Softwaredefinierte Assurance

Helsing White Paper

17. Dezember 2024

Inhaltsverzeichnis

Zusammenfassung

Assurance ist der Schlüssel, um effektive neue Verteidigungsfähigkeiten auf das Gefechtsfeld zu bringen. Da Software und Künstliche Intelligenz (KI) immer zentraler für die Entwicklung von Fähigkeiten werden, müssen bestehende Assurance-Prozesse hinterfragt und passende Ansätze entwickelt werden. Kernaspekte eines neuen Assurance-Ansatz sind:

- Assurance ist ein kontinuierlicher Prozess, der kontinuierliche Fähigkeitsanpassungen ermöglicht
- Die Wiederverwendung von Software über viele verschiedene Hardware-Konfigurationen ist notwendig
- Assurance erfolgt für Systeme als Teile einer sich ständig verändernden Konstellation von Systemen im Verbund
- Spezifische Ansätze und Techniken ermöglichen Assurance auch für komplexe KI-basierte Systeme

Wir bezeichnen dieses Modell als softwaredefinierte Assurance und schlagen gezielte Investitionen in Software-Infrastruktur, digitale Assets und neue Standards vor, um die Assurance von Fähigkeiten und damit Prozesse zu ihrer Adaption rapide zu beschleunigen. Eine erfolgreiche Umsetzung bietet strategische Vorteile bei der Entwicklung, Wartung und dem Einsatz von militärischen Fähigkeiten.

01 Wenn Verteidigung softwaredefiniert wird, muss Assurance folgen

In der Ukraine wird deutlich, dass Software und KI zu zentralen Elementen moderner militärischer Systeme werden. Masse wird im Zeitalter von softwaredefinierter Verteidigung („Software-Defined Defence“) mit softwaredefinierten Fähigkeiten generiert. Intelligenz und Autonomie werden dafür in handelsübliche und preiswerte Hardware-Plattformen integriert. Entscheidungsvorteile entstehen durch ein Lagebild in nahezu Echtzeit, das durch Sensordatenerfassung, -fusion und -verarbeitung entsteht. Softwarebasierte System-Updates ermöglichen es Streitkräften, sich und ihre Waffensysteme schnell an veränderte Einsatzkontexte und rasch entwickelnde Bedrohungen anzupassen. Immer mehr definieren die Softwareanwendungen, nicht Hardware, leistungsstarke und anpassungsfähige Fähigkeiten (Hintergrund: 1, 2).

Um sicherzustellen, dass diese softwaredefinierten Fähigkeiten effektiv und sicher sind, müssen sie durch Assurance qualifiziert werden. Durch Assurance wird nachgewiesen, dass ein System zuverlässig ist, indem die Erfüllung der notwendigen Leistungs- und Sicherheitsanforderungen geprüft werden. Ohne effektive Assurance-Prozesse können sich die Streitkräfte im Einsatz nicht auf die Systeme verlassen. Bestehende Prozesse wurden über Jahrzehnte hinweg aufgebaut, basierend auf dem Wissen aus der Systementwicklung und -produktion und sind in Standards verankert worden, deren Einhaltung von Beschaffungsbehörden erwartet und von Lieferanten bedient wird.

INFO: Wir verwenden das Wort Assurance in diesem Papier, um den Prozess zu beschreiben, durch den Vertrauen in die Eignung und Bereitschaft eines Waffensystems für den operativen Einsatz geschaffen werden soll. Dazu gehören sowohl Qualifizierung als auch Zertifizierung, basierend auf Aktivitäten wie z.B. Designsicherheit, Validierung und Verifikation (V&V), Qualitätsmanagement und Safety.

Da die Fähigkeiten der Streitkräfte zunehmend softwaredefiniert sind, müssen sich unsere Assurance-Prozesse entsprechend weiterentwickeln. Bestehende Assurance-Ansätze sind nicht auf die Anforderungen softwaredefinierter Fähigkeiten zugeschnitten, wodurch Innovation, Entwicklung und Investitionen gebremst werden. Wir könnten bessere Systeme effektiver und schneller entwickeln und insbesondere schnell adaptieren, wenn geeignete Assurance-Prozesse vorlägen.
Auch wenn der, in den letzten Jahrzehnten etablierte, allgemeine evidenzbasierte Systementwicklungsansatz nach wie vor gilt, müssen wir die Vorteile von Software nutzbar machen. Insbesondere muss der Assurance Ansatz folgendes ermöglichen:

01 **Geschwindigkeit:** Software hat einen drastisch kürzeren Entwicklungszyklus, mit mehr Iterationen des gesamten Prozesses von Anforderungen bis hin zu ihrer Validierung. Schnelle Updates können im Gefechtsfeld über Softwareanwendungen bereitgestellt werden, ohne die Hardware zu verändern. Ein neuer Assurance-Prozess kann zur Entwicklung zuverlässiger und sicherer Systeme mit hoher Geschwindigkeit befähigen.

02 **Übertragbarkeit:** Software kann über unterschiedliche Plattformen hinweg wiederverwendet werden. Die gleiche softwaredefinierte Fähigkeit kann auf unterschiedlicher Hardware (und Generationen von Hardware) eingesetzt werden, auch über Hersteller hinweg. Assurance muss diese 1:N-Beziehung zwischen Software und Hardware widerspiegeln.

03 **Autonomie:** Der Grad der Autonomie in Systemen nimmt in allen Bereichen zu, nicht zuletzt getrieben durch die Entwicklung im Bereich der KI. Insbesondere für Anwendungen mit hohem Autonomiegrad bringt KI eine Vielzahl von Herausforderungen für Assurance mit und verlangt die Entwicklung von robusteren technischen Ansätzen, die sich von bestehenden Ansätzen unterscheiden.

04 **Systeme im Verbund:** Historisch betrachtet sind es menschliche Operateure, die Systeme über begrenzte digitale Schnittstellen miteinander verknüpfen. Da heute immer mehr Systeme miteinander verbunden sind, müssen wir zur Entwicklung und Assurance einer Vielfalt von Systemen im Verbund in der Lage sein. Dies umfasst auch komplexe und modulare Konstellationen: Von heterogenen Drohnenschwärmen bis hin zu „Plug-and-Fight“ in geschichteten Luftabwehrsystemen.

Diese Herausforderungen erfordern ein Umdenken, hin zu einem Assurance-Prozess für die Welt der softwaredefinierten Verteidigung. Wir nennen dies softwaredefinierte Assurance. Softwaredefinierte Assurance kann eine effektivere, kosteneffizientere und schnellere Softwarefähigkeitsentwicklung und Adaption ermöglichen.

02 Softwaredefinierte Assurance

Vier Prinzipien unterscheiden softwaredefinierte Assurance von bestehenden Assurance-Ansätzen:

Bestehende Assurance-Ansätze für Waffensysteme	Softwaredefinierte Assurance
Sichert ein Waffensystem einmalig, um Einsatz nach Einführung oder z.B. Midlife-Upgrade zu ermöglichen	Behandelt Assurance als kontinuierlichen Prozess, einschließlich Betrieb und regelmäßiger Updates des Waffensystems
Sichert ein integriertes Waffensystem aus Hardware und Software	Sichert und bewertet ein Softwaresystem für den Einsatz mit vielen Hardware-Systemen (1:N)
Sichert ein Waffensystem in Isolation	Sichert ein System als Teil eines Verbunds von Waffensystemen („System-of-Systems“)
Nimmt an, dass alle Software aus Code entwickelt ist	Definiert Assurance-Pfade für KI

Diese Übersicht vereinfacht die tatsächliche Vielfalt im Bereich Assurance stark: In zahlreichen Bereichen haben spezifische Initiativen zur Entwicklung von Assurance-Ansätzen geführt, die bereits heute im Sinne einer softwaredefinierten Assurance vorgehen. Diese Ansätze sind zu unterstützen. Sie sollten weiter vorangetrieben und universalisiert werden, um den Übergang in softwaredefinierte Assurance zu schaffen.

Hin zu einem kontinuierlichen Assurance-Modell

Bestehende Verfahren der Assurance zielen darauf ab, die Eignung eines Systems für den Einsatz für lange Zeiträume (beispielsweise bis zum Midlife-Upgrade) zu bestimmen. Vorteile, die durch die dynamischere Natur von Software ermöglicht werden, da diese schnell aktualisiert und weiterentwickelt werden kann, sind so aber nicht realisierbar. Für Software muss Assurance als eine Endlosschleife mit zahlreichen „Re-Deployments“ konzipiert werden anstatt eines linearen „Start-Work-End-Prozess“. Dies ist ein grundlegender Perspektivwechsel, motiviert von zwei großen Zielen:

Erstens können wir für Software den Assurance-Prozess bis in den Einsatz und den Betrieb verlängern. Die Performanz einer softwaredefinierten Fähigkeit kann im Betrieb erfasst werden und als Ausgangspunkt eines fortlaufenden Aktualisierungsprozesses dienen. Dadurch lässt sich nicht nur die Fähigkeit verbessern, sondern auch erkennen, wo der Assurance-Prozess möglicherweise unzureichend war oder die Fähigkeit unter Einsatzbedingungen versagt hat.

Zweitens muss nicht jede Iteration des Assurance-Prozesses gleich sein. Vielmehr kann sie auf den spezifischen relevanten operativen Kontext abgestimmt werden. Durch diese Fokussierung kann eine erste Befähigung schneller erreicht werden. Weitere operative Kontexte werden dann hinzufügt, sobald sich dafür eine Notwendigkeit ergibt. Dies ist ein radikal anderer Ansatz als der des traditionellen Assurance-Prozesses, welcher darauf abzielt, eine große Anzahl möglicher operativer Kontexte in einem einmaligen Assurance-Prozess abzudecken und nur schwer um neue operative Kontexte ergänzt werden kann.

1:N - Assurance von Software für den Einsatz mit vielen Hardware-Systemen

Die bestehenden Prozesse der Assurance konzentrieren sich auf die Sicherung eines Gesamtsystems, das aus Software und Hardware besteht, und koppeln dabei die Entwicklung und Assurance von Software und Hardware. Im Fokus dieses Ansatzes steht das Gesamtsystem, das ganzheitlich entwickelt und abgesichert werden muss. Konzeptionell ist die Software nur ein weiterer Teil des Gesamtsystems, das primär als Hardware betrachtet wird. Diese Logik führt zu einem – wie man es in der Softwareentwicklung nennt - wasserfallartigen Ansatz für die Entwicklung und Assurance, mit Vorgehensweisen und Zeitleisten, die sich an der Hardware orientieren, nicht aber an der Software.

Der Entwicklungs- und Assurance-Prozess für Software muss aus den starken Beschränkungen Hardware-fokussierter Ansätze befreit werden – insbesondere um kürzere Zeitleisten zu erreichen. Dafür sollte jedes System in seinen zwei distinkten und gleichwertigen Teilen betrachtet werden: Hard- und Software. Wenn Schnittstellen und Anforderungen zwischen Hardware und Software festgelegt sind, kann Software fortlaufend iteriert und gesichert werden. Bei Bedarf kann dann Software zusammen mit der Hardware getestet werden, um das Gesamtsystem abzusichern. Das „Next Generation Acquisition Model“ der amerikanischen Air Force ist ein klarer Schritt in diese Richtung.

Software kann automatisiert und skaliert getestet werden. Die Leistung der Software kann hinsichtlich der Anforderungen, einschließlich der Einhaltung der Hardware-Schnittstellenspezifikation, mit einem Mix aus realen, erweiterten und künstlichen Daten getestet werden. Dies ermöglicht eine robuste Bewertung der Leistung und erlaubt datengetriebene Verbesserungen der Softwarefähigkeiten. Der Umfang und die Häufigkeit von Tests werden nur durch die Rechenkosten begrenzt und Automatisierung ermöglicht eine schnelle erneute Absicherung des Softwaresystems.

Durch diese Loslösung der Entwicklung und Assurance von Software kann auch die zugrunde liegende Hardware variiert und Ende-zu-Ende-Tests durchgeführt werden, um die Integration zu validieren. Dies ermöglicht, Investitionen in Software über unterschiedliche Plattformen hinweg zu nutzen (sowohl im Zeitverlauf, als auch über verschiedene Hersteller hinweg) und auch ihr Zusammenspiel mit verschiedenen Hardwarekonfigurationen schneller zu iterieren. Hierin liegt der große Vorteil von softwaredefinierter Verteidigung – der sich nur mit softwaredefinierter Assurance erreichen lässt.

Assurance modularerer Strukturen

Bestehende Ansätze der Assurance konzentrieren sich darauf, zu bestätigen, dass ein System spezifische Anforderungen erfüllt. Diese Anforderungen werden im klaren Fokus auf das System an sich definiert. Einige dieser Anforderungen beziehen sich auf die Interaktion mit dem umgebenden Betriebskontext, indem Schnittstellen festgelegt werden, die eingehalten werden müssen (z.B. Link 16). Nur wenige konzentrieren sich darauf, wie Systeme zusammenarbeiten.

Selbst wenn bestimmte Interaktionen zwischen Systemen als Anforderung erfasst werden, ist diese Spezifikation weder umfassend noch dynamisch genug, um die Vielfalt der möglichen Interaktionen zwischen Systemen zu erfassen – insbesondere bei zunehmenden Autonomiegraden der Systeme. Das Problem der Spezifikation wächst kombinatorisch mit der Anzahl der beteiligten Fähigkeiten. Eine vollständige Definition aller Anforderungen und umfassende Tests im klassischen Ansatz der Assurance sind unmöglich.

Mit softwaredefinierter Assurance können wir softwarebasierte Testumgebungen nutzen, um während der Entwicklung das Verhalten eines Systems und seine Interaktionen mit anderen Systemen zu testen. Ein solcher Assurance-Prozess muss datengetrieben sein: Voraussetzung dafür sind Evaluationsumgebungen, in denen die Systeme einer Vielzahl von Betriebssituationen ausgesetzt werden und das daraus resultierende Verhalten bewertet werden kann. Im aktuellen Assurance-Prozess ist die Komplexität dessen, was geprüft werden kann, auf das limitiert, was zuvor als Anforderungen spezifiziert werden konnte. Softwaredefinierte Assurance erlaubt all das zu prüfen, was simuliert werden kann – eine enorme Erweiterung der abdeckbaren Komplexität.

Assurance von Künstlicher Intelligenz

Ansätze zur Assurance von Software sind aus bestehenden Ansätzen für Elektronik entstanden, da Software als eine Erweiterung der elektronischen Systeme betrachtet wurde. Zunächst bestand die Unsicherheit, ob Software effektiv abgesichert werden kann: vorherrschende Assurance-Ansätze waren statistisch, wie z.B. FMEA. Es war unmöglich das Potenzial für Software-Design-Fehler in der gleichen Weise zu analysieren. In der Luftfahrt führte dies zur Schaffung des DO-178, Vorfahre des heute weit verbreiteten DO-178C / ED-12C-Standards, mit einem neuartigen Fokus auf Design-Assurance und die Entwicklung standardisierter Verifikationstechniken für Software.

KI befindet sich heute in einer ähnlichen Position. Zahlreiche bekannte Ansätze, die verwendet werden, um die Zuverlässigkeit von Software zu gewährleisten, lassen sich nur schwer oder gar nicht auf KI-basierte Software anwenden, da hier Modelle aus Daten erstellt werden, anstatt, dass Software-Entwickler händisch Code schreiben. Dies führt zu Reibungen bei der Inbetriebnahme und Entwicklung von KI-basierter Software, da unklar ist, welche Kriterien zu ihrer Assurance herangezogen werden. Im schlimmsten Fall könnte die Assurance von Systemen mit KI sowohl unter schlecht passenden bestehenden Anforderungen als auch unter neuen, aber unzureichend spezifizierten Anforderungen für die Assurance von KI leiden.

Softwaredefinierte Assurance erkennt an, dass sich die Art und Weise, wie wir Software entwickeln, verändern wird und dass dies Auswirkungen darauf haben wird, wie Assurance für Software erfolgen sollte. Softwaredefinierte Assurance unterscheidet eindeutig die Anteile, die unabhängig von der Methode der Implementierung der Software sind (z.B. sog. high-level requirements) von denen, die spezifisch an eine Methode der Implementierung gebunden sind (wie z.B. Code-Abdeckung). Da sich die Ansätze zur Erstellung von KI in den kommenden Jahren fortlaufend verändern werden, muss die Struktur für softwaredefinierte Assurance regelmäßige Aktualisierungen und die Integration neuer Techniken ermöglichen.

03 Der Weg zu softwaredefinierter Assurance

Für einen Paradigmenwechsel hin zu softwaredefinierter Assurance sind klare Schritte und entschiedene Investitionen notwendig:

01 **Infrastruktur für softwaredefinierte Assurance:** Software-Infrastruktur, die Entwicklung, Assurance, Bereitstellung, schnelle Re-Assurance, Aktualisierungen und Überwachung über tausende von Plattformen ermöglicht.

02 **Digitale Assets:** Digitale Assets in der Hand der Streitkräfte - Daten, Umgebungen, Modelle -, die kontinuierlich entwickelt und programmübergreifend für Assurance genutzt werden können.

03 **Standards für Software-Assurance:** Anpassung von Standards für die Softwareentwicklung im Bereich der Verteidigung, um Assurance-Prozesse zugeschnitten auf Software zu ermöglichen.

Notwendig ist eine Strategie, die in diesen Bereichen einen klaren Kurs vorgibt und die, durch gezielte Investitionen, den Veränderungsprozess in Gang setzt. Zudem bedarf es einer umfassenden Betrachtung der bestehenden Herausforderungen in der Beschaffung, um sicherzustellen, dass die Vorteile softwaredefinierter Assurance so weit wie möglich realisiert werden.

Infrastruktur für softwaredefinierte Assurance

Ein grundlegender Vorteil der Assurance von Software besteht darin, dass der Prozess selbst in Software kodiert werden kann. Traditionell werden Assurance-Prozesse in Standards beschrieben, durch Prozesse umgesetzt und durch Audits geprüft. Dies ist zeitaufwendig, fehleranfällig und bringt eine hohe Belastung durch z.B. notwendige Schulungen und Wissensmanagement mit sich.

Für die Software-Assurance – einschließlich KI – können Prozesse hingegen in die Entwicklungsinfrastruktur integriert werden: von der Entwicklung über die Assurance bis hin zum Einsatz, zu Aktualisierungen und zum fortlaufenden Monitoring von Fähigkeiten. Diese Infrastruktur kann als zentrales Managementsystem für die Fähigkeitsentwicklung dienen, um:

- Anforderungen an Assurance im Entwicklungszyklus zu stützen (z.B. Provenienz für Daten bei der Entwicklung von KI)
- Die für Entwicklung und Assurance notwendigen digitalen Assets zu verwalten und zu integrieren
- Die richtigen Werkzeuge bereitzustellen, um den Assurance-Prozess zu definieren – und, wo möglich, zu automatisieren
- Die Erfüllung der notwendigen Assurance-Anforderungen für die Ausbringung von Software-Fähigkeiten vorauszusetzen

Eine solche Infrastruktur muss nicht monolithisch sein, aber sie muss integriert sein, um Kohärenz sicherzustellen. Verschiedene Organisationen - Streitkräfte oder Industrie - werden unterschiedliche Präferenzen für bestimmte Werkzeuge haben, aber diese müssen unter einem System zusammengeführt werden, das den gesamten Software-Assurance-Prozess verwaltet. Die Aufgabe dieses Systems besteht darin, den Prozess zu orchestrieren und diesen trotz der hohen Sicherheits- und Geheimhaltungsanforderungen im Bereich der Verteidigung zu ermöglichen. Die Verteidigungsministerien müssen dabei eine aktive Rolle bei der Implementierung und Einführung solcher Infrastrukturen im gesamten Ökosystem spielen.

Digitale Assets in Software und KI-Assurance

Die Fähigkeit für die Assurance von Software und KI wird im Laufe der Zeit durch kontinuierliche Investitionen in Infrastruktur aber auch durch die Erstellung digitaler Assets aufgebaut. Es gibt mehrere Kategorien digitaler Assets, die für die Assurance von Software und KI verwendet werden:

- **Simulationsumgebungen mit präzisen Modellen:** Simulatoren können die Leistung von Systemen in einer Vielzahl von Szenarien und Bedingungen modellieren und testen, einschließlich extremer und seltener Ereignisse, deren reale Umsetzung nur schwer zu realisieren ist. Simulation ermöglicht umfangreiche Tests zu einem Bruchteil der Kosten und der Zeit, was den Assurance-Prozess insbesondere für Updates beschleunigt.
- **Operative Design-Domains (ODDs):** Standardisierte Definitionen des erwarteten Betriebskontextes, welche die Grenzen definieren, innerhalb der die Leistung eines Systems und seiner Komponenten bewertet werden. Die Ausrichtung von ODDs ermöglicht die Wiederverwendung von Softwarekomponenten und „System-of-Systems-Level-Auswertung“.
- **Daten:** Sammlungen von realen, erweiterten und künstlichen Daten. Strenge Tests und Auswertungen von Software und KI-Systemen hängen von der Erhebung von Daten zur Auswertung ab, welche die ODD ausreichend darstellen und abdecken.

Diese digitalen Assets müssen im Eigentum und unter der Kontrolle der Streitkräfte sein, um sicherzustellen, dass die Systeme unterschiedlichste Akteure entwickelt und durch Assurance-Prozesse gesichert werden können. Die Industrie kann dabei durch Entwicklung und Wartung beitragen, wie es bei zahlreichen Bestandssystemen der Fall ist, die Kontrolle muss aber bei den Streitkräften liegen.

Diese Assets müssen im Rahmen einer langfristigen Roadmap der Streitkräfte aufgebaut werden. Spezifische Programme können genutzt werden, um die Entwicklung dieser digitalen Assets zu priorisieren und zu finanzieren, gleichzeitig wird aber eine Vision für einen kohärenten Ansatz benötigt, der programmübergreifend vorgeht. Erste Beispiele gibt es im Bereich digitaler Zwillinge, wie Investitionen der amerikanischen Air Force zeigen. Sowohl Tempo als auch Ambition dieser Ansätze müssen jedoch wachsen.

Standards für die Assurance softwaredefinierter Fähigkeiten

Bestehende Standards für Software-Assurance in der Verteidigung sind im Wesentlichen aus zwei Pfaden enstanden:

01 Standards im Bereich der Verteidigung, für Hardware entwickelt und erweitert, um Software abzudecken (z.B. AQAP 2310 + 2210)

02 Software-Sicherheitsstandards aus der zivilen Welt angepasst an die Verteidigung (z.B. DO-178C)

Natürlich wird Software weiterhin in vielerlei Art und Weise in militärischen Systemen eingesetzt werden. Ein Sicherheitsmechanismus für ein Kraftstoffspeichersystem wird mehr von der kumulativen Erfahrung, welche in der IEC 61508 gefasst ist, profitieren, als von einem zukünftigen Prozess für die schnelle Adaption von Software. Der Fokus von softwaredefinierter Assurance sollte darauf liegen, zu klären, wie softwaredefinierte Fähigkeiten gesichert werden können, anstatt sämtliche Software in Waffensystemen abzudecken.

Für softwaredefinierte Fähigkeiten sind standardisierte Ansätze notwendig, die berücksichtigen, dass sich (a) Software von Hardware unterscheidet und, dass sich (b) Verteidigung von der zivilen Welt unterscheidet. System Engineering Prinzipien müssen mit der Zielsetzung der Sicherung von Softwaresystemen angewendet werden – im Sinne von “Software-first”. Neue Standards müssen dabei folgendes sicherstellen:

- Bereitstellung von Anleitungen zur Entwicklung und Überprüfung von maschinellem Lernen und KI. Standards, die davon ausgehen, dass alle Software händisch in Code geschrieben ist, sind veraltet. Leitlinien für eine wirksame Überprüfung von Algorithmen (insbesondere KI) können bewährte Verfahren verbreiten und die Entwicklung von Fähigkeiten beschleunigen. Das EASA-Konzeptpapier für künstliche Intelligenz ist ein großer Schritt in diese Richtung.
- Die Vorteile fortlaufender Adaption von Fähigkeiten mit den Risiken in Ausgleich zu bringen, die mit iterativer Assurance von Fähigkeiten verbunden sind. Ein explizites Risikomanagement zur Abwägung von Schnelligkeit gegen Zuverlässigkeit kann bewusste Kompromisse in diesen Dimensionen ermöglichen, anstelle eines „Alles (Friedenszeit) oder Nichts (Kriegszeit)“ - Ansatzes.
- Die Notwendigkeit einer schnellen „Re-Assurance“ von Software, die schrittweise aktualisiert wird widerspiegeln (z.B. Re-Training eines KI-Modells auf Basis neuer Missionsdaten, um die Leistung für die nächste Mission zu verbessern). Dieses Thema wird weder durch hardwareorientierte Verteidigungsstandards noch durch zivile Standards für Software und KI-Assurance abgedeckt. Selbst das EASA Konzeptpapier, das sich auf die zivile Luftfahrt konzentriert, befasst sich nicht mit der Frage der raschen Integration von Missionsdaten.

Initiativen wie die Europäische Initiative für Collaborative Air Combat Standardisation (EICACS) existieren, um Standards in der Verteidigung zu entwickeln. Sie müssen die Sicherheit von softwaredefinierten Fähigkeiten fokussieren und dürfen dabei nicht zu stark an bestehenden zivilen oder hardwareorientierte Ansätze gebunden sein. Ähnliche Anstrengungen sind in allen militärischen Domänen - Luft, See und Land - erforderlich, um sicherzustellen, dass operationelle Anforderungen im Paradigma Software-Defined Defence umfassend erhoben werden.

Darüber hinaus spielen die Verteidigungsministerien und Beschaffungsbehörden eine entscheidende Rolle, indem sie ihre Innovationsbereitschaft in Bezug auf sowohl Assurance als auch auf militärische Fähigkeiten signalisieren. Führungskräfte im Verteidigungs- und Beschaffungswesen müssen den Fokus wieder auf die angestrebten Ergebnisse – zuverlässige und leistungsfähige Systeme – richten, anstatt stets auf bestehende Standards oder Prozesse zu setzen. Es wird Anstrengung erfordern, Lösungen mit breiter Akzeptanz zu finden. Aber ein oder zwei bedeutende Programme, die Innovationen sowohl im Bereich der Assurance als auch im Bereich der softwaredefinierten Fähigkeiten voranzutreiben, können als Wegbereiter dienen und so zum Wendepunkt für die Assurance und den Einsatz von softwaredefinierten Fähigkeiten werden.

Beschaffung und offene Architekturen

Es ist essenziell anzuerkennen, dass eine Modernisierung der Assurance allein nicht ausreichen wird. Auch der Prozess der Beschaffung muss sich im Großen und Ganzen verändern. Auch hier hebt das „Next Generation Acquisition Model“ der amerikanischen Air Force einige der Schlüsselthemen hervor, die unter dem Stichwort der „agilen Beschaffung“ behandelt werden. Ohne Änderungen in der Art und Weise, wie die Streitkräfte beschaffen, werden die Vorteile der softwaredefinierten Assurance durch verschiedene Formen der Abhängigkeit von einzelnen Industriespielern – sowohl technischer als auch kommerzieller Art – eingeschränkt bleiben.

Eine umfassende Darstellung übersteigt den Rahmen dieses Papiers, besonders relevant sind aufgrund des engen Bezugs zu den zuvor besprochenen Themen allerdings offene Architekturen. Um die 1:N-Möglichkeiten von Software und KI – insbesondere über Plattformen hinweg, die von verschiedenen Anbietern stammen – zu nutzen, müssen offene Architekturen definiert und konsequent implementiert werden, damit Software und KI integriert werden können.

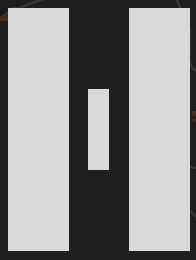
04 Softwaredefinierte Assurance ist eine strategische Fähigkeit

Es gibt - zu Recht - viele Diskussionen über die transformative Rolle, die Software und KI auf dem modernen Gefechtsfeld spielen können und in einigen Fällen bereits spielen. Ohne einen geeigneten Ansatz der Assurance wird dieses Potenzial jedoch nie erreicht werden. Die Entwicklung und der Einsatz von Fähigkeiten würden weiterhin verlangsamt. Investitionen in softwaredefinierte Fähigkeiten würden aufgrund der erwarteten Reibungsverluste ausbleiben oder in ihrer Wirkung geschwächt. Insgesamt würden die den NATO-Streitkräften zur Verfügung stehenden Fähigkeiten so erheblich beeinträchtigt.

Wir müssen in eine softwaredefinierte Assurance investieren, um das volle Potenzial softwaredefinierter Fähigkeiten für die Verteidigung zu erschließen. Ähnlich wie in der skalierten Produktion von Hardware werden die Länder, die in der Lage sind, die Assurance von Software im industriellen Maßstab aufzubauen und damit eine schnelle Produktion qualitativ hochwertiger Software-Fähigkeiten ermöglichen, einen strategischen Vorteil auf dem Gefechtsfeld der Gegenwart haben. Der aus softwaredefinierter Assurance resultierende Vorteil reicht von der Forschung und Entwicklung von Software und KI bis hin zum Einsatz auf dem Gefechtsfeld.

Um softwaredefinierte Assurance zu erreichen müssen bestehende Ansätze überdacht werden. Eine Konzentration auf Software als eigenständiges System ist notwendig – nicht bloß als Anhang zur Hardware. So kann die Assurance von Software von der Hardware entkoppelt werden, als kontinuierlicher Prozess gestaltet werden und die Herausforderungen lösen, die durch Autonomie und modulare Verbünde von Waffensystemen entstehen werden. Die Definition und Umsetzung von Wegen für die Assurance von softwaredefinierten Fähigkeiten auf Basis von KI werden besonders entscheidend sein. Obwohl es bereits Schritte in diese Richtung gibt, sind diese bisher lückenhaft, zu langsam und unkoordiniert – wir müssen die Bemühungen bündeln und beschleunigen.

Softwaredefinierte Assurance ist ein Nordstern, um das tiefe Fachwissen – sowohl aus dem öffentlichen als auch aus dem privaten Sektor – in den NATO-Staaten zu mobilisieren und die Entwicklung unserer Fähigkeiten insgesamt zu beschleunigen. Um dies zu unterstützen, müssen Aufmerksamkeit und Ressourcen auf drei Bereiche konzentriert werden: Infrastruktur für Software Assurance, digitale Assets in der Kontrolle der Streitkräfte und neue Standards für Software im Bereich der Verteidigung. Mit diesen Grundlagen kann ein Modell für softwaredefinierte Assurance geschaffen werden, um softwaredefinierte Fähigkeiten schnell und zuverlässig zu entwickeln und für das Gefechtsfeld fortlaufend zu adaptieren.



Helsing