

IT-Grundschatz-Profil  
für den Betrieb von UAS  
Band 2: UAS-Betriebskategorie  
„Specific (Speziell)“

# Inhalt

1. Einleitung .....	3
2. Management Summary .....	7
3. Festlegung des Geltungsbereichs .....	9
4. Abgrenzung Informationsverbund.....	11
5. Referenzarchitektur .....	13
6. Feststellung des Schutzbedarfs.....	19
7. Zu erfüllende Anforderungen und umzusetzende Maßnahmen.....	23
8. Restrisikobetrachtung.....	28
9. Anwendungshinweise .....	29
10. Unterstützende Informationen.....	30
Anlage 1 – Bausteine/Systemkomponenten .....	31
Anlage 2 – Elementare Gefährdungen.....	32
Anlage 3 – Begriffsdefinitionen .....	34
Anlage 4 – Abkürzungen .....	35

# 1. Einleitung

Der Betrieb von Uncrewed Aircraft Systems (UAS) stellt neben den Anforderungen an die Flugsicherheit auch Anforderungen an die Informationssicherheit. Als fliegende Rechnerverbünde sind sie schutzbedürftig, denn korrumpierte Firmwareupdates, ein Ausfall der Kommunikationsinfrastruktur oder manipulierte Datenbanken können zu einem Fehlverhalten des Fahrzeugs führen und damit dieses zu einer Gefahr für Menschen und Umwelt werden lassen. Der Datenschutz und die sichere Kommunikation mit dem unternehmensinternen Netzwerk machen daher eine genauere Betrachtung in punkto Informationssicherheit erforderlich. Informationssicherheit bei UAS ist aus zwei Perspektiven zu betrachten: zum einen aus der Sicht des UAS als Teilnehmer am Luftverkehr und zum anderen aus der Sicht des mobilen Endgeräts und Datenspeichers.

Grundsätzlich soll das vorliegende IT-Grundschutz-Profil den Beteiligten diese Bürde abnehmen und anhand einer Referenzarchitektur die wichtigen Fragen zur Informationssicherheit beim Betrieb von UAS klären. Insbesondere sollen folgende Fragen adressiert werden: Wie kann durch geeignete Maßnahmen der Informationssicherheit eine Beeinträchtigung des sicheren Flugbetriebs vermieden werden, und wie können Gefahren beim Datenschutz und für ein verbundenes Netzwerk vermieden werden? Zu den Gefahren im Bereich Datenschutz zählen insbesondere die Datenerhebung für den Betrieb der Drohne, die Datenverarbeitung von Bilddaten aus der Luft und die Datensicherheit.

Die Gründe sich mit der Informationssicherheit beim Betrieb von UAS auseinanderzusetzen sind vielfältig. Die wichtigsten dürften sein, Personen- und Sachschäden durch mangelhafte Informationssicherheit zu vermeiden. Dieses IT-Grundschutz-Profil ist dazu geeignet, Prozesse, die für die gebräuchliche IT-Landschaft etabliert wurden, auf den Betrieb von UAS zu übertragen. Da, wo dies nicht möglich ist, wurden individuelle Bausteine entwickelt. Das IT-Grundschutz-Profil kann weiterhin als Element für eine Risikoanalyse zur Vorlage bei Luftfahrtbehörden dienen.

In Band 1 des Grundschutzprofils wird die UAS-Kategorie „Open“ (Offen) behandelt. Der hier vorliegende Band 2 ist analog aufgebaut, geht aber auf die Anforderungen der UAS-Kategorie

„Specific“ (Spezifisch) und die damit verbundenen Herausforderungen ein. In der Specific-Kategorie wird u.a. ein Betriebshandbuch auf Grundlage einer Risiko-Analyse nach EASA SORA (Specific Operations Risk Analysis) gefordert. Das hier mit Band 2 vorgelegte IT-Grundschutzprofil kann dazu einen Beitrag für den Bereich der IT- bzw. Cybersicherheit leisten.

Das Luftfahrtbundesamt (LBA) stellt für die vollständige Risikobewertung nach den Betriebsdetails auf Grundlage der DVO (EU) 2019/947 ein Entscheidungsschema zur Verfügung, das die Einordnung des Betriebs auf Basis mehrerer Kriterien unterstützt. Die nachfolgende Abbildung gibt einen Ausschnitt des Entscheidungsbaums wieder, der insbesondere die Unterscheidung offene Kategorie vs. Spezielle Kategorie adressiert. Die darin aufgeführten Kriterien finden sich im weiteren Verlauf als Unterkategorien der Geschäftsfälle wieder.

**Vollständige Risikobewertung nach den Betriebsdetails  
auf Grundlage der DVO (EU) 2019/947 (gültig ab 01.01.2024)**

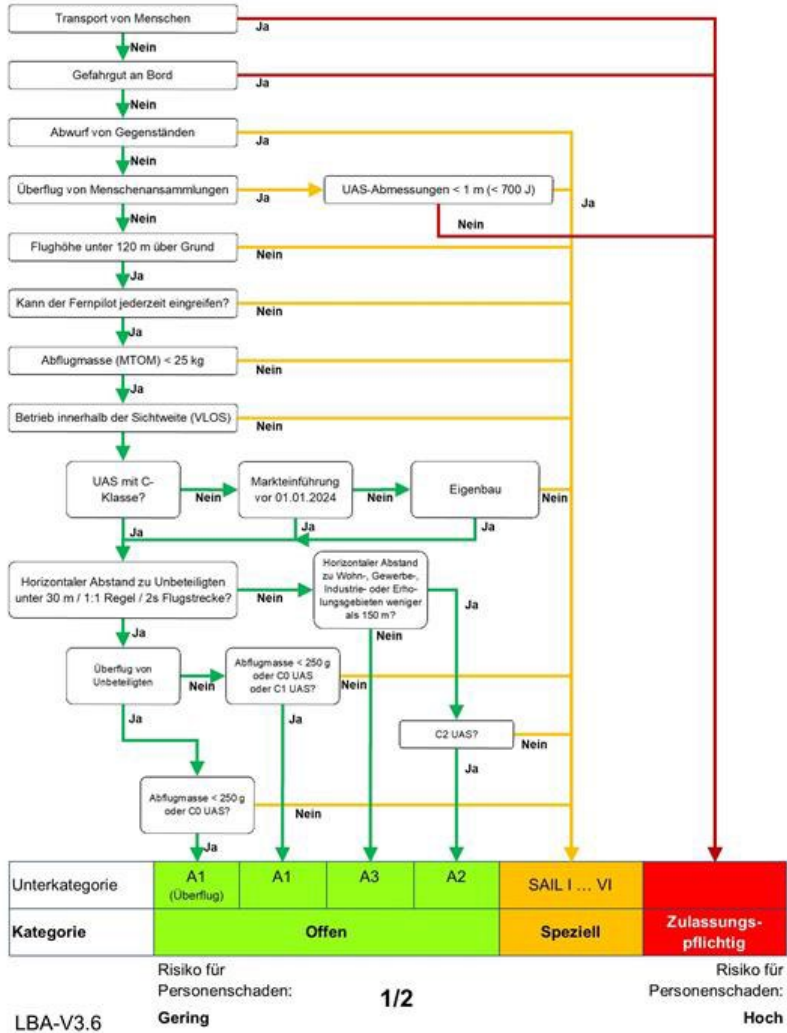


Abbildung 2: Risikobewertung für unterschiedliche Anwendungen in der Offenen versus der Speziellen Klasse ([https://www.lba.de/DE/Drohnen/Allgemeine\\_Informationen/Risikobewertung/Risikobewertung\\_node.html](https://www.lba.de/DE/Drohnen/Allgemeine_Informationen/Risikobewertung/Risikobewertung_node.html))

In Band I wurde ein IT-Grundschutzprofil für UAS der Kategorie "Offen" ("Open") vorgestellt. Die Kategorie „Offen“ ist im Wesentlichen durch risikoarme Anwendungen gekennzeichnet, – so können beispielsweise keine Gegenstände abgeworfen oder Menschenansammlungen dürfen nicht überflogen werden (siehe Abb. 1). Band 2 stellt ein IT-Grundschutzprofil für UAS in der Kategorie "Specific" mit höheren Anforderungen vor. Die Specific-Kategorie sieht mit den Standard-Szenarien (STS) relativ klar definierte Geschäftsprozesse wie auch weitere bislang nicht beschriebene Geschäftsprozesse vor. Beide Anwendungsfelder sind Gegenstand dieses IT-Grundschutzprofils. In der Specific-Kategorie wird u.a. ein Betriebshandbuch auf Grundlage einer Risiko-Analyse nach EASA SORA (Specific Operations Risk Analysis) gefordert.

## 1.1 Formale Aspekte

Aspekt	Beschreibung
<b>Titel</b>	IT-Grundschatz-Profil für den Betrieb von UAS Band 2: UAS-Betriebskategorie "speziell"
<b>Autorenschaft</b>	Jens Fehler (Mediator Consult GbR) Andreas J. Henke (UAV DACH) Marco Müller-ter Jung, LL.M. (Grant Thornton Rechtsanwaltsge- sellschaft mbH) Corinna Schmitt (Universität der Bundeswehr München) Burkhard Wrenger (Technische Hochschule Ostwestfalen-Lippe)
<b>Herausgeber</b>	UAV DACH e.V.
<b>Versionsstand</b>	1.0
<b>Revisionszyklus</b>	Es wird nach Freigabe der Version 1.0 eine zwei-jährliche Überprü- fung angestrebt.
<b>Vertraulichkeit</b>	Dieses Dokument darf in unveränderter Version weitergegeben werden.

## 1.2 Haftungsausschluss

Dieses Dokument wurde mit größter Sorgfalt erstellt, erhebt aber keinen Anspruch auf Vollständigkeit und Richtigkeit. Die Autorinnen haben keinen Einfluss auf die Nutzung dieses IT-Grundschatz-Profiles durch Anwenderinnen und Anwender und kennen auch nicht die individuellen Anforderungen an ihre Sicherheitskonzepte, sodass sie naturgemäß für die Auswirkungen auf die Rechtsposition der Parteien keine Haftung übernehmen können.

## 2. Management Summary

### 2.1 Zielgruppe

Dieses IT-Grundschutz-Profil richtet sich an alle Organisationen, Behörden und Unternehmen in denen UAS im Rahmen der Betriebskategorie „Specific“ (Speziell) zum Einsatz kommen. Es ist insbesondere gedacht für die Verantwortlichen in der Geschäftsleitung und der IT-Administration, sowie jene Fachbereiche, in denen UAS eingesetzt werden.

Nutzer von UAS-Diensten sollten das vorliegende IT-Grundschutz-Profil als Grundlage für die Auswahl und Beauftragung entsprechender Dienstleister verwenden mit den hier formulierten Anforderungen als Bestandteil der Vertragsbedingungen.

### 2.2 Zielsetzung

Das IT-Grundschutz-Profil definiert Anforderungen im Sinne des IT-Grundschutzes, um die Absicherung der verarbeiteten Daten hinsichtlich deren Vertraulichkeit, Integrität und Verfügbarkeit zu erreichen. Der Betrieb von UAS wird beispielhaft dargestellt durch die Prozesse

- GP1: Flugbetrieb in der Kategorie Speziell mit den Teilprozessen
  - Startvorbereitungen,
  - Start,
  - Flug,
  - Landung,
  - Außerbetriebnahme;
- GP2: Wartung und Instandsetzung für UAS in der Kategorie Speziell mit den Teilprozessen
  - Austausch oder Aktualisierung der mechanischen Antriebskomponenten,
  - Aktualisierung der Flugbetriebssoftware,
  - Aktualisierung aller weiteren Softwarekomponenten nach Herstellervorgabe,
  - Analyse der System-Dateien (Log-Dateien).

In Anlehnung an den oben in Abbildung 2 dargestellten Entscheidungsbaum wird der Geschäftsprozess GP1 wie folgt ausdifferenziert:

- GP1a: Flugbetrieb mit Abwurf von Gegenständen. Dieses kann beispielsweise das Ausbringen von Saatgut, Düngemittel oder Pflanzenschutzmittel durch ein UAS sein.
- GP1b: Flugbetrieb mit Überflug von Menschenansammlungen, beispielsweise für Luftbildaufnahmen im Rahmen von Konzerten oder Sportveranstaltungen.
- GP1c: Flugbetrieb mit Flughöhen auch oberhalb von 120 m über Grund, beispielsweise für meteorologische Messungen und andere Formen des Umweltmonitorings.
- GP1d: Komplett automatisierter Flugbetrieb ohne Einwirkungsmöglichkeit durch den Fernpiloten.
- GP1e: Flugbetrieb mit einer Abflugmasse des UAS von 25 kg und mehr wie er bei Logistik-Aufgaben oder in der Landwirtschaft auftreten kann.
- GP1f: Flugbetrieb mit Entfernungen, die nicht mehr innerhalb der Sichtweite und Sichtlinie liegen. Dieses kann bei Befliegungen zu Dokumentationszwecken (Landwirtschaft, Forstwirtschaft, Vermessung) oder Infrastrukturinspektionen auftreten.

Der Geschäftsprozess GP2 kann analog ausdifferenziert werden.

### 2.3 Aufgaben der Leitungsebene

Die Anwendung dieses IT-Grundschutz-Profiles im Rahmen des Flugbetriebes mit UAS ist Teil einer Sicherheitskonzeption und kann als Element der Zulassung oder Genehmigung von Luftfahrtbetrieben nach den einschlägigen Richtlinien und Bestimmungen dienen.

Die Autorinnen empfehlen, dass Organisationen, die UAS-Dienste in Anspruch nehmen wollen, das vorliegende IT-Grundschutz-Profil Bd. 2 als Grundlage für die Beauftragung entsprechender Dienstleister verwenden. Die hier formulierten Anforderungen sollten in geeigneter Form in den Vertragsbedingungen enthalten sein.

### 3. Festlegung des Geltungsbereichs

Die in diesem IT-Grundschutz-Profil aufgeführten Anforderungen sind Empfehlungen des UAV DACH e.V. für UAS-Betreiber.

Die Geschäftsprozesse GP1 und GP2 werden in der speziellen Kategorie mit einem erweiteren Betriebsspektrum und damit einem höheren Risikoprofil betrieben. So kann in der speziellen Kategorie u.A. ein Betrieb außerhalb der Sicht (BVLOS) in Betracht gezogen werden, ein Abwurf von Gegenständen oder ein Überflug von Menschenansammlungen. Daraus resultieren höhere Anforderungen an die Absicherung der Informationssicherheit wie der Telemetrie- und Datenverbindungen.

Die Geschäftsprozesse GP1 und GP2 können beispielsweise einen Betrieb außerhalb der Sicht (BVLOS) beinhalten. Damit ist ein direktes Eingreifen während des Fluges nicht durchgängig möglich und sowohl die Überwachung des Systemzustands bzw. Betriebs wie auch die Steuerung des UAS erfordern eine elektronische Kommunikation. Diese ist damit ein wesentlicher und sensibler Bestandteil der Betriebssicherheit. Zusätzlich können sich aus besonderen Einsatzszenarien bzw. Fluggebieten erhöhte Schutzanforderungen ergeben. Bei der hierfür geforderten Risikoanalyse ist das vorliegende IT-Grundschutzprofil zu berücksichtigen.

Risikoanalysen hier beziehen sich auf IT und gehen dann aber in die Risikoanalysen bzw. -minderungen der Geschäftsprozesse ein.

Die Umsetzung des IT-Grundschutzes deckt die Anforderungen der "Standard-Absicherung" der BSI-Standards 200-2 und 200-3 ab. Die Umsetzung der Standard-Absicherung ist kompatibel zur ISO 27001. Die in diesem IT-Grundschutz-Profil dargestellten Anforderungen berücksichtigen zusätzlich Teile der Vorgaben der DSGVO, des BDSG, des TTDSG, des TMG, insbesondere § 13 TMG, und für U-Space-Service-Provider zusätzlich den Anhang III der Durchführungsverordnung 2021/664 für den U-Space.

Es wird darauf hingewiesen, dass zum Zeitpunkt der Veröffentlichung dieses IT-Grundschutz-Profiles sämtliche EU-Cybersecurity-Zertifikate von ENISA (vgl. Art. 8, 48 ff der Verordnung EU 2019/881 (Cybersecurity Act)) noch immer im Aufbau sind. Dieses IT-Grundschutz-Profil ist

daher auf eine Selbstimplementierung und bei Verfügbarkeit der Zertifikate auf eine Selbstbewertung der Konformität durch den Hersteller oder Betreiber des UAS ausgelegt. Daher wäre im Rahmen der Einstufung Vertrauenswürdigkeit nach den europäischen Schemata<sup>1</sup> der ENISA gem. Art. 53 des Cybersecurity Acts höchstens eine Erreichung der Vertrauenswürdigkeitsstufe „niedrig“ möglich. Für die weiteren Stufen „mittel“ und „hoch“ wären hingegen Prüfungen durch akkreditierte unabhängige Dritte erforderlich.

---

1 Drohnen dürften nach Art. 2 Nr. 12 Cybersecurity Act als ein **IKT-Produkt** einzustufen sein, jedenfalls aber – je nach Bauart der Drohne – die verbauten Komponenten (Video- und Fotokamera, Mikrofone, Netzwerkverbindung zu U-Space-Service-Providern, etc.). Es gilt das Schema „**Cybersecurity Certification: EUCC Scheme V1.1.1**“ (im Aufbau), das IKT-Produkte behandelt, zu beachten. Ferner ist ggf. das Schema „**EUCS – Cloud Services Scheme**“ zu beachten, sofern U-Space-Service-Provider als Cloud-Dienstleister i.S.d Art. 2 Nr. 13 Cybersecurity Act anzusehen sind.

## 4. Abgrenzung Informationsverbund

### 4.1 Bestandteile des Informationsverbunds

Zum Informationsverbund gehören alle Komponenten und Verfahren bei einem UAS-Betreiber, die für die Durchführung des Flugbetriebs einschließlich Wartung und Instandsetzung notwendig sind (siehe Referenzarchitektur, siehe Ziffer 5.).

### 4.2 Nicht berücksichtigte Objekte

Nicht berücksichtigt werden Komponenten, die nicht unmittelbar mit dem Flugbetrieb zusammenhängen, sowie Verfahren, die über den Flugbetrieb hinausgehen, wie z.B. Auftragswesen, Rechnungsstellung, usw.

### 4.3 Verweis auf andere IT-Grundschutz-Profile

Neben dem vorliegenden IT-Grundschutz-Profil wurde in dieser Reihe der Band „IT-Grundschutz-Profil für den Betrieb von UAS Band 1: UAS-Betriebskategorie „Offen“ publiziert. Der Band 3 „UAS Betriebskategorie „Zertifiziert“ ist noch in Erstellung. Parallel dazu werden IT-Grundschutz-Profile für BOS-relevante Einsatzszenarien erstellt.

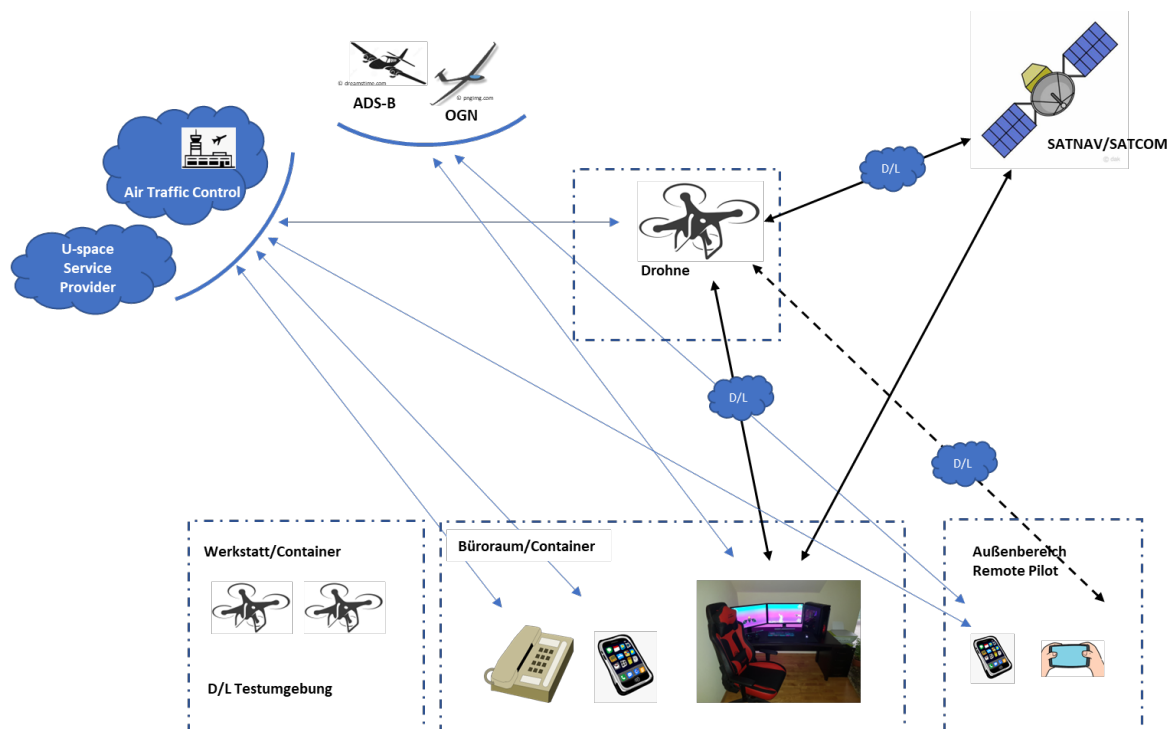


Abbildung 3: Informationsverbund eines UAS.

Im Bild dargestellt ist das UAS mit den möglichen direkten und indirekten Datenverbindungen des UAV zur Bodenstation bzw. zum Remote Pilot sowie zur Luftraumkoordination („Air Traffic Control“ bzw. „U-Space Service Provider“). Zudem sind die weiteren Teilnehmer:innen des Luftraums sowie die von ihnen genutzten Informationskanäle (ADS-B, OGN) aufgeführt. Für den Geschäftsprozess GP2 ist zudem am Boden die Lokation „Werkstatt/Container“ zu berücksichtigen.

## 5. Referenzarchitektur

Der vom IT-Grundschutz-Profil betrachtete Informationsverbund beinhaltet alle wesentlichen mobilen und stationären Objekte des UAS, die für den Betrieb im Rahmen der nachfolgend dargestellten Geschäftsprozesse essenziell sind. Eine schematische Darstellung des Informationsverbunds ist Abbildung 3 zu entnehmen. Der Schutzbedarf bezieht sich auf Gebäude und Räume, Computernetze und Kommunikation, IT-Systeme und Geschäftsprozesse/Anwendungen. Es findet eine Kommunikation zwischen unterschiedlichen Endgeräten statt, beispielsweise Desktop-Rechner, Laptops, Tablet sowie Steuerrechnern. Dafür werden unterschiedliche Kommunikationsverfahren verwendet. Die Sicherheitsanforderungen sind von jeder Institution individuell zu prüfen. Gegenüber der Kategorie „Open“ ist zu beachten, dass den Kommunikationsverbindungen eine deutlich höhere Relevanz zukommt, da eine visuelle Rückmeldung zu Status und Aktivitäten des UAS entfällt.

### 5.1 Geschäftsprozesse und Anwendungen

Das betrachtete IT-Grundschutz-Profil bezieht sich auf die Geschäftsprozesse mit dem erhöhten Risikoprofil der speziellen Klasse:

- GP1: Flugbetrieb mit den Spezialisierungen GP1a bis GP1f, siehe Kap. 2.2.
- GP2: Wartung und Instandsetzung für die unterschiedlichen Varianten von GP1

Die hier beschriebenen Geschäftsprozesse dienen zur Veranschaulichung der unterschiedlichen Teilaspekte und Relevanz der Schutzziele im operativen Kontext. Sie können durch die konkreten Geschäftsprozesse der Organisation ersetzt oder konkretisiert werden.

GP1 beinhaltet die Inbetriebnahme des UAS, dessen Start, den Flug, die Landung, die anschließende Außerbetriebnahme, sowie mit dem Flug unmittelbar verbundene Tätigkeiten wie z.B. die Flugvorbereitung.

Für GP1 sind daher der Aufbau des UAS am Startort oder in dessen Nähe, die vor dem Start durchzuführenden mechanischen, elektrischen und elektronischen Tests und Selbsttests, die kommunikationstechnische Verbindung zwischen den Teilkomponenten des UAS wesentlich. Nach dem Start sind weitere Tests des UAS und seiner Nutzlast, die automatische oder manuelle Überwachung des Flugkorridors und des Systemzustands sowie des Flugfortschritts zu berücksichtigen. Nach der Landung erfolgen weitere (Selbst-)Tests, die Dokumentation und

Sicherung der Flugdaten sowie mechanische und elektronische Tests. Zudem sind ggf. Nutzlastdaten zu sichern.

GP2 beinhaltet alle Wartungs- und Instandsetzungsarbeiten, die durchgeführt werden müssen, um die Betriebssicherheit aufrechtzuerhalten.

GP2 beinhaltet alle Teilprozesse, die zwischen den Flügen des UAS durchzuführen sind, um die Betriebssicherheit zu erhalten. Dazu gehören die Prüfung und bei Bedarf Instandsetzung, der Austausch von informationsverarbeitenden Komponenten, die Aktualisierung der Flugbetriebssoftware, z.B. der Firmware oder Systemsoftware des zentralen Steuerrechners im UAS, sowie die Aktualisierung aller weiteren Softwarekomponenten nach Herstellervorgabe. Einige dieser Aufgaben sind nach bzw. vor jedem Flug durchzuführen, für andere gelten spezifische Vorgaben des Herstellers.

Zum Informationsverbund gehören neben den Geschäftsprozessen GP1 und GP2 weitere Anwendungen, mit denen die zu erledigenden Aufgaben unterstützt werden.

Die nachfolgende Tabelle gibt einen Überblick über die typischen Anwendungen des Informationsverbundes.

Tabelle 1: Typische Anwendungen im Informationsverbund (zur Anwendung der Grundschatz Bausteine siehe auch Tabelle 6)

A01	Flugplanungssoftware
A02	Kartensoftware
A03	Wartungssoftware
A04	Flight-Control-Software
A05	Ground-Control-Software
A06	Logbuch/Flight-Data-Recorder
A07	Payload-Steuerung
A08	Steuerung Zusatzaufgaben
A09	Configuration-Management-Software
A10	Cloud-Schnittstellen (Infrastructure as a Service/IaaS, Platform as a Service/PaaS, Service as a Service/SaaS)

## 5.2 IT-Systeme

Im Informationsverbund sind neben den Geschäftsprozessen und Anwendungen auch die IT-Systeme zu betrachten.

Die nachfolgende Tabelle gibt eine Übersicht über die typischen IT-Systeme im Informationsverbund.

Tabelle 2: Typische IT-Systeme im Informationsverbund (zur Anwendung der Grundschutz Bausteine siehe auch Tabelle 6)

C01	Desktoprechner
C02	Laptop
C03	Tablet oder Smartphone
S01	Server
S02	Cloud-Server
S03	Cloud-Speicher
D01	Flight-Controller
D02	Companion-Computer

### 5.3 Netze und Netzkomponenten

Der Informationsverbund ist durch heterogene Netzwerke gekennzeichnet. Neben kabelgebundenen Netzen kommen Funknetze wie WLAN/IEEE 802.11 für die lokale Kommunikation, Mobilfunkstandards, IEEE 802.15.4 und spezifische Long-Range- und Satellitenkommunikationsverbindungen für die Kommunikation zwischen der Drohne in der Luft und der kontrollierenden Bodenstation zum Einsatz. Im Einzelnen sind dies in der Regel die Datenverbindung zwischen der Drohne und der Bodenkontrollstation (Telemetrie und Fernsteuerung/Controller), Verbindungen zwischen der Drohne und anderen Luftfahrzeugen (ADS-B, OGN) und/oder Verbindungen zwischen der Bodenkontrollstation und anderen Luftverkehrsteilnehmern bzw. Kontroll- und Managementinstitutionen (USSP, ANSP etc), siehe auch Abb. 2.

Die folgende Tabelle gibt einen Überblick über die typischen Netzwerkkomponenten im Informationsverbund.

Tabelle 3: Netzwerkkomponenten (zur Anwendung der Grundschutz Bausteine siehe auch Tabelle 6)

NET01	Aktive Komponenten kabelgebundenes Organisationsnetzwerk
NET02	Aktive Komponenten drahtloses Organisationsnetzwerk
NET03	Schnittstelle zwischen Organisations- und Datennetzwerk
NET04	On-board-Netzwerk der Drohne

NET05	Aktive Komponenten der Verbindung Drohne zu Bodenkontrollstation
NET06	Aktive Komponenten der Verbindung Drohnen und/oder Bodenkontrollstation zu Kontroll- und Managementinstitutionen
NET07	Cloudimport-/exportschnittstelle, Datenmodem

## 5.4 Infrastruktur: Räume und Gebäude

Komponenten des Informationsverbundes können in einem Gebäude, in einem Fahrzeug (dazu sogleich unter Kapitel 5.5), außerhalb von Gebäuden oder Fahrzeugen und in der Drohne untergebracht sein. Diese Infrastrukturbestandteile sind aus Sicht der Informationssicherheit ggf. unterschiedlich zu behandeln. Daher erfolgt hier und im nächsten Unterkapitel eine Differenzierung zwischen mobilen und stationären Infrastrukturobjekten.

Die nachfolgende Tabelle gibt einen Überblick über die typischen stationären Infrastrukturkomponenten im Informationsverbund.

Tabelle 4: Typische Infrastrukturkomponenten im Informationsverbund (zur Anwendung der Grundschatz Bausteine siehe auch Tabelle 6)

R01	Allgemeiner Raum, zugangskontrolliert
R02	Leitstand/Bodenkontrollstation
R03	Halle, Werkstattbereich
R04	Labor
R05	Serverraum
R06	Außenbereich, zugangskontrolliert
R07	Flugtest- und Demonstrationsfläche
R08	Öffentlicher Raum

Die Cloud-basierten Systeme sind hier nicht Gegenstand der Betrachtung, da sie außerhalb der Systemgrenzen/dem Informationsverbund liegen. Gleiches gilt für den USSP-Bereich.

## 5.5 Infrastruktur: Fahrzeuge

Die UAS werden üblicherweise nicht am Sitz des UAS-Betreibers betrieben. Im Regelfall ist also der Transport von UAS zu berücksichtigen.

Die nachfolgende Tabelle gibt einen Überblick über die typischen mobilen Infrastrukturkomponenten im Informationsverbund.

Tabelle 5: Typische mobile Infrastrukturkomponenten im Informationsverbund (zur Anwendung der Grundschatz Bausteine siehe auch Tabelle 6)

F01	Transportfahrzeug für UA bzw. UAS
F02	Operation Vehicle
UA01	Uncrewed Aircraft/Drohne

In vielen Fällen sind F01 und F02 identisch, d.h. Transport und Betriebsunterstützung erfolgen in einem Fahrzeug.

## 5.6 Umgang mit Abweichungen

Weicht der zu schützende Informationsverbund von der in diesem Kapitel dargestellten Referenzarchitektur ab, so sind die zusätzlich vorhandenen Zielobjekte im Rahmen der Strukturanalyse zu dokumentieren. Diesen Zielobjekten müssen passende Komponenten des IT-Grundschatz-Kompodiums zugeordnet werden.

Zielobjekte aus diesem IT-Grundschatz-Profil, die im zu schützenden Informationsverbund nicht vorkommen, brauchen entsprechend nicht berücksichtigt zu werden.

## 5.7 Komponenten in Beziehung zu den Zielobjekten im Informationsverbund

Die folgende Tabelle ordnet die Komponenten den Zielobjekten im Informationsverbund zu. Diese Beziehung stellt den Rahmen für die Auswahl der relevanten Bausteine für die jeweilige Organisation dar, die das IT-Grundschatz-Profil anwendet.

Tabelle 6: Anzuwendende Bausteine

Komponente	Anzuwenden auf Zielobjekt
A01 Flugplanungssoftware	GP1
A02 Kartensoftware	GP1
A03 Wartungssoftware	GP2
A04 Flight-Control-Software	GP1
A05 Ground-Control-Software	GP1
A06 Flight-Data-Recorder	GP1
A07 Payload-Steuerung	GP1
A08 Steuerung Zusatzaufgaben	GP1
A09 Configuration-Management-Software	GP2

C01 Desktoprechner	A01, A03, A05, A07, A08, A09
C02 Laptop	A01, A03, A05, A07, A08, A09
C03 Tablet	A01, A03, A05, A07, A08, A09
S01 Server	A02
S02 Cloud-Server	A01, A02, A04, A05, A09, A10
S03 Cloud-Speicher	A07, A08, A09, A10,
D01 Flight-Controller	A04
D02 Companion-Computer	A07, A08
NET01 Kabelgebundenes Netzwerk	C01, C02, S01
NET02 Drahtloses Netzwerk	C01, C02, C03
NET03 Schnittstellen Nw/Datennw.	C01, C02, C03, S01, D01, D02
NET04 On-board-Netzwerk	D01, D02
NET05 Drohne Bodenkontrollstation	C01, C02, C03, D01, D02
NET06 Aktive Komponenten der Verbindung UAS und/oder Bodenkontrollstation zu Kontroll- und Managementinstitutionen	C01, C02, C03, S01, D01, D02
NET07 Cloudimport-/exportschnittstelle, Datenmodem	A10
R01 Allgemeiner Raum, zugangskontrolliert	C01, C02, C03, NET01, NET03
R02 Leitstand/Bodenkontrollstation	C01, C02, C03
R03 Halle, Werkstattbereich	C01, C02, C03, D01, D02
R04 Labor	C01, C02, C03, D01, D02
R05 Serverraum	S01
R06 Außenbereich, zugangskontrolliert	C02, C03, D01, D02
R07 Flugtest- und Demonstrationsfläche	C02, C03, D01, D02
R08 Öffentlicher Raum	C02, C03, D01, D02
F01 Transportfahrzeug	D01, D02
F02 Operation Vehicle	C01, C02, C03, S01
UA01 Uncrewed Aircraft	D01, D02

## 6. Feststellung des Schutzbedarfs

Für die im Rahmen der Strukturanalyse ermittelten Prozesse, Anwendungen, IT- und Kommunikationssysteme sowie Infrastrukturkomponenten ist zunächst der Schutzbedarf festzulegen. Grundlage dafür sind die Auswirkungen, die Verletzungen der Grundwerte der Informationssicherheitsaspekte *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* hätten. Geeignete Ansprechpartner für die Schutzbedarfsfeststellung sind beispielsweise die jeweiligen Prozessverantwortlichen oder der Dateneigentümer der im jeweiligen Prozess verarbeiteten Daten. Der Schutzbedarf richtet grundsätzlich sich nach dem Umfang aller Daten, die in den Prozessen verarbeitet werden. Die Vorgehensweise bei der Feststellung des Schutzbedarfes ist im BSI-Standard 200-2 (siehe Kapitel 8.2) im Detail beschrieben. Der IT-Grundschutz benennt verschiedene Szenarien, auf die sich ein Schaden beziehen kann. Diese sind in der folgenden Tabelle aufgeführt:

Tabelle 7: Potenzielle Schadensszenarien

Identifikator	Schadensszenario
SZ1	Verstöße gegen Gesetze, Vorschriften oder Verträge
SZ2	Beeinträchtigungen des informellen Selbstbestimmungsrechts
SZ3	Beeinträchtigungen der persönlichen Unversehrtheit
SZ4	Beeinträchtigungen der Aufgabenerfüllung
SZ5	Negative Innen- oder Außenwirkung
SZ6	Finanzielle Auswirkungen

Die konkreten Auswirkungen und möglichen Schadensszenarien können je nach Anwendungsfall variieren. In der nachfolgenden Tabelle sind mögliche Beispiele zu den Schadensszenarien aufgeführt:

Tabelle 8: Beispiele von Schadensszenarien

Identifikator	Beispiele für Schadensszenarien
SZ1	Veränderte oder unvollständige Daten können zu Verstößen gegen Gesetze und Vorschriften (beispielsweise Flug innerhalb eines nicht erlaubten Fluggebietes) oder Verstößen gegen Verträge mit Geschäftspartnerinnen (beispielsweise Videoaufzeichnung nicht im vereinbarten Fluggebiet) führen.

SZ2	<p>Personenbezogene Daten von Mitarbeiterinnen oder Geschäftspartnerinnen oder sensible Unternehmensdaten werden ohne Autorisierung öffentlich oder unbefugten Dritten zugänglich.</p> <p>Unternehmenskritische bzw. -vertrauliche Daten werden ohne Autorisierung öffentlich oder unbefugten Dritten zugänglich. Dieses kann zu finanziellen Nachteilen führen.</p>
SZ3	<p>Eine unvollständige oder fehlerhafte Datenübertragung oder die Übertragung schädlich veränderter Daten führt zur Fehlsteuerung des UAS, zu falschen Entscheidungen im Prozessablauf (Flugbetrieb oder Wartung/Instandsetzung) und in Folge zu Unfällen mit Personenschäden.</p>
SZ4	<p>Eine unvollständige oder schädlich veränderte Datenübertragung führt zu einem Abbruch des Flugbetriebs (GP1), der Videoaufzeichnung (GP1) oder zu einer fehlerhaften Wartung bzw. Instandsetzung des UAS (GP2) und damit zu einer eingeschränkten oder ausgefallenen Aufgabenerfüllung.</p> <p>Ein nicht- oder nur eingeschränkt verfügbares Teil des Informationsverbundes führt zu einem Abbruch des Flugbetriebs oder zu einer Beendigung der Videoaufzeichnung und damit zu einer eingeschränkten Aufgabenerfüllung.</p>
SZ5	<p>Ein eingeschränkter oder abgebrochener Flugbetrieb (GP1) bzw. eine unvollständige Videoaufzeichnung (GP1) führen zu Imageschäden und Vertrauensverlust.</p> <p>Eine unvollständige oder fehlerhafte Wartung und Instandsetzung führt zu Imageschäden und Vertrauensverlust.</p>
SZ6	<p>Ein unvollständiger Flugbetrieb (GP1) bzw. eine unvollständige Videoaufzeichnung (GP1) führt zu Dienstleistungs- oder Prozessausfällen bzw. Kosten für die erneute Durchführung des Prozesses.</p> <p>Ein fehlerhafter Flugbetrieb mit Schadensfolge führt zu zusätzlichen Kosten.</p> <p>Eine fehlerhafte oder unvollständige Wartung und Instandsetzung führen zu zusätzlichen Material- und Personalkosten.</p>

Die Auswirkung eines Schadens ist im Voraus nicht bestimmbar. Daher empfiehlt die Methodik des IT-Grundschutzes des BSI die Klassifizierung in die drei Kategorien *normal*, *hoch* und *sehr hoch* im Zusammenhang mit der Schutzbedarfsermittlung. In der folgenden Tabelle sind die Kategorien, ergänzt um die generischen Schadensauswirkungen aufgeführt. Die Auswirkungen können sich auf Komponenten, das Unternehmen oder betroffene Dritte beziehen:

Tabelle 9: Vom BSI empfohlene Schutzbedarfskategorien

Kategorie	Schadensauswirkung
normal	Die Schadensauswirkungen sind begrenzt und überschaubar.
hoch	Die Schadensauswirkungen können beträchtlich sein.

sehr hoch	Die Schadensauswirkungen können ein existenziell- oder lebensbedrohliches Ausmaß erreichen.
-----------	---

Werden in einem Schadensszenario beträchtliche, existenzbedrohende oder lebensbedrohliche Auswirkungen festgestellt, so ist der betroffene Grundwert im Schutzbedarf mit hoch oder sehr hoch einzustufen, in allen anderen Fällen mit normal. Im Weiteren wird der ermittelte Schutzbedarf je Grundwert auf die Schicht der Anwendungen vererbt, anschließend in weiteren Schritten auf die IT-Systeme, auf die Netze, die Räumlichkeiten und Infrastrukturobjekte.

## 6.1 Risikobetrachtung

Auch bei Umsetzung aller Anforderungen ist keine hundertprozentige Sicherheit zu erreichen. Dies muss sowohl den Anwendern des IT-Grundschutz-Profiles als auch den Entscheidungsträgern bewusst sein. Aufgrund der Besonderheiten beim Flugbetrieb mit Drohnen ist in jedem Fall eine Risikoanalyse zu erstellen.

Insbesondere für die Zielobjekte UAV und Bodenkontrollstation gibt es im IT-Grundschutz-Kompendium keine passenden Bausteine, sodass bis auf Weiteres eine Risikoanalyse zwingend erforderlich ist. Es wird das Vorgehen der Risikoanalyse nach dem BSI-Standard 200-3 empfohlen. In diesem BSI-Standard werden 47 elementare Gefährdungen aufgeführt, die im IT-Grundschutz-Kompendium näher erläutert werden. Diese Gefährdungen sollten dabei Ausgangspunkt für die Erstellung der Gefährdungsübersicht sein und bei Bedarf ergänzt werden. Um sicher zu stellen, dass im Rahmen der Risikoanalyse definierte höherwertige Sicherheitsmaßnahmen auch auf Objekte mit normalen Schutzbedarf Anwendung finden können sollten im Rahmen der Risikoanalyse folgende Schritte durchlaufen werden:

1. Erstellen einer Gefährdungsübersicht,
2. Vornehmen einer Risikoeinschätzung,
3. Festlegung der Risikobehandlung und
4. Konsolidierung der erweiterten Sicherheitsmaßnahmen mit den Ergebnissen des IT-Grundschutz-Checks.

Dabei ist zu berücksichtigen, dass Aspekte der Flugsicherheit (engl. Flight Safety) im Rahmen des Flugsicherheitsmanagements separat betrachtet werden. Sie sind daher nicht Bestandteil

dieses IT-Grundschatz-Profiles, welches die Informationssicherheit im Blick hat (engl. Information Security).

## 1.1 Zu berucksichtigende Gefahrdungen

Als Grundlage fur die Ermittlung des Gefahrdungspotentials der Komponente, fur die dieses IT-Grundschatz-Profil angewendet wird, dient folgende Tabelle:

Tabelle 10: Gefahrdungsmatrix

*Verweis: siehe externe Tabelle 10*

## 7. Zu erfüllende Anforderungen und umzusetzende Maßnahmen

Das IT-Grundschutz-Kompendium des BSI stellt Prozess- und Systembausteine bereit, die anwendungsbezogene Anforderungen zur Umsetzung des IT-Grundschutzes vorgeben.

### 7.1 Auswahl relevanter Bausteine

#### 7.1.1 Auswahl der Prozessbausteine

Auf jeden Informationsverbund sind die übergreifenden Prozess-Bausteine anzuwenden. Diese behandeln Sicherheitsaspekte, die für große Teile des Informationsverbundes gleichermaßen gelten.

Tabelle 11 Prozessbausteine und Anwendungskriterien

ID	Baustein	relevant	Begründung (falls nicht relevant)
<i>ISMS:</i>	<i>Sicherheitsmanagement</i>		
ISMS.1	Sicherheitsmanagement	ja	
<i>ORP:</i>	<i>Organisation und Personal</i>		
ORP.1	Organisation	ja	
ORP.2	Personal	ja	
ORP.3	Sensibilisierung und Schulung zur Informationssicherheit	ja	
ORP.4	Identitäts- und Berechtigungsmanagement	ja	
ORP.5	Compliance Management	ja	
<i>CON:</i>	<i>Konzeption und Vorgehensweise</i>		
CON.1	Kryptokonzept	Ja	Im Rahmen der Beschaffung, durch CE Verfahren definiert
CON.2	Datenschutz	ja	
CON.3	Datensicherungskonzept	ja	
CON.4			
CON.5			
CON.6	Löschen und Vernichten	ja	Durch Hersteller im Rahmen CE Verfahren
CON.7	Informationssicherheit auf Auslandsreisen	nein	Nicht im Betrachtungsbereich; konzeptionell irrelevant

CON.8	Software-Entwicklung	nein	Keine Software-Entwicklung im Informationsverbund
CON.9	Informationsaustausch	ja	
CON.10	Entwicklung von Webanwendungen	nein	Keine Entwicklung von Webanwendungen im Informationsverbund
<i>OPS:</i>	<i>Betrieb</i>		
OPS.1.1.1			
OPS.1.1.2	Ordnungsgemäße IT-Administration	ja	
OPS.1.1.3	Patch- und Änderungsmanagement	ja	
OPS.1.1.4	Schutz vor Schadprogrammen	ja	
OPS.1.1.5	Protokollierung	ja	
OPS.1.1.6	Software-Tests und Freigaben	ja	Eingeschränkt gem. Herstellervorgaben
OPS.1.1.7	Systemmanagement	ja	
OPS.1.2.1			
OPS.1.2.2	Archivierung	ja	
OPS.1.2.3			
OPS.1.2.4	Telearbeit	nein	nicht anwendbar
OPS.1.2.5	Fernwartung	ja	Eingeschränkt gem. Herstellerangaben
OPS.1.2.6	NTP-Zeitsynchronisation	ja	
OPS.2.1	Outsourcing für Kunden	nein	Hier nicht betrachtet, konzeptionell irrelevant
OPS.2.2	Cloud-Nutzung	ja	(je nach Konfiguration)
OPS.3.1	Outsourcing für Dienstleister	ja	(je nach Anwendungsszenario)
<i>DER:</i>	<i>Detektion und Reaktion</i>		
DER.1	Detektion von sicherheitsrelevanten Ereignissen	ja	
DER.2.1	Behandlung von Sicherheitsvorfällen	ja	
DER.2.2	Vorsorge für die IT-Forensik	ja	Flugsicherheit/Flugunfalluntersuchung
DER.2.3	Bereinigung weitreichender Sicherheitsvorfälle	ja	
DER.3.1	Audits und Revisionen	nein	Hersteller
DER.3.2	Revision auf Basis des Leitfadens IS.Revision	nein	Nur für Bundesbehörden vorgeschrieben
DER.4	Notfallmanagement	ja	In Verbindung mit Hersteller

## 7.1.2 Auswahl der System-Bausteine

In den folgenden Tabellen werden die System-Bausteine aufgeführt. Hier ist entscheidend, ob der jeweilige Baustein für eine spezifische Komponente des hier betrachteten Informationsverbunds relevant ist.

Tabelle 12 Systembausteine und Auswahlkriterien

ID	Baustein	Zielobjekte	relevant	ggf. Begründung
<i>APP:</i>	<i>Anwendungen</i>			
APP.1.1	Office-Produkte		nein	nicht Teil des Informationsverbundes
APP.1.2	Web-Browser	C01, C02, C03, S01	Ja (ggf.)	
APP.1.4	Mobile Anwendungen		Ja (ggf.)	
APP.2.1	Allg. Verzeichnisdienst		Ja (ggf.)	
APP.3.1	Webanwendungen		ja (ggf.)	
APP.3.2	Webserver		ja	
APP.3.3	Fileserver	C01, C02, C03	ja	
APP.3.4	DNS-Server		nein	nicht Teil des Informationsverbundes
APP.4.2	SAP-ERP-System		nein	nicht Teil des Informationsverbundes
APP.4.3	Relationale Datenbanksysteme		nein	nicht Teil des Informationsverbundes
APP.4.6	SAP-ABAP-Programmierung		nein	nicht Teil des Informationsverbundes
APP.5.2	Microsoft Exchange und Outlook		nein	nicht Teil des Informationsverbundes
APP.5.3	Allgemeiner E-Mail-Client und – Server		nein	nicht Teil des Informationsverbundes

APP.6	Allgemeine Software		Ja	
APP.7	Entwicklung von Individualsoftware		nein	Es findet keine Entwicklung von Software im Informationsverbund statt.
<i>SYS:</i>	<i>IT-Systeme</i>			
SYS.1.1	Allgemeine Server	S01	ja	
SYS.2.1	Allgemeiner Client	C01		
SYS.3.1	Laptops	C02, C03		
SYS.4.3	Eingebettete Systeme	D01, D02		
SYS.4.4	Allgemeines IoT-Gerät			
<i>IND:</i>	<i>Industrielle IT</i>			
IND.2.3	Sensoren und Aktoren			
<i>NET:</i>	<i>Netze und Kommunikation</i>			
NET.1.1	Netzarchitektur und -design			
NET.1.2	Netzmanagement			
NET.2.1	WLAN-Betrieb			
NET.2.2	WLAN-Nutzung			
NET.3.1	Router und Switches			
NET.3.2	Firewall			
NET.3.3	VPN			
NET.3.4	Network Access Control			
NET.4.1	TK-Anlagen			
NET.4.2	VoIP			
NET.4.3	Faxgeräte und Faxserver			
<i>INF:</i>	<i>Infrastruktur</i>			
INF.1	Allgemeines Gebäude			

INF.2	Rechenzentrum sowie Server- raum			
INF.4	IT-Verkabelung			
INF 5	Server- raum/Technik- raum			
INF.6	Datenträgerar- chiv			
INF 7	Büroarbeitsplatz			
INF.8	Häuslicher Ar- beitsplatz			
INF.9	Mobiler Arbeits- platz			
INF.10	Besprechungs-, Veranstaltungs- und Schulungs- raum			
INF.11	Allgemeines Fahrzeug			
INF.12	Verkabelung			
INF.13	Technisches Ge- bäudemanage- ment			
INF.14	Gebäudeauto- mation			

## 7. 2 Zugangskontrollen

Daten unterliegen u. U. Regularien, so dass man gewährleisten muss, dass der Zugriff entsprechend limitiert ist und dokumentierbar sein muss. Gleichzeitig sollte eine leichte Pflege ermöglicht werden. Die hier oft umgesetzten Modelle sind IBAC, RBAC und ABAC oder hybride Varianten dieser 3 Modelle.

## 8. Restrisikobetrachtung

Der Flugbetrieb mit unbemannten Luftfahrzeugen der Kategorie „Specific“ erfordert derzeit bei Einhaltung der Grundsätze dieses IT-Grundschutz-Profiles keine allgemeine Restrisikobetrachtung über die SORA<sup>2</sup> hinaus.

---

2 <https://www.easa.europa.eu/en/domains/drones-air-mobility/operating-drone/specific-category-civil-drones/specific-operations-risk-assessment-sora>

## 9. Anwendungshinweise

Die ermittelten Anforderungen sind in das Gesamtsicherheitskonzept zu integrieren und umzusetzen. Dazu hat sich der PDCA-Zyklus (Plan, Do, Check, Act) bewährt, d.h. ein sich wiederholender Prozess der Planung, Umsetzung, Überprüfung und Anpassung, um kontinuierlich das gewünschte Sicherheitsniveau aufrecht erhalten zu können. Zudem wird die Einführung eines neuen bzw. die Erweiterung eines bestehenden Managementsystems empfohlen, um die Arbeiten des PDCA-Zyklus zu systematisieren.

## 10. Unterstützende Informationen

Detailliertere Informationen zu den einzelnen Anforderungen finden sich in den Umsetzungshinweisen der einzelnen Bausteine des IT-Grundschutzes.

Spezielle Informationen zur Umsetzung der Anforderungen des § 13 TMG finden sich in der BSI-Publikation "Absicherung von Telemediendiensten nach Stand der Technik".

Darüber hinaus gelten die einschlägigen nationalen und internationalen Vorschriften und Regelungen für den Flugbetrieb mit unbemannten Luftfahrzeugen.

## Anlage 1 – Bausteine/Systemkomponenten

A01	Flugplanungssoftware
A02	Karten-Software
A03	Wartungssoftware
A04	Flight Control-Software
A05	Ground Control-Software
A06	Logbuch/Flight Data Recorder
A07	Payload-Steuerung
A08	Steuerung Zusatzaufgaben
A09	Configuration Management-Software
C01	Desktoprechner
C02	Laptop
C03	Tablet
S01	Server
D01	Flightcontroller des UA
D02	Companion-Computer
NET01	Aktive Komponenten kabelgebundenes Firmennetzwerk
NET02	Aktive Komponenten drahtloses Firmennetzwerk
NET03	Schnittstelle zwischen Firmen- und Datennetzwerk
NET04	OnBoard-Netzwerk des UA
NET05	Schnittstelle Drohne Bodenkontrollstation
NET06	Aktive Komponenten der Verbindung UAS und/oder Bodenkontrollstation zu Kontroll- und Managementinstitutionen
R01	Zugangskontrollierter Raum <sup>1</sup>
R02	Leitstand (Bodenkontrollstation)
R03	Halle, Werkstattbereich
R04	Labor
R05	Serverraum
R06	Außenbereich, zugangskontrolliert <sup>1</sup>
R07	Flugtest- und Demonstrationsfläche
R08	Öffentlicher Raum
F01	Transportfahrzeug für UA bzw. UAS
F02	Operation Vehicle
UA01	Unmanned Aircraft/Drohne

<sup>1</sup>Die Zugangskontrollen sind spezifisch für die Institution und die Gefährdungslage und sind individuell anzupassen. Im Idealfall sind alle Räume und Flächen zugangskontrolliert.

## Anlage 2 – Elementare Gefährdungen

G 0.1	Feuer
G 0.2	Ungünstige klimatische Bedingungen
G 0.3	Wasser
G 0.4	Verschmutzung Staub Korrosion
G 0.5	Naturkatastrophen
G 0.6	Katastrophen im Umfeld
G 0.7	Großereignisse im Umfeld
G 0.8	Ausfall oder Störung der Stromversorgung
G 0.9	Ausfall oder Störung von Kommunikationsnetzen
G 0.10	Ausfall oder Störung von Versorgungsnetzen
G 0.11	Ausfall oder Störung von Dienstleistern
G 0.12	Elektromagnetische Störstrahlung
G 0.13	Abfangen kompromittierender Strahlung
G 0.14	Ausspähen von Informationen (Spionage)
G 0.15	Abhören
G 0.16	Diebstahl von Geräten Datenträgern oder Dokumenten
G 0.17	Verlust von Geräten, Datenträgern und Dokumenten
G 0.18	Fehlplanung oder fehlende Anpassung
G 0.19	Offenlegung schützenswerter Informationen
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle
G 0.21	Manipulation von Hard- und Software
G 0.22	Manipulation von Informationen
G 0.23	Unbefugtes Eindringen in IT-Systeme
G 0.24	Zerstörung von Geräten oder Datenträgern
G 0.25	Ausfall von Geräten oder Systemen
G 0.26	Fehlfunktion von Geräten oder Systemen
G 0.27	Ressourcenmangel
G 0.28	Software-Schwachstellen oder -Fehler
G 0.29	Verstoß gegen Gesetze oder Regelungen
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen
G 0.32	Missbrauch von Berechtigungen
G 0.33	Personalausfall
G 0.34	Anschlag
G 0.35	Nötigung, Erpressung oder Korruption
G 0.36	Identitätsdiebstahl
G 0.37	Abstreiten von Handlungen
G 0.38	Missbrauch personenbezogener Daten
G 0.39	Schadprogramme
G 0.40	Verhinderung von Diensten (Denial of Service)
G 0.41	Sabotage
G 0.42	Social Engineering
G 0.43	Einspielen von Nachrichten
G 0.44	Unbefugtes Eindringen in Räumlichkeiten
G 0.45	Datenverlust

G 0.46	Integritätsverlust schützenswerter Informationen
G 0.47	Schädliche Seiteneffekte IT-gestützter Angriffe

## Anlage 3 – Begriffsdefinitionen

Informationssicherheit	Umfassende Bezeichnung für alle Elemente im Zusammenhang mit der Erfassung, Nutzung und Speicherung von Daten einschließlich Informationstechnik
Grundschutz	Zustand, der durch die geeignete Kombination von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsanforderungen ein Sicherheitsniveau erreicht, das für den jeweiligen Schutzbedarf angemessen und ausreichend ist, um institutionsrelevante Informationen zu schützen. (BSI – IT-Grundschutzkompendium Kapitel 1.2)
Erhöhter Schutzbedarf	Der Schutzbedarf beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist. Dabei können szenariobedingte Besonderheiten auftreten, die unabhängig von der Schutzbedarfskategorie eine spezifische Risikoanalyse erfordern und ggf. punktuelle oder zeitliche Maßnahmen bewirken.
Risikoanalyse	Bezeichnung des kompletten Prozesses, um Risiken zu beurteilen (identifizieren, einschätzen und bewerten) sowie zu behandeln. (BSI – IT-Grundschutzkompendium Glossar)
Organisationsnetzwerk	das IT- und Kommunikationsnetzwerk des jeweiligen Luftfahrtbetriebs
Datennetzwerk	digitale Ablagedienste außerhalb des Organisationsnetzwerks, ugs.: Cloud
Uncrewed Aircraft Systems	In diesem IT-Grundschutz-Profil wird einheitlich der international standardisierte Oberbegriff verwendet. Er umfasst alle Systembezeichnungen und Unterkategorien, die unbemannte Luftsysteme bezeichnen, wie z.B. Drohne, Remotely Piloted Aircraft System (RPAS) etc. In diesem Zusammenhang bezeichnet der Begriff Uncrewed Aircraft (UA) das fliegende Element des Systems. Der Begriff Uncrewed Aerial Vehicle (UAV) ist veraltet und sollte nicht mehr verwendet werden.

## Anlage 4 – Abkürzungen

ABAC	Attribute Based Access Control
ADS-B	Automatic Dependent Surveillance - Broadcast
ANSP	Air Navigation Service Provider
BDSG	Bundesdatenschutzgesetz
DNS	Domain Name System
DSGVO	Datenschutzgrundverordnung
GP	Geschäftsprozess
IBAC	Identity Based Access Control
IT	Informationstechnik
JARUS	Joint Authorities for Rulemaking on Unmanned aircraft Systems
OGN	Open Glider Network
RBAC	Role Based Access Control
SAP ABAP	Advanced Business Application Programming (SAP-Produkt)
SAP ERP	Enterprise Resource Planning (SAP-Produkt)
TMG	Telemediengesetz
TTDSG	Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien
UAS	Uncrewed Aircraft System
USSP	U-Space Service Provider