

AFCEA-Fachveranstaltung Software Defined Defense – Industrie im Dialog mit BMVg: Positionsbestimmung und ein Blick nach Vorn

Über die Relevanz von Software Defined Defense (SDD) herrscht Konsens. Aber wo steht die Amtsseite, wo steht die Industrie und haben wir ein gemeinsames Verständnis dieses paradigmatischen Wechsels im Verteidigungssektor?

Im Nachgang der AFCEA-Fachveranstaltung „Software Defined Defense – Industrie im Dialog mit BMVg“ am 18. April im Berliner Capgemini Office bietet dieses Papier einen Überblick über die wesentlichen Fragen und Inhalte, die auf der Veranstaltung besprochen wurden und über die nächsten Schritte, die wir – Industrie und Amtsseite – gemeinsam angehen müssen.

Positionsbestimmung – die zentralen Aussagen



- **Die Amtsseite** ist weiter als breit bekannt. Das BMVg treibt die Entwicklung von SDD mit fünf Schwerpunkten voran (siehe Folien) und arbeitet eng mit Industrieverbänden zusammen. Die BWI arbeitet daran, den SDD-Gedanken u.a. mit der „Platform42“ zu unterstützen. Es wird auch Initiative/Unterstützung seitens Industrie erwartet.



- Aus **Sicht der Industrie** - dargestellt durch CGI und in der Diskussion vertieft - erfordert SDD technische Anpassungen, eine organisatorische Umstrukturierung und eine geeignete Governance, die Führungs-, Waffen- und Kommunikationssysteme miteinander verzahnt. Die Optimierung rechtlicher/vertraglicher Rahmenbedingungen und Anpassung der Beschaffungsprozesse sind Schlüsselfaktoren für erfolgreiche SDD.



- Laut Capgeminis „strategic foresight“ Beitrag könnte Deutschland Gefahr laufen im Bereich SDD abgehängt zu werden, wenn alle Beteiligten nicht **gemeinsam das Steuer herumreißen**. Dazu muss bei zentralen Treibern einer erfolgreichen SDD-Umsetzung nachgebessert werden. (siehe unten - Umfrage für 3 exemplarische Treiber).



- Aus Sicht eines Innovators (CIHBw) ist es wichtig, **schnell Wirkung zu erzielen**. Für Innovationen müssen langwierige Fragestellungen nach der richtigen Architektur auch mal hintenangestellt werden und die Industrie sollte in einigen Bereichen den **Mut haben**, im Sinne eines Wettbewerbs, in Vorleistung zu treten.



- Nach den Erfahrungen der Telekom kann das Open Radio Access Network (Open RAN) ein **Model für SDD** sein. Für SDD ist wie bei Open RAN die **Standardisierung von Schnittstellen** sowie die Festlegung von Test-, Zulassungs- und Zertifizierungsbedingungen zentral.

Ergebnisse der Umfrage zur drei exemplarischen Treibern von SDD:



Dialog – die wesentlichen (offenen) Fragen

Wir freuen uns darauf, die besprochenen **Fragen mit Ihnen weiter zu diskutieren** und auf den nächsten Veranstaltungen zu vertiefen:

- Wie kann der Widerstand der Anpassung von Wertschöpfungsketten und die Wandlung von einzelnen **Systemanbietern hin zu Ökosystemen** überwunden werden?
- Wie erreicht dieser **Paradigmenwandel** auch die Politik und plattformzentrierte Rüstungshersteller?
- Wie wird die **Finanzierung von Projekten** im Bereich SDD sichergestellt? Welchen Spielraum wird es dafür in den kommenden Haushalten geben?
- Wie viel **Zeit** haben wir noch bzw. in welchem (juristischen) Rahmen findet die Umsetzung von SDD statt – Frieden, Krieg, hybrid (Stichwort: Verteidigungsfähigkeit)?
- Wie entwickeln wir Prozesse/eine Kultur, die das „Tal des Todes“ bei Innovationen überwinden? Wie kann der **Wettbewerb zwischen etablierten Marktteilnehmern** zum Bereitstellen der besten Lösungen angeregt werden?
- Wie schaffen wir **Vertrauen/Handlungssicherheit** und die richtigen Rahmenbedingungen zwischen Marktteilnehmern und der öffentlichen Hand z.B. bei **Haftungsfragen**? Wie kann die Beschaffungsregulatorik für SDD aktualisiert werden?
- Welche **validen Business Cases** gibt es für die Industrie?
- Wie können **Leuchtturmprojekte** mehr Sichtbarkeit erlangen und weitere Akteure begünstigen Teil der SDD-Entwicklung zu werden?

Blick nach vorn – die nächsten Schritte

Zum Schluss der Veranstaltungen wurden in **drei Working-Sessions** verschiedene Handlungsfelder von SDD einschließlich ihrer Herausforderungen, Best Practices und nächsten Schritte diskutiert.

Konsolidierte Ergebnisse der Working-Sessions:

Aufbrechen von Hardware-zentrierten Ökosystemen	Beschleunigung von Innovationen in die Bw	Lessons Learned aus dem Krieg in der Ukraine
• Anpassung gesetzlicher Vorgaben • Erarbeitung von Business Cases • Mehr Einbindung von Industrie • Nationale Schlüsseltechnologie stärken • Geeignete (IT) Kräfte vorhalten	• Mindset bei Politik und Gesellschaft muss sich ändern • gelebte Fehlerkultur • Vertrauen stärken zwischen Industrie und Bundeswehr • Mehr Handlungssicherheit & Nutzerzentrierung • Schaffung einer gemeinsamen Plattform für Ideenaustausch	• Schnittstellen einheitlich definieren • Ansatz „digitaler Zwilling“ weiter verfolgen • Nutzung des etablierten Entwicklungsframeworks der SW-FactoryBw • Schaffung einer gemeinsamen Experimentalumgebung • Konsolidiertes InfoMgmtSys nutzen

Wir danken allen Teilnehmenden für diese konstruktive und gewinnbringende Veranstaltung und bitten um Fortführung des Dialogs wo immer möglich!



Software Defined Defence (SDD)

Oberst i.G. Michael P. Jäger
Referatsleiter CIT I 3

AFCEA Fachveranstaltung „Software Defined Defence“

Berlin, 18. April 2024

Software Defined Defence

Das Paradigma für zukunftsfähige Streitkräfte

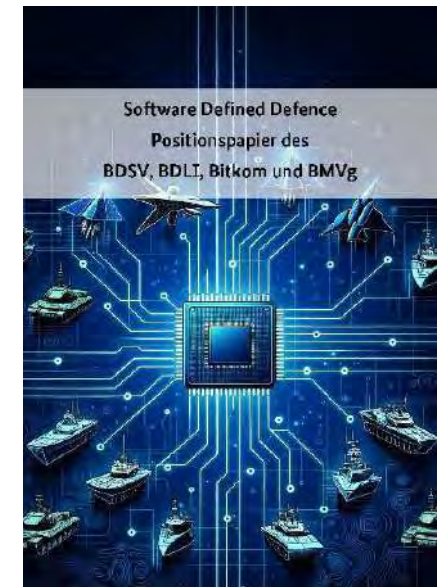
SDD beschreibt die **enormen Potenziale von Software** für stetige Verbesserung bzw. **Erweiterung der Fähigkeiten der Waffensysteme** und damit der **Steigerung der Leistungsfähigkeit der Bundeswehr**

SDD schafft Mehrwert durch:

-  **plattformübergreifende Vernetzung** und Einbinden der hierfür erforderlichen plattformspezifischen Fähigkeiten
-  **schnellere Anpassung** von Software an neue kurzfristig auftretende, einsatzinduzierte Anforderungen
-  Fähigkeitsaufwüchse und **Leistungssteigerungen bestehender Systeme** durch Software

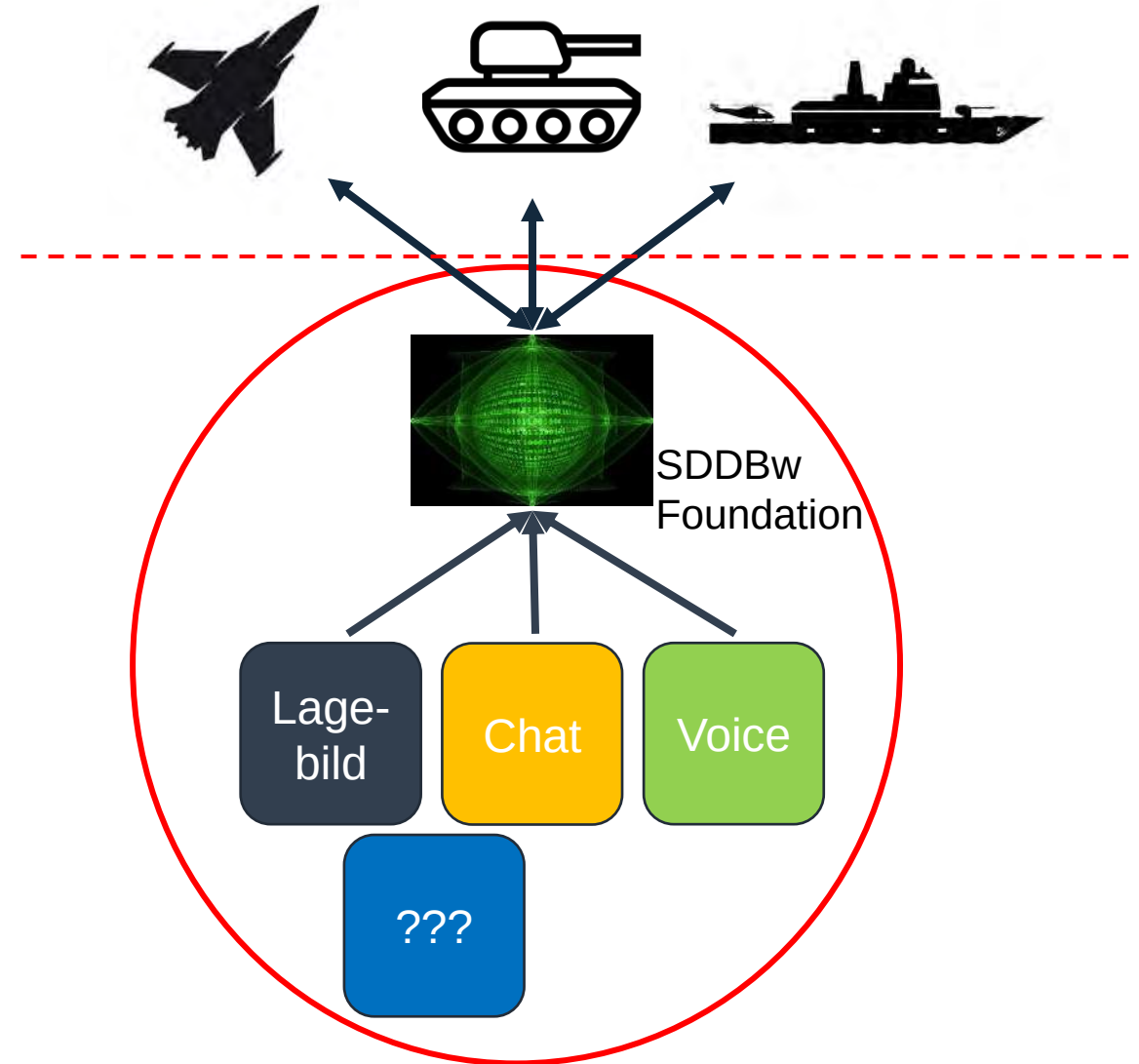
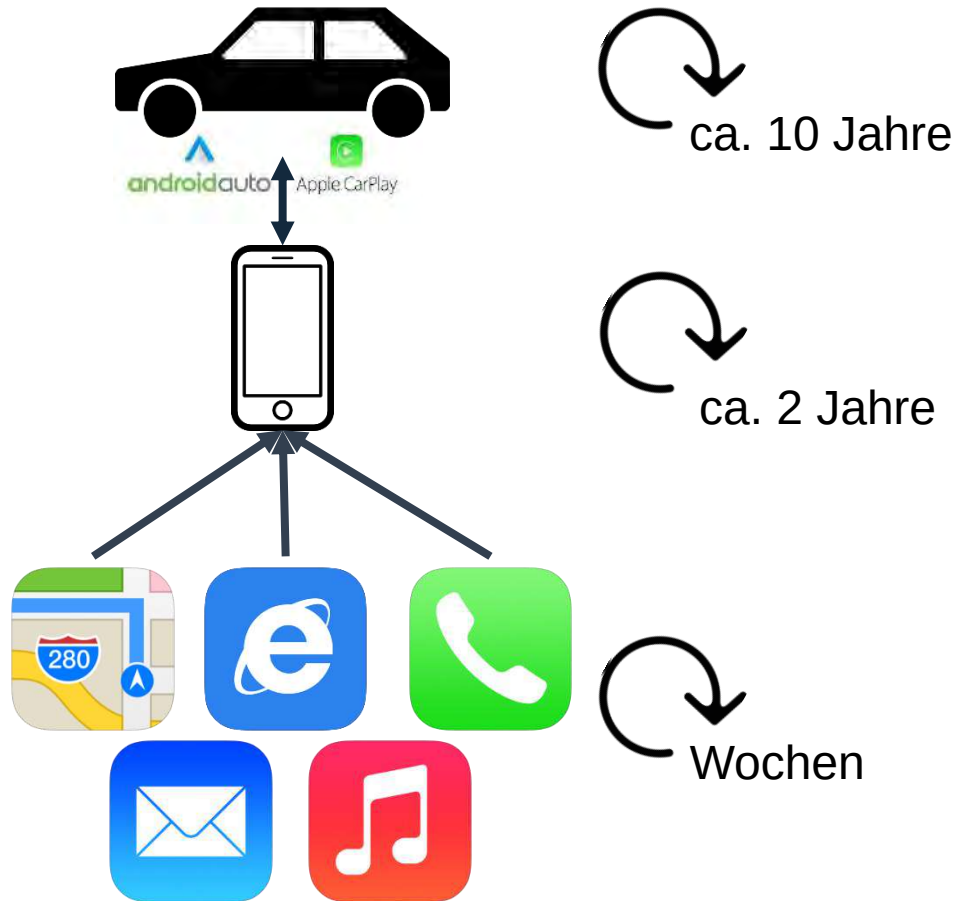
Dabei sind u.a. folgende Aspekte in der Umsetzung zentral:

- Aufbau eines offenen modularen Systems mit definierten Schnittstellen i.S. eines Digitalisierungs-Ökosystems
- Beschleunigung von (Software-) Entwicklungs- und Bereitstellungsprozessen in der Bw und Industrie
- Umdenken bei Planungs- und Rüstungsprozessen sowohl bei öAG und Industrie (inkl. Vergabeverfahren)



Software Defined Defence – Ziel Architektur

Innovationszyklen



Ebenenmodell der (technischen) Interoperabilität

Ebene

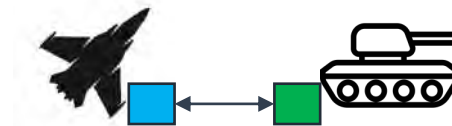
0

Keine Interoperabilität



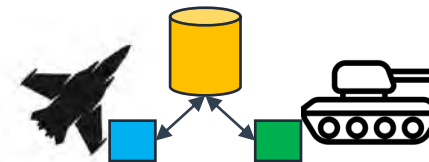
1

System zu System



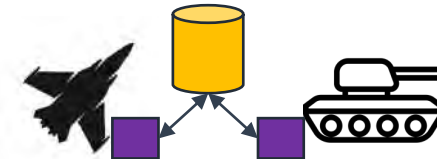
2

Gemeinsame Datenbasis



3

Gemeinsame Code-Basis (→
Microservices)



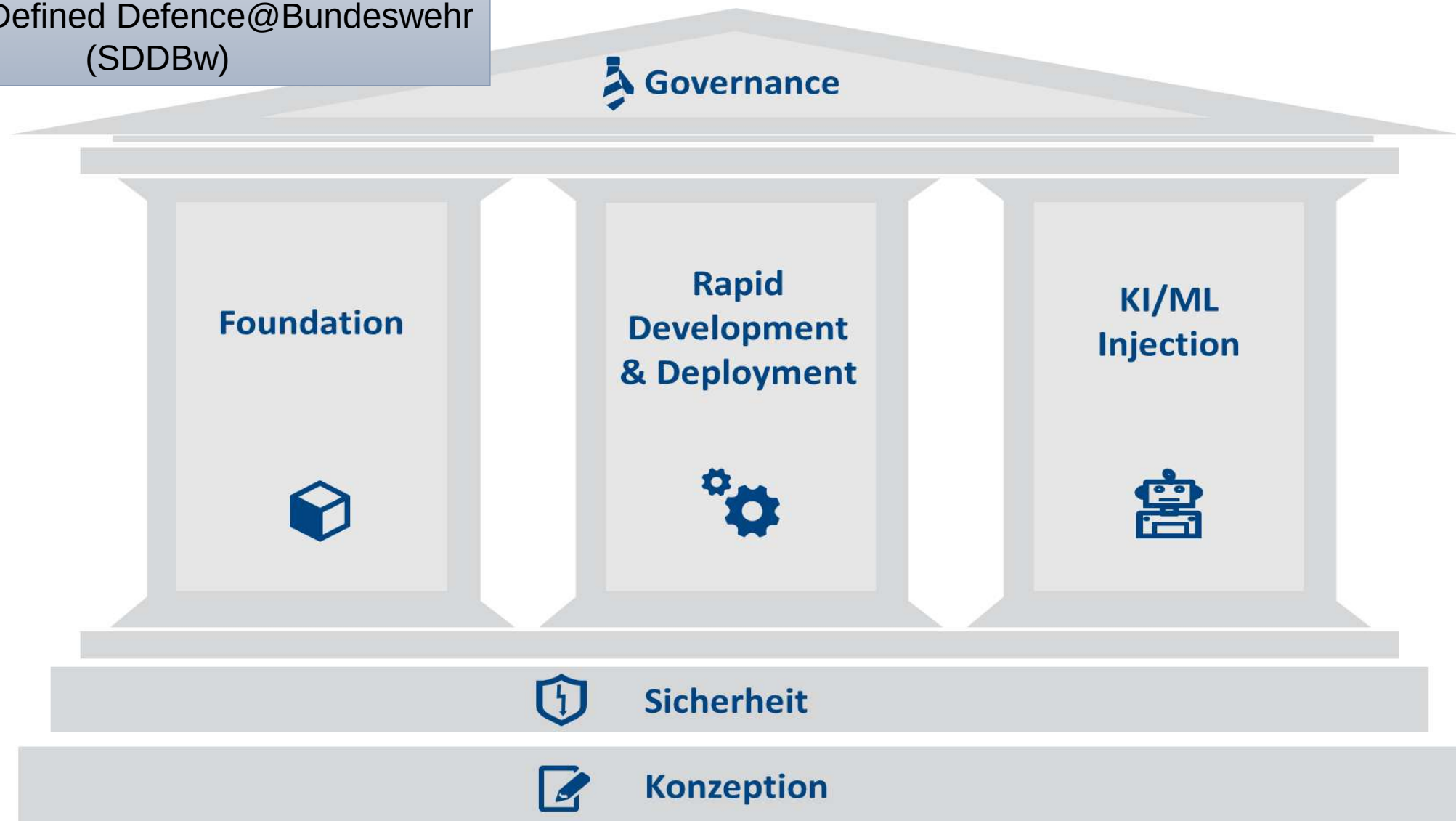
Entkopplung der Hardware von den Fähigkeiten eines Waffensystems

- missionsspezifische Applikationen für **Informationsüberlegenheit**
- kürzere **Innovationszyklen** (Monate statt Jahre)
- reduzierte **Kosten** für Upgrades
- **Information Sharing** für alle Teilnehmer im Netz
- **Kompensation** einer geringeren Verfügbarkeit von Plattformen

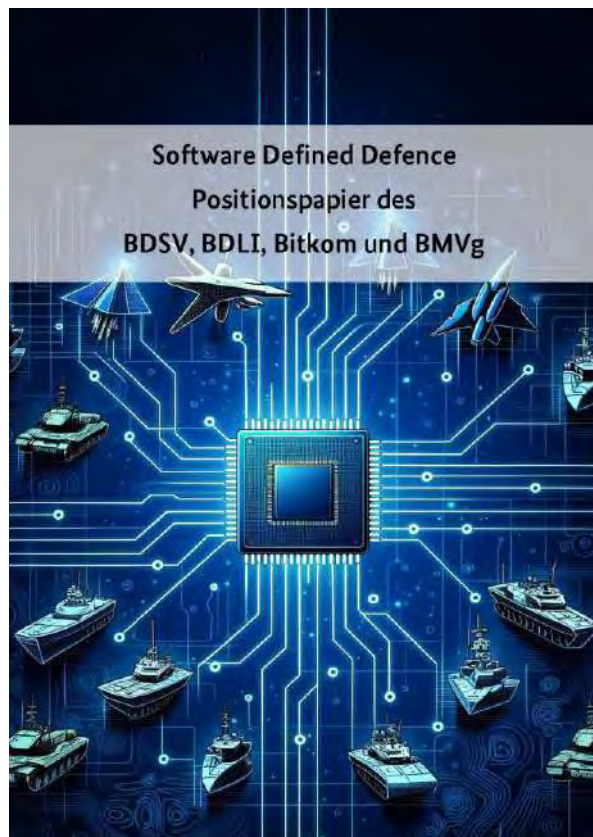


Gesamtbild Umsetzung Software Defined Defence

Software Defined Defence@Bundeswehr
(SDDbW)

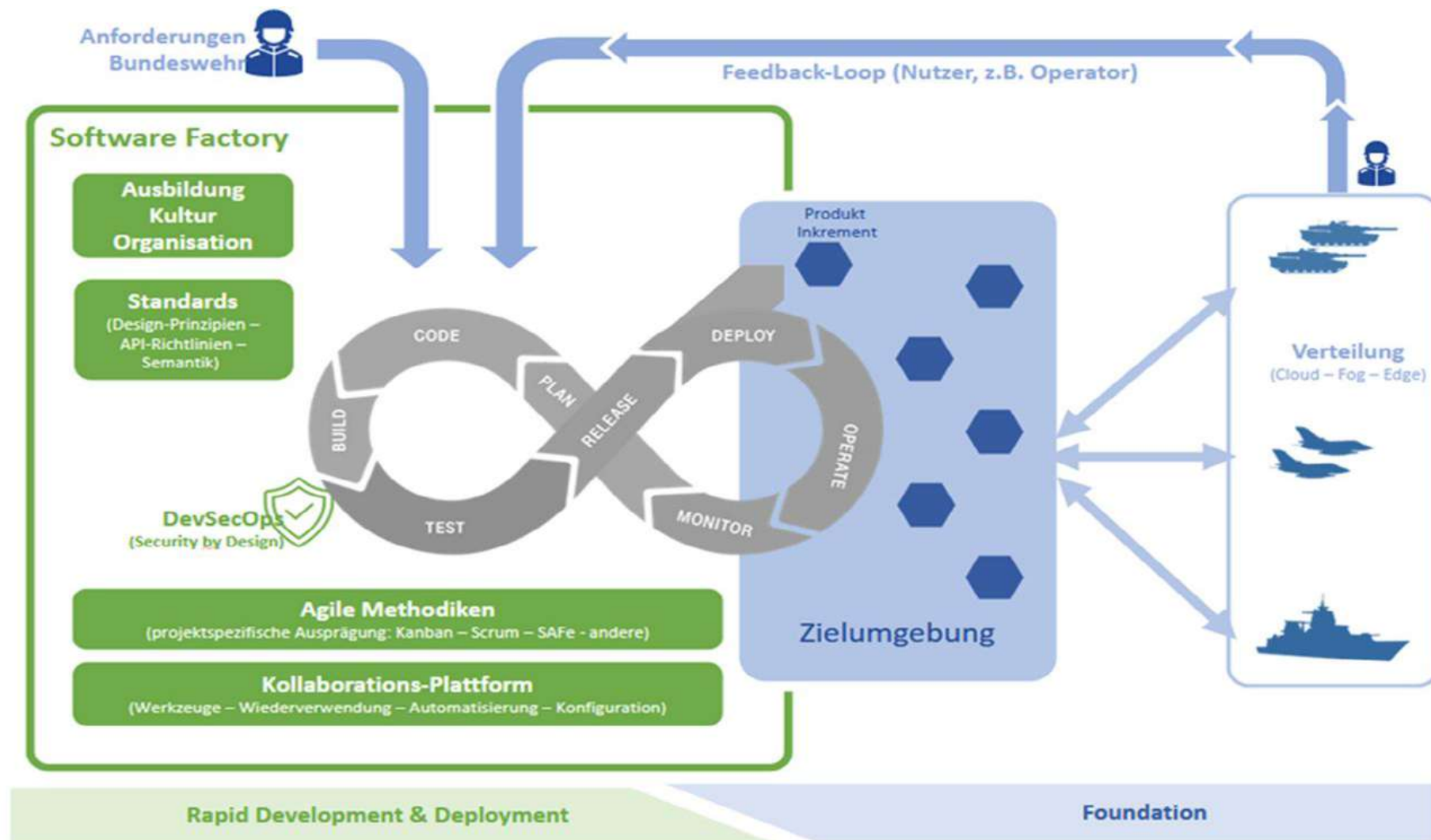


Veröffentlichung gemeinsames Positionspapier





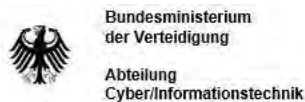
SDD - Software Factory Bw





Plattform42

Software
Engineering
Ecosystem für eine
grenzenlose
Kooperation





SDD – Foundation



Stationär



Verlegefähig



Mobil



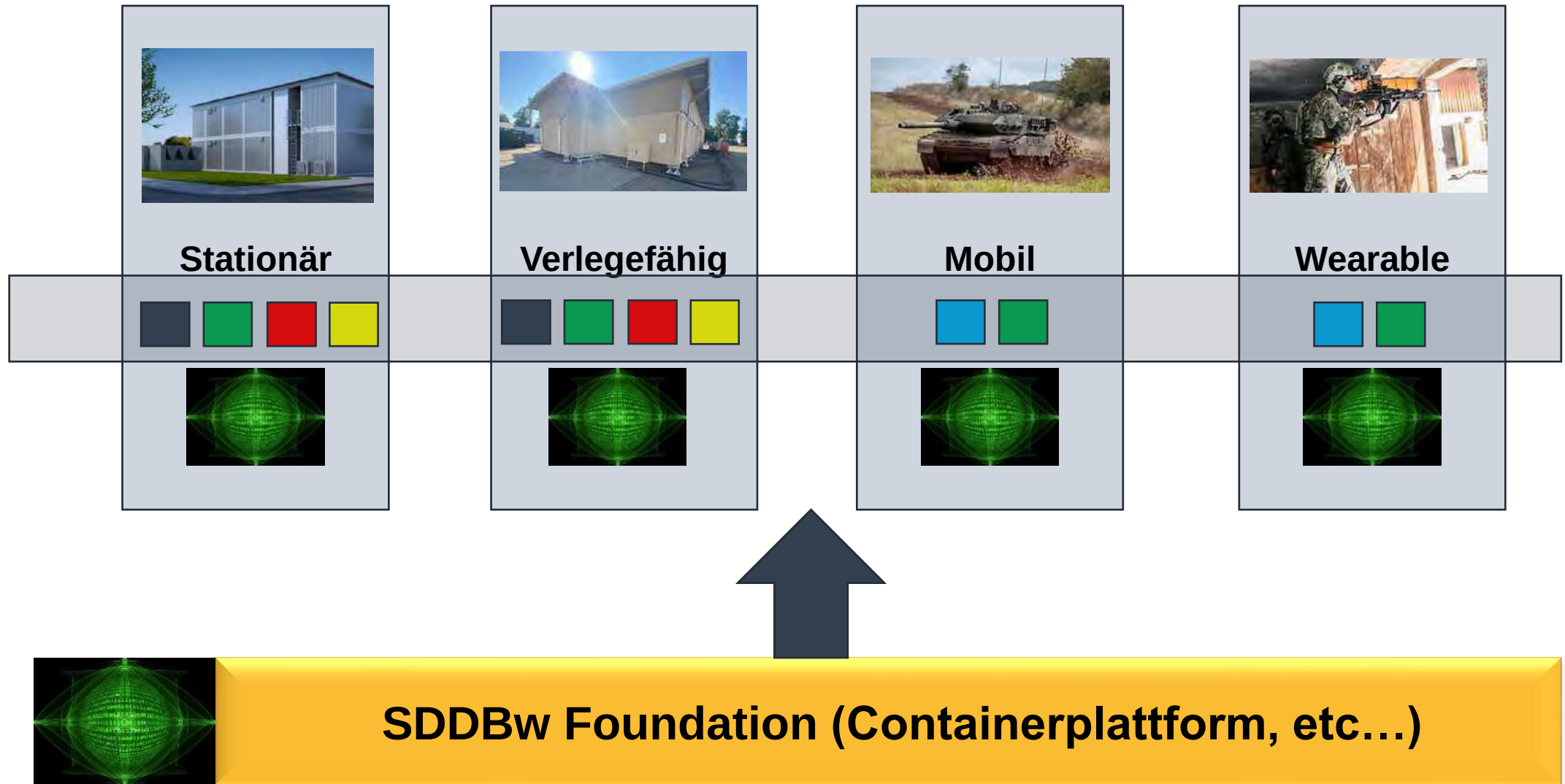
Wearable



SDDBw Foundation (Containerplattform, etc...)



SDD – Einheitliche IT-Services/Applikationen

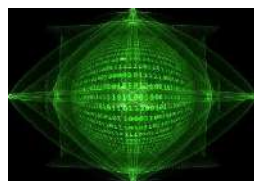
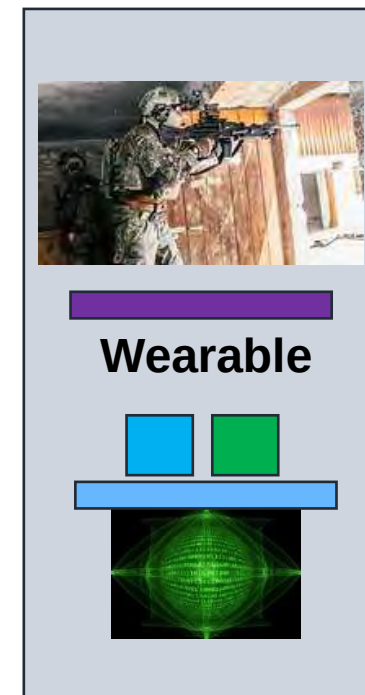
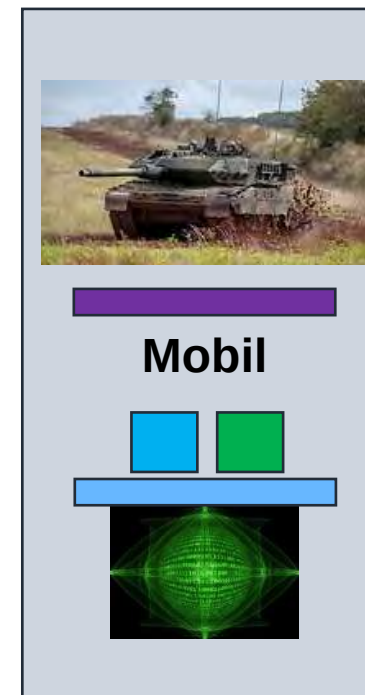
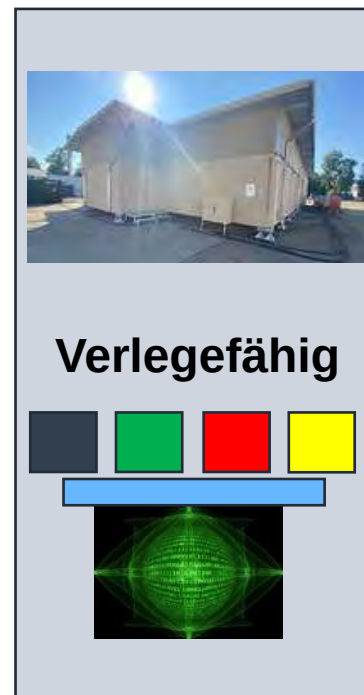
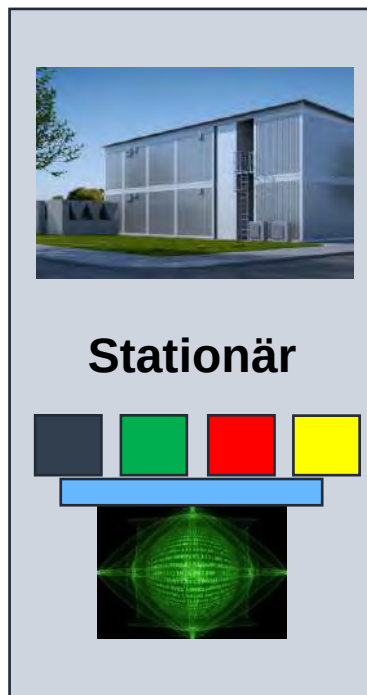


SDD – Einheitliche APIs

Cross Application API



Sensor/Effector API



SDDBw Foundation (Containerplattform, etc...)

GK 4 / EK 1

Strategischer Industriedialog

Rapid Development & Deployment	KI (Methoden)	Foundation	InfoSec	Legal
Konzept „Etablierung Software Factory“ erstellt.	Konzept „Aspekte zur Entwicklung sicherer KI Modelle“ erstellt.	Eckpunkte für eine Foundation definiert & mögliche Standards identifiziert.	SWOT-Analyse durchgeführt. Untersuchung zur Absicherung Lieferkette durchgeführt.	Untersuchung zu Rechtesituation bei SDD (IPR, Nutzungsrechte, Rechte an Daten) Untersuchung zu Finanzaspekten

Software Defined Defence – Weiteres Vorgehen

Aktivitäten GB BMVg

Umsetzen in Bw-interne Konzeption

04/2023 – 06/2024

Prototyp Software Factory

Use Case / Demonstration
DevSecOps Cycle

Prototyp Foundation



BDSV



bitkom

BOLI

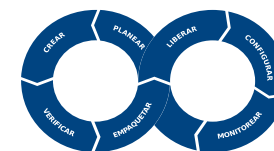
Gemeinsame Aktivitäten im GK4



Nachweis Legacy Systemen

Standardisierung von Sensor/Effektor APIs

Best Practices SDD Entwicklung



Fortführung auf Ebene GK 4



FRAGEN?

Oberst i.G. Michael P. Jäger
Referatsleiter CIT I 3

Software Defined Defence als Voraussetzung für dimensionsübergreifende Führungsfähigkeit

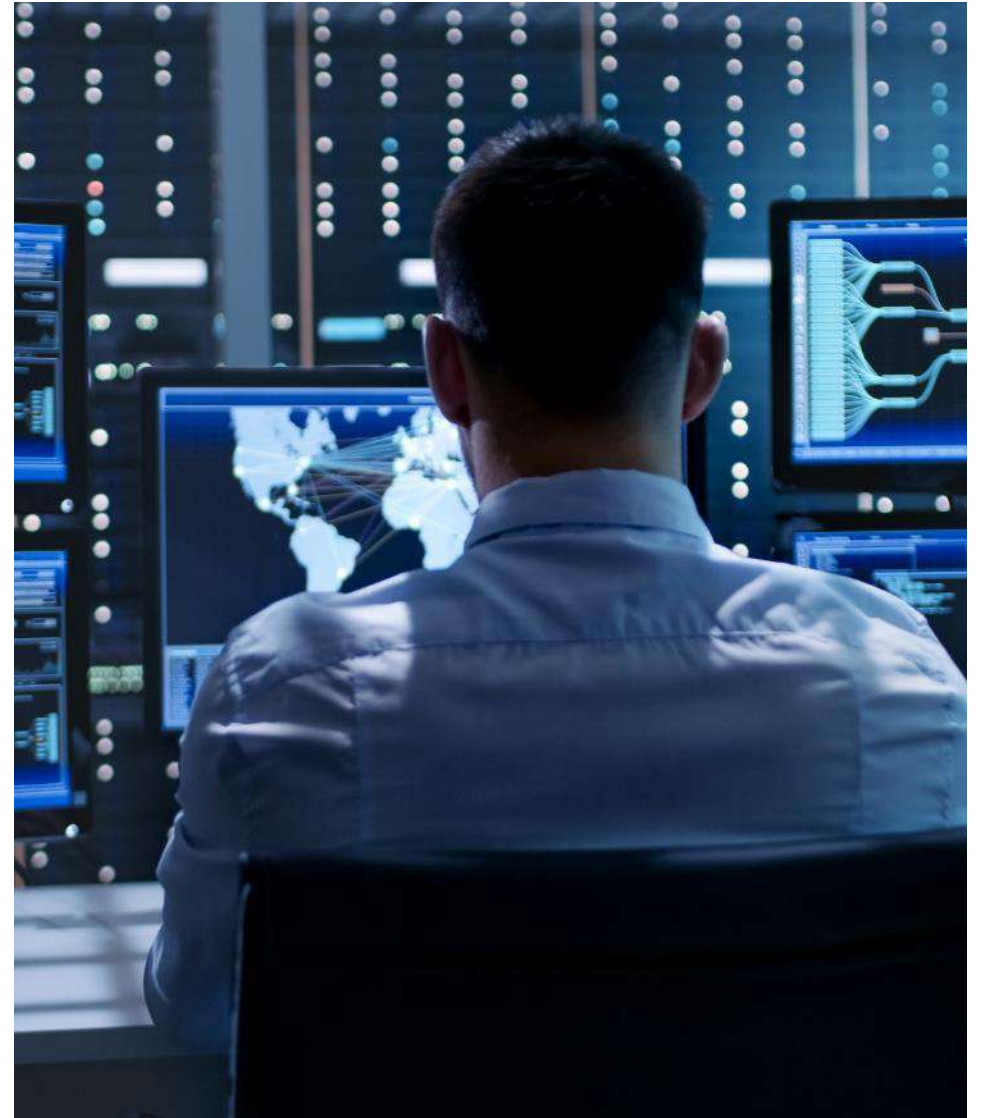
Eine Industrieperspektive

Jens Elstermeier
18. April 2024



Paradigma

SDD ist die Voraussetzung, um zukünftig schnell genug auf veränderte Umgebungsbedingungen reagieren zu können, um so siegfähig zu bleiben.



Voraussetzungen für Software Defined Defence

Führungssystem

- InfoSec
- Life Cycle Management
- Liability
- Akkreditierung
- Contracting
- API-Management

Kommunikationssystem

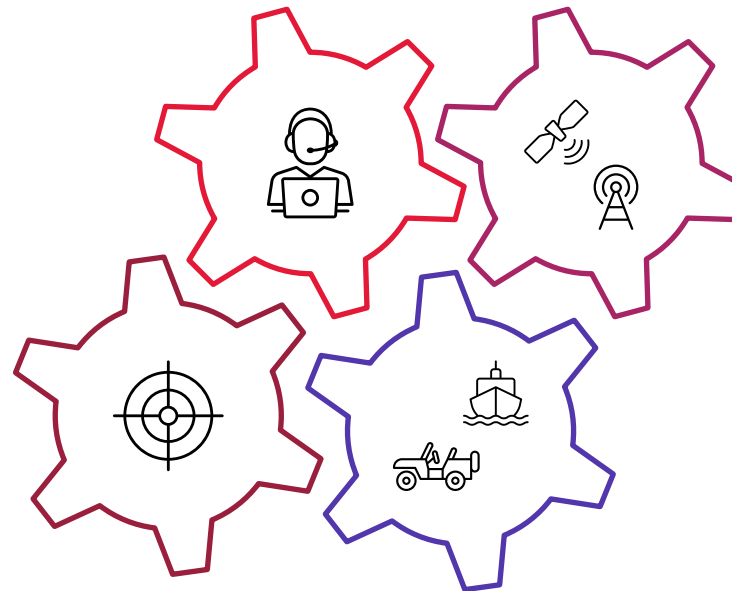
- InfoSec
- Life Cycle Management
- Liability
- Akkreditierung
- Contracting
- API-Management

Waffensystem

- InfoSec
- Life Cycle Management
- Liability
- Akkreditierung
- Contracting
- API-Management

Fahrzeug-/technik

- InfoSec
- Life Cycle Management
- Liability
- Akkreditierung
- Contracting
- API-Management



Voraussetzungen für Software Defined Defence

Führungssystem

- InfoSec
- Life Cycle Management
- Liability
- Akkreditierung
- Contracting
- API-Management

Kommunikationssystem

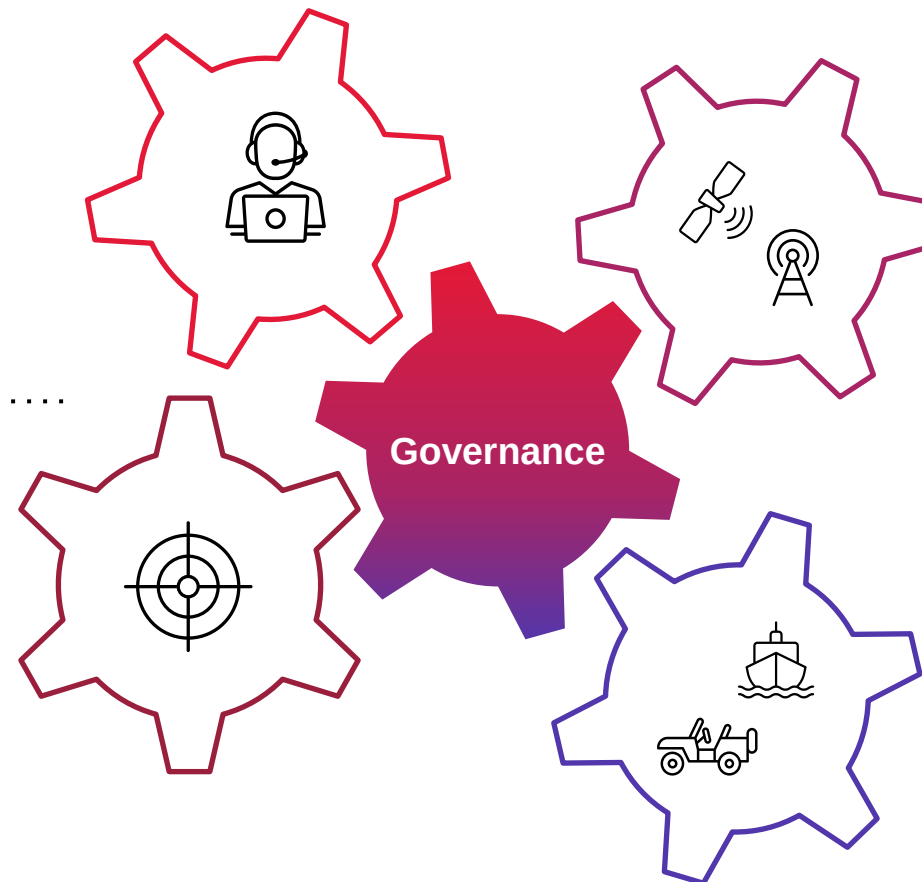
- InfoSec
- Life Cycle Management
- Liability
- Akkreditierung
- Contracting
- API-Management

Waffensystem

- InfoSec
- Life Cycle Management
- Liability
- Akkreditierung
- Contracting
- API-Management

Fahrzeug-/technik

- InfoSec
- Life Cycle Management
- Liability
- Akkreditierung
- Contracting
- API-Management



Zusammenfassung

Dimensionsübergreifende Führungsfähigkeit

- Führungs- & Kommunikationssysteme zentral bereitstellen
- Denken über alle Systembestandteile hinweg, vom stationären Rechenzentrum über verlegefähige Hauptquartiere, Landfahrzeuge oder seegehende Einheiten bis zum mobilen Endgerät

erstes Ziel von SDD: schnelle (agile) Reaktion auf veränderte Rahmenbedingungen

- Auswirkungen auf das gesamte Ökosystem:
 - SDD ist damit ein Organisationsprojekt und nicht nur ein IT-Projekt
 - Ohne einen organisatorischen Umbau lässt sich eine agile Entwicklung, ein agiler Betrieb nicht umsetzen



Jens Elstermeier

Senior Vice President Consulting Services
Head of Business Development & Strategy

Mobile: +49-175-9387558

Mail: jens.elstermeier@cgi.com



Über CGI

Wir sind ein globales Dienstleistungsunternehmen für IT- und Geschäftsprozesse und wurden 1976 gegründet. Heute sind wir an 400 Standorten in 40 Ländern vertreten. Unsere flexiblen End-to-End-Services umfassen strategische IT- und Business-Beratung, Systemintegration, Managed IT und Intellectual Property auf Top-Niveau. Wir unterstützen unsere Kunden bei der Transformation ihres Unternehmens zu einer agilen Organisation und setzen unsere IP-Lösungen dafür ein, Innovation zu beschleunigen. Durch intelligente Systemintegration treiben wir die IT-Modernisierung unserer Kunden voran; mit unseren Managed IT Services und Geschäftsprozess-Dienstleistungen helfen wir ihnen, den Kostendruck zu mindern und ihre Technologie-Lieferketten optimal einzusetzen.

cgi.com/de/defence →

Die Zukunft von Software Defined Defense (SDD) in Deutschland

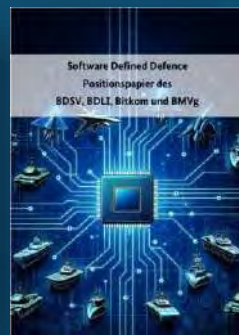
Unsicherheiten, Treiber und Szenarien

Software Defined Defense ist zentrale Befähigungskraft moderner Streitkräfte – und Unsicherheitsfaktor in Deutschland

Zur Relevanz von SDD herrscht zurzeit großer Konsens...

Die Ausgestaltung von SDD in Deutschland bleibt unsicher!

2022



Heute

1

SDD-Vorreiter

2

SDD-Nachzügler

3

SDD-Abgehängte

Wie begegnen wir dieser Unsicherheit von Software Defined Defense in Deutschland?

Zusammen zeichnen wir das Bild und gestalten die Zukunft von Software Defined Defense in Deutschland

Bildquelle: generiert mit Image Creator/Microsoft Designer

Bildquelle: Libkos, AP: <https://www.theatlantic.com/photo/2023/05/photos-ukraine-war-drones/674160/>

Vision und Praxis

Bildquelle: generiert mit Image Creator/Microsoft Designer

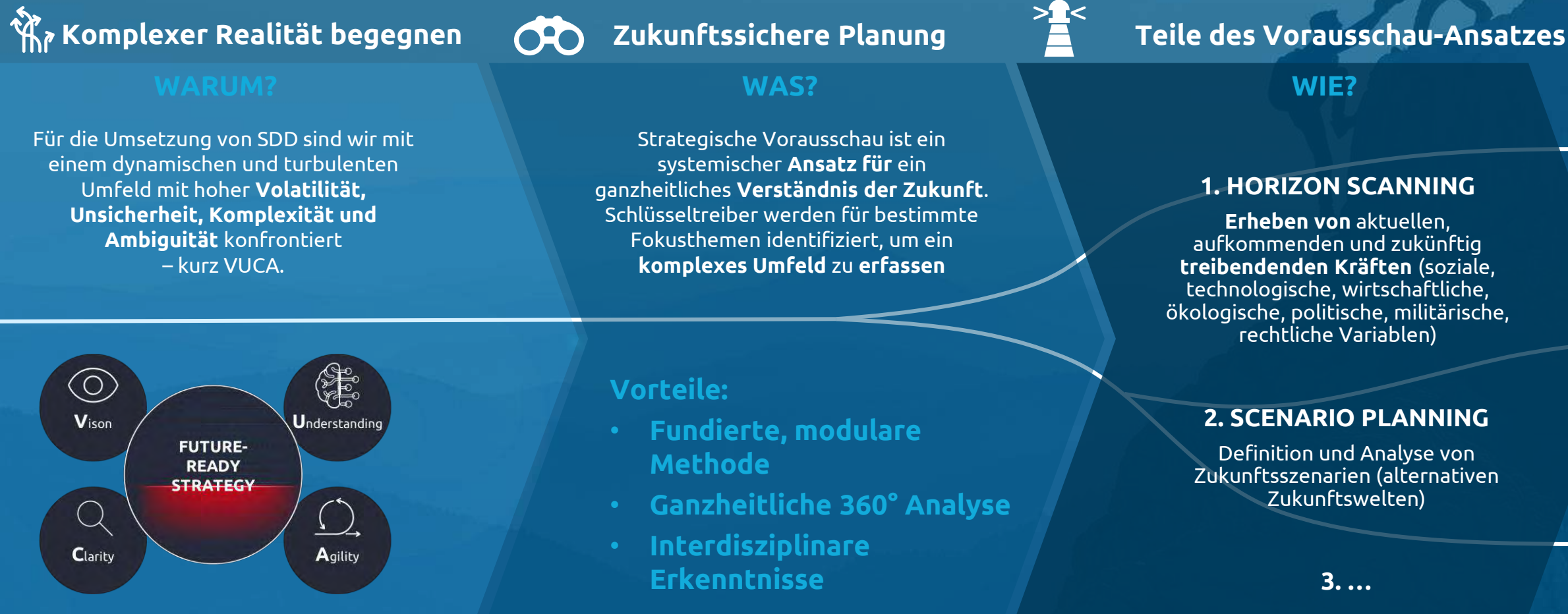
Bildquelle: Lysenko: <https://www.welt.de/politik/ausland/plus250806214/Ukraine-Krieg-Wo-Kiews-Truppen-den-russischen-Durchbruch-verhindern.html>

Umsetzung von SDD – so viel Vision wie nötig, so viel Praxis wie möglich!

Bildquelle: Jason Rose, The Future of Defense: Embracing Software Defined Warfare: <https://www.linkedin.com/pulse/>

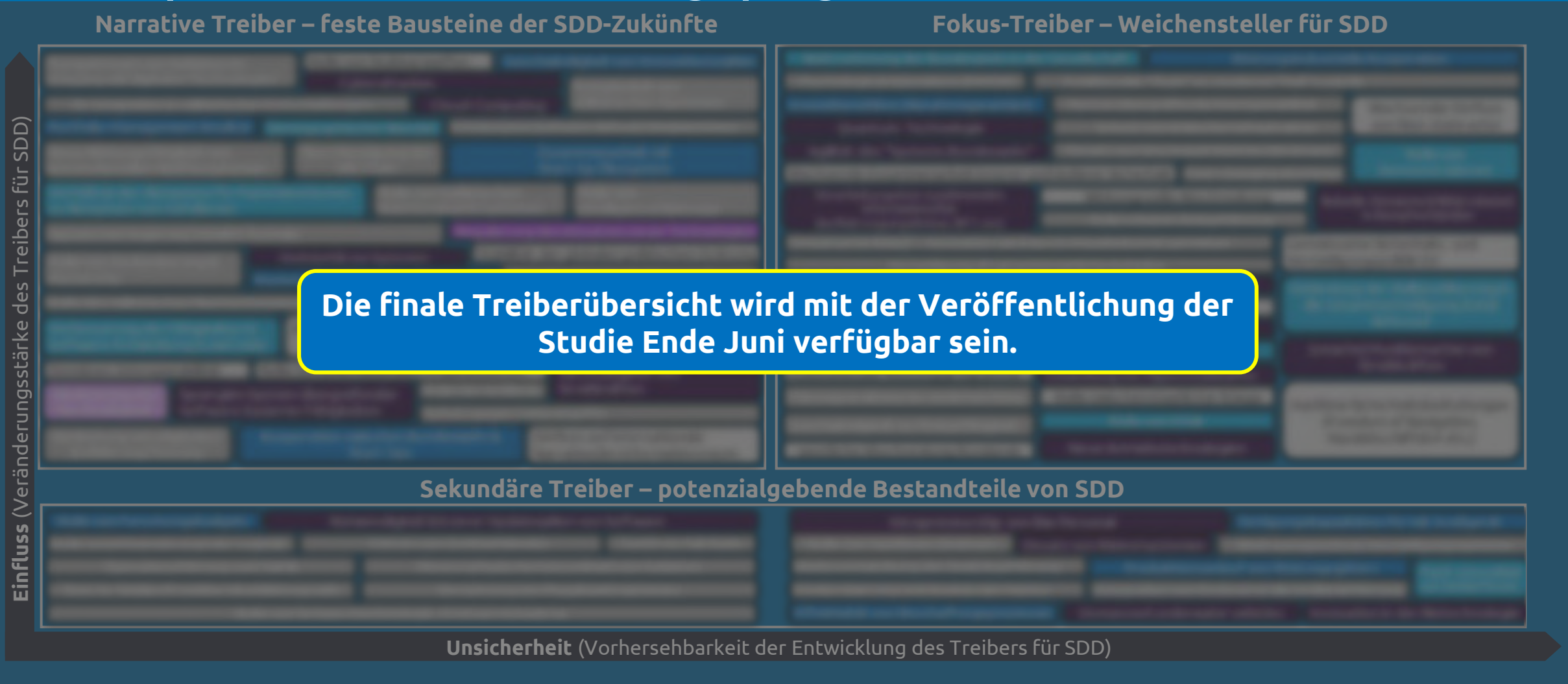
Bildquelle: Sergei Svoinsky, AFP: <https://www.theatlantic.com/photo/2023/05/photos-ukraine-war-drones/674160/>

Mit dem Ansatz zur Strategischen Vorausschau können wir die Unsicherheiten der Umsetzung von SDD adressieren



Strategische Vorausschau hilft uns, eine positive Zukunft von SDD zu unterstützen

Die Zukunft von Software Defined Defense ist von einer Vielzahl an komplexen Einflusskräften geprägt



Drei Treiber zeigen uns exemplarisch den Weg für eine Umsetzung von SDD

Drei Treiber stehen exemplarisch für die Umsetzung von Software Defined Defense in Deutschland



Welchen Blickwinkel nehmen wir auf diese exemplarischen SDD-Treiber/Szenarien ein?

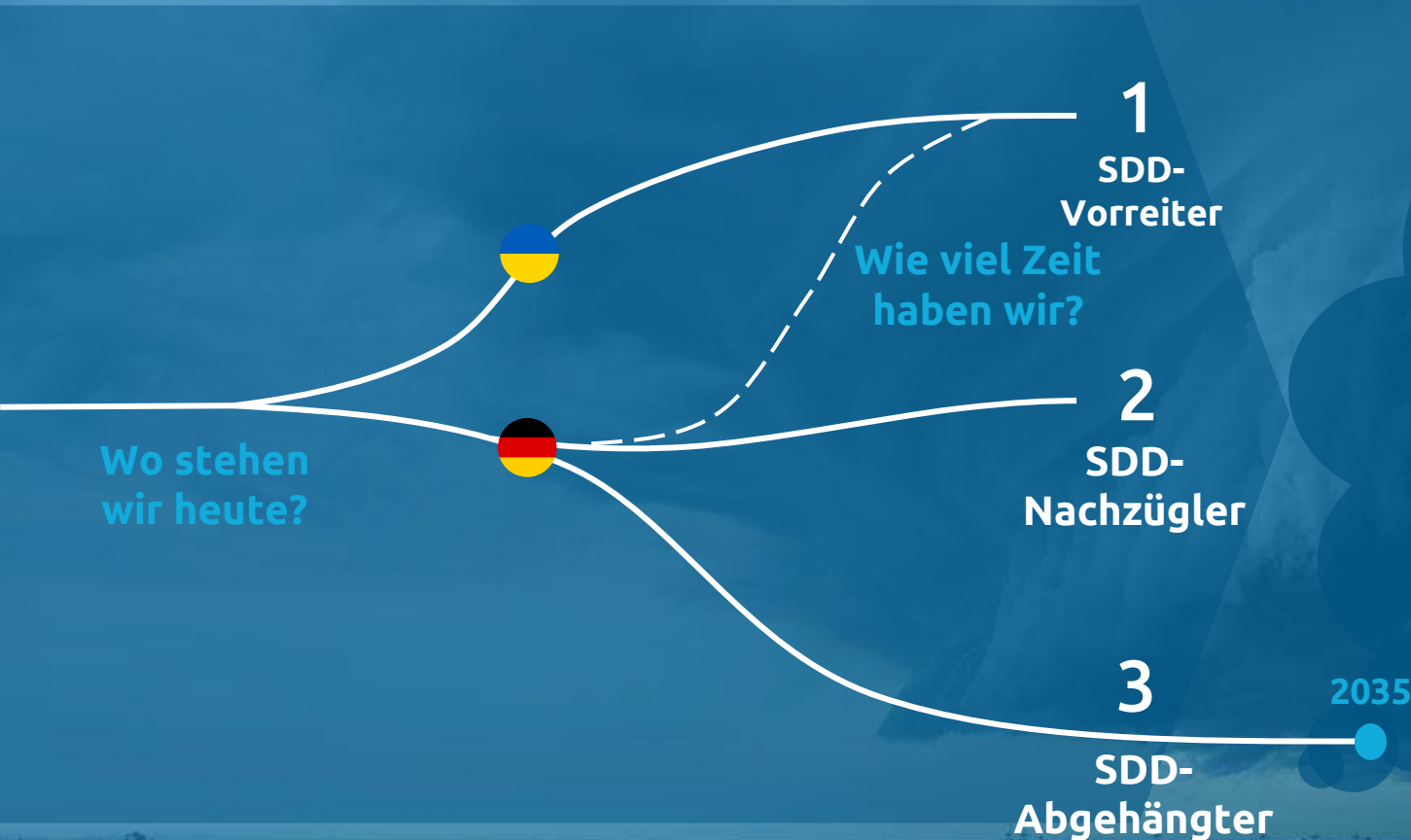
Deutschland auf dem Pfad zum SDD-Abgehängten – Es gilt, das Steuer herumzureißen!



Die SDD-Fähigkeitslücke zu Partnernationen wächst



Deutschland als SDD-Abgehängter



In Deutschland ...



... wurde ein software-zentrierter Ansatz und die technologische Entwicklung vernachlässigt



... wurde eine prägende technologische Rolle innerhalb der EU und NATO nicht wahrgenommen



... herrscht eine unsichere Zeit, die von wachsenden Spannungen und globalen Konflikten geprägt ist



... herrscht eine weiter wachsende Unzufriedenheit zur Digitalisierung der Bundeswehr

Um das Steuer herumzureißen, müssen wir Handlungsfelder zu den zentralen SDD-Treibern identifizieren

Zusammen gestalten wir die Zukunft von Software Defined Defense in Deutschland



Marc Akkermann | Vice President
Head of Public Defense Germany
+49 (0) 151 40250630
marc.akkermann@capgemini.com



Juri Denecke
Senior Manager
+49 (0) 151 29281452
juri.denecke@capgemini.com



Nemo Buschmann
Consultant
+49 (0) 151 40251882
nemo.buschmann@capgemini.com

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of nearly 350,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2022 global revenues of €22 billion.

Get The Future You Want | www.capgemini.com



This presentation contains information that may be privileged or confidential and is the property of the Capgemini Group.

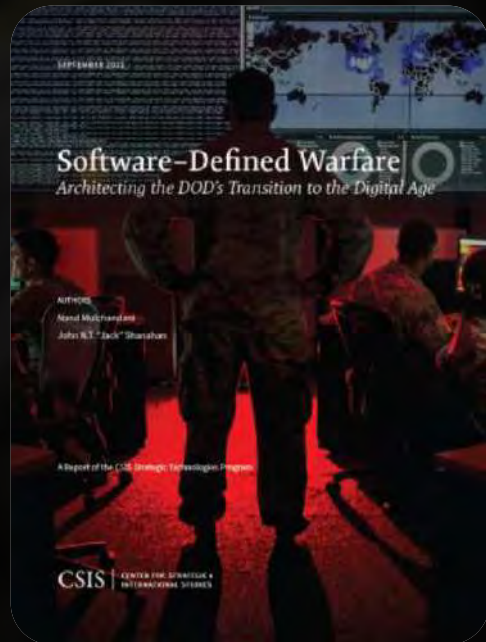
Copyright 2024 Capgemini. © All rights reserved.

SOFTWARE DEFINED DEFENCE

hardware has always been king and software largely an afterthought

HAUPTBEZUGSDOKUMENTE

09637
1000V
4710N
hubbw



Software-defined Defence: Algorithms at War

Dr Simona R. Soare, Pavneet Singh and Meia Nouwens

February 2023



IISS
The International Institute
for Strategic Studies



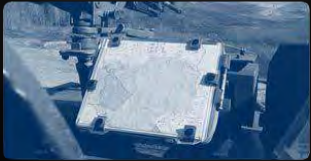
SOFTWARE DEFINED DEFENCE

Positionspapier Seminar HEER LGAN 2022
Oktober 2023



BUNDESWEHR

SCHRITTE DER DIGITALEN TRANSFORMATION



Analoge Welt

Größtenteils heutiger
Zustand im Militär und in
der Rüstung



Digitization

Überführung analoger
Informationen in digitale
Daten und Medien



Digitalisierung

Vernetzung, Nutzung
und Austausch von
Daten und Systemen



Digitale Transformation

Software Defined Defence -
Datenzentrierte Auslegung von
Systemen

DEFINITION LGAN 2023



Software Defined Defence (SDD) bezeichnet ein zentrales Leitprinzip für die Streitkräfteentwicklung der Zukunft. Durch KI-unterstützte, softwaredominierte und dimensionsübergreifende Systeme werden **Fähigkeitszuwächse primär** über die Änderung der **Software** und nicht, wie bisher, überwiegend über die Weiterentwicklung der Hardware erzielt. Auf Basis einer **datenzentrierten, anschlussfähigen Architektur** wird Software zum Träger militärischer Fähigkeiten aufwachsen. Durch die weitreichenden Potentiale der Software werden **Analyse-/Planungs- und Entscheidungsprozesse optimiert** und so Wirkungsüberlegenheit auch auf dem Gefechtsfeld der Zukunft erzielt.

DEFINITION IISS 2023



Software-defined defence is considered to be a fundamental architectural, organisational and operational principle of modern military operations. Software-defined defence entails a new logic for capability development which disaggregates sensors from effectors, software from hardware, and data from specific applications, while connecting them in data-centric, multi-modal, multi-domain, adaptative battle networks;

DEFINITION CIT



„Software Defined Defence (SDD) ist ein zentrales Leitprinzip für die Streitkräfteentwicklung der Zukunft. Im Kern hat SDD das Ziel, die enormen Potenziale von Software und damit ihrer Entwicklung und Integration zur Verbesserung der Fähigkeiten von Führungs-, Einsatz- und Waffensystemen systematisch zu nutzen.“

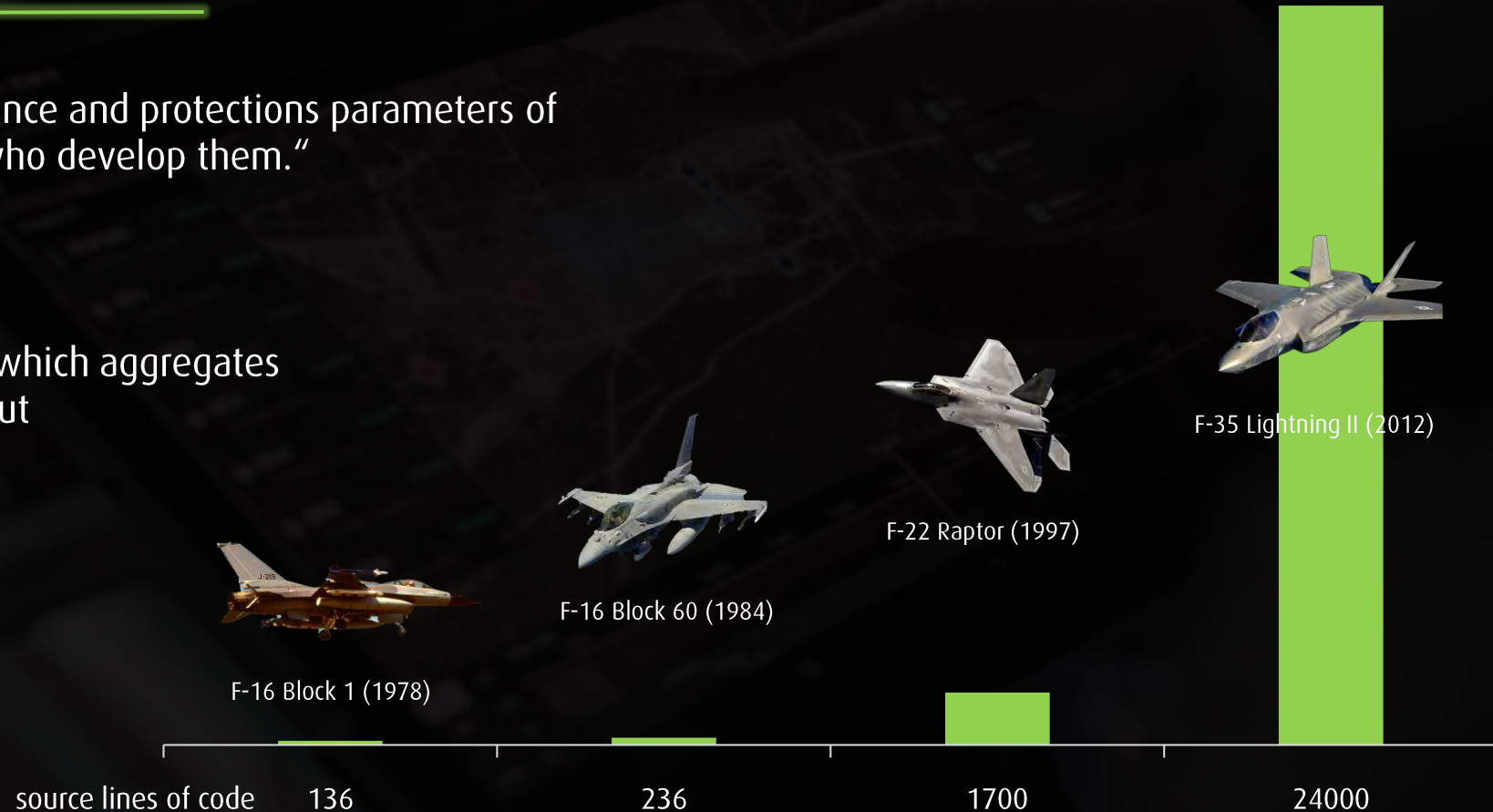
BEDEUTUNG VON SOFTWARE FÜR HARDWARE



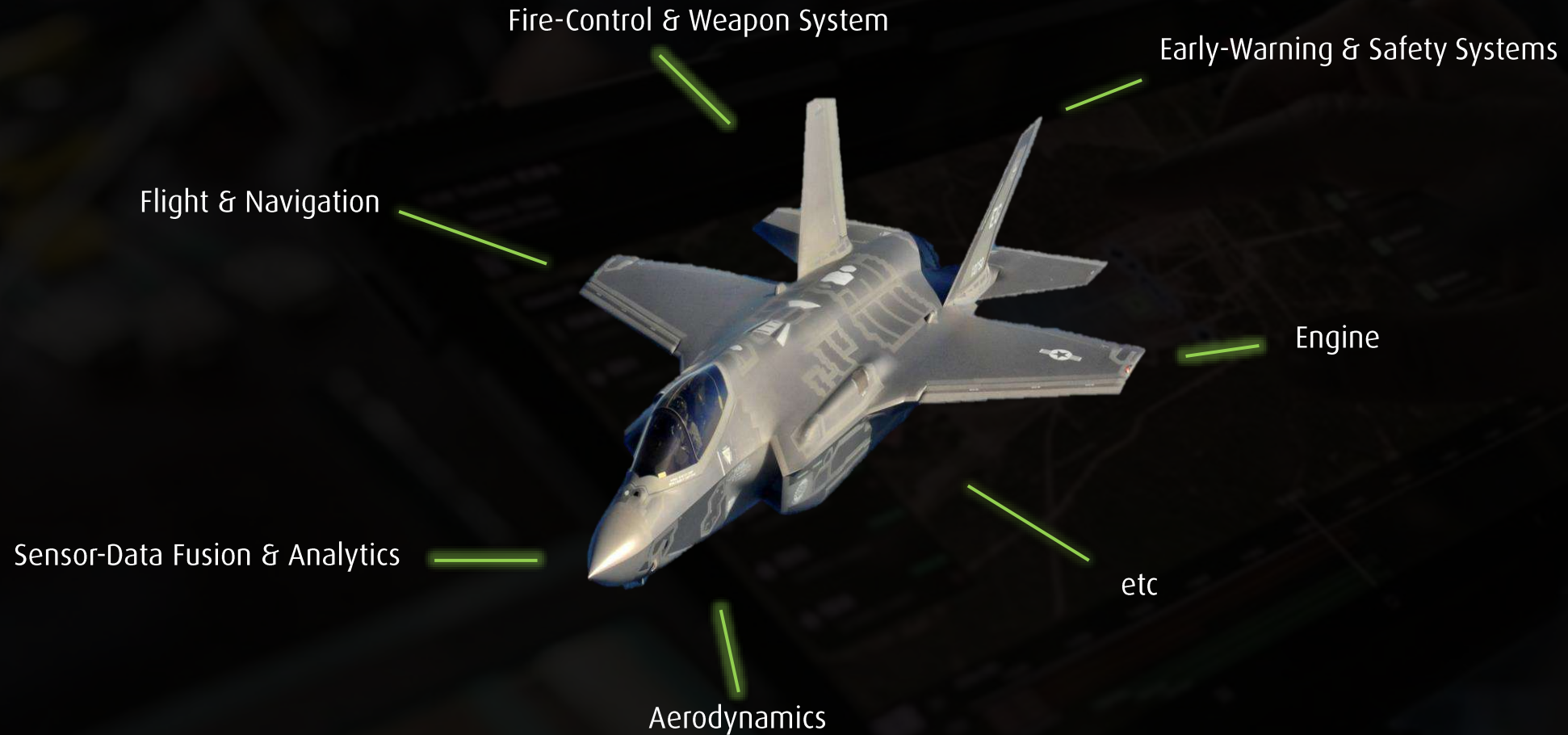
„The rate of technology progress in software and (software related hardware) is superior to technological breakthroughs in conventional military hardware“

„[...] software defines the function, performance and protections parameters of military capabilities alongside the humans who develop them.“

„reliance on conventional military hardware which aggregates sensors and effectors [...] is untenable without reorientation towards SSD.“



FÄHIGKEITSBEITRAG SOFTWARE > 80 %



DATENVERARBEITUNGSKAPAZITÄTEN



CSO 2, FR



1000 Bilder/ Tag



95 % loss*

Human Capacity



AI/ML Algorithmen

- Datenzentrierte Architektur
- Datenmanagementsysteme
- Data Fabrics



MQ-1 Predator, US



14h Video /Mission



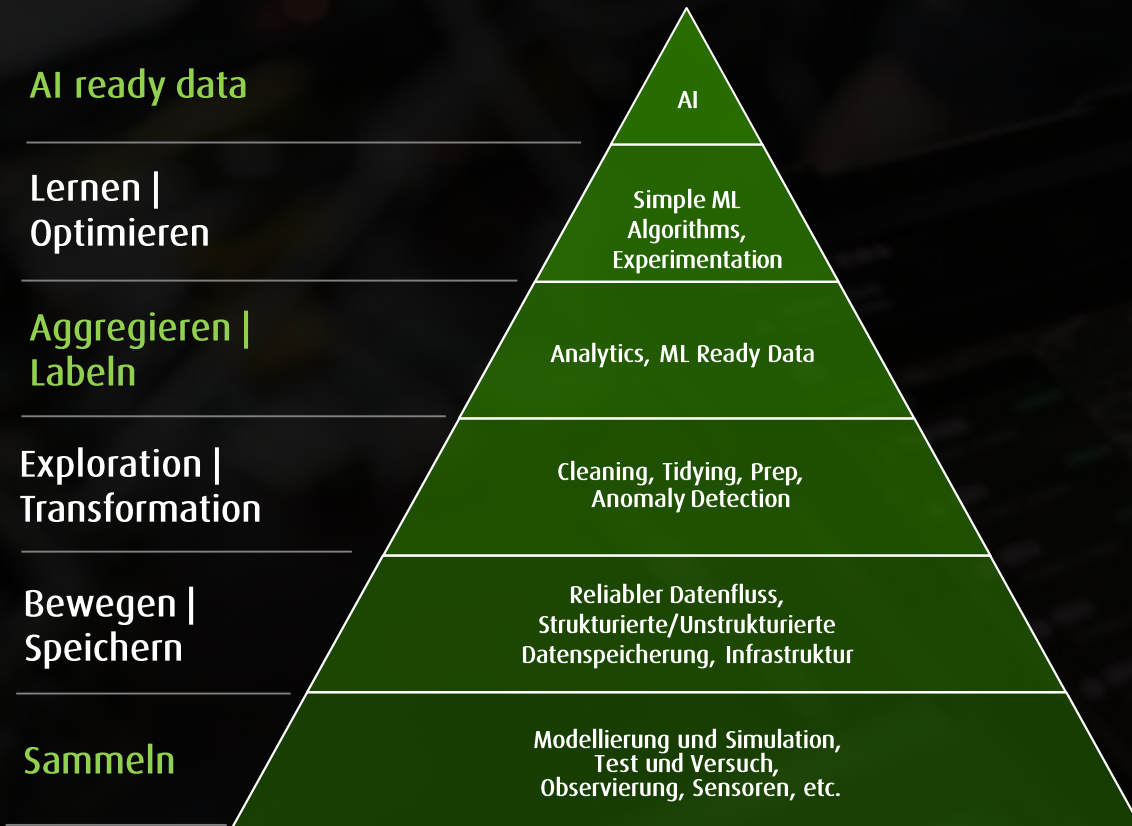
99 % loss*



Sensoren als stärkste wachsende
Position in Verteidigungshaushalten

„The more software deployed in defence capabilities, the more defence data it generates. The human capacity to process the exponentially growing volume of data collected by battlefield sensors has already been reached.“

DATENZENTRIERTE ARCHITEKTUREN



Aktuelle Herausforderungen

- Von Datensilos zu Multi-Domain DataMgmtSystemen
- Entkopplung der Daten von Systemen/Applikationen
- Bereitstellung von Data Lakes (insb Trainingsdaten)
- Rollout relevanter Infrastruktur (Cloud und Edge Computing)
- Schaffung von Software Factories
- Konsolidierung des Datenrechts

„In a nutshell, in software-defined defence, military networks are built to accomodate the flexible real-time sharing and exploitation of data across domains rather than data flows having to accomodate hardware protocols [...]. Enabling military battle networks not just to dynamically share information with each other but to use algorithms that can fuse and process all formats of available data is a fundamental quality and functionality differentiator for SDD.“

NUTZERZENTRIERTES DESIGN END-2-END



MQ-9 Reaper: over 100 operational and logistics staff for one military capability



NGWS: one human controls several military capabilities simultaneously



... by design

Nutzerzentrierung
ethische Abwägungen
rechtlicher Rahmen

„Software defined weapon architectures may enable end-to-end electronic workflows which override the need for manual human controls of individual weapon systems, but humans continue to define the requirements and mission goals for the performance and employments of such capabilities on and off the battlefield, and human factors remain a critical consideration for the development of advanced algorithms for defence applications.“

MODULARES WAFFEN-UND NETZWERKDESIGN



IST Systemlandschaft Bw



System 1



System 2



System 3



System 4

Eigenschaften SOLL-System

- normierte Zwischenebene (Middleware)
- standardisierte Schnittstellen
- wiederverwendbare Softwaremodule
- individuelle Fähigkeiten einfügen/entfernen in Echtzeit
- Softwareupdates simultan und in Echtzeit
- kein Austausch zugrundeliegender IT-Infrastruktur
- keine Einschränkung in Performance oder Funktionalität

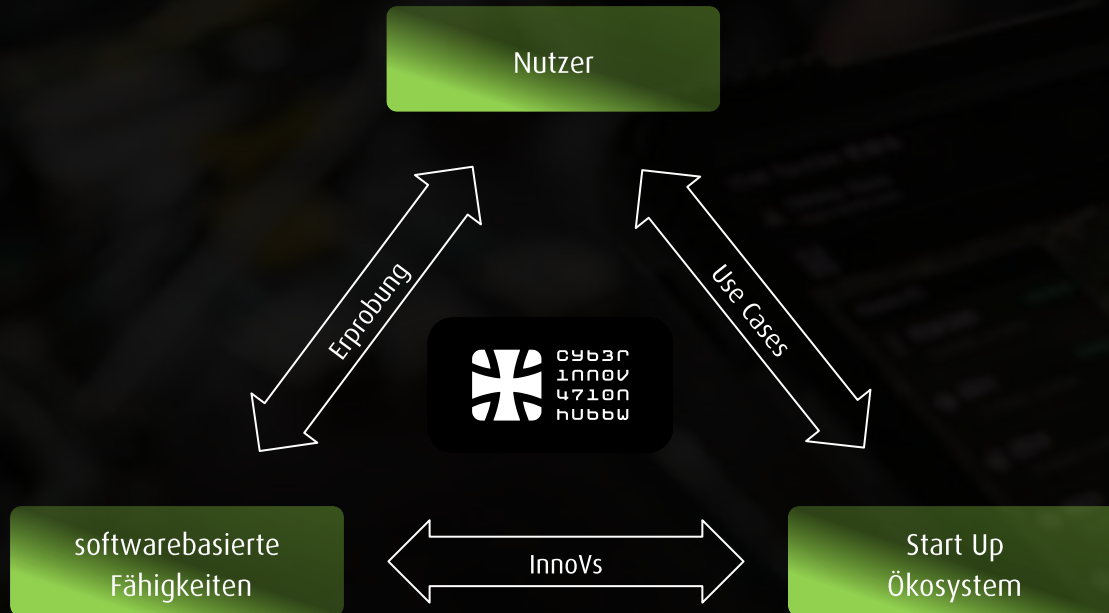
„[...] software considerations drive the architectural design of weapons systems and of complex military system-of-systems to turn ‚a bunch of disconnected hardware products‘ into an integrated whole that can be operated and managed as a single platform that centralises direction and decentralises execution of individual tasks, in pursuit of human defined mission goals, but without the need for manual human intervention.“

DEFENCE-AS-A-PLATFORM ANSATZ



„Just as Apple runs operating systems such as macOS, iOS (for iPhones) and iPadOS, the DOD should envision a day when it has a TankOS, FighterOS and ShipOS – each running individual hardware systems.“

BINDEGLIED ZWISCHEN NUTZER & STARTUPS



SDD als Chance für Start Ups und Bundeswehr

- Öffnung klassischer OEM-Verträge
- Förderung des Wettbewerbs
- Inno Schnellspur SDD: vom Nutzer zum Service zum Nutzer
- Stärkung des Start Up Ökosystems
- Erhöhung des Budget für Innovation
- unterjährige Einführung

„Mit dem CIHBw kann schnell Wirkung erzielt werden. Dazu braucht es ein Ökosystem mit den richtigen Rahmenbedingungen.“

Open RAN – ein Modell für SDD?

AFCEA FACHVERANSTALTUNG

„SOFTWARE DEFINED DEFENSE –
INDUSTRIE IM DIALOG MIT DEM BUNDESMINISTERIUM
DER VERTEIDIGUNG“

18.04.2024, BERLIN

MARKUS LEHMANN -- DEUTSCHE TELEKOM, LEITER DEFENCE





Technology made large populations possible; large populations now make technology indispensable.

Joseph Krutch,
Amerikanischer Schriftst. 1893 - 1970



Agenda

- Die Non-SDD-Welt heute
- Traditionelles Radio Access Network
- Evolution des Radio Access Network
- Das Open Radio Access Network
- Beispiele von Open RAN in der Praxis
- Erkenntnisse und Schlussfolgerung

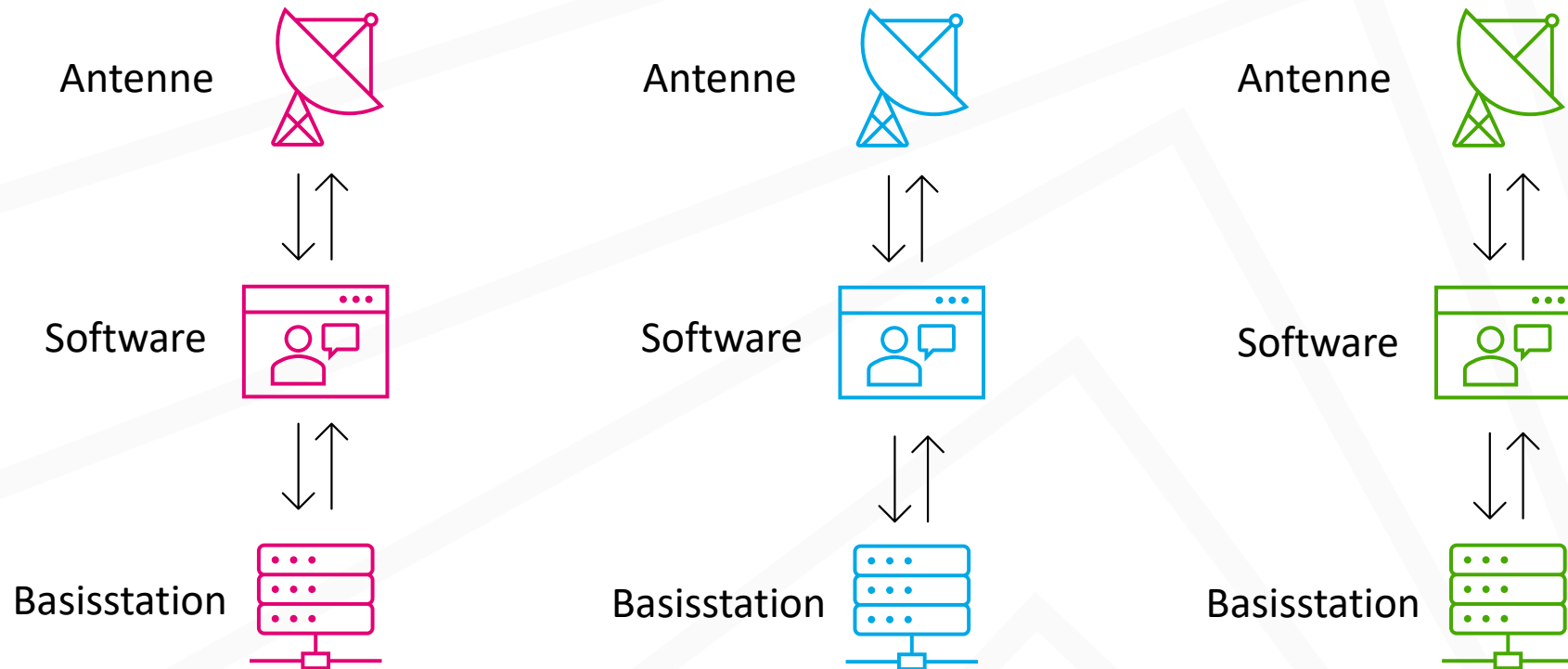
Die Non-SDD-Welt heute

Beispiel: Fregattenprogramme der letzten Jahrzehnte

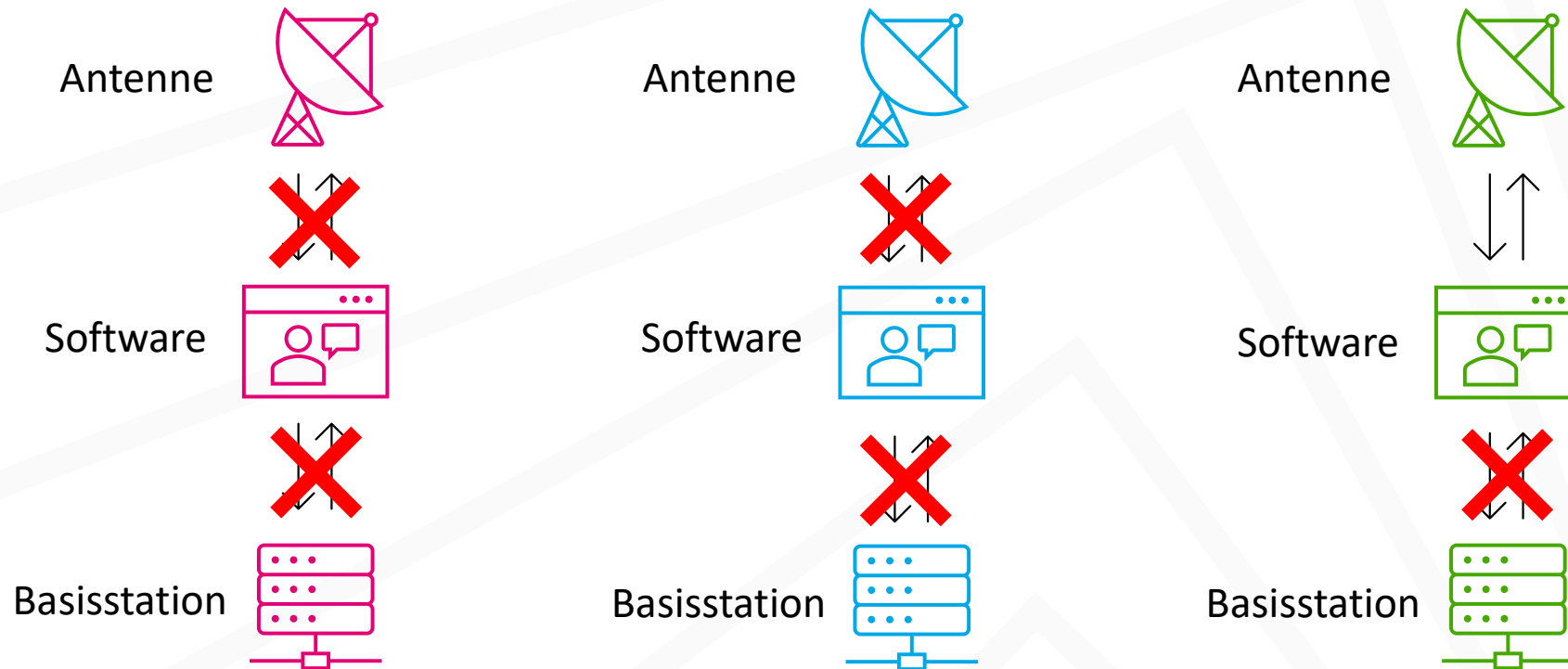


- F123: Bauvertrag 1989 – Indienststellung erstes Schiff 1994
- F124: Bauvertrag 1996 – Indienststellung erstes Schiff 2004
- F125: Bauvertrag 2007 – Indienststellung erstes Schiff 2019
- F126: Bauvertrag 2020 – Indienststellung erstes Schiff 2028?

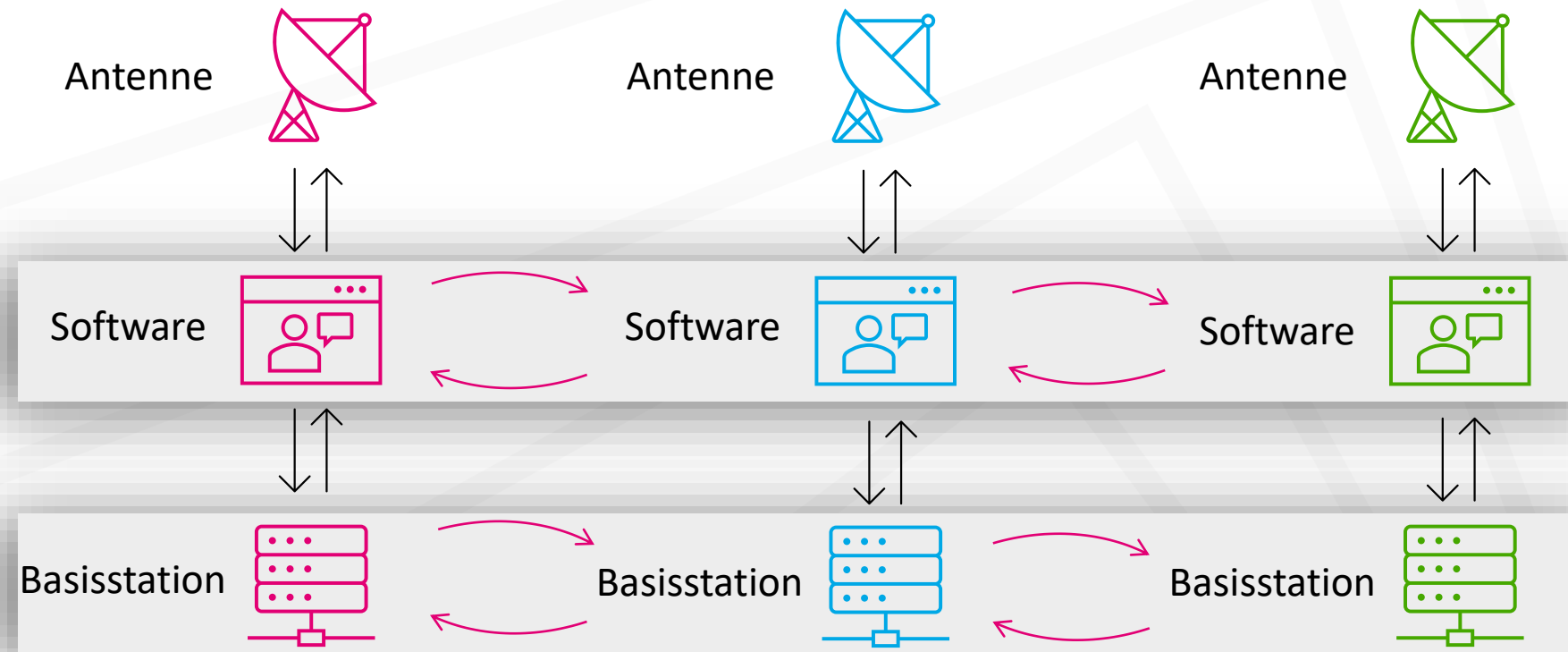
Traditionelles Radio Access Network



Evolution des Radio Access Network



Das Open Radio Access Network



Das Open Radio Access Network

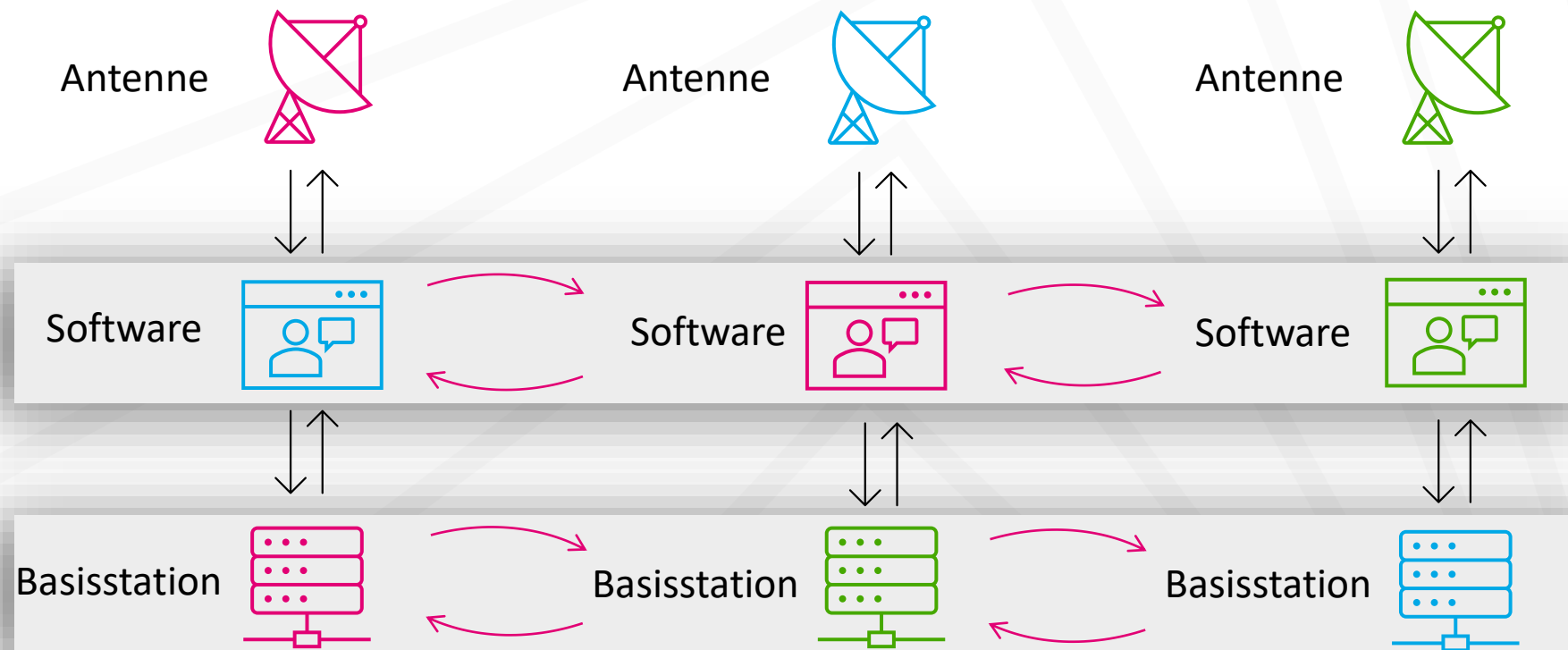
Vorteile:

- Interoperabilität und Flexibilität
- effiziente Kostensenkung
- Innovation und Beschleunigung
- skalierbar und zukunftssicher
- Offenheit und Sicherheit
- Programmierbarkeit
- Softwareisierung
- Automatisierung

Wettbewerb

Nachteile:

- Erhöhter Abstimmungsbedarf
- Zeitlicher Vorlauf für Standardisierung
- Zertifizierung und Zulassung zeitkritisch



Beispiele von Open RAN in der Praxis

„Das 1&1 O-RAN ist nun voll funktionsfähig und deutschlandweit mobil verfügbar.“

„Anders als herkömmliche Mobilfunknetze trennt die innovative Open-RAN-Technologie konsequent zwischen Soft- und Hardware.“

Quelle: [1&1 - Open RAN](#), 08.12.2023

„Nokia und die Deutsche Telekom haben bekannt gegeben, dass sie gemeinsam mit Fujitsu mit dem Aufbau eines herstellerübergreifenden Open RAN-Netzes in Deutschland begonnen haben.“

Quelle: [Telekom und Nokia](#), 21.12.2023

„Telefonica O2 und Samsung Electronics testen gemeinsam moderne Antennennetz-Technologien wie vRAN (virtualized Radio Access Network) und Open RAN in Deutschland. Damit können Netzbetreiber flexiblere Netzarchitekturen errichten, bei denen die Hard- und Software voneinander getrennt und einzelne Komponenten in der Cloud virtualisiert werden.“

Quelle: [Telefonica O2](#), 31.10.2023

Erkenntnisse

Vorteile von Open RAN:

- Weiterentwicklung von Funktionalitäten
- Erhöhung der Innovationsgeschwindigkeit
- Lebensdauererhalt durch längere Nutzung der Komponenten
- Kürzere Wartungszyklen durch Komponententausch
- Schnellere Zulassung auf Komponentenebene
- keine „Security by Obscurity“ bei proprietären Lösungen
- kürzere Testzyklen durch bekannte Schnittstellen
- gemeinsame Nutzung von Komponenten auf verschiedenen Systemen
- kürzere Ausbildungszeiten für Betriebspersonal

Vorteile von SDD:

- Weiterentwicklung der Fähigkeiten und Kampfwertsteigerung
- Erhöhung der Innovationsgeschwindigkeit
- Lebensdauererhalt durch längere Nutzung der Komponenten
- schnellere Einsatzbefähigung
- Schnellere Zulassung auf Komponentenebene
- keine „Security by Obscurity“ bei proprietären Lösungen
- kürzere Testzyklen durch bekannte Schnittstellen
- gemeinsame Nutzung von Komponenten auf verschiedenen Systemen
- kürzere Ausbildungszeiten für Einsatzkräfte

Erkenntnisse

Grundsätzlich sind die potenziellen Herausforderungen bei der Implementierung von Open RAN und SDD identisch:

1. Gemeinsame Entwicklung und Standardisierung der Schnittstellen (Anforderer und Technologiepartnern)

Beispiel: O-RAN Alliance



2. Sicherheit – No Security by Obscurity
3. Festlegung der Test-, Zulassungs- und Zertifizierungsbedingungen

Schlussfolgerung

- Konzept der offenen virtualisierten Architektur mit HW und SW verändert die Art und Weise wie wir Systeme bauen
- Für Greenfield-Ansätze geeignet – langfristig der Standard auch bei Brownfield
- Traditionelle „Anbieter“ sind (noch) zurückhaltend
- Es braucht definierte Schnittstellen – Aufbau eines Innovation Lab
- Es gilt ein Lieferanten- und Produktökosystem zu entwickeln
- Einführung von SDD bedingt die Anpassung der Begleitprozesse an die beschleunigte Realisierung
- Implementierung neuer Zulassungs- und Zertifizierungsprozesse* mit Hilfe von:
 - Digitaler Zwilling
 - Simulationssysteme und Pen.-testing

*siehe **Studienansatz: Sicherheitsuntersuchung vernetzter Systeme**

Open RAN – ein Modell für SDD!

VIELEN DANK!

FRAGEN?

