegen Cyber-Bedrohungen geschützt werden. Rahmenwerke wie das Risk Management Framework sowie Sicherheitsstandards wie NIST SP 800-53 definieren hierfür umfassende Anforderungen an Risikomanagement, Zugriffskontrolle und Sicherheitsüberwachung.

Ein weiterer wichtiger Aspekt sind Exportkontrollvorschriften. Regelwerke wie die International Traffic in Arms Regulations (ITAR) und die Export Administration Regulations (EAR) regeln den Umgang mit sicherheitsrelevanten Technologien und Daten. In multinationalen Entwicklungsprogrammen müssen Unternehmen daher sicherstellen, dass sensible Informationen nur autorisierten Personen zugänglich sind und kontrolliert zwischen Partnerorganisationen ausgetauscht werden können. **Digitale Kollaborationsplattformen** benötigen dafür Funktionen wie rollenbasierte Zugriffskontrolle, Datenklassifikation und nachvollziehbare Freigabeprozesse.

Um die regulatorische Compliance sicherzustellen, müssen diese Vorgaben und Standards in den IT-Systemen und -Prozessen der Unternehmen verankert werden. PROSTEP kann ihnen helfen, ihre IT-Landschaften entsprechend anzupassen. Mit unserer Erfahrung haben wir z.B. die Sierra Nevada Corp. bei der Umsetzung der DoDI 5000.97 Richtlinie und von MOSA unterstützt.

# Integration der Unternehmensprozesse und IT-Landschaften

Eine wesentliche Voraussetzung für die Digitalisierung in der Verteidigungsindustrie ist die Integration der bestehenden Engineering- und IT-Landschaft. Viele Unternehmen verfügen über historisch gewachsene Systemumgebungen, die nicht oder nur partiell miteinander verbunden sind. Das führt zu fragmentierten Datenstrukturen, redundanten Informationen und eingeschränkter Transparenz die eine durchgängige Digitalisierung behindern und damit den Entwicklungsprozess verlangsamen.

Moderne Entwicklungsansätze wie modellbasierte Systementwicklung, virtuelle Simulation oder der Einsatz von Digital Twins setzen voraus, dass **Daten aus unterschiedlichen Disziplinen konsistent miteinander verknüpft werden können**. Gleichzeitig erfordern internationale Entwicklungsprogramme eine organisationsübergreifende Zusammenarbeit, bei der Engineering-Daten sicher zwischen verschiedenen Partnern ausgetauscht werden können. Eine integrierte Engineering- und IT-Architektur wird damit zur Grundvoraussetzung für effiziente Entwicklungsprozesse und kollaborative Projekte.

Der erste Schritt auf diesem Weg ist eine systematische Analyse der bestehenden IT-Landschaft. Dabei geht es nicht nur um eine Bestandsaufnahme vorhandener Systeme, sondern vor allem um die Bewertung ihrer zukünftigen Rolle im Kontext einer digitalen Entwicklungsarchitektur. Diese Architektur unter Berücksichtigung der Unternehmensprozesse und –ziele zu **gestalten ist die Aufgabe eines ganzheitlichen Enterprise Architecture Managements (EAM).** Unternehmen müssen prüfen, inwieweit ihre bestehenden Lösungen die künftig erforderlichen Fähigkeiten eines **modernen PLM-Ökosystems** unterstützen können. Dazu gehört insbesondere die Fähigkeit, Daten entlang eines **durchgängigen Digital Thread** miteinander zu verknüpfen und unterschiedliche Ausprägungen von Digital Twins zu unterstützen. Gleichzeitig müssen neue Entwicklungsmethoden wie **modellbasierte Systementwicklung** in die bestehenden Engineering-Prozesse integriert werden.

Ein zentrales Element dieser Architektur ist ein integriertes PLM-Ökosystem, das als strukturierender Rahmen für Produkt- und Systemdaten dient. Über standardisierte Schnittstellen können Daten aus MBSE-Tools, Softwareentwicklungsumgebungen, Simulationsplattformen oder Produktionssystemen integriert werden. Dadurch entsteht eine durchgängige Informationsbasis, die den Aufbau eines Digital Thread unterstützt und gleichzeitig die Grundlage für verschiedene Digital-Twin-Anwendungen bildet.

Neben der technischen Integration spielt auch die organisatorische Dimension eine wichtige Rolle. In internationalen Entwicklungsprogrammen müssen unterschiedliche Unternehmen mit individuellen Softwaresystemen unterschiedlicher Anbieter zusammenarbeiten. Eine **integrierte Engineering-Architektur** muss daher nicht nur interne Systeme verbinden, sondern auch sichere Kollaborationsmechanismen für den Austausch von Daten zwischen Partnerorganisationen bereitstellen. Föderierte Datenarchitekturen und standardisierte Integrationsmechanismen können dabei helfen, unterschiedliche Systemlandschaften miteinander zu verbinden, ohne dass alle Beteiligten ihre bestehenden Werkzeuge vollständig ersetzen müssen.

Für Unternehmen der Verteidigungsindustrie ist die Integration ihrer Engineering- und IT-Landschaft damit ein zentraler Schritt auf dem Weg zu einer umfassenden digitalen Transformation. Sie schafft die Voraussetzungen für **effizientere Entwicklungsprozesse**, eine **bessere Zusammenarbeit in multinationalen Programmen** und eine langfristige Beherrschung der steigenden Komplexität moderner Verteidigungssysteme.

Dank seiner mehr als 30jährigen Erfahrung auf dem Gebiet der PLM/ALM-Integration und seiner leistungsfähigen Integrationslösungen ist PROSTEP der richtige Partner, um die Unternehmen der Verteidigungsindustrie bei der den Herausforderungen der System- und Prozessintegration zu unterstützen.

# Digitale Kollaborationslösungen und sicherer Datenaustausch

Große Rüstungsprogramme werden heute häufig von multinationalen Konsortien oder Joint Ventures durchgeführt, in denen Industriepartner, Behörden und Streitkräfte über Länder- und Organisationsgrenzen hinweg zusammenarbeiten. Aktuelle Beispiele dafür sind das Joint Venture MBDA von Airbus, BAE Systems und Leonardo, das ein neues Lenkflugkörper- und Luftverteidigungssystem entwickelt, NH Industries von Airbus Helicopters, Leonardo und Fokker zur Entwicklung der Hubschrauber-Plattform NH90 oder ARTEC, ein Joint Venture von Rheinmetall und KNDS, das für das Radpanzer-Programm Boxer verantwortlich ist.

Die Fähigkeit zur **effizienten und sicheren Kollaboration** wird damit zu einem zentralen Erfolgsfaktor in der Verteidigungsindustrie. Gleichzeitig unterliegt der Datenaustausch in dieser Industrie besonders hohen Sicherheitsanforderungen. Informationen sind häufig sicherheitsklassifiziert, unterliegen Exportkontrollvorschriften und müssen vor unbefugtem Zugriff geschützt werden. Regelwerke wie die International Traffic in Arms Regulations (ITAR) oder die Export Administration Regulations (EAR) definieren strenge Vorgaben für den Umgang mit sensiblen Technologien und Daten. Darüber hinaus müssen nationale Sicherheitsanforderungen sowie Vorgaben internationaler Bündnisse berücksichtigt werden.

Diese Rahmenbedingungen führen zu einem Spannungsfeld: Einerseits ist eine enge, möglichst nahtlose Zusammenarbeit zwischen Partnern erforderlich, um komplexe Systeme effizient zu entwickeln. Andererseits müssen Daten strikt kontrolliert, klassifiziert und abgesichert werden. Das erfordert den Einsatz von **Kollaborations-Lösungen**, die über rollenbasierte Zugriffskonzepte, fein granulare Datenklassifikation, verschlüsselte Übertragungsmechanismen sowie die vollständige Protokollierung von Zugriffen und Änderungen den sicheren und kontrollierten Datenaustausch ermöglichen.

Eine besondere Herausforderung ergibt sich in diesem Kontext aus der **Integration heterogener Systemlandschaften**. Unterschiedliche Partner nutzen häufig unterschiedliche Engineering-Tools und Datenmodelle. Eine effektive Kollaboration erfordert daher Mechanismen, um Informationen zwischen diesen Systemen zu übersetzen, zu synchronisieren und konsistent zu halten. Unternehmen müssen ihre Kollaborationsarchitekturen daher so gestalten, dass sie sowohl technische Integration als auch sichere, regelkonforme Zusammenarbeit ermöglichen. Gleichzeitig müssen Änderungen nachvollziehbar bleiben, um die Integrität des Gesamtsystems zu gewährleisten.

PROSTEP bietet mit seiner Digital Thread Platform die geeigneten Werkzeuge, um komplexe Kollaborationsszenarien wie sie für die Verteidigungsindustrie typisch sind zu orchestrieren und den sicheren Datenaustausch über Unternehmensgrenzen hinweg zu ermöglichen. Dank unserer langjährigen Erfahrung im Automotive-Umfeld und unserer umfangreichen Kenntnis der gängigen PLM- und ALM-Systeme können wir die Unternehmen der Verteidigungsindustrie beim Aufbau von Kollaborationslösungen unterstützen.

# Digital Twins für Entwicklung und Betrieb

Der Digital Twin spielt in der Verteidigungsindustrie eine zentrale Rolle für die digitale Transformation. Er beschreibt ein digitales Abbild eines realen Systems, das über den gesamten Lebenszyklus hinweg mit Daten angereichert wird und so Entwicklung, Produktion und Betrieb miteinander verbindet. Damit wird der Digital Twin zu einem zentralen Baustein moderner Digitalisierungsstrategien. Im Kern **verbindet er die virtuelle Welt der Produktentwicklung mit der realen Nutzung** komplexer militärischer Systeme und ermöglicht eine durchgängige digitale Repräsentation über den gesamten Lebenszyklus, von den frühen Entwicklungsphasen bis zum Betrieb.

Der Digital Twin entwickelt sich entlang verschiedener Lebenszyklusphasen. Zu Beginn existiert er als „as designed"-Modell, das die geplanten Eigenschaften eines Systems beschreibt. Parallel dazu entsteht ein „as planned"-Abbild der Produktionsprozesse. Während der Fertigung wird daraus der „as built"-Twin, der die tatsächliche Konfiguration eines Systems dokumentiert. Im Betrieb ergänzt der „as operated"-Twin diese Informationen durch reale Nutzungs- und Sensordaten. Zusammen ermöglichen diese Modelle eine vollständige digitale Nachverfolgbarkeit eines Systems über Jahrzehnte hinweg – ein entscheidender Faktor im Verteidigungsbereich.

Die Grundlage des Digital Twins bilden Anforderungen, Systemarchitekturen, mechanische und elektronische Modelle sowie Softwarebeschreibungen. Diese Kerndaten entstehen in unterschiedlichen Autorensystemen und müssen strukturiert miteinander verknüpft werden, um eine konsistente digitale Repräsentation komplexer Systeme zu ermöglichen. Zur Unterstützung eines ganzheitlichen Digital-Twin-Konzepts werden daher erweiterte Lösungen benötigt, die es ermöglichen, Kerndaten aus unterschiedlichen Systemen zu integrieren, semantisch zu verknüpfen und für Simulation, Analyse oder Entscheidungsunterstützung zu nutzen. Eine systemübergreifende Digital Thread-Lösung bildet dafür eine Lösung.

Der Verteidigungsindustrie eröffnet der Digital Twin erhebliche Nutzeneffekte. Bereits in der Entwicklung ermöglicht er eine frühzeitige **virtuelle Validierung** komplexer Systeme. Das minimiert Risiken und beschleunigt Design-Entscheidungen. In der Produktion verbessert er Transparenz und Rückverfolgbarkeit, da Abweichungen zwischen geplantem und realem System digital dokumentiert und analysiert werden können.

Besonders große Vorteile entstehen im Einsatz militärischer Systeme. Durch die kontinuierliche Integration von Sensordaten lassen sich Wartungsbedarfe frühzeitig erkennen und Systemzustände präzise überwachen. Dies ermöglicht vorausschauende Wartungskonzepte, **reduziert Ausfallzeiten und erhöht die Einsatzbereitschaft** der Waffensysteme. Darüber hinaus unterstützt der Digital Twin das Closed-Loop Engineering: Erkenntnisse aus dem realen Betrieb können direkt in zukünftige Entwicklungszyklen zurückgeführt werden, um die Systeme kontinuierlich zu


verbessern. Bei der **Missionsplanung** bietet ein Digital Twin, der die aktuellen Fähigkeiten eines Waffensystems abbildet, erhebliche Vorteile.

Die Entwicklung eines ganzheitlichen Digital Twin-Konzepts erfordert nicht nur neue PLM-Fähigkeiten, sondern auch ein klares Verständnis dafür, welche Anwendungsfälle den größten Nutzen versprechen und sich effektiv umsetzen lassen. Als Beratungshaus mit langjähriger Expertise auf dem Gebiet der digitalen Transformation unterstützt PROSTEP die Unternehmen der Verteidigungsindustrie bei der Identifizierung relevanter Anwendungsfälle für den Digital Twin und beim Aufbau einer entsprechenden Enterprise-Architektur. Unter anderem hat PROSTEP eine umfassende Konzeptstudie über die IT-technischen Anforderungen des Digital Twins für Airbus Defense and Space entwickelt.

## Bedeutung des Digital Thread

Während der digitale Zwilling eine digitale Repräsentation eines Systems für bestimmte Anwendungsfälle oder Lebenszyklusphasen darstellt, bildet der Digital Thread die übergeordnete Daten- und Informationsstruktur, die diese digitalen Modelle zusammenhält. Er beschreibt eine **durchgängige digitale Verbindung** zwischen relevanten Artefakten. Dies können z. B. Anforderungen, Software-Komponenten, Testresultate, Produktionsdaten oder Betriebsdaten sein. Er bildet eine nachvollziehbare Informationskette, die es ermöglicht, Systementscheidungen und Änderungen über den gesamten Lebenszyklus hinweg zu verfolgen. Damit bildet er das verbindende Rückgrat für eine durchgängige digitale Repräsentation der Waffensysteme.

In der Verteidigungsindustrie ist die lebenszyklusübergreifende Verknüpfung von Daten von zentraler Bedeutung, weil militärische Waffensysteme häufig mehrere Jahrzehnte im Einsatz bleiben und während dieser Zeit kontinuierlich weiterentwickelt werden. Neue Sensoren, Subsysteme oder Softwarefunktionen müssen integriert werden, während gleichzeitig sichergestellt werden muss, dass bestehende Systemanforderungen weiterhin erfüllt werden. Ohne eine **konsistente Datenbasis** wird es schwierig, die Auswirkungen solcher Änderungen auf Systeme und Architekturen, Schnittstellen oder sicherheitskritische Funktionen zuverlässig zu bewerten. Diese konsistente Datenbasis bildet auch die Basis für KI-Anwendungen wie sie im PROSTEP Whitepaper „Mehr Engineering-Effizienz durch Künstliche Intelligenz“ beschrieben sind.

Der Digital Thread ist die **Basis für die verschiedenen Ausprägungen des Digital Twins**. Indem er z. B. Entwicklungsmodelle, Simulationsdaten, Produktionsinformationen und Betriebsdaten verbindet, schafft er die Voraussetzung, die Betriebsdaten eines Systems mit den zugrunde liegenden Entwicklungsmodellen zu vergleichen oder die Auswirkungen eines geplanten Upgrades auf bestehende Systemkonfigurationen zu analysieren. Besonders relevant ist diese Fähigkeit im Zusammenhang mit der zunehmenden Softwareintegration in militärischen Systemen. Softwareupdates, neue Missionsfunktionen oder Änderungen an Systemarchitekturen müssen zuverlässig getestet und validiert werden, bevor sie in operative Systeme integriert werden können.

Hier spielt die **virtuelle Validierung** eine wesentliche Rolle. Durch die virtuelle Analyse des Systemverhaltens können potenzielle Probleme bereits in frühen Entwicklungsphasen identifiziert und behoben werden, bevor sie sich in späteren Projektphasen kostenintensiv auswirken. Gleichzeitig reduziert sich der Bedarf an physischen Prototypen und aufwendigen Tests erheblich, was zu einer deutlichen Senkung von Entwicklungszeiten und -kosten führt. Der Digital Thread der virtuellen Validierung führt alle wesentlichen Informationen zusammen. Angefangen von den

Anforderungen, der ausgewählten Simulationsmodelle über die eingesetzten Simulationssyteme und Ergebnisse sowie der finalen Bewertung führt er alle wesentlichen Informationen zusammen. Er bietet damit auch die Möglichkeit den Umfang der Simulation für Nachweise eindeutig zu dokumentieren.

Wie wichtig der Digital Thread für den Aufbau von digitalen Zwillingen ist, zeigt der Digital Thread-Benchmark, den die Aerospace & Defense PLM Action Group, eine Initiative führender Unternehmen der Luft- und Raumfahrt- sowie Verteidigungsindustrie, unlängst durchgeführt hat. Ziel des Benchmarks war es, den Reifegrad kommerzieller Digital Twin- und Digital Thread-Lösungen anhand einer Reihe von verschiedenen Anwendungsfällen zu bewerten und Best Practices für eine lebenszyklusübergreifende Datenintegration zu definieren. PROSTEP wurde eingeladen an diesem Benchmark teilzunehmen und konnte die Funktionalität seiner Lösungen erfolgreich demonstrieren. Der Benchmark unterstreicht, dass beim Aufbau des Digital Thread die Integration heterogener IT-Systemlandschaften und der Aufbau offener, modularer PLM/ALM-Architekturen die große Herausforderung darstellt. Als Digital-Thread-Experte verfügt PROSTEP nicht nur über die entsprechende Expertise und Erfahrung auf dem Gebiet der Systemintegration, sondern auch über die geeigneten Software-Lösungen.

## MBSE und Software-Defined Defense

Die dargelegte Komplexität moderner Verteidigungssysteme stellt hohe Anforderungen an Entwicklungsprozesse, Systemarchitekturen und die Zusammenarbeit zwischen Industriepartnern. Waffensysteme integrieren heute eine Vielzahl digitaler Subsysteme, Sensoren, Kommunikationslösungen und softwarebasierter Funktionen, die über sehr lange Lebenszyklen hinweg kontinuierlich weiterentwickelt und modernisiert werden. Vor diesem Hintergrund gewinnen modellbasierte Entwicklungsansätze und softwaredefinierte Systemarchitekturen zunehmend an Bedeutung.

Parallel zur zunehmenden Nutzung modellbasierter Entwicklungsansätze verändert sich auch die grundlegende Architektur militärischer Systeme. **Viele Fähigkeiten werden zunehmend in Software statt in Hardware implementiert**. Dadurch können **neue Funktionen schneller** entwickelt und über Software-Updates in bestehende Plattformen integriert werden. Dieser Paradigmenwechsel wird als Software-Defined Defense bezeichnet.

Ein zentraler Ansatz zur Beherrschung dieser Komplexität vor allem zwischen Software und Hardware liegt das **Model-Based Systems Engineering** (MBSE). Im Gegensatz zu klassischen dokumentenbasierten Entwicklungsprozessen verwendet MBSE konsistente digitale Systemmodelle, die Anforderungen, Funktionen, Lösungen, Architekturen und Schnittstellen strukturiert abbilden. Diese Modelle bilden eine gemeinsame Grundlage für verschiedene Engineering-Disziplinen und ermöglichen eine deutlich bessere Transparenz über das Gesamtsystem.

Durch die **Nutzung konsistenter Systemmodelle** können Änderungen frühzeitig analysiert und ihre Auswirkungen auf andere Systembereiche besser bewertet werden. Dies ist insbesondere in großen, arbeitsteiligen Entwicklungsprogrammen von Bedeutung, in denen verschiedene Industriepartner an unterschiedlichen Subsystemen arbeiten. MBSE unterstützt hier eine gemeinsame technische Referenz, die den Austausch von Architekturinformationen erleichtert und Missverständnisse zwischen verschiedenen Entwicklungsteams reduziert.

Die **Kombination aus MBSE und softwaredefinierten Systemarchitekturen** schafft somit die Grundlage für eine flexiblere und langfristig nachhaltigere Entwicklung militärischer Systeme. Software-Updates müssen zuverlässig validiert werden. Dies beinhaltet auch den Integrationstest in das Gesamtsystem, um sicherzustellen, dass Änderungen keine unerwarteten Auswirkungen auf andere Systemfunktionen haben.

Die Digitalisierung der Verteidigungsindustrie erfordert ein Umdenken in der Entwicklung und Integration komplexer Systeme. Die Kombination aus modellbasierten Entwicklungsansätzen und softwaredefinierten Architekturen bietet dabei entscheidende Vorteile: Sie ermöglicht eine höhere Flexibilität, eine bessere Zusammenarbeit zwischen Partnern und eine nachhaltige Modernisierung

über den gesamten Lebenszyklus militärischer Plattformen hinweg. Gleichzeitig steigen jedoch die Anforderungen an Entwicklungsprozesse, Validierungsmethoden und das Zusammenspiel der beteiligten Akteure. Nur wenn diese Herausforderungen ganzheitlich adressiert werden, können die Potenziale der Digitalisierung effektiv ausgeschöpft und die Einsatzbereitschaft moderner Verteidigungssysteme langfristig sichergestellt werden.

# PROSTEP als Partner der Verteidigungsindustrie

Internationale Kooperationen, strikte regulatorische Anforderungen und die steigende Komplexität der Waffensysteme stellen die Unternehmen der Verteidigungsindustrie vor große Herausforderungen. Sie müssen Konzepte wie Digital Thread und Digital Twin umsetzen, neue Entwicklungsmethoden adaptieren und sichere Kollaborationslösungen implementieren, um die Transformation hin zu einer softwaredefinierten Verteidigungsarchitektur zu schaffen, in der Innovationen schneller umgesetzt und Systeme flexibel weiterentwickelt werden können.

Die PROSTEP Group ist der führende unabhängige Anbieter von Beratungsdienstleistungen und Software rund um das Product und Application Lifecycle Management (PLM/ALM). Mit mehr als 30 Jahren Erfahrung in der Strategieberatung und Prozessoptimierung unterstützen wir Kunden in der Fertigungsindustrie beim Aufbau des Digital Thread und der Schaffung durchgängiger digitaler Informationsflüsse. Seit dem Eurofighter-Programm, in dem wir den Datenaustausch zwischen den Partnern auf Basis des STEP-Standards organisierten, haben wir auch zahlreiche Unternehmen und Konsortien in der Verteidigungsindustrie bei der Digitalisierung ihrer Engineering- und Kollaboration-Prozesse begleitet.

PROSTEP unterstützt die Unternehmen der Verteidigungsindustrie bei:

- der Integration ihrer Unternehmensprozesse und IT-Landschaften, einschließlich der Analyse ihrer bestehenden IT-Bebauung und der erforderlichen PLM/ALM-Fähigkeiten;
- der Definition und Implementierung von Digital Twin-Anwendungsfällen für die Entwicklung, aber auch für die vorausschauende Wartung oder die Einsatzplanung;
- Aufbau eines Digital Thread zur Sicherstellung der domänenübergreifenden Traceability und bei der Realisierung der verschiedenen Digital Twin-Anwendungen;
- der Implementierung eines zuverlässigen Simulationsprozesses für die virtuelle Validierung der Waffensysteme in einem frühen Entwicklungsstadium;
- der Implementierung von ALM-Lösungen sowie von Werkzeugen und Methoden des MBSE zur Unterstützung der Entwicklung softwaredefinierter Verteidigungssysteme;
- der Abbildung von Anforderungen wie MOSA in den eingesetzten IT-Architekturen und der Sicherstellung der regulatorischen Compliance.

PDF Version des Whitepapers:
www.prostep.com/whitepaper
oder scannen Sie den QR Code

## Sie haben Anmerkungen oder Fragen?

Wir freuen uns auf Ihr Feedback an
infocenter@prostep.com

**IMPRESSUM**

Herausgeber
PROSTEP Group

**Ansprechpartner:**
Dr. Martin Holland
martin.holland@prostep.com
Véronique Lutz
veronique.lutz@b-h-c.de

Edition 1, 2026

PROSTEP Group
Heinrich-Hertz-Straße 3-7 · 64295 Darmstadt · Deutschland