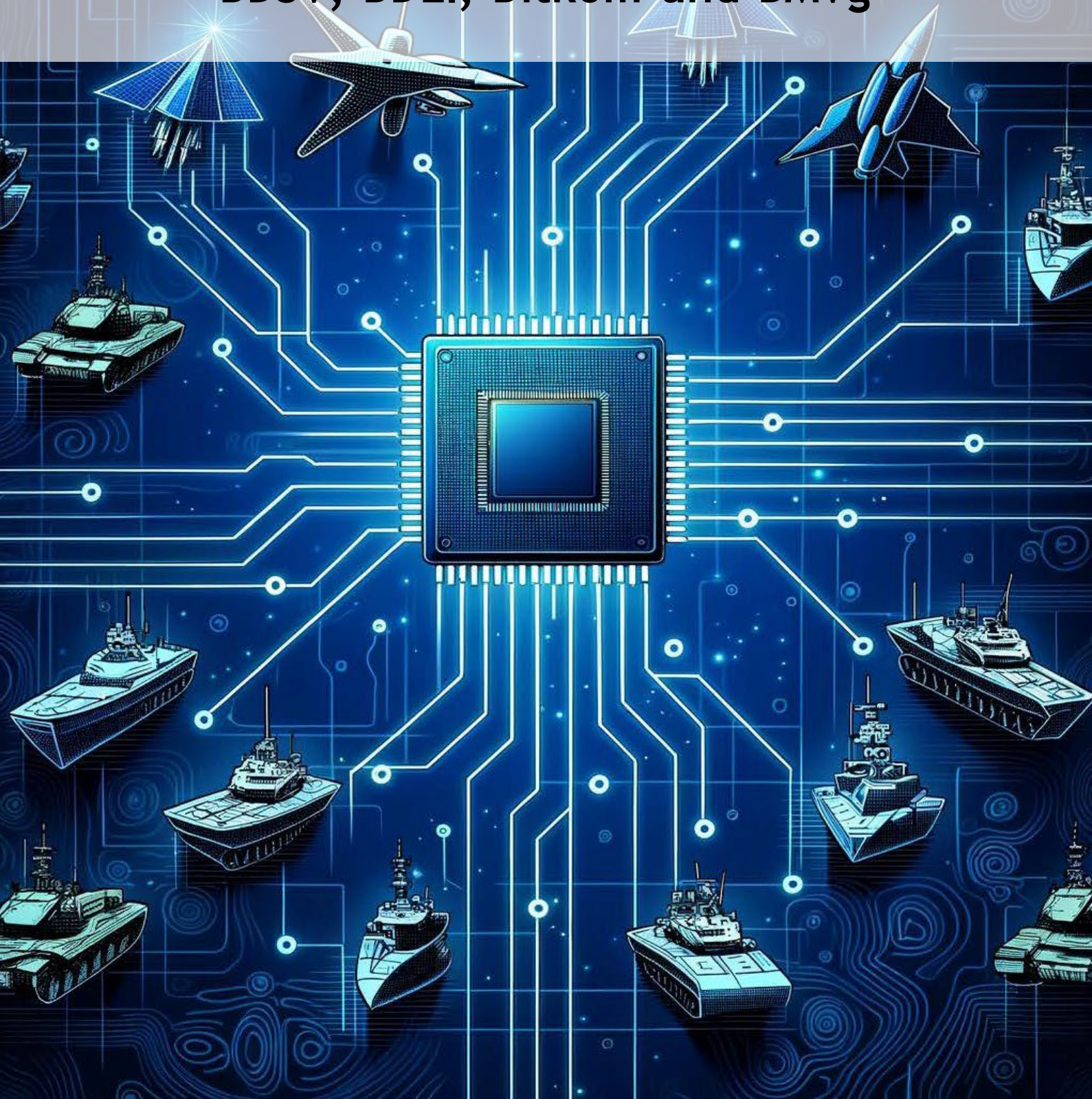
Software Defined Defence

Positionspapier des

BDSV, BDLI, Bitkom und BMVg



Positionspapier

Software Defined Defence

Ergebnisse des Expertenkreises 1 (EK1) Software Defined Defence

im Rahmen des Gesprächskreises 4 (GK4) „Innovation Cyber/IT“ des strategischen Industriedialogs (SSID)

zwischen

dem Bundesministerium der Verteidigung, Abteilung Cyber/Informationstechnik,

dem Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V.,

dem Bundesverband der Deutschen Luft- und Raumfahrtindustrie e.V. und

dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

Version: Mitgeprüfte und mitgezeichnete Version zur Veröffentlichung

Stand: 31.10.2023

Einstufung: Öffentlich – Zur freien Verwendung nach Maßgabe des strategischen Industriedialoges

BMVg
Bundesministerium der Verteidigung, Abteilung Cyber / Informationstechnik (CIT)
Stauffenbergstraße 18
10785 Berlin

BDSV e. V.
Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e. V.
Friedrichstraße 60
10117 Berlin

BDLI e.V.
Bundesverband der Deutschen Luft- und Raumfahrtindustrie e.V. und
Friedrichstraße 60
10117 Berlin

Bitkom e. V.
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10
10117 Berlin

Hinweise

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung der Herausgeber zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität. Eine Verwendung liegt in der eigenen Verantwortung des Lesers.

Inhaltsverzeichnis

1 Einleitung

Weltweit schwelende und offen ausgetragene Konflikte, wie z. B. in der Ukraine, haben in Bevölkerung und Politik ein neues Sicherheitsbewusstsein geschaffen und stellen moderne, bestmöglich ausgerüstete Streitkräfte als ein wesentliches Element der gesamtstaatlichen Sicherheitsvorsorge in einen breiten Fokus. Sie zeigen aber gleichzeitig brennglasartig Herausforderungen und auch Defizite sowie Nachholbedarfe für die Streitkräfte auf, um ihre Aufgaben in einem Future Operating Environment, welches von einem hohen Grad an Vernetzung, Digitalisierung und Interoperabilität, hoher Veränderungsgeschwindigkeit sowie Anpassungsfähigkeit und -notwendigkeit geprägt ist, zu erfüllen.

Digitalisierung verändert in zunehmendem Maße und immer größerer Geschwindigkeit sämtliche Lebensbereiche der Gesellschaft. Hierfür verantwortlich sind insbesondere die rasante Weiterentwicklung von Software in immer kürzeren Zyklen, zunehmende Datenmengen sowie exponentiell steigende Rechenkapazitäten. In der Privatwirtschaft wirkt sich Software disruptiv auf ganze Branchen aus, u. a. durch den Einsatz von Künstlicher Intelligenz (KI).

Die o. a. Herausforderungen und auch Chancen sind nun an den heute bereits in der Nutzung befindlichen Waffensystemen zu spiegeln und entsprechende Handlungsmöglichkeiten für eine Modifikation/Anpassung an die künftigen Anforderungen von Vernetzung und Digitalisierung zu untersuchen. Besonders die Aspekte

- plattformübergreifende Vernetzung und Einbinden der hierfür erforderlichen plattformspezifischen Fähigkeiten (z.B. Bereitstellung von Sensordaten),
- Möglichkeiten einer schnelleren Anpassung der Software an neue kurzfristig auftretende, einsatzinduzierte Anforderungen u. a. durch funktionale Erweiterungen und agile Verfahren der Softwarepflege und –änderung (SWPÄ) sowie
- Fähigkeitsaufwüchse und Leistungssteigerungen bestehender Systeme durch Software

verdienen hierbei besondere Aufmerksamkeit.

Um die Leistungsfähigkeit der Bundeswehr gem. Auftrag der „Zeitenwende“ kurz- und mittelfristig zu steigern und an neue Anforderungen des sich immer schneller verändernden Gefechtsfeldes anpassen zu können, ist eine größtmögliche Nutzung der Möglichkeiten von Digitalisierung zur digitalen Ertüchtigung von bereits in Nutzung befindlichen Systemen und bei der Entwicklung von neuen Systemen entscheidend – Software ist der wesentliche Enabler moderner militärischer Operationen ganz im Sinne von Multi-Domain-Operations (MDO).

Ein zentrales Leit-Prinzip für die Streitkräfteentwicklung der Zukunft ist hierbei „Software Defined Defence“ (SDD). Im Mittelpunkt steht das Ziel, die enormen Potenziale von

Software für die stetige Verbesserung bzw. Erweiterung der Fähigkeiten der Waffensysteme und damit der (flächendeckenden) Steigerung der Leistungsfähigkeit der Bundeswehr zu nutzen.

Klassische militärische Plattformen sollen damit nicht in ihrer Relevanz abgewertet werden, sondern von den weitreichenden Potenzialen der Softwareentwicklung profitieren. So können durch die spezifischen Eigenschaften von zeitgemäßer Software-Entwicklung Innovationspotenziale für die Fähigkeitsentwicklung der Streitkräfte erschlossen werden. Dazu zählen u. a. kurze Entwicklungszyklen, flexible Anpassungsfähigkeit, Skalierbarkeit und Resilienz.

Es ist also zu prüfen, ob und wie die Leistungsfähigkeit militärischer Systeme künftig mithilfe von standardisierten und wiederverwendbaren Softwaremodulen, auf Basis einer normierten Zwischenebene (Middleware) und standardisierten Schnittstellen schneller, kostengünstiger und kontinuierlich angepasst werden kann, ohne dass die zugrunde liegende IT-Infrastruktur ersetzt oder signifikant angepasst werden muss und dadurch ihre Betriebsfähigkeit für längere Zeit eingeschränkt ist (vergleichbar App-Stores auf Mobiltelefonen).

Die Bundeswehr hat als wesentliche Grundlage hierfür das Portfolio ihrer IT-Landschaft entlang der NATO C3-Taxonomie in neun Clustern strukturiert und einem gemeinsamen Portfoliomanagement unterworfen, damit die IT der Bundeswehr zielgerichtet weiterentwickelt werden kann. Der resultierende methodische Ansatz der Digitalisierungsplattform des Geschäftsbereichs (GB) BMVg ist dabei die Voraussetzung für die Implementierung des Design-Paradigmas Software Defined Defence in der Bundeswehr (SDDBw).

Um die mit der Digitalisierungsplattform des GB BMVg geschaffenen Voraussetzungen ganzheitlich zu nutzen und die durch SDDBw beabsichtigte Zielsetzung - insbesondere aber auch für die Plattformen, Fähigkeitsträger und Waffensysteme - zu erreichen, ist für alle Beteiligten ein Umdenken und Umlenken bei der Gestaltung und/oder Umsetzung der Rüstungs- und Planungsprozesse sowohl auf Seiten des öffentlichen Auftraggebers (öAG) als auch auf Seiten der Industrie, einschließlich der Systemhäuser, notwendig.

SDDBw soll somit einerseits die Interoperabilität der Systeme mit- und untereinander erhöhen, um bspw. Aufklärungsergebnisse verschiedener Systeme in Lagebildern zusammenführen zu können und Entscheidern zu erlauben, zielgerichtete und wirkungsvolle Maßnahmen ergreifen zu können. SDDBw zielt andererseits aber auch darauf ab, Anpassungen an und für die Plattformen als Reaktion auf technische und taktische Anforderungen zielgerichtet vornehmen zu können. Fähigkeitsverbesserungen/-erweiterungen können damit schnell und durch die Wiederverwendung vorhandener Softwaremodule auch wirtschaftlich vorgenommen werden.

2 Software Defined Defence für die Bundeswehr im Detail

Der Komplex SDDBw wurde in sechs Untersuchungsschwerpunkte gegliedert, von denen jeder für sich Fragestellungen aufgreift, die für den Aufbau eines Digitalisierungsökosystems betrachtet werden müssen. Zusammen bilden diese Anteile ein holistisches Gesamtkonstrukt, dass die Thematik weitestgehend erfasst und eine strukturierte Vorgehensweise für die zukünftigen Arbeiten erlaubt:

- **Foundation@SDDBw**, die IT-Basisinfrastruktur als Voraussetzung für eine modulare Softwarearchitektur
- **Rapid Development & Deployment@SDDBw**, eine agile Softwareumgebung mit zugehörigen Prozessen und Verfahren zur raschen Entwicklung, Testung, Qualitätssicherung und regelmäßigem Deployment von Software bzw. Softwareanpassungen auf den Plattformsystemen über deren gesamten Lebenszyklus – auch während deren Einsatz,
- **KI (Methoden)@SDDBw**, die disruptive Zukunftstechnologie als Enabler einer Vielzahl von fähigkeitssteigernden Anwendungen,
- **InfoSec@SDDBw**, eine an das Paradigma SDD angepasste Information Security Umgebung,
- **Economics@SDDBw**, wirtschaftliche Aspekte, die bei der Einführung von SDD zu beachten sind sowie
- **Contracting@SDDBw**, vertragsrelevante Themen, die durch SDD entstehen und gelöst werden müssen.

Diese Untersuchungen befassten sich mit vielfältigen Aspekten, wovon ausgewählte in weiteren Schritten detaillierter betrachtet werden sollen. Die aktuellen Zwischenergebnisse der Untersuchungen werden im Folgenden im Sinne einer Executive Summary zusammengefasst.

2.1 Foundation@SDDBw

Kurzbeschreibung

Foundation@SDDBw beschreibt eine gemeinsame IT-Architektur, Funktionen und Schnittstellen. Dabei sollen IT-Plattform und Applikationslogik logisch getrennt werden, um sie weitestgehend unabhängig voneinander nutzen und anpassen zu können oder aber auch einzelne Softwaremodule in mehreren Systemen zu instanziieren. Hierzu gehört aber auch die plattformübergreifende Vernetzung und das Einbinden der hierfür erforderlichen plattformspezifischen Fähigkeiten im Sinne einer „Föderierbarkeit“ gemäß Federated Mission Networking (FMN).

Erstes Analyseergebnis:

Wesentlich ist das Thema der Konzeptionierung der grundlegenden IT-Architektur und des dazugehörigen Infrastruktursystems einer Software Defined Defence-Strategie. Das Ziel muss es sein, eine flexible, interoperable IT-Plattform, adäquat für nationale und internationale Einsatzszenarien zu definieren. Die Architektur beinhaltet dabei u.a. Vorschläge zu einer Container-Orchestrierung, agile Betriebsmodelle sowie Kooperationen unter Beteiligung der Industrie und ausgewählten Stellen des GB BMVg. Zu diesem Zweck wird empfohlen, die Einführung einer Governance zu prüfen, Best Practices zu beachten, ein vollumfängliches API[1]-Management einzuführen und Pilotprojekte zur Verwirklichung eines softwaredefinierten Verteidigungssystems durchzuführen. Dies wird einen innovativen Wandel, stärkere Anpassungsfähigkeit und nahtlose Interoperabilität in einer modernen IT-Landschaft der Bundeswehr ermöglichen.

Ausgewählte Aspekte für weitere Detailbetrachtung

- Erstellung eines Grobkonzepts zur Containerisierung und Container-Orchestrierung
- Erarbeiten von Vorschlägen für die Anpassung der bestehenden Systemarchitektur

2.2 Rapid Development & Deployment@SDDBw

Kurzbeschreibung

Rapid Development und Deployment (schnelle Entwicklung und Bereitstellung) stellt ein Framework bestehend aus Tools und Prozessen dar, mit dem Software in kürzerer Zeit und mit höherer Geschwindigkeit entwickelt, getestet, qualitätsgesichert und auf den Plattformsystemen bereitgestellt bzw. ausgebracht werden kann. Rapid Development zielt darauf ab, den Softwareentwicklungs- und Bereitstellungsprozess zu beschleunigen, indem iterative und inkrementelle Methoden eingesetzt werden.

Erstes Analyseergebnis:

Die steigende Bedeutung von Daten und Software für die Fähigkeiten militärischer Plattformen und der Bedarf, diese deutlich schneller zu aktualisieren als bisher, erfordert einen Paradigmenwechsel bei der Softwareentwicklung. Die notwendige Geschwindigkeit im Development und Deployment bedingt die durchgängige Etablierung agiler, nutzerzentrierter Entwicklungsmethodiken, einen hohen Simulations- und Automationsgrad durch Standardisierung sowie den Schulterschluss von Bundeswehr und Industrie, unterstützt durch moderne Kollaborationswerkzeuge. Offene Schnittstellen, gepaart mit Security by Design sowie Verfahren für standardisierte Rollouts sorgen für

[1] Application Programming Interface, Anwendungsprogrammierschnittstelle

schnelle und sichere Verteilung von Aktualisierungen und Servicebereitstellungen für alle verfügbaren Plattformen im Einsatz. Für den Erfolg werden moderne Konnektivitätstechnologien benötigt.

Ausgewählte Aspekte für weitere Detailbetrachtung

- Analyse von Softwareentwicklungsmethodiken
- Erarbeitung eines Konzeptes für Zusammenarbeitsplattformen für die Softwareentwicklung

2.3 KI (Methoden)@SDDBw

Kurzbeschreibung

KI als die disruptive Zukunftstechnologie ist ein Enabler einer Vielzahl von fähigkeitssteigernden Anwendungen und spielt eine wesentliche Rolle als Fähigkeitstreiber für militärische Plattformen.

Erstes Analyseergebnis:

Für KI-basierte Services müssen neue Muster (z. B. Tarnung, Radiosignale) generiert wie identifiziert, Services nachtrainiert, getestet, zertifiziert und bis auf die taktische Ebene ausgerollt werden. Dabei sollen diese Modelle schnell und mit wenig Integrationsaufwand in die jeweilige Plattform implementiert werden können. Ein Anwendungsfall ist bspw. die Nutzung der Daten sämtlicher Sensoren und anderer Quellen (C4I-Systeme) für KI-basierte Funktionen (Konnektivität und Interoperabilität).

Ausgewählte Aspekte für weitere Detailbetrachtung

- Erarbeitung eines Konzeptes für sichere Entwicklung und Bereitstellung von zertifizierten KI-Modellen

2.4 InfoSec@SDDBw

Kurzbeschreibung

Die Einführung von SDD in die Bundeswehr hat eine starke Verbindung zur Informationssicherheit (InfoSichh). Zum einen werden inhärent Verbesserungen ermöglicht bspw. durch schnelleres und zielgerichtetes Einbringen von Sicherheitspatches. Allerdings werden auch neue Sicherheitsrisiken und potenzielle Angriffsvektoren eröffnet. Security-by-Design und Security-by-Default als Prinzipien und Ansätze wie Zero-Trust und grundlegende Informationssicherheits-Funktionalitäten, wie Verschlüsselung, Authentisierung, etc. müssen von Beginn an mitberücksichtigt werden.

Erstes Analyseergebnis:

Ein wesentliches Ergebnis ist die Feststellung, dass aktuell bekannte Vorgaben zu InfoSichh im GB BMVg den Ansatz SDDBw grundsätzlich unterstützen. Handlungsbedarf besteht hinsichtlich der Operationalisierung und der Ergänzung von grundlegenden Vorgaben. Dies umfasst u. a. eine Weiterentwicklung des Risikomanagements (Berücksichtigung Komplexität und Dynamik), Möglichkeiten einer angepassten VS-Einstufung, sowie erweiterte Grundlagen in der Handhabung/Umsetzung Informationssicherheit und die Etablierung von Lieferkettentransparenz und -sicherheit.

Ausgewählte Aspekte für weitere Detailbetrachtung

- Untersuchung zur Absicherung der Lieferkette, insbesondere bei Software-Deployment.
- SWOT-Analyse SDDBw zu InfoSichh, Ressort-VSA[2] GB BMVg und VS-Einstufung.

2.5 Economics@SDDBw

Kurzbeschreibung

Traditionelle Ansätze für spezifische IT in den Systemen führen zu geringen Stückzahlen und Margen und adressieren i.d.R. eine kleine „Zielgruppe“ bei gleichzeitig hoher Komplexität, hohen Anforderungen an die Sicherheit und einer starken Regulierung (Industriestandards, NATO, …). SDD eröffnet bzw. erfordert neue Geschäftsmodelle, kann im Ergebnis Kosten reduzieren und den Wettbewerb fördern. Urheberrechte und geistiges Eigentum, Nutzungsrechte an Systemen sowie beispielsweise die Rechte an benötigten Daten dürfen bei der Operationalisierung von SDD für die Bundeswehr nicht außer Acht gelassen werden.

Erstes Analyseergebnis:
SDDBw muss als offenes und modulares System mit klar definierten Schnittstellen ausgelegt werden. Folgende Ziele müssen erreicht werden:

- Die Schnittstellen der einzelnen Software-Module sind offen/verifiziert und stehen dem Nutzer aber auch dem OEM[3] ggf. zur Nutzung in anderen Projekten zur Verfügung, um eine wirtschaftliche Anwendung zu ermöglichen.
- Die Verantwortlichkeiten für die plattformbezogene und plattformübergreifende Funktionalität und Sicherheit des Gesamtsystems ist geregelt.
- Die bisherigen OEM-Rechte (Intellectual Property Rights – (IPR) etc.) sind sowohl für OEM, Auftraggeber als auch ggf. Dritten adäquat geregelt und berücksichtigt. Bei der Schaffung einer „Bw-eigenen Softwarekompetenz als Katalysator“ ist weiterhin

[2] Allgemeinen Verwaltungsvorschrift zum Geheimschutz (Verschlusssachenanweisung – VSA).

[3] Original Equipment Manufacturer, Originalausrüstungshersteller

sichergestellt, dass die Industrie Zugriff auf die Software-Module hat. Hier gilt es auch die Verantwortung für Systemmodifikationen und ihre Auswirkungen auf die jeweiligen Waffensysteme zu definieren.
- Die Prozesse der Systemverifikation für den GB BMVg und beispielsweise das Bundesamt für die Sicherheit in der Informationstechnik (BSI) sind angepasst und ggf. erweitert

Ausgewählte Aspekte für weitere Detailbetrachtung

- Untersuchung zu Rechtesituation bei SDDBw (u.a. IPR, Nutzungsrechte, Rechte an Daten)
- Untersuchung zu Finanzaspekten wie Preisrecht, Haftungsfragen, Bürgschaften etc.

2.6 Contracting@SDDBw

Kurzbeschreibung

Prozesse für Planung und Ausrüstung der Bundeswehr, wie z. B. Rüstungsprozess inkl. Vergabeverfahren, Vertragsgestaltungen und Realisierung müssen bei Neuvorhaben SDDBw vom Grundsatz her ermöglichen. Bezüglich in Nutzung befindlicher Systeme müssen Maßnahmen getroffen werden, um SDDBw zumindest weitestgehend zu ermöglichen, sofern Restnutzungszeiten und erwartbare Potentiale der SDDBw-getriebenen Verbesserungen dies rechtfertigen.

Erstes Analyseergebnis:

Will die Bundeswehr das Prinzip SDD erfolgreich implementieren und somit deren erwartetes Potenzial ausnutzen, müssen hierfür kompatible (rechtlich, kommerziell, funktional) Rahmenbedingungen für die Planung, Beauftragung und die Realisierung inklusive der Nutzungsphase geschaffen werden.

Die klassischen OEM-Verträge bei den Waffensystemen müssen „geöffnet“ werden – hierbei müssen das Erbringen der geschuldeten Leistung, die funktionale Verantwortung und damit die Haftungsverteilung alt/neu, Rollenverteilungen, Zusammenarbeit mit/zwischen SDD-Akteuren geregelt sein. Darüber hinaus muss insbesondere, wenn neue Software- oder KI-basierte Fähigkeiten implementiert werden und eine erfolgreiche Abnahme/Zertifizierungsverfahren durchlaufen wurde, die nachfolgende Nutzungsverantwortung klar geregelt sein. Rechte für Betriebsdaten und gelernte Erkenntnisse sind vertraglich zu regeln.

Ausgewählte Aspekte für weitere Detailbetrachtung

- Erarbeitung von „geöffneten“ OEM Vertragsmustern
- Erarbeitung von Anpassungserfordernissen für Vergaberecht und weitere gesetzliche Vorschriften und Formen bis hin zur Anpassung des V-Modells

3 Ausblick

Die mittels SDDBw beschriebene Transformation zielt im Ergebnis auf eine Verbesserung der Interoperabilität eigener aber auch verbündeter bzw. föderierbarer Systeme, eine Steigerung der Resilienz und Skalierbarkeit, die Erweiterbarkeiten der Fähigkeiten bestehender/eingeführter Waffensysteme durch schnell bereitgestellte Softwareupdates sowie mehr Flexibilität und Agilität, um langwirkenden (strategischen) Fehlentscheidungen vorzubeugen.

Aufbauend auf den erzielten Ergebnissen sind weitere Detailbetrachtungen zu ausgewählten Fragestellen erforderlich und vorgesehen, um die weitere Umsetzung SDDBw aktiv zu begleiten.

Der Strategische Industriedialog und die Bundeswehr werden auf Basis dieser Handlungsstränge weitergehende Untersuchungen initiieren, um das Paradigma SDD soweit zu operationalisieren, dass anschließend zukünftige und bereits in Nutzung befindliche Systeme der Bundeswehr erste Vorgaben und Anpassungen erfahren können[4].

[4] Für die bereits in Nutzung befindlichen Systeme ist jeweils individuell der Aufwand, Nutzen u.a. unter Berücksichtigung der Restlaufzeiten zu bewerten.

4 Urheberschaftsnachweis

An diesem Dokument als Ergebnis der Arbeiten des EK 1 haben Vertreter der Mitgliedsunternehmen der Verbände BDSV e.V., BDLI e.V und Bitkom e.V. sowie das Bundesministerium der Verteidigung und der Geschäftsbereich BMVg aktiv mitgewirkt.

Seitens der Verbände BDSV e.V., BDLI e.V. und Bitkom e.V. haben folgende Mitgliedsunternehmen im EK 1 und bei der Erstellung dieses Dokumentes mitgewirkt:

- Airbus Defence and Space GmbH
- Blackned GmbH
- CAE Elektronik GmbH
- Capgemini Deutschland GmbH
- CGI Deutschland B.V. & Co. KG
- Cisco Systems GmbH
- CONET Solutions GmbH
- Dassault Systemes Deutschland GmbH
- Dynamit Nobel Defence GmbH
- Eviden Germany GmbH
- Helsing GmbH
- Hensoldt Holding Germany GmbH
- IBM Deutschland GmbH
- Krauss-Maffei Wegmann GmbH & Co. KG
- Liebherr-Aerospace Lindenberg GmbH

- Materna Information & Communications SE
- MBDA Deutschland GmbH
- Microsoft Deutschland GmbH
- msg systems ag
- PLATH GmbH & Co. KG
- Red Hat GmbH
- Rheinmetall AG
- Rheinmetall Electronics GmbH
- Rohde & Schwarz GmbH & Co. KG
- Schönhofer Sales and Engineering GmbH
- T-Systems Information Services GmbH
- VMware Global, Inc. Zweigniederlassung Deutschland

Referenzen und Quellen

1. Titelbild generiert bei OpenAI's DALL·E 3