



## **Embedded Systeme in der Verteidigungsindustrie: Die Bedeutung der Embedded-Computing-Lieferkette**

Eine Handlungsempfehlung  
Lieferketten resilienter, sicherer und  
zukunftsfähig zu gestalten

## Executive Summary

Die Lieferkette ist heute einer der entscheidenden Erfolgsfaktoren für die Verteidigungsindustrie. Mit der fortschreitenden Digitalisierung und der starken Abhängigkeit von Embedded-Computing-Komponenten – etwa Prozessoren, Kommunikationsmodulen, Speicherlösungen und Sensorik – werden moderne Waffensysteme leistungsfähiger, aber zugleich verwundbarer. Geopolitische Spannungen, technologische Engpässe, Sicherheitsrisiken und lange Lebenszyklen machen die Absicherung dieser Lieferketten zu einer strategischen Notwendigkeit.

Sichere Lieferketten -  
der Schlüssel zur  
Verteidigungs-  
fähigkeit

Rund 90 Prozent der modernsten Halbleiterfertigungskapazitäten befinden sich in Ostasien, was die Verteidigungsindustrie besonders anfällig für Störungen und Abhängigkeiten macht. Zusätzlich erschweren Exportkontrollen, regulatorische Anforderungen und eine wachsende Bedrohung durch Supply-Chain-Angriffe die Beschaffung kritischer Komponenten. Gleichzeitig konkurrieren zivile Branchen um die gleichen Ressourcen, während militärische Systeme Einsatzzeiten von 10 bis 20 Jahren erfüllen müssen. Zudem wirken gesetzliche Vorgaben, wie das deutsche Lieferkettensorgfaltspflichtengesetz sowie eine geplante EU-weite Regelung zur Transparenz in der Lieferkette ebenfalls auf Unternehmen ein.

Abhängigkeit von  
Ostasien erhöht  
Risiken erheblich

Dieses Whitepaper analysiert die damit verbundenen Risiken und zeigt praxisnahe Lösungsansätze auf: Von der Diversifizierung und Lokalisierung der Lieferketten, über Investitionen in eigene Kapazitäten und Open-Source-Technologien, bis hin zur Nutzung digitaler Risikoanalyse-Tools. Es stellt außerdem dar, wie aktuelle politische Maßnahmen – wie das Planungs- und Beschaffungsbeschleunigungsgesetz (BwPBGG) – die Resilienz und Handlungsfähigkeit der Industrie stärken können.

Proaktive Strategien  
stärken Resilienz  
und Zukunft

Nur durch einen ganzheitlichen, proaktiven Ansatz kann die Verteidigungsindustrie ihre Embedded-Computing-Infrastruktur langfristig absichern, ihre Einsatzbereitschaft gewährleisten und gleichzeitig technologisch an der Spitze bleiben.

## Einleitung

Die Verteidigungsindustrie steht vor einer doppelten Herausforderung: Der technologische Wettlauf um immer leistungsfähigere Systeme – von unbemannten Drohnen über moderne Radarsysteme bis hin zu KI-gestützten Kommando- und Kontrollnetzen – wird zunehmend von der Verfügbarkeit hochspezialisierter Embedded-Computing-Komponenten bestimmt. Gleichzeitig sind die globalen Lieferketten, die diese Schlüsseltechnologien bereitstellen, fragiler denn je.

Die Halbleiterkrise der Jahre 2020 – 2023 hat gezeigt, wie abhängig selbst hochpriorisierte Industrien von globalen Produktionsengpässen und geopolitischen Spannungen sind. Infolgedessen entstehen signifikante Verzögerungen entlang militärischer Beschaffungsprogramme. Hinzu kommen neue geopolitische Realitäten: Exportkontrollen, Sanktionsregime und wachsende Spannungen zwischen China, den USA und Europa bedrohen die Stabilität und Verfügbarkeit kritischer Komponenten. Für die Verteidigungsindustrie, die aufgrund langer Systemlebenszyklen und höchster Sicherheitsanforderungen besonders verwundbar ist, bedeutet dies ein erhebliches strategisches Risiko.

Embedded Computing ist dabei ein neuralgischer Schwerpunkt. Diese Systeme bilden die Rechen- und Steuerungsbasis für nahezu alle modernen militärischen Plattformen. Ohne verlässlichen Zugang zu leistungsfähigen Prozessoren, Speicher-Bausteinen, Kommunikationsbausteine oder sicherheitszertifizierten Betriebssystemen kann kein Rüstungsunternehmen langfristig konkurrenzfähig bleiben. Gleichzeitig erfordert der Schutz vor Manipulation, Wirtschaftsspionage, Social Engineering und Insider Aktivitäten in der Lieferkette höchste Sorgfalt.

Dieses Whitepaper untersucht die Relevanz der Lieferkette für Embedded-Computing-Komponente in der Verteidigungsindustrie aus einer strategischen Perspektive, welche durch technische Hintergründe aus Sicht eines Elektronikunternehmens ergänzt werden. Ziel ist es, Entscheidungsträgern entlang der Industrie und Behörden konkrete Handlungsempfehlungen aufzuzeigen, um ihre Lieferketten resilienter, sicherer und zukunftsfähig zu gestalten.



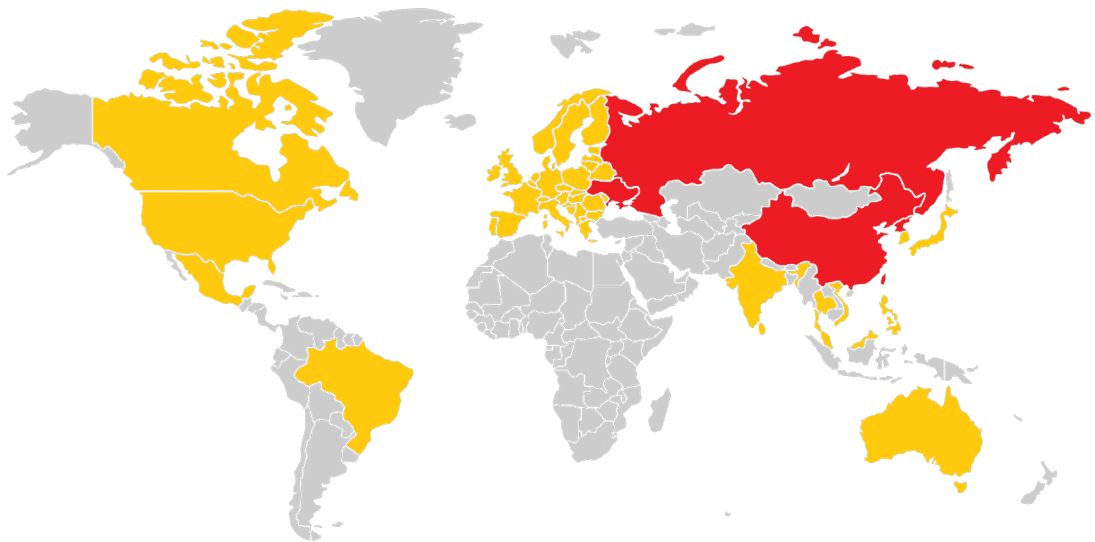
Dennis Nejdrowski  
CCO und Geschäftsführer der iesy GmbH

***Die Resilienz der Embedded-Computing-Lieferketten entscheidet über technologische Souveränität und Einsatzbereitschaft.***

## Die Lieferkette als strategischer Erfolgsfaktor

Die Lieferkette hat sich in der Verteidigungsindustrie von einer rein operativen Notwendigkeit zu einem strategischen Kernelement entwickelt. Der Grund liegt in der zunehmenden Komplexität und Globalisierung von Beschaffungsprozessen. Während klassische Rüstungsgüter früher überwiegend lokal gefertigt wurden, ist nahezu jedes moderne System heute auf hochspezialisierte Elektronik, Halbleiter und andere eingebettete Komponenten angewiesen, die aus internationalen Quellen stammen.

Die Halbleiterkrise hat verdeutlicht, wie empfindlich diese Abhängigkeiten sind. Selbst Systeme, die höchsten militärischen Prioritäten unterliegen, konnten aufgrund fehlender Komponenten nicht oder nur verspätet ausgeliefert werden. Geopolitische Spannungen, insbesondere die zunehmende Rivalität zwischen China und dem Westen, verschärfen die Lage: Sanktionen, Exportkontrollen und mögliche Handelskonflikte bedrohen die kontinuierliche Versorgung.



Weltkarte mit Lieferketten-Hotspots für Embedded-Computing-Komponenten

Risikostufen:

rot - „extrem kritisch“ = China, Taiwan, Nordkorea, Russland, Ukraine

gelb - „kritisch“ = Japan, Südkorea, Vietnam, Malaysia, Singapur, Thailand, Philippinen, Australien, Indien, Europa, Nordamerika, Mexiko, Brasilien

## Herausforderungen in der Embedded-Computing-Lieferkette im Überblick

Die kritischen Engpässe in der Verteidigungsindustrie lassen sich auf verschiedene Kernfaktoren zurückführen:

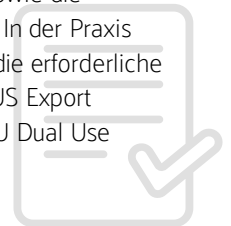
### Geopolitische Abhängigkeiten

Ca. 90% der modernsten Halbleiterfertigungskapazitäten befinden sich in Ostasien (TSMC, Samsung, SMIC). Politische Risiken wie beispielsweise der stets drohende China / Taiwan-Konflikt oder bestehende Exportkontrollen gegen China können die Versorgung abrupt unterbrechen. USA & EU haben zwar begonnen, mit Programmen wie dem „CHIPS Act“ (oder auch Chips and Science Act) gegenzusteuern, erste belastbare Ergebnisse werden jedoch erst in 5 – 10 Jahren wirksam.



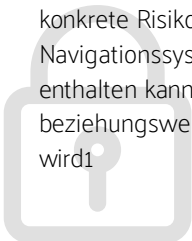
### Regulatorische und rechtliche Hürden

Regularien wie beispielsweise ITAR (International Traffic in Arms Regulation) schränken den Export und die Verwendung vieler US-amerikanischer Komponenten stark ein. EU- und NATO-Regulierungen hingegen erfordern komplexe Zertifizierungen, welche durch Rüstungsunternehmen zwingend eingehalten werden müssen. Diese Regularien schützen zwar vor Technologieabfluss, erhöhen jedoch Entwicklungszeiten sowie die Abhängigkeit von wenigen Anbietern. In der Praxis entsteht zusätzlicher Aufwand durch die erforderliche Harmonisierung zwischen ITAR, den US Export Administration Regulations und der EU Dual Use Verordnung.



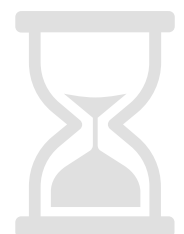
### Sicherheitsrisiken

Manipulationen in der Lieferkette (Hardware-Backdoors, kompromittierte Firmware) stellen ebenfalls eine zunehmende Bedrohung dar. Außerdem nehmen Cyberangriffe durch staatlich unterstützte Gruppen stark zu. Das Landesamt für Verfassungsschutz Hamburg und das Bundesamt für Verfassungsschutz haben bereits im Juni 2020 davor gewarnt, dass die Digitalisierung in der maritimen Industrie neue Angriffsvektoren für Spionage und Sabotage durch fremde Staaten eröffnet. Im Fokus steht hierbei das konkrete Risiko, wonach die Software maritimer Navigationssysteme bereits bei der Übergabe Malware enthalten kann oder diese in Update-Prozessen beziehungsweise per Fernsteuerung gezielt eingespielt wird<sup>1</sup>



### Langzeitverfügbarkeit

Militärische Systeme müssen oft 10 – 20 Jahre lang einsatzfähig bleiben, was neben der Vorauswahl von Komponenten entlang der Entwicklungsphasen vor allem auch Ersatzteil- und Wartungsstrategien extrem anspruchsvoll gestaltet.



## Embedded Computing als technologische Schlüsselfunktion & seine Fehlannahmen

Embedded Computing ist das Rückgrat moderner Waffensysteme. Es umfasst Prozessoren, Speicher, Kommunikationsmodule und spezialisierte Betriebssysteme, die hochgradig anwendungsoptimiert sind.

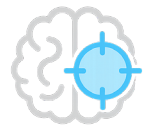
Typische Einsatzfelder sind hierzu aktuell:



Sensorfusion & Steuerung entlang von Radarsystemen, Drohnen oder autonome Landfahrzeuge



Sichere Kommunikation entlang von kryptographisch abgesicherten Funknetzen oder globaler Satellitenkommunikation



KI-gestützte Systeme entlang von Anomalie Erkennungen oder Zielerkennungssysteme

Zudem müssen diese Systeme in Echtzeit agieren und extremen Umweltbedingungen standhalten, wie beispielsweise Temperatur, Schock & Vibration oder elektromagnetische Interferenzen.

Trotz seiner zentralen Bedeutung wird Embedded Computing in der Verteidigungsindustrie häufig von strategischen Entscheidern und teilweise technischen Projektleitern unterschätzt oder missverstanden.

Die gängigsten Fehlannahmen – und welche Konsequenzen sich daraus ableiten:

Fehlannahme	Realität	Handlungsbedarf
<p>„Embedded Systeme sind austauschbar.“ Man könne spezialisierte Komponenten jederzeit durch handelsübliche Standardhardware ersetzen.</p>	<p>Militärische Systeme erfordern langzeitverfügbare, sicherheitszertifizierte und oft maßgeschneiderte Hardware.</p>	<p>Frühzeitige Lieferantenbindung, Aufbau redundanter Bezugsquellen und Investition in eigene Entwicklungs- und Fertigungskapazitäten.</p>
<p>„Einmal entwickelt ist ein Embedded System zukunftssicher.“ Embedded-Computing-Architekturen bleiben über Jahrzehnte unverändert nutzbar.</p>	<p>Technologische Sprünge, Obsoleszenz und neue Bedrohungslagen erzwingen regelmäßige Anpassungen.</p>	<p>Lebenszyklus-Management als kontinuierlichen Prozess etablieren und Budgets für Lifetime-Updates einplanen.</p>
<p>„Sicherheitsrisiken liegen nur in der Software.“ Manipulationen oder Spionage erfolgen ausschließlich auf Software-Ebene.</p>	<p>Böswillige Schadfunktionen können bereits auf Chip- oder Board-Level eingebracht werden.</p>	<p>Hardware-Security-Audits, Supply-Chain-Forensik und Sicherheitszertifizierungen als festen Bestandteil der Beschaffung verankern.</p>
<p>„Globale Märkte sichern die Versorgung.“ Internationaler Wettbewerb garantiere stabile Lieferketten.</p>	<p>Geopolitische Abhängigkeiten, Exportkontrollen und zivile Massenmärkte priorisieren andere Kunden.</p>	<p>Lokalisierung der Fertigung, strategische Lagerhaltung und politische Flankierung durch Beschaffungsregelungen.</p>
<p>„Tests im Labor decken alle Risiken ab.“ Umfassende Laborprüfungen spiegeln den späteren Einsatz realistisch wider.</p>	<p>Erst operative Szenarien zeigen versteckte Schwachstellen unter realen Umwelt- und Bedrohungsbedingungen und offenbaren häufig komplexe Wechselwirkungen, die in isolierten Tests nicht sichtbar sind.</p>	<p>Feldtests unter Extrembedingungen, Red-Teaming und Szenario-Simulationen als Standard etablieren.</p>

## Strategien zur Absicherung der Lieferkette

Um die Risiken zu minimieren, müssen Unternehmen und Staaten ihre Ansätze grundlegend überdenken. Mögliche Strategien können wie folgt lauten:

### Diversifizierung & Lokalisierung

- Aufbau regionaler Fertigungskapazitäten (z. B. europäische Chipwerke)
- Sicherung von Produktionsslots bei strategisch relevanten Herstellern
- Kooperationen mit „Trusted Suppliers“, die NATO- oder EU-Standards erfüllen und einem kontinuierlichen Monitoring ihrer Lieferkette entlang regelmäßiger Audits

### Vertikale Integration

- Beteiligungen oder eigene Kapazitäten in der Halbleiterfertigung
- Partnerschaften zwischen Industrie und staatlichen Akteuren entlang klar definierter Vereinbarungen bzgl. Lieferprioritäten & Notfallkapazitäten

### Technologische Unabhängigkeit

- Förderung von Open-Source-Hardware (RISC-V) und lokalem Design
- Reduzierung von proprietären, schwer zugänglichen Plattformen

### Digitale Transparenz und Risikoanalyse

- Einsatz von KI-gestützten Tools zur Überwachung der gesamten Lieferkette
- Frühwarnsysteme für geopolitische oder logistische Störungen

Durch den Einsatz gezielter Maßnahmen lässt sich die Resilienz von Lieferketten deutlich steigern :

- Frühe Risikoerkennung
- Zwischenpuffer zur Überbrückung
- Kontinuierliche Risikobewertung
- Alternative Lieferoptionen

Die übergeordnete Zielstellung ist der Aufbau einer Supply Chain, die auch bei Störungen weiterhin funktioniert und den Kunden zuverlässig versorgt – besonders wichtig bei Embedded-Computing-Komponenten, die oft zeitkritisch und sicherheitsrelevant sind.

**Beispiel für einen Trusted Supplier:**

## **Die Rolle der iesy GmbH bei der Stärkung der Embedded-Computing-Lieferkette**

Die Absicherung der Embedded-Computing-Lieferkette erfordert neben politischen Maßnahmen und strategischer Planung auch konkrete, leistungsfähige Industriepartner. Ein Beispiel für einen solchen Partner ist die iesy GmbH mit Sitz in Meinerzhagen (NRW). Seit 1966 entwickelt und produziert sie kundenspezifische Embedded-Computing-Systeme für sicherheitskritische Anwendungen.

Auf 2.800 m<sup>2</sup> Fertigungs- und Bürofläche arbeitet bei iesy ein Team von 50 Fachkräften, darunter Spezialisten für Hard- und Software-Entwicklung. Damit kann das Unternehmen regionale Wertschöpfung in Deutschland und Europa sichern und sicherheitskritische Fertigungsschritte komplett innerhalb vertrauenswürdiger Lieferketten durchführen. Dadurch trägt das Unternehmen aktiv zur Verringerung der Abhängigkeit von globalen Lieferketten bei und bietet Kunden ein hohes Maß an Planungssicherheit, selbst entlang geopolitischer Spannungen.

## **iesy's Kompetenzen für die Verteidigungsindustrie**

### **Zertifizierte Hochsicherheitslösungen**

Entwicklung und Produktion von Systemen, die nach MIL-STD, STANAG, BSI GEHEIM, EU SECRET und NATO SECRET zugelassen sind. Referenzen umfassen High Security Gateways für Luftfahrt-, Marine- und Gefechtsfahrzeuge sowie Rechnersysteme für mobile- und verlegfähige Systeme.

### **Maßgeschneiderte, COTS-basierte Embedded-Systeme**

Flexible Kombination aus Standardkomponenten und kundenspezifischer Entwicklung, wodurch Beschaffungssicherheit und Time-to-Market verbessert werden.

### **Cybersicherheit und digitale Souveränität**

Fokus auf Kryptographie, Netzwerksicherheit und Supply-Chain-Transparenz, um Risiken durch Manipulation und Cyberangriffe zu minimieren.

### **End-to-End-Projektabwicklung**

Von Prototyping über Evaluierungsplattformen und Zertifizierung bis zur Serienproduktion – inklusive Begleitung bei NATO- und BSI-Zertifizierungen und der Ausarbeitung umfassender Sicherheits- und Testdokumentationen für Behörden & Auftraggeber.

Darüber hinaus unterstützt iesy die Verteidigungsindustrie bei der Umsetzung des Planungs- und Beschaffungsbeschleunigungsgesetzes (BwPBBG). Durch kurze Entscheidungswege, lokalisierte Fertigung und enge Kooperation mit Behörden und Industrie kann iesy Projekte schnell und resilient realisieren.



#### Damit zeigt sich:

Lokale Player wie die iesy GmbH sind ein zentraler Baustein, um Versorgungssicherheit, technologische Souveränität und Innovation in der Verteidigungsindustrie gleichzeitig sicherzustellen.

## Handlungsempfehlungen

Einleitend sei erwähnt, dass bereits das BMVg im Papier „Element der digitalen Souveränität“ eine vollständige Transparenz zu Herkunft und Eigenschaften aller elektronischen Bauteile, die idealerweise von Beginn an im Lebenszyklus digital erfasst und über offene Standards austauschbar sein sollen, fordert.<sup>2</sup>

Außerdem unterstreicht das Ideenpapier „Vertrauenswürdige IT: Element der digitalen Souveränität“ des BMVg, dass weder Staat noch Industrie allein handeln können. Interdisziplinäre Kooperation ist essenziell, besonders bei Sicherung vertrauenswürdiger IT innerhalb der Verteidigungswirtschaft, sodass sich folgende Schritte ableiten lassen<sup>3</sup>:

- Aufbau eines Lieferketten-Resilienzplans mit Szenarien und Risikoklassen
- Integration der Verteidigungsindustrie in nationale und europäische Chip-Strategien
- Förderung von Langfristverträgen mit Herstellern, um Planungssicherheit zu schaffen
- Investitionen in Forschung und Entwicklung sicherer Embedded-Systeme
- Aufbau von Cybersecurity-Standards für alle Zulieferer

## Fazit

Die zunehmenden geopolitischen Spannungen, die Abhängigkeit von globalen Embedded-Computing-Komponenten und die dynamische Innovationsgeschwindigkeit stellen die Rüstungsindustrie vor nie dagewesene Herausforderungen. Gleichzeitig wächst der Druck, die Einsatzfähigkeit der Streitkräfte ohne Verzögerung sicherzustellen.

Mit dem Planungs- und Beschaffungsbeschleunigungsgesetz (BwPBBG), das am 23. Juli 2025 verabschiedet wurde, schafft die Bundesregierung einen strategischen Rahmen, der diese Anforderungen erfüllt. Direktvergaben, vereinfachte Vergabeverfahren und die Möglichkeit, Unternehmen aus Drittstaaten auszuschließen, stärken die Resilienz und Sicherheit der Lieferketten. Die Integration von Vorauszahlungen fördert zudem die Einbindung innovativer KMU und Start-ups – gerade im hochspezialisierten Embedded-Computing-Sektor.



### ***Strategische Resilienz durch vertrauenswürdige Lieferketten***



Damit entsteht ein doppelter Mehrwert:

- Versorgungssicherheit und technologische Souveränität durch die bevorzugte Einbindung vertrauenswürdiger Lieferanten innerhalb Deutschlands und der NATO/EU
- Innovations- und Wettbewerbsförderung durch flexiblere Verfahren, die Start-ups und mittelständischen Technologieunternehmen den Zugang zu Beschaffungsprogrammen erleichtern

Für die Verteidigungsindustrie bedeutet dies:

- Unternehmen, die Embedded-Computing-Systeme entwickeln oder integrieren, können künftig schneller, sicherer und mit größerer Planbarkeit agieren
- Der Erfolg hängt jedoch davon ab, dass Firmen diese Chancen aktiv nutzen – etwa durch Investitionen in transparente Lieferketten, Kooperationen mit staatlichen Stellen und den konsequenten Ausbau eigener Kapazitäten

Nur so lässt sich der Spagat zwischen technologischer Spitzenleistung und strategischer Resilienz meistern.

## Quellenverzeichnis

<sup>1</sup> „Ideenpapier für sichere IT-Lieferketten“ der Ergebnisse des EK2 im Rahmen des GK4 des strategischen Industriedialoges zwischen dem Bundesministerium der Verteidigung, Abteilung Cyber/Informationstechnik und dem Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V. und Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., Version: Mitgeprüfte und mitgezeichnete Version zur Veröffentlichung, Stand: 08.06.2021

<sup>2</sup> „Vertrauenswürdige IT: Element der digitalen Souveränität“ der Zusammenfassung des Ideenpapiers des EK2 im GK4 des strategischen Industriedialoges zwischen dem Bundesministerium der Verteidigung, Abteilung Cyber/Informationstechnik und dem Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V. und Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., Stand: 23.10.2019

<sup>3</sup> Ideenpapier „Vertrauenswürdige IT: Element der digitalen Souveränität“ der EK2 im Rahmen des GK 4 ICIT zwischen dem Bundesministerium der Verteidigung, Abteilung Cyber/Informationstechnik, dem Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V. und dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. im Rahmen des strategischen Industriedialoges zwischen dem Bundesministerium der Verteidigung und dem Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V., Version: Mitgeprüfte und mitgezeichnete Vordruckversion nach Vorlage Leitung BMVg, Stand 07. August 2019



## **iesy GmbH**

Darmcher Grund 22  
58540 Meinerzhagen  
+49 (2354) 70655 - 0

[info@iesy.com](mailto:info@iesy.com)

Copyright © 2025 iesy. Alle Rechte vorbehalten.