

## DIGITAL INDUSTRIES SOFTWARE

# Automatisierung der Verifikation, Validierung und Regelkonformität von Softwaresystemen für die Luft- und Raumfahrt

Beschleunigte Einhaltung der funktionalen Sicherheit gemäß DO178C, DO254 und DO278

### Kurzdarstellung

Es steht außer Frage, dass Sicherheit und Leistung in der Luft- und Raumfahrt- und Verteidigungsindustrie von größter Bedeutung sind. Verifikations- und Zertifizierungsverfahren sind während des gesamten Lebenszyklus des Flugzeugsystems ausschlaggebend. Unternehmen stehen derzeit vor der Herausforderung, die Verifikation, Validierung und Regelkonformität schnell zu automatisieren und gleichzeitig ihre Produkte termingetreu und im Budgetrahmen zu liefern. Um dies zu ermöglichen, müssen Unternehmen darauf achten, dass alle Elemente für den Compliance-Nachweis im Kontext des digitalen Zwillings sind. Dies gilt unabhängig davon, ob diese Elemente auf Vergleichen oder Ähnlichkeiten mit vorherigen Programmen, auf virtuellen oder physischen Tests beruhen.

Die Luft- und Raumfahrtindustrie wird ständig mit dem Nachweis der Regelkonformität konfrontiert. Dies gilt insbesondere für die Software. Dieses White Paper beschreibt die Notwendigkeit, Synergien zwischen unterschiedlichen Entwicklungsteams voranzutreiben und zu fördern und alle Beteiligten mit den Funktionen und Informationen auszustatten, die sie benötigen, um sich im hochkomplexen Ökosystem der Luft- und Raumfahrt erfolgreich zu behaupten.

# Einführung

Softwareprobleme, die sowohl bei Verkehrs- als auch bei Militärflugzeugen auftreten, haben den Lufttüchtigkeitsprozess beeinträchtigt, Projekte verzögert, Fertigstellungstermine verlängert und die Kosten drastisch erhöht. Wie das Government Accounting Office (GAO) im Jahr 2021 berichtete, haben Rückschläge beim F35-Kampfflugzeugprogramm allein durch Probleme in Verbindung mit der Leistungsfähigkeit der endgültigen Software (Block IV) die Kosten um mehr als 40 % in die Höhe getrieben und Lieferungen bis 2029 aufgeschoben. Die Projektabwicklung hat sich um mehr als acht Jahre verzögert und das ursprüngliche Budget wird um 165 Mrd. Dollar überschritten. Fast die gesamte neueste Technologie hängt von der Software und ihrer Beziehung zu den Steuerungssystemen ab, die für die Lufttüchtigkeit entscheidend sind.

In der zivilen Luft- und Raumfahrt spürt Boeing immer noch die Auswirkungen der 737 Max-Softwarelösung, um das Problem der für die größeren Triebwerke erforderlichen Lagekorrektur zu lösen. Zusätzlich zu den drei großen Fehlern in der Software wurde das Problem auch dadurch verschärft, dass das Zusammenspiel der Software mit Flugsteuerungssystemen nicht umfassend getestet wurde. Im Jahr 2020 wurde berichtet, dass dieses softwarebasierte Problem Boeing wahrscheinlich Kosten in Höhe von mehr als 18 Milliarden US-Dollar verursachen würde. Obwohl das Problem nicht vollständig in der Disziplin der Softwareentwicklung lag, deckte es Diskrepanzen in der Kommunikation zwischen Engineering-Teams auf, als sie versuchten, ein funktionsübergreifendes technisches Problem zu lösen. Darüber hinaus wurden bei einem komprimierten Qualitätskontrollprozess wichtige Aspekte der Verifikation und Validierung der im technischen Ökosystem eingesetzten Software übersehen. Infolgedessen unterliegt Boeing bei der Genehmigung von Konstruktionsdaten und der Durchführung von Qualitätsprüfungen einem viel höheren Maß an Kontrolle und Aufsicht durch die FAA, was seine Fähigkeit einschränkt, Beauftragte und damit sein gesamtes System von Lufttüchtigkeitszulassungen einzusetzen.

Software in Flugzeugen stellt die wichtigste Innovationsquelle dar und ist gleichzeitig zu dem Bereich mit den größten Herausforderungen und der größten Komplexität geworden. Start-ups in den Bereichen autonomes Fahren, VTOL und urbane Mobilität haben in den letzten zehn Jahren eine explosionsartige Entwicklung zurückgelegt. Diese Organisationen sowie traditionelle Luft- und Raumfahrtunternehmen sind in hohem Maße auf agile Methoden angewiesen, um die Markteinführung in einem wettbewerbsorientierten und stark regulierten Umfeld zu beschleunigen. Die Einführung agiler Methoden in den Konformitätsprozess bringt viele Herausforderungen für den Fortgang eines Projekts mit sich.

Den Mehrwert dieser Chancen freizusetzen, erfordert neue Denkansätze und mehr Zusammenarbeit – einschließlich einer intensiveren Zusammenarbeit zwischen Erstausrüstern und Lieferanten und zwischen der Automobilbranche und den Regulierungsbehörden. Darüber hinaus wird der Arbeitskräftemangel bei qualifizierten Softwareentwicklern die Hersteller zwingen, ihre Teams mit weniger hochwertigen technischen Ressourcen aus der ganzen Welt zu besetzen, ein weiterer Faktor, der zu den Problemen der 737 Max beiträgt. Dies wiederum erfordert optimierte Prozesse, Transparenz und Informationsaustausch in Echtzeit auf globaler Ebene, um Kommunikationsprobleme zu vermeiden, die zu einem kontinuierlichen Anstieg an Defekten und einer rekordverdächtigen Anzahl an Projektauswirkungen geführt haben. Im Laufe der Zeit werden Probleme der funktionalen Sicherheit, die zum Teil auf unterschiedliche Teams zurückzuführen sind, die auf verschiedenen Kontinenten arbeiten, immer schwieriger zu bewältigen sein und möglicherweise auch häufiger auftreten.

Doch wir müssen nicht in die Zukunft schauen, um festzustellen, dass Entwicklungsunternehmen sich neu erfinden und ihr digitales Werkzeug-Portfolio erweitern müssen, um profitabel zu bleiben. Fast jeden Tag wird über ein neues Softwareproblem berichtet. Der Umfang dieser Probleme ist nicht wirklich überraschend, wenn man die Anzahl der softwarebasierten Funktionen in modernen Avionik- und Funktionssystemen betrachtet. Ein großer Teil der innovativen Funktionen zur Steuerung eines Flugzeugs ist softwarebasiert. Dazu gehören unter anderem kritische Funktionen wie Flugsteuerung, Full Authority Digital Engine Controls (FADEC) und Navigation. Die komplexe Software-Entwicklungsumgebung bringt die Entwicklungsteams an den Rand des Machbaren. Normen und Prozesse haben sich in den letzten Jahren weiterentwickelt, wie z. B. der funktionale Sicherheitsstandard DO178C der Radio Technical Commission for Aeronautics (RTCA) für luftgestützte Softwaresysteme sowie der Sicherheitsstandard DO254 für elektronische Hardware und DO278 für bodengestützte Systeme. Diese Normen, auf die in Vorschriften verwiesen wird, sollen die Sicherheit gewährleisten und Fehler vermeiden, die zu

katastrophalen Ereignissen führen, die durch Mängel oder Defekte in luftgestützter Software verursacht werden.

Hersteller aus Luft- und Raumfahrt investieren immer mehr Zeit und Geld in die Entwicklung und Optimierung ihrer Prozesse und Prozessmodelle, um diesen neuen Normen gerecht zu werden. Um diese Initiativen zu unterstützen, suchen führende Hersteller nach neuen, besseren Werkzeugen, um die Beschränkungen ihrer Altsysteme zu überwinden und die Einhaltung der Lufttüchtigkeit effizienter zu erreichen. Viele Hersteller erkennen immer häufiger, dass unzusammenhängende Entwicklungssysteme ihre Fähigkeit einschränken, ihre spezifischen Umgebungen anzupassen und sich mit dem integrierten Wissen und neuen Werkzeugen auszurüsten, um aktuelle und zukünftige Herausforderungen zu meistern.

Bei den Überlegungen zu den Parametern und der Art der einzusetzenden Werkzeuge, die eine effiziente und wertvolle Entwicklungserfahrung ermöglichen, ist es wichtig, sich der Grundlagen bewusst zu sein, die für eine solche Verwaltungsumgebung erforderlich sind.



### Architektur

Die Architektur sollte als einheitliche Umgebung strukturiert sein, um die Verwaltung aller Softwareentwicklungsfunktionen innerhalb der Umgebung zu ermöglichen. Dazu wird eine universelle Benutzeroberfläche verwendet, in der sich jedes der funktionsübergreifenden Teams leicht zurechtfindet und die einen einfachen Rahmen für die Zusammenarbeit bietet.



### Digitalisierung

Der erste Schritt zur Digitalisierung besteht darin, homogene Inhalte in Form von Dokumenten (elektronisch oder in Papierform) in ihre einzelnen Elemente (Anforderungen, spezifische Dokumentenformatierung, unstrukturierte Inhalte, Metadaten, Grafiken usw.) zu zerlegen, damit sie nachverfolgt und verwaltet werden können. Einmal digitalisiert, lassen sich diese Inhalte leicht organisieren, in Beziehung setzen, kontrollieren, verteilen, durchsuchen und auf verschiedene Arten zugänglich machen.

### Dokumente

Das erste Konzept kann man sich als einen Container vorstellen, der sowohl unstrukturierte Inhalte als auch strukturierte Projektdaten in einem Format organisiert, das einem vertrauten Textverarbeitungsprogramm ähnelt. Das Erstellen, Definieren und Bearbeiten von Dokumenten wie Anforderungen, Sicherheitsziele, Risiken und Testfälle dürfte so einfach wie mit Microsoft® Word sein.

Mit einem vertrauten und einfach zu bedienenden Online-Textverarbeitungsprogramm lassen sich Inhalte leicht erstellen, bearbeiten und formatieren. Eine wichtige Funktion besteht darin, dass bestimmte Dokumentinhalte als Artefakte gekennzeichnet und als wesentliche Projektkomponenten eingestuft werden können. Auf diese Weise kann eine Benutzerrolle die Vorteile des Workflow- und Projektmanagements nutzen, während Autoren von Dokumenten weiterhin mit Inhalten aus der Perspektive der Dokumente arbeiten können. Dieser Ansatz bietet das Beste aus zwei Welten: Verwendbarkeit als Office-Dokument und ein datenorientierter Prozess, der das Projektmanagement für das Unternehmen ermöglicht.

Geschäftsanalysten und Anforderungsautoren, die beide üblicherweise mit Dokumenten arbeiten, müssen nicht umdenken oder Funktionalität oder Benutzerfreundlichkeit opfern, während technisches Personal die Workflow- und Verwaltungsfunktionen der datenorientierten Benutzeroberflächenoption nutzen kann. Führungskräfte und weitere für Regelkonformitätsprobleme verantwortliche Personen erhalten die erforderlichen Berichte, und das gesamte Unternehmen profitiert von verbesserter Effizienz, Transparenz und Kommunikation.

Teammitglieder sollten in der Lage sein, vorhandene Assets mithilfe einer regelbasierten Importmethode, die Artefakte entsprechend ihrer beabsichtigten Funktion im Projekt analysiert, einfach zu importieren und zu nutzen. Idealerweise sollte es so konfiguriert sein, dass es Artefakte wie Anforderungen, Testfälle, Defekte und andere in Microsoft Word oder Excel® enthaltene Elemente erkennt und diese einfach importieren kann, um einen schnellen Weg zur Digitalisierung zu ermöglichen.



Umgekehrt besteht die Möglichkeit, Projektdaten in Form von Microsoft Word- oder Excel®-Dokumenten für Überprüfungen, Genehmigungen und Bearbeitungen zu exportieren. Diese bearbeiteten Dokumente sollten nahtlos wieder importiert werden können und Teil des Projektinhalts werden, der in den Projekt-Workflow einbezogen und vollständig nachverfolgt werden kann.

### **Artefakte**

Ein Artefakt kann alles sein, was im Projekt verfolgt werden soll. Dieses Grundkonzept lässt sich aufschlüsseln und als Artefakttypen für Anforderungen, Aktivitäten, Änderungsanträge und Testfälle definieren. Benutzerdefinierte Arbeitsaufgabentypen – für Arbeitsprodukte, Sicherheitsziele oder alles, was man sich vorstellen kann, können ebenfalls nach Bedarf definiert werden.

#### **• Artefakt-Datenfelder, benutzerdefinierte Felder**

In jedem Artefakt sollten viele Standarddatenfelder verfügbar sein. Mit diesen wird das Element beschrieben und kategorisiert, einem Benutzer zugewiesen, in die Projektplanung und die Verfolgung integriert, dessen Status eingestellt usw. Benutzerdefinierte Felder sollten für jeden Artefakttyp definiert werden können, um die Verfolgung und Abfrage jeder Art von Informationen zu ermöglichen. Das Design Assurance Level und das Ziel einer Anforderung können mithilfe eines vordefinierten benutzerdefinierten Felds für Arbeitselemente verwaltet und verfolgt werden, um die Konformität in einem Audit nachzuweisen. Für jedes Arbeitselement kann die Ansicht und Darstellung vollständig angepasst werden.

#### **• Lebenszyklus und Workflow von Artefakten**

Jeder Artefakttyp sollte über eine eigene Lebenszyklus- oder Workflow-Definition verfügen. Ein Workflow besteht aus einer Reihe von Stati und Statusübergängen, Übergangsbedingungen und Abhängigkeiten, die ein Artefakt in seinem Lebenszyklus durchläuft. Jeder Status, Übergang und jede Abhängigkeit und Bedingung eines Elements kann angepasst werden. So lassen sich Workflows an jeden Prozess anpassen.

#### **• Verknüpfungen zwischen Artefakten; Verknüpfungs-Attribute und Rollen**

Das Verknüpfen der Artefakte ist der Schlüssel, um von den Funktionen der Verfolgbarkeit und Auswirkungsanalyse zu profitieren. Artefakte sollten in einem Projekt oder zwischen verschiedenen Projekten und sogar zwischen verschiedenen Repositories verknüpft werden können. Mit dieser Funktion lassen sich zugehörige Artefakte mit verschiedenen Produkten oder Produktvarianten in Beziehung setzen und Verfolgbarkeits- und Auswirkungsinformationen gewinnen, die nicht durch den Projektumfang begrenzt sind.

Die Verknüpfungen zwischen Artefakten müssen nach Verknüpfungsrollen definiert und kategorisiert werden. Verknüpfungsrollen unterscheiden sich durch ihre Namen (bezieht sich auf, implementiert, verifiziert usw.) Die Rollen können verschiedene Bedeutungen haben und an Ihre Anforderungen angepasst werden. Mit Verknüpfungen ist es einfach, den kompletten Anforderungsfluss von der Konzeptphase bis hinunter zu Software- und Hardwareanforderungen und zugehörige Aktivitäten, Arbeitsprodukte, Risikoelemente und Testfälle zu verwalten.

#### **Rückverfolgbarkeit**

##### *Protokollierung/Audit-Protokoll*

Jede Artefaktänderung in einem Projekt muss mithilfe eines zugrunde liegenden Konfigurationsmanagementsystems verfolgt und gemeldet werden. Es sollte immer ein vollständiger Audit-Trail zur Verfügung stehen (wer hat was, wann und warum getan). Im Kern sollte es einfach nicht möglich sein, etwas zu ändern, ohne eine Spur zu hinterlassen, selbst wenn ein Artefakt gelöscht wird. Alle Konfigurationsänderungen sollten bei Bedarf rückgängig gemacht werden können.

##### *Verfolgbarkeits- und Auswirkungsanalyse*

Alle Verfolgbarkeits- und Auswirkungsanalysen müssen auf den Verknüpfungen zwischen Artefakten basieren. Eine Vielzahl unterschiedlicher Ansichten und Berichte, die die Ergebnisse der Verfolgbarkeits- und Auswirkungsanalyse darstellen, sind erforderlich, um der Zielgruppe einen Kontext zu bieten. Berücksichtigen Sie diese wesentlichen Komponenten, die die Verfolgbarkeit ermöglichen:

- Der aktuelle Stand jedes Dokuments ist jederzeit online verfügbar.
- Der Zugriff wird durch Anwenderberechtigungen gesteuert.

- Eine Historie zu jedem Dokument ist leicht verfügbar. Jedes Mal, wenn ein Dokument gespeichert wird, wird ein neuer Eintrag oder ein Änderungsstand in der Historie erstellt. Änderungsstände lassen sich leicht anzeigen, und durch Vergleiche zwischen zwei Änderungsständen lässt sich erkennen, welche Änderungen zwischen dem älteren und dem neueren Änderungsstand vorgenommen wurden.
- Die URL des Dokuments kann mit anderen Benutzern geteilt werden, um die Zusammenarbeit am Inhalt zu ermöglichen.
- Ein robuster Mechanismus für den Export und Reimport ermöglicht die Zusammenarbeit zwischen externen Stakeholdern, die keine registrierten Benutzer sind, und bringt deren Beiträge in den Datenfluss ein.

### Anforderungsmanagement

Die Definition und das Management von Anforderungen im Rahmen einer einzigen Lösung bieten erhebliche Vorteile gegenüber herkömmlichen Ansätzen:

- Das Beste aus beiden Welten wird unterstützt: Diejenigen, die an einen dokumentenzentrierten Ansatz gewöhnt sind, können weiterhin mit Dokumenten arbeiten, und diejenigen, die mit einzelnen Datenelementen arbeiten müssen, können sie in Listen in einem vertrauten Tabellenkalkulationsformat anzeigen.
- Integration der Anforderungen in den Gesamtprozess: Erfasste Anforderungen sind ein integraler Bestandteil des gesamten Entwicklungsprozesses von Anfang bis Ende, sodass es nicht mehr darum geht, isolierte Office-Dokumente zu verwalten, die von den Prozessen der Implementierung und des Testens abgekoppelt sind.
- Auf Standards basierende Anforderungen, die für mehrere Projekte gültig sind, können in verschiedenen Projekten wiederverwendet werden.
- Effizientere und zeitsparende Zusammenarbeit: alle Beteiligten haben jederzeit Zugriff auf dieselbe Version der Anforderungen. Änderungen werden in Echtzeit dargestellt – keine Verzögerungen durch Warten auf Kopien in E-Mails. Der Prozess ist in Projekt-Workflows integriert und automatisiert, damit kein Schritt aufgrund von Fehlkommunikation ausgelassen oder übersprungen wird. Jeder kann den aktuellen Status sehen und jeder wird benachrichtigt, wenn Änderungen vorgenommen werden und die Anforderung im Prozess fortschreitet. Verantwortliche für Genehmigung und Freigabe können diese Aufgaben online ausführen.

- Einfachere und robustere Verfolgbarkeit: Bei anderen herkömmlichen Ansätzen war eine strenge und gründliche Verfolgbarkeit schwierig. Um die Anforderungen der funktionalen Sicherheit zu gewährleisten, muss die Rückverfolgbarkeit vom Artefakt auf höchster Ebene bis hinunter zum kleinsten Artefakt reichen, insbesondere einer einzigen Zeile Quellcode für DO178C und DO254. Dies sollte einfach zu implementieren und für den Benutzer völlig transparent sein.

### Test- und Qualitätsmanagement

Einige Überlegungen zum Testmanagement für die Bereitstellung dieser Funktionen:

- Angeben und Verwalten von Tests mithilfe vertrauter Benutzeroberflächen oder integrierten Werkzeugen
- Einfaches Erstellen von Verfolgbarkeit von Defekten bis zu den Anforderungen auf Systemebene
- Manuelle oder automatische Testläufe; optionaler Import von Ergebnissen aus externen Testwerkzeugen
- Automatischer Testausführungsverlauf mit detaillierten Statistiken
- Anpassbare Testläufe aus vordefinierten Vorlagen

### Änderungs- und Konfigurationsmanagement

Für integriertes Änderungsmanagement:

- Sammeln, Verwalten und Protokollieren von Änderungsanfragen in einer einheitlichen Lösung
- Auswirkungs- und Verfolgbarkeitsanalyse, um zu entscheiden, welches Projektartefakt geprüft, geändert oder hinzugefügt werden muss
- Verknüpfen der Änderungsanforderungen mit zugehörigen Anforderungen
- Anwenden des Verdachtsmanagements als Unterstützung bei der Verbreitung von Änderungen
- Verwenden von Audit-Protokollen (Verlauf) für Arbeitselemente, um anzuzeigen, wer was und wann geändert hat
- Zusammenarbeit über Kommentarfunktion mit Thread-Struktur, Abstimmung und Benachrichtigungen zu implementierten Änderungen

Um all diese Elemente zu verfolgen und die notwendige Verfolgbarkeit zu gewährleisten, sollte die zugrunde liegende Datenstruktur eine hochgranulare und endliche Verfolgbarkeit unterstützen. In der Regel sollte dies ein System sein, das auf keinen Fall ein Artefakt löscht, sondern die Artefakte, die nicht mehr aktiv sind, aus der Ansicht entfernt. Die Forensik ermöglicht den Zugriff auf all diese Informationen und die Berichterstellung, um alle mit dem Artefakt verbundenen Aktivitäten abzudecken.

In einer solchen Architektur werden Änderungen bei jedem Speichern automatisch versioniert. Jeder Änderungsstand ist über Verlaufsinformationen eines Artefakts immer verfügbar. Unterschiede zwischen Änderungsständen von Artefakten – Arbeitselemente und Dokumente – können grafisch angezeigt werden. Dadurch können alle im System verwalteten Arbeitselemente visuell miteinander verglichen werden, einschließlich Anforderungen, Änderungsanfragen, Testfällen, Quellcode, Aktivitäten und weitere.

### **Audit-Protokoll**

Es sollte nicht möglich sein, eine Änderung im System vorzunehmen, ohne dass diese protokolliert wird. Es muss immer der vollständige Audit-Trail verfügbar sein (wer, wann, was, warum usw.). Selbst wenn etwas gelöscht wurde, muss es nachverfolgt werden, um eine vollständige und lückenlose Verfolgbarkeit darzustellen.

### **Baselines**

Baselines sind wichtige Funktionen, die dazu dienen, den aktuellen Stand des Projekts zu kennzeichnen, einschließlich aller Projektartefakte. So können Teammitglieder die Unterschiede zwischen verschiedenen Baselines oder zwischen einer Baseline und dem aktuellen Projektstatus nachvollziehen. Durch Auswahl einer Baseline für den Vergleich ist es möglich, eine oder mehrere Änderungsstände anzugeben, die mit einer einzelnen Baseline verglichen werden sollen.

### **Build- und Release-Management**

Für jedes Artefakt des Projekts sollte die Möglichkeit bestehen, es mit Releases zu verknüpfen. Informationen können mithilfe der Polarion-Suche und Reporting-Funktionen abgerufen werden. Vorteile:

- Schnellere Zusammenstellungs- und Fehlerbehebungsprozesse mit E-Mail-Benachrichtigungen über Build- oder Testfehlschlägen
- Schnelles Finden von Problemen mit vollständigen Audit-Protokollen von Builds und Releases
- Messen der Wiederverwendung von Anforderungen, Testfällen und weiteren Artefakten über Projekte hinweg

### **Zusammenarbeit**

#### **Team-Zusammenarbeit**

Stakeholder müssen auf verschiedenen Ebenen zusammenarbeiten und kommunizieren können. Die nahtlose Zusammenarbeit beschleunigt den Projektverlauf und trägt zur Förderung einer agilen Methodik und agiler Prozesse bei. Für Diskussionen und Zusammenarbeit auf höheren Ebenen wird die

persönliche und individuelle Interaktion durch digitale Mittel sowohl innerhalb als auch außerhalb der Entwicklungsumgebung gefördert.

Detailliertere Zusammenarbeit und Kommunikation findet in Kommentaren zu einzelnen Arbeitselementen statt. Zwischen Projektteammitgliedern finden Diskussionen in mehreren Threads statt. Die Sichtbarkeit von Kommentaren sollte optional gesteuert und eingeschränkt werden können; z. B. können manche Kommentare nur für Führungskräfte sichtbar sein.

### **Austausch/Zusammenarbeit zwischen Erstausrüstern und Lieferanten**

- **Native Integrationen mit RIF/ReqIF, MATLAB®, und Simulink®**  
Eine offene Plattform, die Erstausrüstern und Lieferanten verschiedene Optionen für den Datenaustausch bietet, einschließlich nativem ReqIF-Roundtrip (Requirements Interchange Format) und Datenaustausch über die MATLAB/Simulink-Integration, ist eine entscheidende Funktion für die Kommunikation mit anderen Werkzeugen und die Integration von MBSE in den Entwicklungsprozess. Diese Integrationen unterstützen die Optimierung von Überprüfungen, Auswirkungsbewertung und Verfolgbarkeit.
- **Freigeben und Überprüfen von Dokumenten/Arbeitsergebnissen**  
Die Möglichkeit zur Datenmodifikation, einschließlich der Genehmigung von Anforderungen über Standarddokumente, ist ein Schlüsselfaktor in der Zusammenarbeit mit externen Stakeholdern. Dokumente, die verwaltete Artefakte enthalten, können in ein Word- oder Excel-Dokument exportiert werden, das dann von Mitarbeitern, die keinen Zugriff auf das System haben, gemeinsam genutzt und überprüft werden kann. Nach den Änderungen (die Änderungstypen können während des Exports optional eingeschränkt werden) kann das Word- oder Excel-Dokument wieder reimportiert werden. Die enthaltenen Änderungen werden dann in das Data Repository übernommen und die Dokumenthistorie wird aktualisiert.
- **Webbasierte Zusammenarbeit**  
Einladung externer Partner zum Kommentieren von Arbeitselementen oder Dokumenten über eine Webclient-Schnittstelle, für die nur ein Webbrowser und eine Internetverbindung erforderlich sind. Auf diese Weise können Erstausrüster und Lieferanten ohne Medienbarrieren oder Informations- und Datenverlust optimal zusammenarbeiten.

## Risikomanagement

Produktentwicklungsteams managen Risiken auf mehreren Ebenen:

- Sicherstellen, dass die aktuellsten Anforderungen und Spezifikationen für alle verfügbar sind und rechtzeitig und klar kommuniziert werden
- Unterstützen beim Aufdecken von Ressourcen- engpässen, bevor diese kritisch werden
- Aufdecken der Auswirkung (und Kosten) von Änderungen, bevor Ressourcen zugewiesen werden
- Sicherstellen der Befolgung von Prozessen und Erfüllung von Standards
- Sichtbarkeit bezüglich wer was wann weshalb geändert hat

Im Kollektiv bieten diese Funktionen eine solide Basis für die Risikoanalyse und die Erfüllung von DO178C bei jedem Projekt und über alle Projekte hinweg.

## Agile Softwareentwicklung

Die Einführung einer agilen Methodik oder eines agilen Ansatzes auf Unternehmensebene ist mit Herausforderungen verbunden, insbesondere bei der Einführung in einer funktionsübergreifenden Teamumgebung. Für Unternehmen, die über verteilte und nicht miteinander verbundene agile Teams verfügen, ist es eine Herausforderung, alle Teams auf den gleichen Stand zu bringen. Aus diesem Grund ist es wichtig, eine einheitliche Strategie mit Agile zu verfolgen und das Scaled Agile Framework (SAFe) zu verwenden, um Konsistenz zwischen allen Teams zu

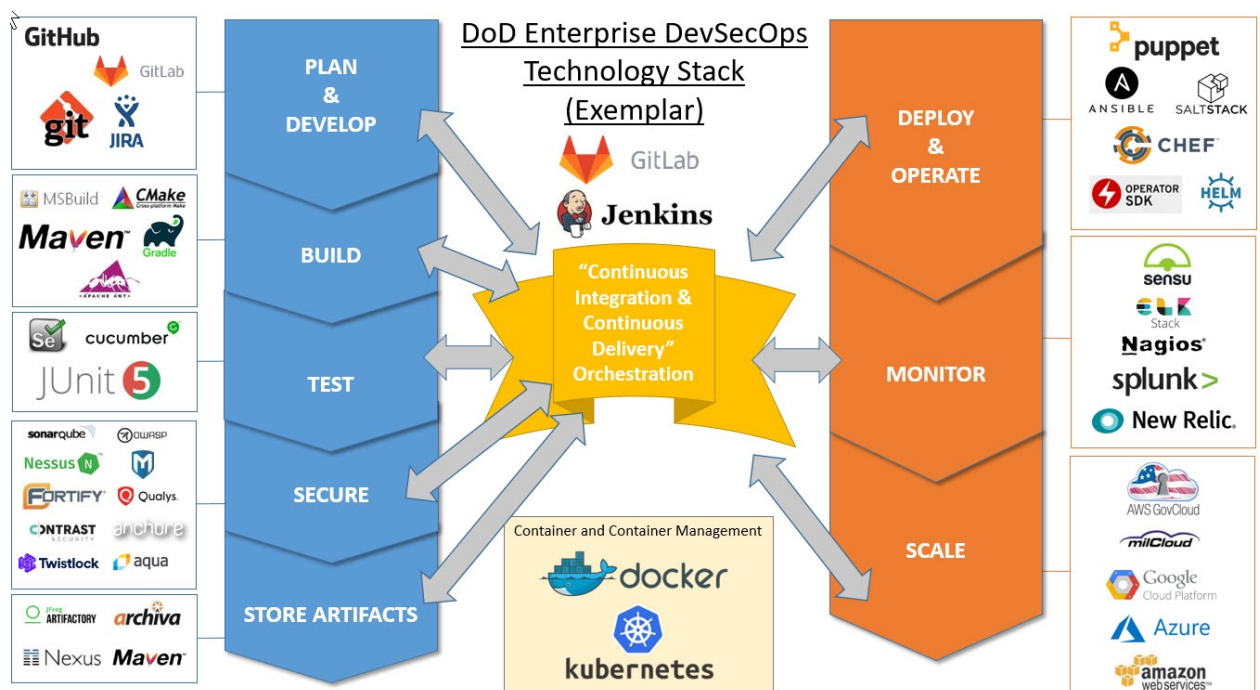
schaffen. Die Einführung eines SAFe-Ansatzes bringt die folgenden Vorteile mit sich:

- Kürzere Markteinführungszeit
- Verbesserung der Qualität
- Steigerung der Produktivität
- Besseres Mitarbeiterengagement

Die Einführung agiler Methoden wird durch die Zusammenarbeit mit SAFe-Plattformpartnern beschleunigt und basiert auf einer genehmigten SAFe-Vorlage innerhalb des Softwareentwicklungs- und -management-Tools.

## Software-Sicherheit

Der Schutz von Software-Code vor Angriffen und Exploits ist zu einer wachsenden und kritischen Herausforderung für Software-Entwicklungsunternehmen und, was ebenso wichtig ist, für deren Endbenutzer geworden. Das Konzept der Einbeziehung von Sicherheitsaspekten in den Entwicklungsprozess, insbesondere bei der Anwendung agiler Verfahren, hat vor allem im Verteidigungsministerium und bei seinen Auftragnehmern eine hohe Sichtbarkeit erlangt. Das geht so weit, dass das Akronym DevSecOps dafür verwendet wird, die Sicherheit in den kontinuierlichen Integrations- und Entwicklungsprozess der Softwareentwicklung zu integrieren. Die Fähigkeit, diese Funktion bereitzustellen, erhöht die Entwicklungsgeschwindigkeit erheblich und stellt die Ausfallsicherheit des Softwarepakets weiter sicher.



DoD DevSecOps-Topologie



Derzeit ist dieser Prozess recht aufwendig und erfordert den Einsatz externer Tools zur Analyse des ausführbaren Codes anhand von Datenbanken mit bekannten Bedrohungen und Schwachstellen. Im Zusammenhang mit diesem Sicherheitsthema wachsen das Interesse und die Diskussion über die Erstellung einer Software Bill of Materials (SBOM), die nicht nur die Sicherheit der Software spezifiziert, sondern auch jede Komponente, die zur Erstellung der Software verwendet wird.

Beide Ideen sind sowohl für Endbenutzer als auch für Unternehmen, die Software für jede Art von Anwendung entwickeln, wichtig und nützlich und sollten in den Entwicklungsprozess einbezogen werden, idealerweise mit demselben Tool, das für die Verwaltung von Anforderungen, Tests, Freigabe und Ressourcen verwendet wird. Letztendlich geht es darum, das Risiko bei der Nutzung von Software-Assets zu mindern.

### Interoperabilität

Software-Entwicklungsteams verwenden eine Vielzahl unterschiedlicher und spezialisierter Tools bei der Erstellung eines Softwareprogramms. Die Koordination der Ergebnisse aus diesen verschiedenen

Tools muss eng in den Entwicklungsprozess integriert werden. Der Zugriff auf eine breite Palette von Konnektoren und Integrationen ist wichtig, um den Prozess im Hinblick auf die Effizienz und Genauigkeit zu optimieren. Idealerweise sollten sich alle Ergebnisse dieser externen Tools im Rahmen des Entwicklungsmanagements verwalten lassen.

### Integration in physische Systeme

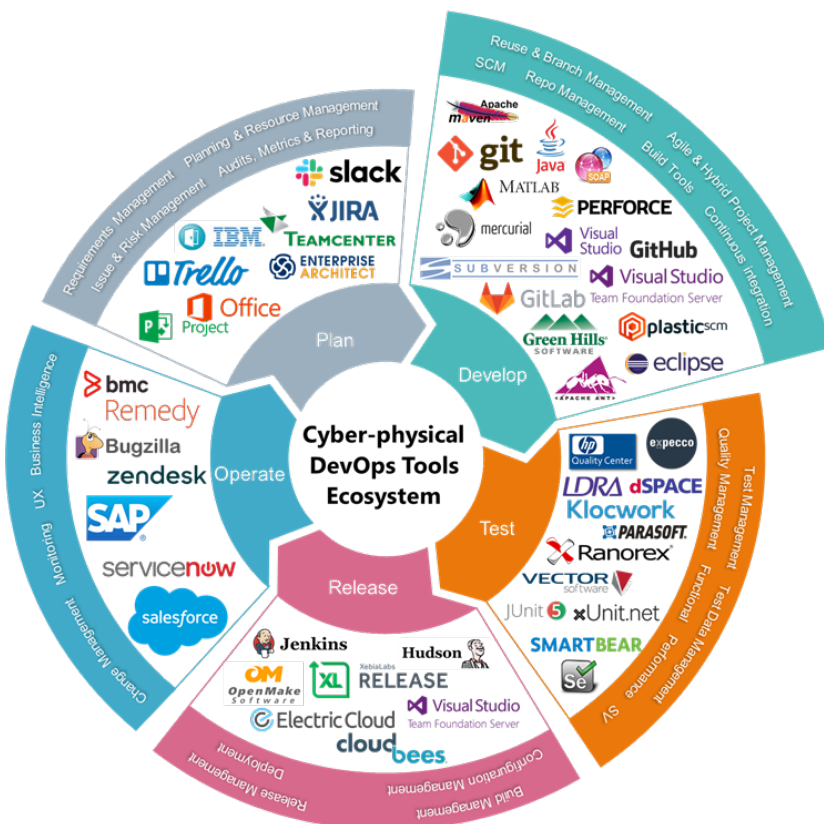
Wie bereits erwähnt, stützen sich die komplexen Produkte von heute zu einem erheblichen Teil auf Software. Daher muss der Softwareprozess mit dem umfassenderen Fertigungsprozess abgestimmt und in den Product Lifecycle Management-Managementprozess (PLM) einbezogen werden. Die Software wird letztendlich in eine Art mechanisches oder elektrisches Gerät eingebettet, um die gewünschte Funktionalität bereitzustellen. Die richtige Version der Software muss mit der richtigen Version der physischen Komponente abgeglichen werden. Um dies zu erreichen, müssen diese Fertigungsprozesse auch Informationen über die Software und deren Implementierung innerhalb des physischen Systems oder Subsystems enthalten. Daher muss eine direkte Verbindung zwischen PLM- und Software Application Lifecycle Management (ALM)-Systemen bestehen, um eine einfache Validierung und Verifikation sowohl der Software als auch ihrer Beziehung zu dem physischen System zu ermöglichen, in dem sie eingesetzt werden soll.

### Electronic Design Automation (EDA)

Immer mehr Produkte setzen Embedded-Software direkt in integrierten Schaltkreisen ein. Die Funktionsfähigkeit der Software muss innerhalb der Grenzen der zugehörigen integrierten Schaltungstopologie validiert und verifiziert werden. Software muss innerhalb dieser Infrastruktur, die etwas anders ausgeführt wird, evaluiert und getestet werden. Die Managementumgebung muss auch die Fähigkeit haben, dies durch Verknüpfungen oder Integrationen in den Softwareentwicklungsprozess einzubeziehen.

### Modellbasiertes Systems Engineering (MBSE)

In der Produktentwicklung werden heute verschiedene Systeme eingesetzt, die die Entwicklung und Analyse mithilfe grafischer Modelle ermöglichen. Wie bei anderen Ingenieurdisziplinen sollte die Softwareentwicklung die verschiedenen Modellierungswerkzeuge umfassen, um das Bild der Software in das Modell einzubeziehen.



DevOps-Landschaft

# Übersicht

## Die 10 wichtigsten Vorteile einer webbasierten Lösung für das Management der Softwareentwicklung in der Luft- und Raumfahrt

- Erfassen und Verwalten von Anforderungen und Änderungen mithilfe einer Lösung in einem Repository
- Optimierung vorhandener Software und Infrastruktur und Wiederverwendung von Anforderungen zur Steigerung der Gesamteffizienz
- Erstellen einer granularen Verfolgbarkeit, um alle wichtigen Artefakte bis zum Quellcode zu nachzuverfolgen
- Software-Sicherheit, um Bedrohungen und Eindringlinge zu erkennen und zu beseitigen
- Bereitstellung von Echtzeit-Sichtbarkeit des Produktstatus
- Aufbau von Anforderungsbibliotheken zur Nutzung von Standards und Anforderungsvarianten
- Automatisieren und Standardisieren von Workflows, um Governance zu etablieren
- Optimierung der Risikomanagement-Funktionalität
- Herstellung einer Verknüpfung zwischen ALM- und PLM-Systemen
- Bereitstellung und Etablierung der Interaktion mit Modellierungswerkzeugen für die Einbeziehung in den MBSE-Prozess



## **Siemens Digital Industries Software**

Nord-, Mittel- und Südamerika: 1 800 498 5351

EMEA: 00 800 70002222

Asien-Pazifik: 001 800 03061910

Für weitere Nummern klicken Sie bitte [hier](#).

**Siemens Digital Industries Software** unterstützt Unternehmen jeder Größe bei der digitalen Transformation mithilfe der Software, Hardware und Services der Siemens Xcelerator Business-Plattform. Mit der Software und der Technologie des digitalen Zwillings von Siemens können Unternehmen aller Branchen ihre Entwicklungs-, Konstruktions- und Fertigungsprozesse optimieren, um aus den Ideen von heute die nachhaltigen Produkte von morgen zu fertigen. Ob Chips oder Komplettsysteme, Produkte oder Prozesse. [Siemens Digital Industries Software](#) – where today meets tomorrow.

**[siemens.com/software](https://www.siemens.com/software)**

© 2023 Siemens. Eine Liste wichtiger Warenzeichen von Siemens findet sich [hier](#). Alle anderen Marken sind Eigentum der jeweiligen Inhaber.

84601-D3-DE 4/23 LOC