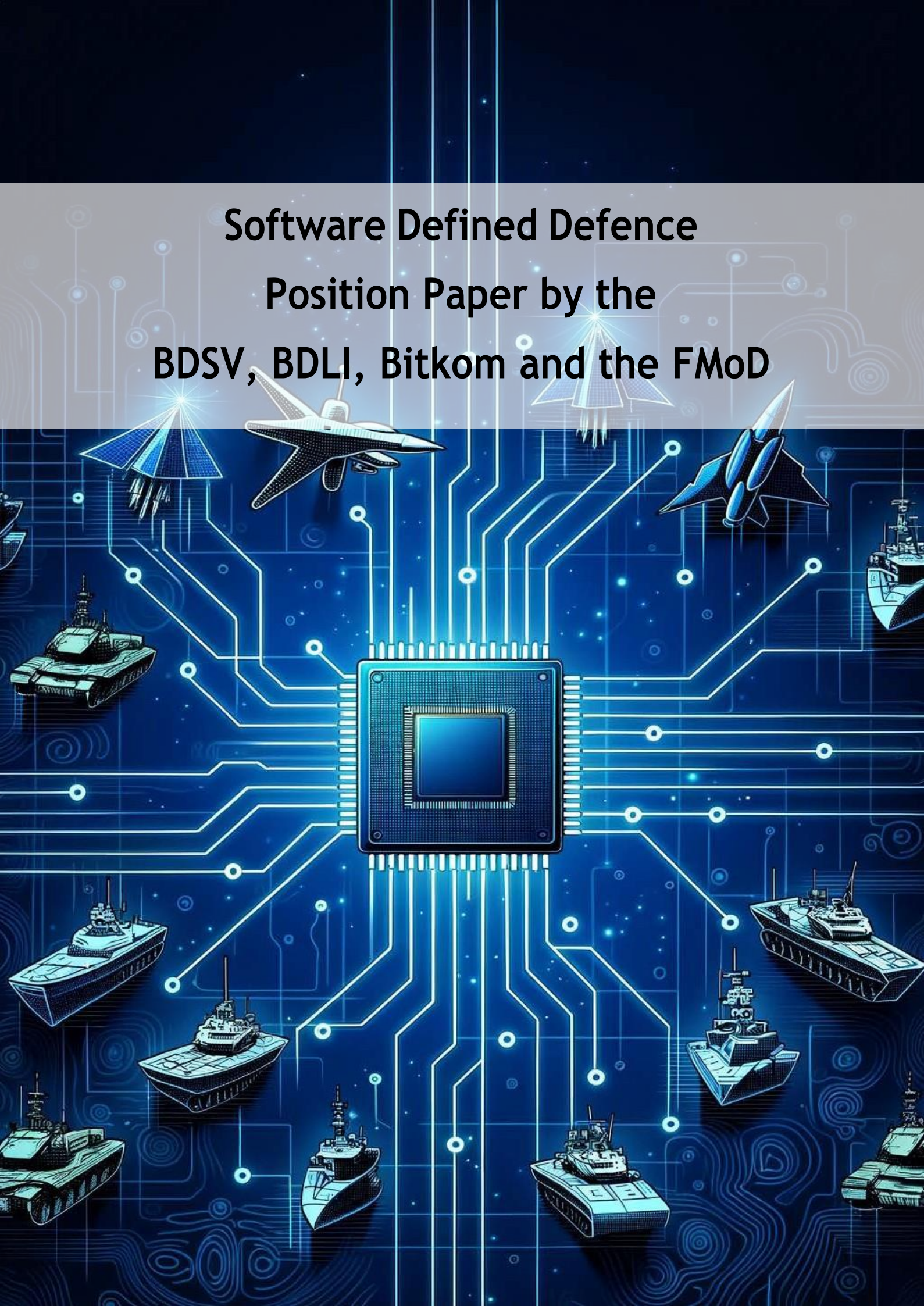
Software Defined Defence
Position Paper by the
BDSV, BDLI, Bitkom and the FMoD



Position Paper

Software Defined Defence

Results of Expert Group 1 on Software-Defined Defence

in the context of Discussion Group 4 “Innovation Cyber/IT” of the Strategic Industry Dialogue between

the Federal Ministry of Defence (FMoD), Directorate-General for Cyber/Information Technology

the Federal Association of the German Security and Defence Industry (BDSV),

the German Aerospace Industries Association (BDLI) and

the Federal Association of Information Technology, Telecommunications and New Media (Bitkom)

Version: Co-reviewed co-signed version intended for publication

Last updated: 31 October 2023

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

Note

This publication contains general non-binding information. The contents reflect the opinion of the publishing agencies at the time of publication. Although the information was prepared with the greatest possible care, there is no claim of factual correctness, completeness and/or up-to-dateness. Any use is the responsibility of the reader.

Table of Contents

1 Introduction

Around the world, simmering and open conflicts, such as the one in Ukraine, have not only created a new security consciousness among politicians and the public but have also placed a broad focus on modern and well-equipped armed forces as an essential element of whole-of-government security provision. At the same time, however, they highlight challenges and deficits that the armed forces must address if they are to fulfil their tasks in a future operating environment characterised by a high degree of networking, digitalisation and interoperability, a high rate of change as well as the need and ability to adapt.

Digital transformation increasingly affects all areas of life and society at an ever-faster pace. This is due, in particular, to the rapid development of software in ever shorter cycles, increasing data volumes and exponentially increasing computing capacities. In the private sector, software is having a disruptive effect on entire industries, including through the use of artificial intelligence (AI).

These challenges and opportunities must now be reflected in the weapon systems that are already in use today. We must also review appropriate options for modification/adaptation to the future requirements of networking and digitalisation. Particular focus should be placed on the aspects of

- cross-platform networking and integration of the platform-specific capabilities required for this purpose (e.g. provision of sensor data),
- options for faster adaptation of software to new short-term, application-oriented requirements, including through functional enhancements and agile software maintenance and modification processes, as well as
- increases in the capabilities and performance of existing systems through software.

In order to increase the effectiveness of the Bundeswehr in the short and medium term as required for the "Zeitenwende", the major shift of policy announced by Chancellor Scholz after Russia's invasion of Ukraine in February 2022, and to be able to adapt to increasingly fast-paced changes on the battlefield, we must exploit the opportunities of digital transformation both for the digital enhancement of systems already in use and in the development of new systems. Software is the essential enabler of modern military operations in the sense of multi-domain operations (MDO).

Software-Defined Defence (SDD) represents a central guiding principle for the future development of our armed forces. The main objective is to exploit the enormous potential of software for the continuous improvement or expansion of the capabilities of weapon systems and thus for a (comprehensive) increase in the capabilities of the Bundeswehr.

Traditional military platforms will not become limited in their relevance but rather benefit from the extensive potential of software development. Thus, the particular features of modern software development allow innovation potential to be tapped for the benefit of

armed forces capability development. These features include short development cycles, flexible adaptability, scalability and resilience.

We must therefore review if and how the performance of military systems can be adapted more quickly, cost-effectively and continuously with the help of standardised and reusable software modules based on a standardised intermediate level (middleware) and standardised interfaces without the need to replace or significantly adapt the underlying IT infrastructure, which would limit its operability for a longer period of time (a setup comparable to app stores on mobile devices).

As an essential basis for this, the Bundeswehr, in accordance with the NATO C3 taxonomy, has structured the portfolio of its IT landscape into nine clusters and subjected it to a common portfolio management so that Bundeswehr IT can be further developed in a targeted manner. The resulting approach of a Digitalisation Platform for the FMoD Area of Responsibility is the prerequisite for implementing Software-Defined Defence in the Bundeswehr (SDDBw) as a design paradigm.

In order to make full use of the conditions created by the Digitalisation Platform for the FMoD Area of Responsibility and to achieve the intended objective of SDDBw – particularly for (capability) platforms and weapon systems – all parties involved must rethink and reorient the design and/or implementation of armaments and planning processes, both on the part of the public contracting authorities and on the part of industry, including system houses.

SDDBw is thus intended to increase the interoperability of systems with and among each other to be able to combine reconnaissance results of different systems into situation pictures and to allow decision-makers to take targeted and effective action, for example. It also aims to enable targeted adjustments to and for platforms in response to technical and tactical requirements. Capability improvements/enhancements can thus be made quickly and economically by reusing existing software modules.

2 Software Defined Defence for the Bundeswehr in Detail

The SDDBw complex was divided into six main areas of investigation, each of which addressed issues that need to be considered in the establishment of a digitalisation ecosystem. Together, these elements form a holistic overall structure that mostly covers the issue and allows a structured approach to future work.

- **Foundation@SDDBw**, the basic IT infrastructure as a prerequisite for a modular software architecture
- **Rapid Development & Deployment@SDDBw**, an agile software environment with associated processes and procedures for the rapid development, testing, quality assurance and regular deployment of software and software adaptations on the platform systems throughout their entire life cycle – including during their deployment
- **AI (Methods)@SDDBw,** the disruptive technology of the future as an enabler of a variety of capability-enhancing applications
- **InfoSec@SDDBw**, an information security environment adapted to the SDD paradigm
- **Economics@SDDBw**, economic aspects to be considered when introducing SDD
- **Contracting@SDDBw**, issues relevant to contracting which both arise as a result of SDD and must be solved by SDD

These investigations dealt with a variety of aspects, a select few of which will be examined in more detail in subsequent steps. The current interim results of the investigations are summarised below in the form of an executive summary.

2.1 Foundation@SDDBw

Brief description

Foundation@SDDBw describes a common IT architecture, functions and interfaces. The IT platform and application logic should be logically separated so that they can be used and adapted largely independently of each other and individual software modules can be instantiated in several systems. This also includes cross-platform networking and the integration of the platform-specific capabilities required for this purpose in the spirit of "federability" in accordance with Federated Mission Networking (FMN).

Initial analysis result:

The conceptual design of the basic IT architecture and the associated infrastructure system of a Software-Defined Defence strategy is essential. The goal must be to define a flexible, interoperable IT platform that is suitable for national and international deployment scenarios. The architecture includes proposals for container orchestration, agile operating models and cooperation with industry and select agencies in the FMoD area of responsibility. To this end, the introduction of governance should be reviewed, best

practices observed, full API [1]management introduced and pilot projects for the implementation of a Software-Defined Defence system conducted. This will enable innovative change, greater adaptability and seamless interoperability in a modern Bundeswehr IT landscape.

Selected aspects for more detailed review

- Preparation of a draft concept for containerisation and container orchestration
- Development of proposals for the adaptation of the existing system architecture

2.2 Rapid Development & Deployment@SDDBw

Brief description

Rapid Development and Deployment is a framework of tools and processes that allows software to be developed, tested, quality-assured and deployed on platform systems in less time and at greater speed. Rapid development aims to accelerate the software development and deployment process by using iterative and incremental methods.

Initial analysis result:

The increasing importance of data and software for the capabilities of military platforms and the need to update them much faster than before necessitate a paradigm shift in software development. The necessary speed in development and deployment requires the consistent establishment of agile, user-centred development methods, a high degree of simulation and automation through standardisation, and close cooperation between the Bundeswehr and industry, supported by modern collaboration tools. Open interfaces coupled with security by design and procedures for standardised rollouts ensure the fast and secure distribution of updates and service provision for all available platforms in use. Success depends on modern connectivity technologies.

Selected aspects for more detailed review

- Analysis of software development methods
- Development of a concept for cooperation platforms for software development

2.3 AI (Methods)@SDDBw

Brief description

AI as the disruptive technology of the future enables a variety of capability-enhancing applications and plays an essential role as a capability driver for military platforms.

[1] Application programming interface

Initial analysis result:

AI-based services require new patterns (e.g. camouflage, radio signals) to be generated and identified and services to be retrained, tested, certified and rolled out to the tactical level. These models should be able to be implemented in the different platforms quickly and with little integration effort. One example of a use case is the utilisation of data from all sensors and other sources (C4I systems) for AI-based functions (connectivity and interoperability).

Selected aspects for more detailed review

- Development of a concept for the secure development and provision of certified AI models

2.4 InfoSec@SDDBw

Brief description

The introduction of SDD into the Bundeswehr is closely tied to information security. On the one hand, inherent improvements are made possible, for example, through faster and more targeted introduction of security patches. On the other hand, however, it also opens up new security risks and potential attack vectors. Principles of security-by-design and security-by-default, approaches such as zero trust, and basic information security functionalities such as encryption, authentication, etc. must be considered from the outset.

Initial analysis result:

One key result is the observation that currently known specifications regarding information security guidelines in the FMoD area of responsibility are generally supportive of the SDDBw approach. Further action is required with regard to the operationalisation and supplementation of basic requirements. This includes the further development of risk management (taking into account complexity and dynamics), options for an adapted security classification process as well as expanded guidelines for the handling/implementation of information security and the establishment of supply chain transparency and security.

Selected aspects for more detailed review

- Investigation to secure the supply chain, especially for software deployment
- SWOT analysis of SDDBw with regard to information security, ministerial instructions on classified information for the FMoD area of responsibility and security classification.

2.5 Economics@SDDBw

Brief description

Traditional approaches for specific IT in the systems lead to low unit numbers and small margins and usually address only a small "target group" while facing high complexity, high security requirements and strong regulation (industry standards, NATO, ...). SDD opens up/requires new business models and can thus reduce costs and promote competition. Copyright and intellectual property rights, rights of use of systems and, for example, rights to required data must be considered when operationalising SDD for the Bundeswehr.

Initial analysis result:
SDDBw must be designed as an open and modular system with clearly defined interfaces. The following objectives must be achieved:

- The interfaces of the individual software modules are open/verified and are available to users as well as to the OEM[2] for use in other projects, as appropriate, in order to facilitate their economical application.
- Responsibilities for the platform-related and cross-platform functionality and security of the overall system are defined.
- The existing OEM rights (intellectual property rights (IPR) etc.) are adequately regulated and taken into account both for the OEM, the customer as well as third parties, if applicable. The establishment of the Bundeswehr's own software expertise as a catalyst ensures that industry continues to have access to the software modules. Responsibility for system modifications and their effects on the different weapon systems must also be defined.
- The system verification processes for the FMoD area of responsibility and, for example, the Federal Office for Information Security (BSI) have been adapted and, if necessary, expanded.

Selected aspects for more detailed review

- Review of the legal situation with regard to SDDBw (including IPR, rights of use, rights to data)
- Investigation of financial aspects such as pricing regulations, liability issues, guarantees etc.

[2] Original equipment manufacturer

2.6 Contracting@SDDBw

Brief description

Processes for Bundeswehr planning and equipment, such as the armaments process, including contracting procedures, contract drafting and implementation, must allow for SDDBw in principle for any new projects. For systems already in use, steps must be taken to at least enable SDDBw as far as possible, provided they are justified by the remaining service life and expected potential of SDDBw-driven improvements.

Initial analysis result:

For the Bundeswehr to successfully implement the SDD principle and thus exploit its expected potential, compatible (legal, commercial, functional) framework conditions must be established for its planning, commissioning and implementation, including the in-service phase.

The classic OEM contracts for weapon systems must be "opened up" – the provision of the services to be rendered, functional responsibility and thus the distribution of liability old/new, role assignments and cooperation with/between SDD actors must be defined. In addition, especially when new software-based or AI-based capabilities are implemented and a successful acceptance/certification procedure has been completed, the subsequent user responsibility must be clearly defined. Rights to operational data and lessons learnt must be contractually agreed.

Selected aspects for further detailed consideration

- Development of "open" OEM contract models
- Development of adaptation requirements in terms of public procurement law and other statutory regulations and forms up to the adaptation of the V-model

3 Way-Ahead

The transformation intended to be achieved through SDDBw aims at improving the interoperability of own as well as allied or federable systems, increasing resilience and scalability, expanding the capabilities of existing/newly introduced weapon systems through rapidly deployed software updates, and increasing flexibility and agility to prevent long-term (strategic) mistakes.

Based on the results already achieved, further detailed analyses of select issues are required and intended to actively support the further implementation of SDDBw.

On the basis of these courses of action, the Strategic Industrial Dialogue and the Bundeswehr will initiate further investigations in order to operationalise the SDD paradigm to such an extent that future Bundeswehr systems as well as those that are already in use can then be provided with initial requirements and adaptations.[3]

[3] For systems already in use, cost and benefit as well as other factors must be assessed individually, taking into account the remaining service life.

4 Proof of Authorship

Representatives of the member companies of the industrial associations BDSV, BDLI and Bitkom as well as the Federal Ministry of Defence and its area of responsibility actively contributed to this document as a result of the work of Expert Group 1.

The following member companies of the industrial associations BDSV, BDLI and Bitkom contributed to Expert Group 1 and to the preparation of this document:

- 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. Deutschland

References and Sources

1. Cover image generated by OpenAI's DALL·E 3