IT-Grundschutz-Profil
für den
Betrieb von Uncrewed Aircraft Systems
in
Behörden und Organisationen
mit Sicherheitsaufgaben

Inhalt

Inhalt 2

1. Einleitung 4

1.1 Haftungsausschluss 6

1.2 Metainformationen 7

2. Zusammenfassung 8

2.1 Zielgruppen 8

2.2 Zielsetzungen 8

2.3 Verantwortlichkeiten 10

3. Festlegung des Geltungsbereichs 10

4. Informationsverbund 12

4.1 Interne Komponenten 14

4.2 Externe Komponenten 15

5. Referenzarchitektur 15

5.1 Prozesse 16

5.2 Anwendungen 18

5.3 Geräte 18

5.4 Netze 19

5.5 Mobile Infrastruktur 21

5.6 Stationäre Infrastruktur 22

5.7 Systemarchitektur des UAS 23

5.8 Akteure 25

5.9 Anpassungen 25

5.10 Zuordnung Komponenten und Prozesse 26

6. Betrachtung des Schutzbedarfs 31
6.1 Risikobetrachtung 35
6.2 Risikoanalyse 36
7. Anforderungen und Maßnahmen 38
7.1 Prozess-Bausteine 38
7.2 System-Bausteine 40
7.3 Rollen und Rechte 43
8. Restrisiken 45
9. Anwendungshinweise 45
9.1 Informationssicherheit 46
9.2 Datensicherheit 46
Anlage 1 – Prozesse 50
Anlage 2 – Elementare Gefährdungen 52
Anlage 3 – Glossar 54
Anlage 4 – Abkürzungen 56
Anlage 5 – Vorlagen 57
Anlage 6 – Quellen 58
Anlage 7 – Abbildungsverzeichnis 59

1. Einleitung

Der Betrieb von Uncrewed Aircraft Systems (UAS) in Behörden und Organisationen mit Sicherheitsaufgaben (BOS) stellt neben den Anforderungen an die Flugsicherheit auch entsprechende Anforderungen an die Informationssicherheit und den Datenschutz.

Als fliegende informationstechnische Systeme unterliegen sie somit einem hohen Schutzbedarf, da sich ein Ausfall von kritischen Teilsystemen unmittelbar auf die Betriebssicherheit auswirken und zu einem Fehlverhalten des UAS und im Ergebnis zu nachteiligen Auswirkungen auf die belebte und unbelebte Umgebung führen kann. Weiterhin erfordert der Schutz der elektronisch erfassten, digital gespeicherten und übermittelten Daten eine anwendungsspezifische Betrachtung aller relevanten Fragestellungen der Informationssicherheit und des Datenschutzes.

Zur ganzheitlichen Betrachtung der Informationssicherheit von Uncrewed Aircraft Systems sind drei Sichtweisen einzunehmen:

(1) in funktionaler Hinsicht als Teilnehmer am Luftverkehr,
(2) in technischer Hinsicht als hochmobiles Endgerät zur Datenerfassung und als Datenspeicher sowie als Sender bzw. Empfänger in einem Netzwerk,
(3) in operationaler Hinsicht als Führungs- und Einsatzmittel einer BOS zur Unterstützung von dienstlichen Tätigkeiten.

Das vorliegende IT-Grundschutz-Profil soll die Anwender und verantwortlichen Leiter in BOS bei einer standardisierten Betrachtung und Bewertung der zugrundeliegenden Fragestellungen zur Informationssicherheit unterstützen und eine geeignete Referenzarchitektur beim Betrieb von UAS beschreiben.

Hieraus ergeben sich die zwei unten aufgeführten Leitfragen:

(1) Wie kann durch geeignete Maßnahmen der Informationssicherheit eine Beeinträchtigung der Betriebssicherheit vermieden werden?
(2) Wie können durch geeignete Maßnahmen der Informationssicherheit die erfassten, gespeicherten und übermittelten Daten geschützt werden?

Die Bearbeitung von Fragestellungen aus dem Bereich des Datenschutzes sind nicht Bestandteil dieses IT-Grundschutz-Profils, die jeweils einzuhaltenden gesetzlichen und sonstigen Bestimmungen

werden somit nicht berücksichtigt. Es wird an dieser Stelle aber darauf hingewiesen, dass eine ganzheitliche, abgestimmte und ausgewogene Betrachtung sowohl des Datenschutzes als auch der Informationssicherheit als zielführend erachtet wird[1].

Die beiden übergeordneten Zielsetzungen bei der Berücksichtigung von Fragestellungen der Informationssicherheit beim Betrieb von UAS sind somit:

(1) Die Vermeidung von Personen- und Sachschäden,

(2) Die Einhaltung der drei elementaren Schutzziele der Informationssicherheit, also der „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“.

Der Begriff Uncrewed Aircraft System (UAS) wird in Bezugnahme zum hier vorgestellten IT-Grundschutz-Profil dahingehend erweitert, dass die Zugehörigkeit von UAS zu einem Systemverbund (mit den Komponenten Technik, Prozesse, Organisation und Akteure) herausgestellt wird und der Einsatz in BOS im Zusammenwirken mit anderen Führungs- und Einsatzmitteln erfolgt.

Das vorgelegte IT-Grundschutz-Profil überträgt Grundsätze der Informationssicherheit aus der allgemeinen Informationstechnik auf den Betrieb von UAS und ergänzt diese erforderlichenfalls durch UAS-spezifische IT-Grundschutz-Bausteine[2]. Es kann weiterhin als Grundlage für die Durchführung einer Risikobewertung und für die Erstellung eines Sicherheitskonzepts herangezogen werden.

Aufgrund der komplexen und vielfältigen Anwendungsfälle beim Betrieb von UAS in BOS erhebt dieses IT-Grundschutz-Profil keinen Anspruch auf Vollständigkeit, eine Anpassung an die spezifischen Schutzbedarfe des jeweiligen Anwenders sollte im Bedarfsfall erwogen werden.

---

[1] Vergleiche hierzu die Festlegung des Geltungsbereichs in Kapitel 3 sowie die Anwendungshinweise in Kapitel 9.

[2] Gemäß der Definition des BSI sind diese den benutzerdefinierten Bausteinen zugeordnet.

1.1 Haftungsausschluss

Dieses Dokument und die zugehörigen Anlagen wurden mit größter Sorgfalt erstellt, es erhebt aber keinen Anspruch auf Vollständigkeit und Richtigkeit oder Aktualität. Dieses Dokument und die zugehörigen Anlagen werden nicht fortgeschrieben oder aktualisiert.

Die in diesem Dokument dargelegten Sichtweisen können von denen der öffentlichen, privaten oder unternehmerischen Institutionen, in denen die Autorinnen und Autoren tätig sind, abweichen.

Die Autorinnen und Autoren und die durch sie repräsentierten Institutionen haben keinen Einfluss auf die Nutzung der im Dokument dargelegten Inhalte durch Anwenderinnen und Anwender oder sonstige Dritte. Auch haben sie keinen Einfluss auf die Inhalte von Dritten, auf die in diesem Dokument verwiesen wird.

Sie haben außerdem keine Kenntnis von den individuellen Anforderungen an die aus diesem IT-Grundschutz-Profil abgeleiteten Sicherheitskonzeptionen, so dass sie naturgemäß keine Haftung für eventuelle Schäden oder sonstige nachteilige Folgen übernehmen können.

Eine Haftung für resultierende Auswirkungen auf die Rechtsposition anderer Parteien durch die direkte oder indirekte Nutzung dieses IT-Grundschutz-Profils wird daher explizit ausgeschlossen.

Für die Inhalte der im IT-Grundschutz-Profil angegebenen externen Internetlinks wird eine Haftung durch die Autorinnen und Autoren und die durch sie repräsentierten Institutionen ebenfalls explizit ausgeschlossen.

1.2 Metainformationen

Aspekt	Beschreibung
Titel	IT-Grundschutz-Profil für den Betrieb von Uncrewed Aircraft Systems in Behörden und Organisationen mit Sicherheitsaufgaben
Autorenschaft	Herr Paul Burmeister Herr Jens Fehler (*Mediator Consult*) Herr Andreas J. Henke (*Subject Matter Expert, Information Security Risk Management and Air Law*) Herr Martin von Kameke (*BeastUAS*) Herr Gunnar Korte[3] Herr Marco Müller-ter Jung, *LL.M. (Informationsrecht), Grant Thornton Rechtsanwaltsgesellschaft mbH* Herr Christoph Nößke Frau Alexandra Pöhland Herr Markus Pöhland Frau Corinna Schmitt (*Universität der Bundeswehr München*) Herr Stefan Thumann Herr Burkhard Wrenger (*Technische Hochschule Ostwestfalen-Lippe*)
Danksagungen	Die Autoren danken Herrn Johannes Oppelt vom Bundesamt für Sicherheit in der Informationstechnik für seine hilfreichen fachlichen Hinweise und für die Unterstützung des Vorhabens. Die Autoren danken Frau Frauke Wendlandt für die Durchführung des Lektorats.
Herausgeber	UAV DACH e.V.
Versionsstand	1.1 (12.12.25): Ergänzung Tabelle 8 Teilprozesse Anwendungen, Geräte.
Revisionszyklus	Es wird nach Freigabe der Version 1.0 eine zweijährliche Überprüfung angestrebt.
Vertraulichkeit	Dieses Dokument darf in unveränderter Version weitergegeben werden.
Genderneutralität	Die in diesem Dokument verwendeten Personenbezeichnungen beziehen sich – sofern nicht anders kenntlich gemacht – auf alle Geschlechter. Zur besseren Lesbarkeit werden in diesem Dokument geschlechtsneutrale Personenbezeichnungen oder das generische Maskulinum verwendet.
Barrierefreiheit	Dieses Dokument ist weitgehend barrierefrei. Inhalte, bei denen keine umfassende Barrierefreiheit erzielt werden kann (z.B. Abbildungen), werden in den zugehörigen Abbildungsbeschreibungen erläutert. Für die in diesem Dokument referenzierten externen Inhalte[4] kann eine Barrierefreiheit seitens der Autoren und des Herausgebers nicht gewährleistet werden.

[3] Erstautor

[4] Vergleiche Kapitel 3 und Anlage 6.

2. Zusammenfassung

Dieses IT-Grundschutz-Profil richtet sich an alle Behörden und Organisationen mit Sicherheitsaufgaben, in denen Uncrewed Aircraft Systems eingesetzt werden. Es soll BOS die Erfüllung der Anforderungen an die Informationssicherheit gemäß den gesetzlichen, vertraglichen und regulatorischen Vorgaben beim Betrieb von UAS erleichtern und die zugehörigen Prozesse standardisieren.

2.1 Zielgruppen

Dieses IT-Grundschutz-Profil richtet sich an alle unmittelbar oder mittelbar im Rahmen ihrer Dienstausübung mit dem Betrieb von UAS befassten Angehörigen von BOS. Insbesondere sind dies Fernpiloten, Luftraumbeobachter, Unterstützungs-, Überwachungs- und Leitungspersonal sowie verantwortliche Beauftragte für Informationssicherheit.

2.2 Zielsetzungen

Das vorgelegte IT-Grundschutz-Profil definiert Anforderungen im Sinne des IT-Grundschutzes gemäß den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) mit der Zielsetzung, die Absicherung der durch den Betrieb von UAS erfassten, übermittelten und verarbeiteten Daten in Übereinstimmung mit den drei elementaren Schutzzielen der Informationssicherheit, also „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“ zu ermöglichen.

Der Betrieb von UAS wird als generalisiertes Modell durch vier Prozesse beschrieben:

(1) **Flugbetrieb** mit den Teilprozessen:

- Einsatzvorbereitung
- Inbetriebnahme
- Start
- Flug
- Landung
- Außerbetriebnahme
- Einsatznachbereitung

(2) **Wartung und Instandsetzung** gemäß den Herstellervorgaben für das jeweilige UAS mit den Teilprozessen:

- Wartung und Instandsetzung der für den Flugbetrieb erforderlichen elektronischen und mechanischen Antriebskomponenten
- Wartung und Instandsetzung der elektronischen und mechanischen sonstigen Komponenten des UAS inkl. Nutzlast und Kalibrierung der Sensorik
- Wartung und Instandsetzung der elektronischen und mechanischen sonstigen Komponenten von zugehörigen Subsystemen inkl. Bediengeräte, Antennensysteme, Batterieladesysteme
- Aktualisierung der digitalen Flugbetriebssoftware des UAS
- Aktualisierung aller weiteren digitalen Softwarekomponenten des UAS inkl. der Nutzlasten
- Aktualisierung aller weiteren digitalen Softwarekomponenten von zugehörigen Subsystemen inkl. Bediengeräte, Antennensysteme, Batterieladesysteme

(3) **Datenhaltung der primären Sensordaten** mit den Teilprozessen:

- Auslesen der lokalen Datenspeicher und ggf. des zentralen Datenraums und ggf. Bereinigung der Daten gemäß den gesetzlichen oder sonstigen regulatorischen Vorgaben
- Speicherung auf dem Zielmedium der Auswerteumgebung
- Löschen der lokalen Datenspeicher und ggf. des zentralen Datenraums

(4) **Auswertung der sekundären UAS-Flugbetriebsdaten** mit den Teilprozessen:

- Technisch-funktionale Auswertung der UAS-Flugbetriebsdaten
- Qualitative Bewertung der primären Sensordaten des UAS und ggf. der Nutzlasten
- Taktisch-operative Auswertung des UAS-Flugbetriebs
- Einhaltung regulatorischer oder sonstiger Vorgaben während des UAS-Flugbetriebs

2.3 Verantwortlichkeiten

Die Anwendung dieses IT-Grundschutz-Profils ist für den Betrieb von Uncrewed Aircraft Systems durch Behörden und Organisationen mit Sicherheitsaufgaben vorgesehen. Es kann als Bestandteil eines allgemeinen Rahmensicherheitskonzepts für den Betrieb von UAS oder eines typenspezifischen Sicherheitskonzepts für den Betrieb einer UAS-Variante zur Erfüllung von gesetzlichen, vertraglichen oder regulatorischen Regelungen gemäß den Empfehlungen des BSI verwendet werden. Weiterhin ermöglicht es leitenden (z.B. Einsatzleiter oder Führungspersonal) und verantwortlichen Personen (z.B. Fernpilot, Sensorbediener, Luftraumbeobachter, Überwachungs- und Unterstützungspersonal), eine Einschätzung hinsichtlich des erforderlichen Schutzbedarfs und des verbleibenden Restrisikos beim Betrieb von UAS vorzunehmen.

Es kann außerdem für die Abstimmung mit anderen BOS sowie für die Erfüllung von Vorgaben von Aufsichtsbehörden herangezogen werden.

Die im IT-Grundschutz-Profil beschriebenen Anforderungen können zusätzlich bei der Beauftragung von externen Anbietern von UAS-Dienstleistungen zur Ausgestaltung von Dienstleistungsverträgen herangezogen werden.

3. Festlegung des Geltungsbereichs

Die Festlegungen des IT-Grundschutz-Profils für den Betrieb von Uncrewed Aircraft Systems in Behörden und Organisationen mit Sicherheitsaufgaben sind ausschließlich als unverbindliche Empfehlungen zu verstehen, ihre vollständige oder anteilige Umsetzung erfolgt in eigenem Ermessen der jeweiligen BOS auf freiwilliger Basis.

Das IT-Grundschutz-Profil ist zur Eigenimplementierung durch die jeweilige BOS ausgelegt, die Einhaltung der Konformität kann grundsätzlich mittels einer Selbstbewertung erfolgen. Alternativ kann eine externe Bewertung durch ein gegenseitiges Audit von BOS erfolgen.

Das IT-Grundschutz-Profil wurde in Hinblick auf die spezialisierten Anforderungen beim Einsatz von UAS in BOS entwickelt, es bildet ausdrücklich nicht die Vorgaben für den Einsatz von UAS im unternehmerischen oder privaten Kontext ab.

Die Struktur und der inhaltliche Aufbau entsprechen den Empfehlungen des BSI IT-Grundschutz-Profils „Strukturbeschreibung“ in der Version 1.0.

Das IT-Grundschutz-Profil entspricht weiterhin den Anforderungen an eine Standard-Absicherung gemäß den Empfehlungen des vom BSI veröffentlichten Standards 200-2 (IT-Grundschutz-Methodik) in der Version 1.0.
Die entsprechende Standard-Absicherung gemäß BSI-Standard 200-2 folgt wiederum den Vorgaben der ISO/IEC 27001:2022 der International Organization for Standardization (ISO).
Das IT-Grundschutz-Profil folgt weiterhin den Empfehlungen zur Risikobetrachtung gemäß dem BSI-Standard 200-3 (Risikoanalyse auf der Basis von IT-Grundschutz) in der Version 1.0.
Außerdem berücksichtigt das IT-Grundschutz-Profil die Empfehlungen des BSI zur Absicherung von Telemediendiensten gemäß den im Dokument BSI-CS 125 (Absicherung von Telemediendiensten nach dem Stand der Technik) in der Version 1.0 beschriebenen Empfehlungen. In diesem Zusammenhang wird außerdem auf die allgemeinen Empfehlungen des BSI „Overview of drone-based cyber threats and aspects of defence“ in der Version 1.0 verwiesen.
Weiterhin werden in Teilbereichen die Vorgaben des Datenschutzes, hier insbesondere der Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) berücksichtigt. Handlungsempfehlungen zur Erfüllung der gesetzlichen Vorgaben aus dem Bereich des Datenschutzes sind allerdings kein Bestandteil dieses IT-Grundschutz-Profils.
Es wird darüber hinaus empfohlen, ergänzend zu diesem IT-Grundschutz-Profil die Vorgaben des europäischen Cyber Resilience Acts zu beachten, mit dem ein Mindestmaß an Cybersicherheit für alle (vernetzten) Produkte mit digitalen Elementen festlegt wird, und der für die Konstruktion, den Vertrieb und die Beschaffung von UAS von entsprechender Bedeutung ist[5]. Eine Analyse der Anforderungen und Auswirkungen des Cyber Resilience Acts ist jedoch nicht Gegenstand dieses IT-Grundschutz-Profils.
Das vorgelegte Grundschutz-Profil geht in wesentlichen Punkten mit dem vom UAV DACH e.V. vorgelegtem „IT-Grundschutz-Profil für den Betrieb von UAS Band 1: UAS-Betriebskategorie Open (Offen)“ in der Version 1.1 konform und folgt teilweise dessen struktureller Gliederung.
Zusätzlich folgt es in weiten Teilen den vom BBK herausgegebenen „Empfehlungen für Gemeinsame Regelungen zum Einsatz von Drohnen im Bevölkerungsschutz“ (EGRED 2) in der Version 2.0.
Darüber hinaus gelten die einschlägigen nationalen und internationalen Vorschriften und Regelungen für den Flugbetrieb mit Uncrewed Aircraft Systems[6].

---

[5] Vergleiche hierzu beispielsweise BSI - Cyber Resilience Act in Anlage 3.

[6] Es wird weiterhin auf die in der Anlage 6 aufgeführten Dokumente verwiesen.

4. Informationsverbund

Im Folgenden werden die Komponenten des Informationsverbunds beschrieben, außerdem erfolgt die Abgrenzung zu nicht berücksichtigten externen Komponenten.

Die in den Informationsverbund eingebundenen IT-Systeme, die Verbindungen zwischen den IT-Systemen sowie die Außenverbindungen der IT-Systeme werden als generalisierte graphische Übersichten anhand von beispielhaften Anwendungsfällen dargestellt[7].

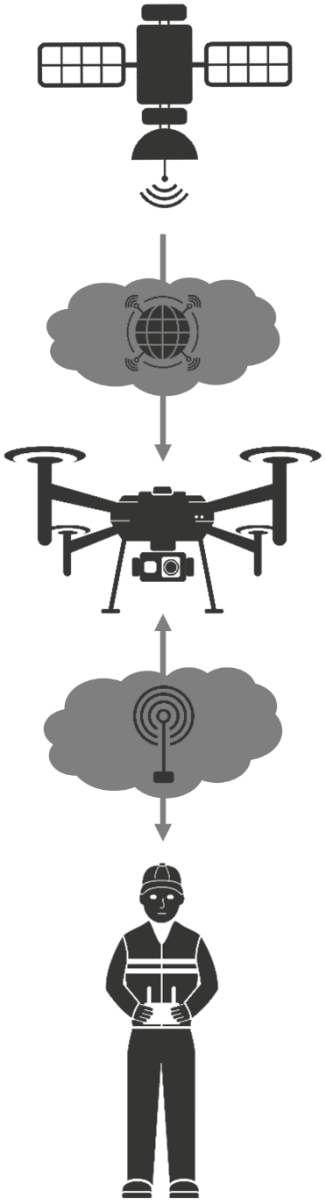

Abbildung 1: Schematische Darstellung eines allgemeinen und generalisierten UAS-Informationsverbunds mit den wesentlichen funktionalen internen und externen Komponenten und den zugehörigen Netzverbindungen.
Das vom Fernpiloten bediente Steuerungsgerät ist über eine lokale drahtlose Netzverbindung mit dem UAS verbunden, um den bi-direktionalen Austausch von Flugdaten (Steuerungsbefehle und Statusinformationen) und die uni-direktionale Übertragung von Sensordaten (Bewegtbilddaten und sonstige Sensordaten) zu gewährleisten.
Das Satellitentelemetrie-Modul des UAS empfängt Navigationsdaten zur Bestimmung der Position im Luftraum über ein drahtloses Weitverkehrsnetz.

[7] Siehe insbesondere die Abbildungen 1 bis 3, 5, 6 und 11.

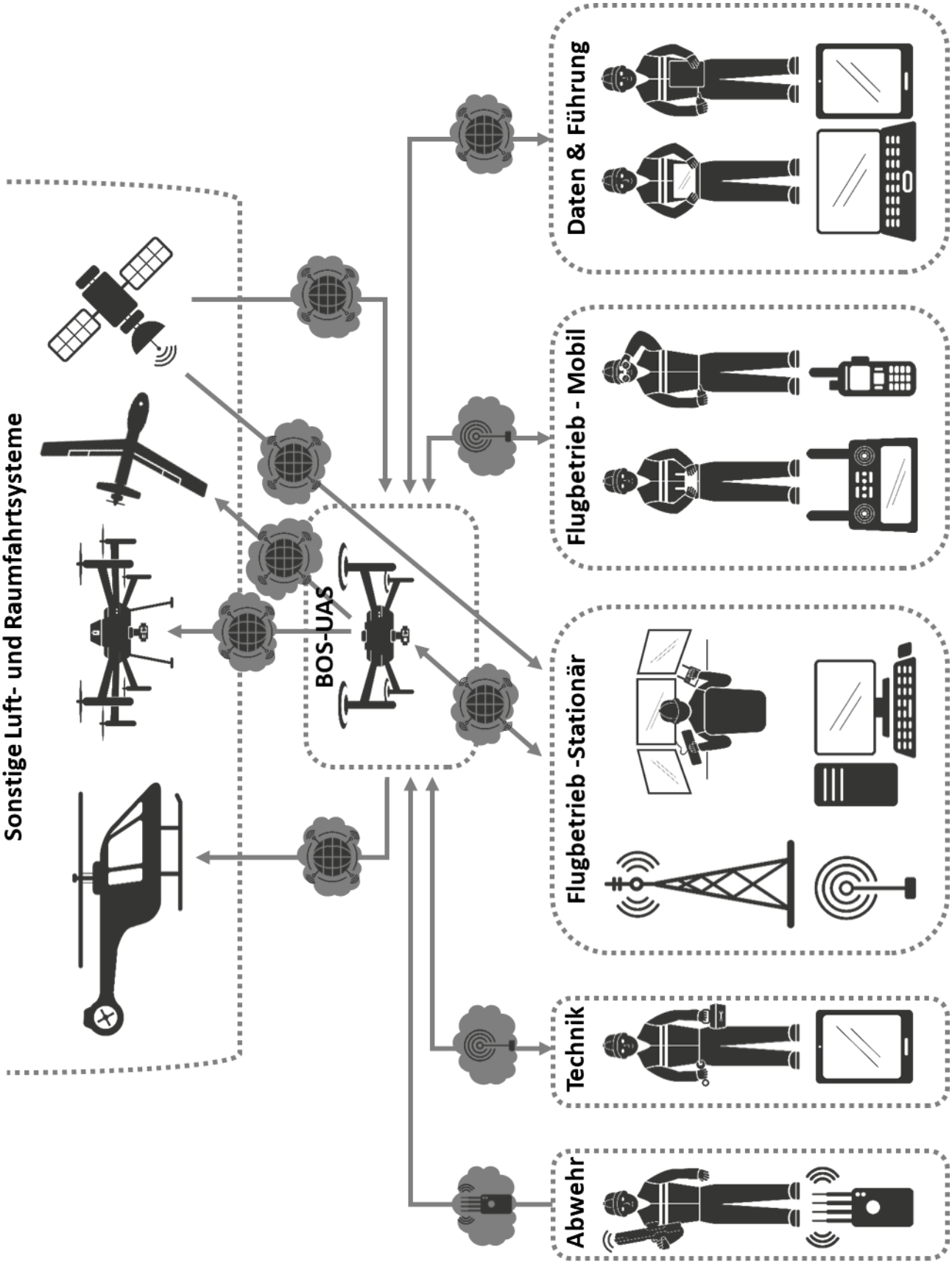

*Abbildung 2: Visualisierung eines generalisierten UAS-Informationsverbunds mit den sonstigen Luft- und Raumfahrtsystemen sowie den Akteuren und beispielhaften Endgeräten. Die Abgrenzung der funktionalen Teilkomponenten wird durch eine grau **gepunktete** Linie dargestellt. Die Netzverbindungen des betrachteten UAS sind als **dunkelgraue** Pfeile dargestellt. Die elektronische UAS-Abwehr wird nicht in diesem IT-Grundschutz-Profil behandelt und hier nur aus Gründen einer vollständigen Übersicht dargestellt.*

4.1 Interne Komponenten

Der Informationsverbund berücksichtigt die internen Komponenten, Verfahren und funktionalen Prozesse einer BOS beim Betrieb von UAS.

Dies beinhaltet insbesondere den **Flugbetrieb** mit den Teilprozessen Einsatzvorbereitung, Inbetriebnahme, Start, Flug, Landung, Außerbetriebnahme und Einsatznachbereitung.

Weiterhin umfasst er die **Wartung und Instandsetzung** mit den Teilprozessen Wartung und Instandsetzung der für den Flugbetrieb erforderlichen elektronischen und mechanischen Antriebskomponenten, der Wartung und Instandsetzung der elektronischen und mechanischen sonstigen Komponenten des UAS inklusive Nutzlast und Kalibrierung der Sensorik, der Wartung und Instandsetzung der elektronischen und mechanischen sonstigen Komponenten von zugehörigen Subsystemen inklusive Bediengeräte, Antennensysteme, Batterieladesysteme sowie der Aktualisierung der digitalen Flugbetriebssoftware des UAS, der Aktualisierung aller weiteren digitalen Softwarekomponenten des UAS inklusive der Nutzlast und der Aktualisierung aller weiteren digitalen Softwarekomponenten von zugehörigen Subsystemen inklusive Bediengeräte, Antennensysteme und Batterieladesysteme.

Außerdem beschreibt er die **Datenhaltung der primären Sensordaten** mit den Teilprozessen Auslesen der lokalen Datenspeicher und bei Bedarf des zentralen Datenraums und gegebenenfalls der Bereinigung der Daten gemäß den gesetzlichen oder sonstigen regulatorischen Vorgaben, der Speicherung auf dem Zielmedium der Auswerteumgebung und das Löschen der lokalen Datenspeicher und gegebenenfalls des zentralen Datenraums.

Zusätzlich wird die **Auswertung der sekundären UAS-Flugbetriebsdaten** mit den Teilprozessen technisch-funktionale Auswertung der UAS-Flugbetriebsdaten, der qualitativen Bewertung der primären Sensordaten der UAS-Nutzlast, der taktisch-operativen Auswertung des UAS-Flugbetriebs sowie der Einhaltung regulatorischer oder sonstiger Vorgaben während des UAS-Flugbetriebs abgebildet.

4.2 Externe Komponenten

Externe Komponenten und die zugehörigen Schnittstellen werden im Informationsverbund nicht berücksichtigt. Dies betrifft alle Teilbereiche, bei denen kein direkter Bezug zum Flugbetrieb, zur Wartung und Instandhaltung, zur Datenhaltung der primären Sensordaten oder zur Auswertung der sekundären Flugbetriebsdaten hergestellt werden kann.

Weiterhin unberücksichtigt bleiben Aspekte der Flugsicherheit im Rahmen des Flugsicherheitsmanagements, der Einsatz von KI-basierten Verfahren zur Erhöhung der Flugsicherheit, der Einsatz von UAS in einem Schwarmverbund, der autonome UAS-Betrieb ohne Überwachung durch einen Fernpiloten, die Auslagerung von Flugsicherheitsrisiken an Dritte (z.B. Versicherungsunternehmen) sowie die elektronische UAS-Abwehr[8].

5. Referenzarchitektur

Der Informationsverbund des IT-Grundschutz-Profils für den Betrieb von Uncrewed Aircraft Systems in Behörden und Organisationen mit Sicherheitsaufgaben umfasst alle zugehörigen statischen und dynamischen Objekte der eingesetzten UAS, die für die Abbildung der jeweiligen Anwendungsfälle erforderlich sind.

Der Schutzbedarf bezieht sich auf die Verfahren und Komponenten innerhalb des Informationsverbunds (z.B. Sensoren und Aktoren, Datenspeicher, Kommunikationssysteme, Bedienstationen) sowie auf den Informationsaustausch (z.B. Kommunikationswege und -protokolle) und die zugehörigen Schnittstellen. Die aus dem Schutzbedarf abgeleiteten Sicherheitsanforderungen sind von den BOS für den jeweiligen Anwendungsfall zu bewerten und bei Bedarf für die betroffenen Objekte anzupassen oder zu ergänzen.

Die verwendeten Begrifflichkeiten (hier insbesondere Prozess und Teilprozess, Verfahren und Komponenten sowie Anwendungsfall und Akteure) weichen teilweise in ihrer Definition und Abgrenzung von den seitens des BSI verwendeten Fachbegriffen ab und sind an die funktionellen Bezeichnungen von BOS angelehnt[9].

---

[8] Vergleiche den in Abbildung 2 dargestellten Informationsverbund, in dem die funktionale Teilkomponente UAS-Abwehr aus Gründen einer ganzheitlichen Betrachtungsweise aufgeführt wird.

[9] Es wird an dieser Stelle auf das Glossar in Anhang 3 verwiesen.

5.1 Prozesse

Grundlage des IT-Grundschutz-Profils für den Betrieb von Uncrewed Aircraft Systems in Behörden und Organisationen mit Sicherheitsaufgaben sind die vier Prozesse des Informationsverbunds:

(1) Flugbetrieb,

(2) Wartung und Instandsetzung,

(3) Datenhaltung der primären Sensordaten,

(4) Auswertung der sekundären UAS-Flugbetriebsdaten.

Die im IT-Grundschutz-Profil aufgeführten Prozesse beschreiben beispielhaft den Betrieb von UAS und können bei Bedarf durch abweichende oder ergänzende Prozesse der jeweiligen BOS ersetzt oder erweitert werden.

Der Prozess **(1) Flugbetrieb** umfasst die Einsatzvorbereitung (z.B. Erstellung eines Flugplans, Beantragung einer Flugerlaubnis), die Inbetriebnahme (z.B. Funktionstests der Aktoren und Sensoren, der Steuerungsgeräte und der Kommunikationsverbindungen), den Start, den Flug (Flug zum Einsatzgebiet, Aufenthalt im Einsatzraum, Flug zur Landezone), die Landung, die Außerbetriebnahme (z.B. Deaktivierung, Trennung vom Energiespeicher, sonstige Vorbereitungen für den Abtransport) und die Einsatznachbereitung (z.B. Dokumentation, Erfüllung Melde- und Berichtspflichten).

Der Prozess **(2) Wartung und Instandsetzung** orientiert sich weitgehend an den Herstellervorgaben für die eingesetzten UAS und beinhaltet die Wartung und Instandsetzung der für den Flugbetrieb erforderlichen elektronischen und mechanischen Antriebskomponenten, die Wartung und Instandsetzung der elektronischen und mechanischen sonstigen Komponenten des UAS (inkl. Wartung und Instandsetzung der Nutzlast und Kalibrierung der Sensorik) sowie die Wartung und Instandsetzung der elektronischen und mechanischen sonstigen Komponenten von zugehörigen Subsystemen (z.B. Steuerungsgeräte, Antennensysteme, Batterieladesysteme).

Der Prozess **(3) Datenhaltung der primären Sensordaten** orientiert sich weitgehend an den gesetzlichen und sonstigen Vorgaben der Datensicherheit[10] und umfasst das Auslesen der lokalen Datenspeicher und des zentralen Datenraums und ggf. die Bereinigung der Daten gemäß der gesetzlichen (z.B. Einhaltung von Löschfristen) oder sonstigen regulatorischen Vorgaben (z.B. Verpflichtung zur Anonymisierung von erfassten Personen, Löschen von Aufnahmen und Datensätzen, die für die Er-

[10] Siehe hierzu Kapitel 9.2 Datensicherheit.

füllung des spezifischen Anwendungsfalls nicht erforderlich sind), die Speicherung auf dem Zielmedium der Auswerteumgebung sowie das Löschen der lokalen Datenspeicher und ggf. des zentralen Datenraums.

Der Prozess **(4) Auswertung der sekundären UAS-Flugbetriebsdaten** beinhaltet die technisch-funktionale Auswertung der UAS-Flugbetriebsdaten (z.B. Entladung der Batterien, Latenz der Datenfernübertragung, Verbindungsabbrüche, Fehlfunktionen), die qualitative Bewertung der primären Sensordaten der UAS-Nutzlast (Qualitätssicherung und -kontrolle), die taktisch-operative Auswertung des UAS-Flugbetriebs (z.B. Abweichungen vom Flugplan, Reaktion auf besondere Ereignisse, operative Zusammenarbeit der UAS-Organisationseinheit) und die Einhaltung regulatorischer oder sonstiger Vorgaben während des UAS-Flugbetriebs (z.B. Sichtflug, Flugverbotszonen, maximale Flughöhen).

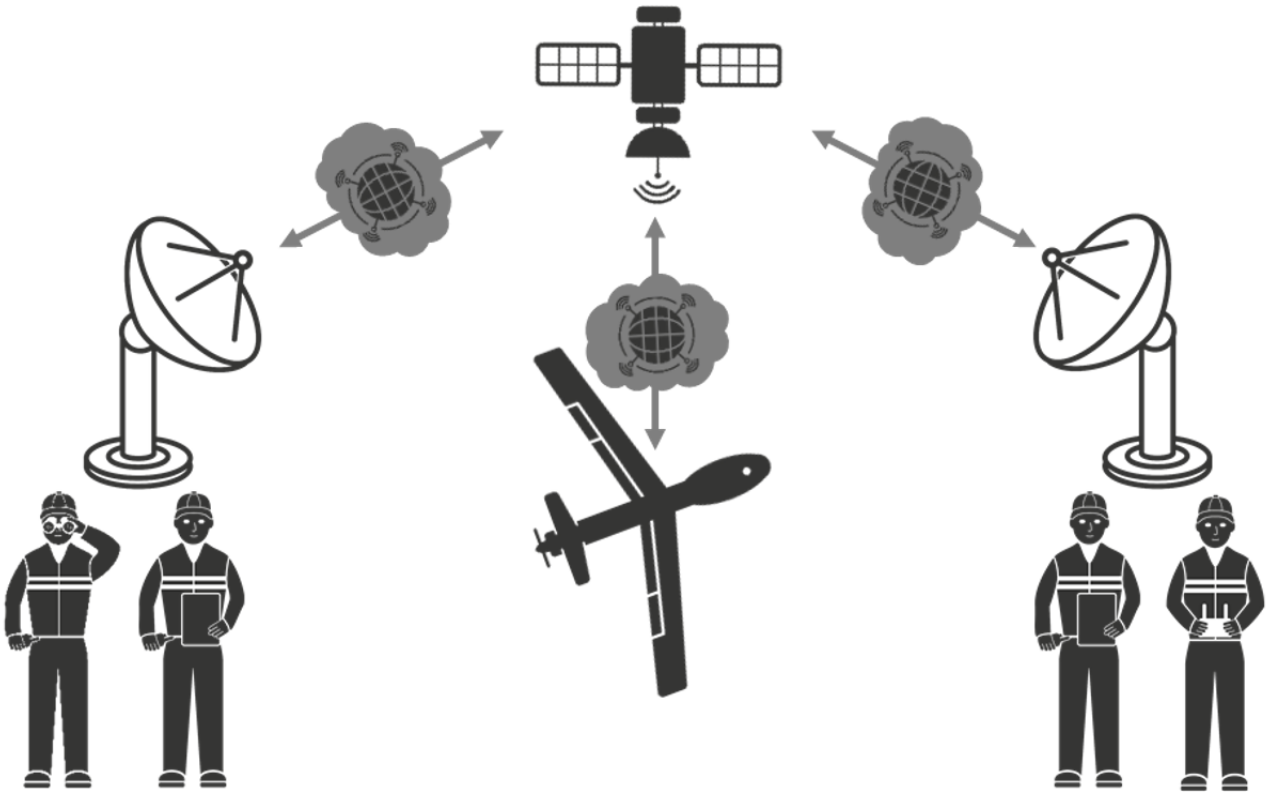

Abbildung 3: Visualisierung der Komponenten beim Betrieb von UAS außerhalb der Sichtlinie des Fernpiloten unter Mitwirkung eines Luftraumbeobachters über eine bi-direktionale Satellitenverbindung.

5.2 Anwendungen

Die Durchführung der beschriebenen Prozesse wird durch den Einsatz von informationstechnischen Anwendungen unterstützt, diese sind ebenfalls Bestandteil des Informationsverbunds.

Die nachfolgende Tabelle beinhaltet eine Aufstellung von beispielhaften informationstechnischen Anwendungen bzw. IT-Fachverfahren.

ID	Anwendungen
A 01	Flugplanung
A 02	Geographische Informationssysteme
A 03	Wartung und Instandhaltung
A 04	Fernsteuerung
A 05	Fernüberwachung
A 06	Datenübertragung
A 07	UAS-Betriebssystem
A 08	Fernsteuerung Nutzlast
A 09	Batterieverwaltung
A 10	BOS-Kommunikation
A 11	Leitstelle
A 12	Luftraumüberwachung

Tabelle 1: Übersicht der informationstechnischen Anwendungsgebiete.

5.3 Geräte

Im Informationsverbund sind neben den Prozessen, Teilprozessen und Anwendungsfällen auch die eingesetzten informationstechnischen Geräte zu betrachten.

Die nachfolgende Tabelle beinhaltet eine Auswahl von beispielhaften Geräten.

ID	Geräte
C 01	Arbeitsplatz-Computer
C 02	Mobil-Computer
C 03	Mobiltelefon
C 04	BOS-Digitalfunkgerät
S 01	Virtueller Datenspeicher (Datenraum)
S 02	Physischer Datenspeicher
D 01	Steuergerät Bodenkontrollstation
D 02	Steuergerät UAS (on-board-unit)

Tabelle 2: Übersicht der informationstechnischen Geräte.

5.4 Netze

Die Gesamtheit der Netze bildet das Netzwerk des Informationsverbunds. Die einzelnen Komponenten der informationstechnischen Netze weisen oftmals eine heterogene Struktur auf.

Die technische Kommunikation wird in der Regel durch lokale Netzwerke (LAN) sowie Weitverkehrsnetze (WAN) als leitungsloses „over the air“-Verfahren gewährleistet. Alternativ erfolgt die technische Kommunikation ganz oder anteilig über leitungsgebundene (z.B. „tethered drone“ im stationären Überwachungseinsatz) oder netzlose bzw. UAS-gebundene (z.B. „drone-to-drone mesh“) Verfahren[11].

Beispiele für lokale Netzverbindungen für den Betrieb von UAS sind dezidierte lokale Netze als direkte Verbindungen, hierfür werden oftmals die Frequenzbereiche 2.4 GHz und 5.8 GHz sowie teilweise 900 MHz und 1.3 GHz verwendet.

Beispiele für häufig genutzte terrestrische Weitverkehrsnetze sind Mobilfunknetze als indirekte Verbindungen, je nach lokaler Verfügbarkeit können hierfür GSM (2G), UMTS (3G), LTE (4G) oder FR1/FR2 (5G) Netze genutzt werden. Beispiele für orbitale Weitverkehrsnetze sind Satellitenkommunikationsnetze (z.B. Angebote von privatwirtschaftlichen Dienstleistern oder öffentlichen Institutionen). Allgemein wird hier zwischen Satelliten in niedriger („low earth orbit“), geostationärer oder nicht-geostationärer Umlaufbahn unterschieden. Für die Positionsbestimmung im Luftraum werden oftmals Satellitennavigationssysteme („global navigation satellite systems“) herangezogen, die Positionsbestimmung kann durch terrestrische Echtzeit-Korrektursignale („real-time kinematics“) ergänzt werden, um die Messgenauigkeit bei der Positionsermittlung zu erhöhen. Darüber hinaus bestehen weitere technische Möglichkeiten zur Herstellung einer Netzverbindung, zum Beispiel über einen vom UAS während des Flugbetriebs abgespulten Lichtwellenleiter oder über ein Mesh-Netzwerk, in dem eine dynamische Verbindung zwischen mehreren UAS aufgebaut wird.

Allgemein wird die Auswahl von geeigneten Netzverbindungen für den Betrieb von UAS in BOS durch die Verfügbarkeit und die Anforderungen an die Reichweite, die erforderlichen Datenübertragungsraten, die akzeptable Zeitspanne zwischen der Signaländerung am Systemeingang und der Signalantwort am Systemausgang (Latenz), die Ausfallsicherheit und die Redundanz sowie die Anforderungen an die Informationssicherheit, hier insbesondere die Systemhärtung und technische Resilienz, bestimmt[12].

---

[11] Vergleiche hierzu insbesondere Abbildung 4.

[12] Vergleiche hierzu Kapitel 9.2.

Es werden verschiedene Netzbereiche wie das Sprachnetz zur Kommunikation zwischen Steuerungs-, Beobachtungs-, Leitungs- und Luftraumüberwachungspersonal, das Funknetz zur Übermittlung von Steuerungsbefehlen, das Datennetz zur Übermittlung von Sensor- und sonstigen Daten sowie das Signalisierungsnetz zur Steuerung der Kommunikationsverbindung verwendet.

Die Netzverbindungen sind im Allgemeinen bi-direktional und werden zwischen dem UAS und der Bodenkontrollstation, zwischen dem UAS und anderen bemannten und unbemannten Luftfahrzeugen, zwischen dem UAS und Satelliten (z.B. Positionsbestimmung mittels Satellitentelemetrie) oder zwischen der Bodenkontrollstation und Akteuren des Luftverkehrs oder der Luftraumüberwachung über direkte oder indirekte (z.B. über eine Basis- oder Relaisstation) Kommunikationsverfahren hergestellt.

Die nachfolgende Tabelle beinhaltet eine Aufstellung von beispielhaften Netzen.

ID	**Netze**
N 01	Leitungslose Netzwerkkomponenten (*UAS <- > Bodenkontrollstation*)
N02	Leitungsgebundene Netzwerkkomponenten (*UAS <- > Bodenkontrollstation*)
N 03	Leitungslose Netzwerkkomponenten (*sonstige Verbindungen*)
N 04	Leitungsgebundene Netzwerkkomponenten (*sonstige Verbindungen*)
N 05	Schnittstellen zwischen Netzwerkkomponenten
N 06	Primäre interne UAS-Netzwerkkomponenten (*Flugsicherheit*)
N 07	Sekundäre interne UAS-Netzwerkkomponenten (*sonstige Funktionalitäten*)

Tabelle 3: Übersicht der informationstechnischen Netze.

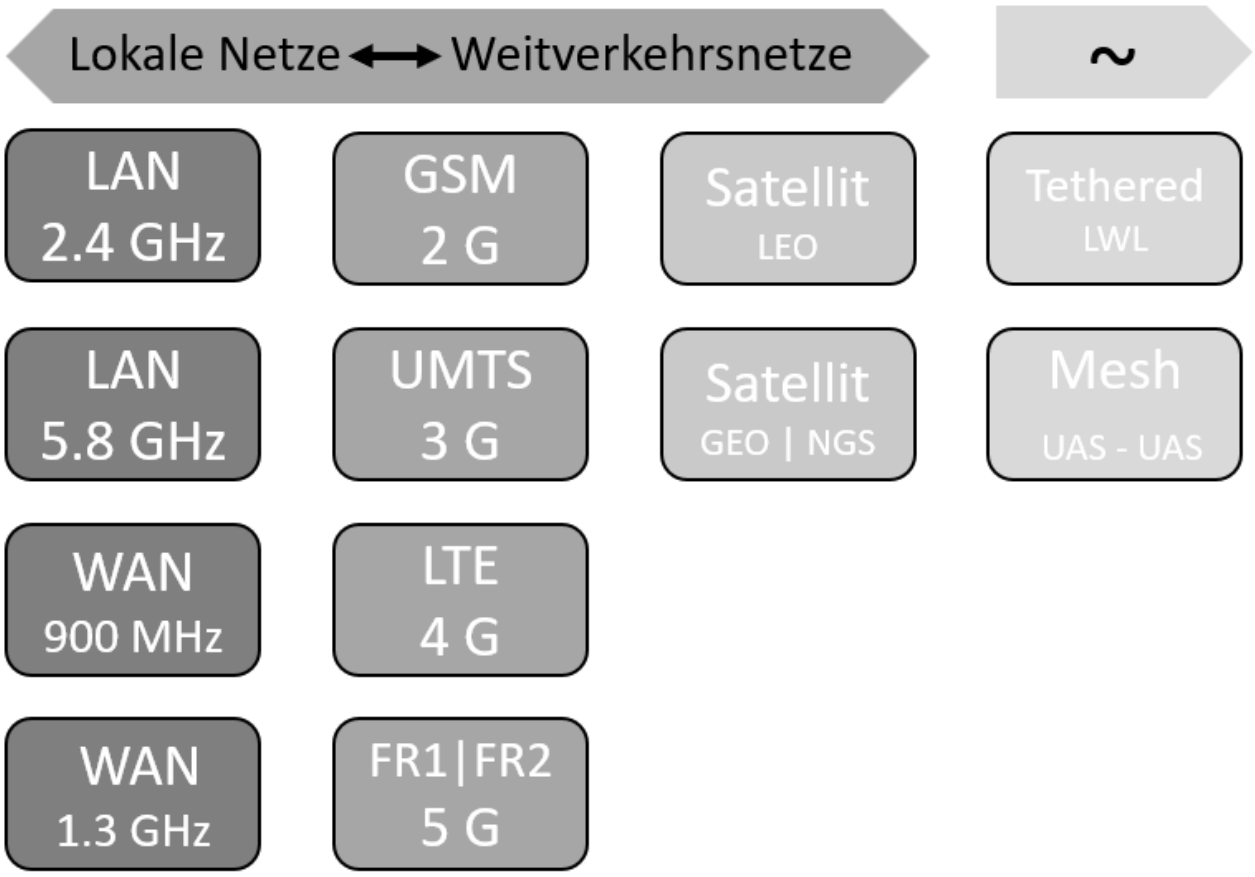

Abbildung 4: Beispielhafte Darstellung von Netzverbindungen und technischer Standards sowie der zugehörigen Verfahren. Zusätzlich zu lokalen Netzen und Weitverkehrsnetzen werden technische Sonderverfahren aufgeführt.

5.5 Mobile Infrastruktur

Die für den Betrieb von UAS am oder in der Nähe des Einsatzorts erforderliche technische Infrastruktur ist oftmals für eine mobile Verlagerung ausgelegt. Die entsprechenden Komponenten und die eingesetzten UAS sind Bestandteil der mobilen Infrastruktur des Informationsverbunds.

Die nachfolgende Tabelle benennt beispielhafte Infrastrukturkomponenten.

ID	**Mobile Infrastruktur**
U 01	UAS (*Multicopter*)
U 02	UAS (*Starrflügler*)
F 01	Bodenkontrollstation als mobiler Leitstand, Einsatzleitzentrale
F 02	Transportfahrzeug
F 03	Unterstützungsfahrzeug
F 04	Sonstige mobile Systeme (*z.B. Antennenanlagen*)

Tabelle 4: Übersicht der informationstechnischen mobilen Infrastrukturkomponenten.

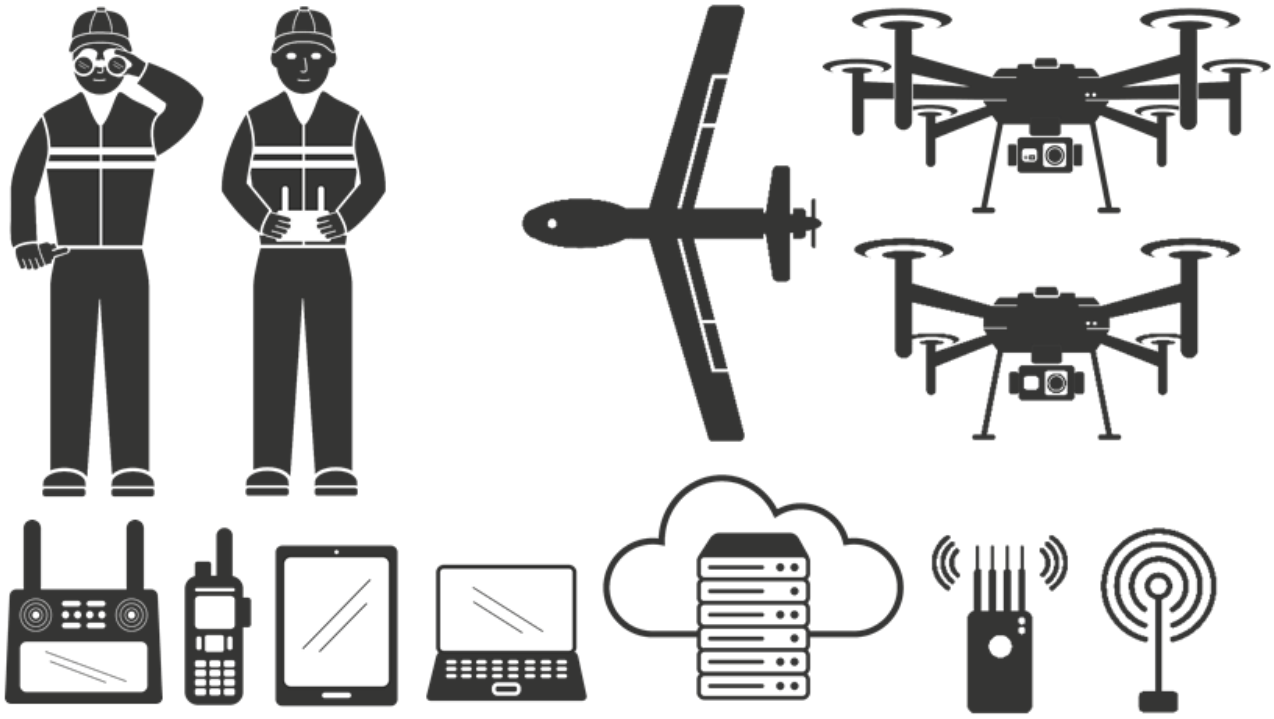

Abbildung 5: Visualisierung beispielhafter mobiler Infrastrukturkomponenten und beteiligter Akteure.

5.6 Stationäre Infrastruktur

Die stationäre Infrastruktur zum Betrieb eines UAS kann ebenfalls als Bestandteil des Informationsverbundes betrachtet werden und wird hier aus Gründen einer ganzheitlichen Betrachtung beschrieben.

Die nachfolgende Tabelle führt beispielhafte stationäre Infrastrukturkomponenten auf.

ID	**Stationäre Infrastruktur**
R 01	Innenbereich mit Zugangskontrolle
R 02	Außenbereich mit Zugangskontrolle
R 03	Bodenkontrollstation als stationärer Leitstand, Einsatzleitzentrale
R 04	Werkstatt (*Wartung und Instandhaltung*)
R 05	Datenzentrum (*Datenspeicherung und -aufbereitung*)
R 06	Kontrollierter Luftraum (*Übung, Erprobung und Ausbildung*)
R 07	Offener Luftraum (*Einsatz*)

Tabelle 5: Übersicht der informationstechnischen stationären Infrastrukturkomponenten.

Abbildung 6: Visualisierung beispielhafter stationärer Infrastrukturkomponenten und beteiligter Akteure.

5.7 Systemarchitektur des UAS

Die Systemarchitektur des jeweiligen UAS kann ebenfalls als Bestandteil des Informationsverbundes betrachtet werden und Bestandteil einer Sicherheitskonzeption sein. Dieser Betrachtungsweise unterliegen insbesondere typenbezogene Sicherheitskonzepte für eine spezifische Variante eines UAS. Die Systemarchitektur von UAS ist allerdings kein primärer Bestandteil des vorgelegten IT-Grundschutz-Profils und wird hier nur aus Gründen einer ganzheitlichen Betrachtungsweise allgemein beschrieben.

Auf die Angabe von beispielhaften Systemkomponenten als tabellarische Übersicht wurde daher aufgrund der großen Anzahl der technisch möglichen Realisierungsvarianten verzichtet. Alternativ werden die Daten- und Energieflüsse am Beispiel eines Quadcopter-UAS als schematische Übersicht dargestellt[13].

[13] Vergleiche hierzu die Abbildungen 7 und 8.

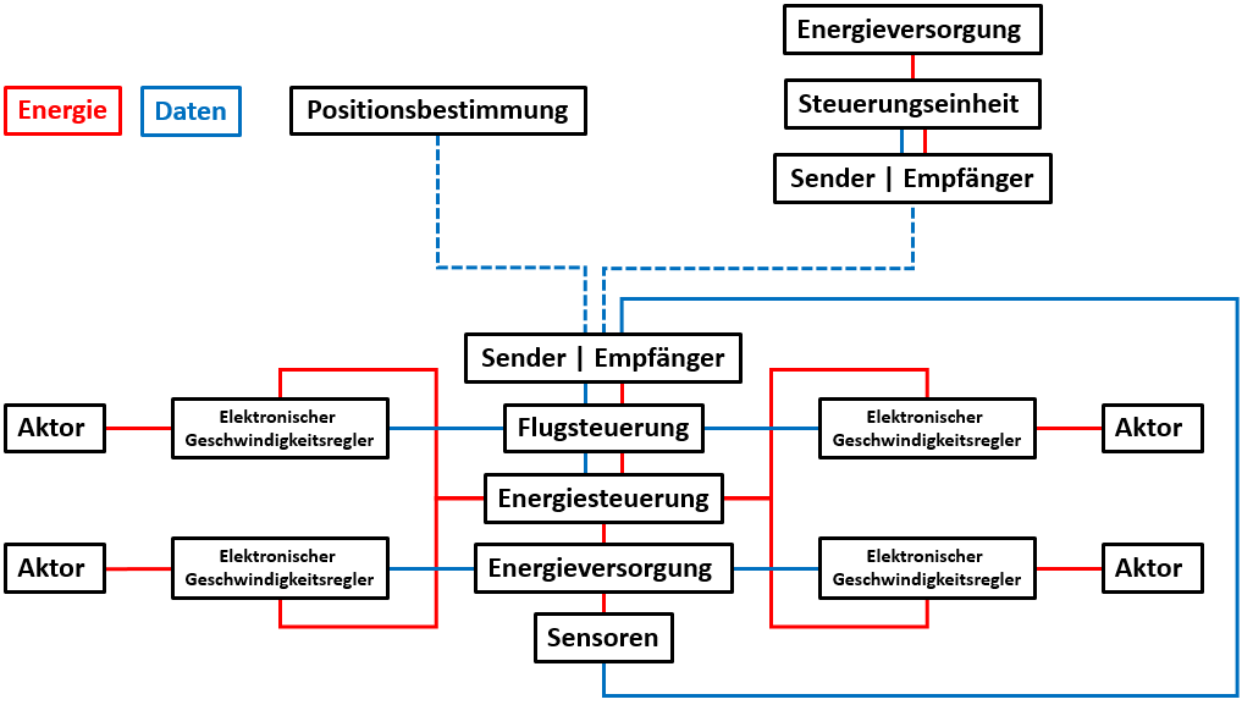

*Abbildung 7: Schematische Übersicht der funktionalen Systemkomponenten eines UAS (Quadcopter) und der Steuerungseinheit sowie der internen und externen **Energie**- und **Daten**verbindungen. Eine **durchgehende** Linie bildet leitungsgebundene Verbindungen ab, eine **durchbrochene** Linie bildet leitungslose Verbindungen ab.*

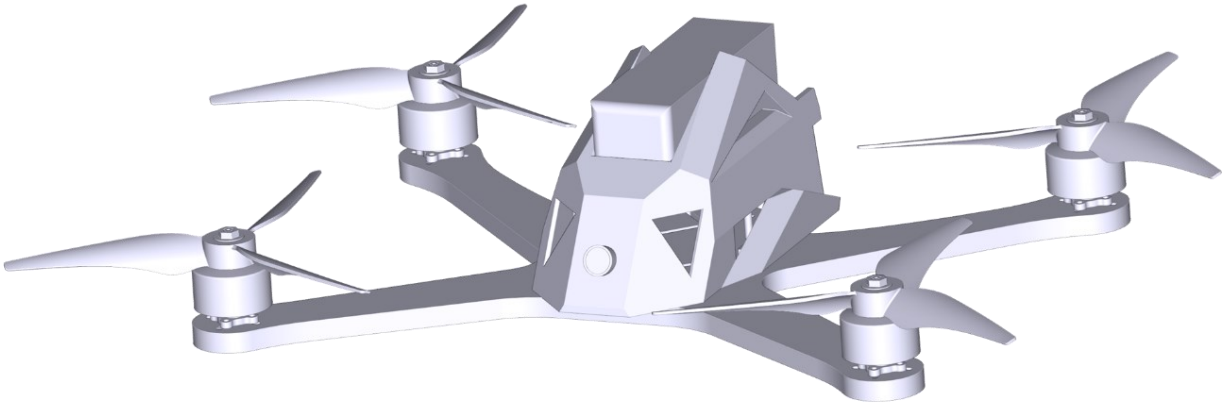

Abbildung 8: Beispielhafte Darstellung eines UAS in der Konfiguration als Quadcopter mit den funktionalen Komponenten Zentrales Kontrollmodul, Kamerasystem, Energieversorgung, Antriebsmodule an Auslegern (Quelle: Donaustahl GmbH).

5.8 Akteure

Der Betrieb von UAS erfordert sachkundiges und erfahrenes Bedienungspersonal, um Aufgaben bei der Durchführung des Flugbetriebs (Fernpilot, eventuell Co-Fernpilot), bei der Betriebsüberwachung (z.B. Luftraumbeobachter, Nutzlastspezialist) sowie in unterstützender Funktion (z.B. Wartungstechniker, Auswerter Bild- und Sensordaten) auszuüben.

Außerdem sind internes (z.B. Einsatzleiter, Fach- und Disziplinarvorgesetzte) und externes Leitungspersonal (z.B. Luftraumüberwachungspersonal) in den Betrieb der UAS eingebunden. Die Akteure sind kein primärer Bestandteil des Informationsverbunds und werden aus Gründen einer ganzheitlichen Betrachtungsweise beschrieben. Weiterhin soll so eine Konformität zwischen den Zielsetzungen des IT-Grundschutz-Profils und den davon abgeleiteten Rollen- und Rechtekonzepten gewährleistet werden[14].

Die nachfolgende Tabelle enthält potenzielle Akteure im UAS-Informationsverbund[15].

ID	Akteure
P 01	Fernpilot
P 02	Betriebsüberwachung
P 03	Betriebsunterstützung
P 04	Leitungspersonal - intern
P 05	Leitungspersonal - extern
P 06	Unbeteiligte Dritte

Tabelle 6: Übersicht der Akteure beim Betrieb von UAS in BOS.

5.9 Anpassungen

Falls der Informationsverbund nicht der Referenzarchitektur entspricht, so ist dieser entsprechend anzupassen. Im Rahmen der Strukturanalyse ist diese Anpassung zu dokumentieren. Den zusätzlich zu schützenden Prozessen und den zugehörigen Komponenten, welche nicht in diesem IT-Grundschutz-Profil enthalten sind, müssen geeignete Komponenten des IT-Grundschutz-Kompendiums des BSI zugeordnet werden.

Prozesse und Komponenten dieses IT-Grundschutz-Profils, die nicht Bestandteil des spezifischen Informationsverbunds sind, können unberücksichtigt bleiben[16].

---

[14] Vergleiche hierzu auch Kapitel 7.3 Rollen und Rechte.

[15] Vergleiche hierzu die Abbildungen 5 und 6.

[16] Zur Anpassung von Prozessen und Teilprozessen wird auf die Vorlage in Anhang 5 verwiesen.

5.10 Zuordnung Komponenten und Prozesse

Die nachfolgenden Tabellen ordnen die einzelnen Komponenten den entsprechenden Prozessen[17] zu. Die beschriebenen funktionalen Beziehungen bilden die Grundlage für die Auswahl der anzuwendenden Prozesse und der zugehörigen Bausteine dieses IT-Grundschutz-Profils.

Die jeder Komponente zugehörigen Prozesse sind nicht als verbindliche Vorgabe anzusehen, im anwendungsbezogenen Einzelfall können diese ganz oder teilweise unberücksichtigt bleiben oder um weitere Prozesse ergänzt werden[18].

	ID	**Teilprozesse Unbemannte Luftfahrtsysteme**	**Zugehörige Prozesse bzw. Zielobjekte**					
Flugbetrieb	TP 1.1	Einsatzvorbereitung	A 01 N 04	A02 N 05	A 11 R 04	A 12 P 01	C 01 P 03	N 03
	TP 1.2	Inbetriebnahme	A 04 N 01 U 02 P 01	A 05 N 02 F 01 P 03	D 01 N 05 F 04	D 02 N 06 R 03	C 03 N 07 R 06	C 04 U 01 R 07
	TP 1.3	Start	A 04 A 11 N 05 F 04 P 03	A 05 A 12 N 06 R 03 P 04	A 06 D 01 N 07 R 06 P 05	A 07 D 02 U 01 R 07	A 08 C 03 U 02 P 01	A 10 C 04 F 01 P 02
	TP 1.4	Flug	A 04 A 11 N 05 F 04 P 03	A 05 A 12 N 06 R 03 P 04	A 06 D 01 N 07 R 06 P 05	A 07 D 02 U 01 R 07 P 06	A 08 C 03 U 02 P 01	A 10 C 04 F 01 P 02
	TP 1.5	Landung	A 04 A 11 N 05 F 04 P 03	A 05 A 12 N 06 R 03 P 04	A 06 D 01 N 07 R 06 P 05	A 07 D 02 U 01 R 07	A 08 C 03 U 02 P 01	A 10 C 04 F 01 P 02
	TP 1.6	Außerbetriebnahme	A 04 N 07 R 06	A 05 U 01 R 07	D 01 U 02 P 01	D 02 F 01 P 03	N 05 F 02	N 06 R 03
	TP 1.7	Einsatznachbereitung	A 03 N 05	A 09 R 04	S 01 P 01	S 02 P 03	N 03	N 04

[17] Gemäß der Definition des BSI werden die zugehörigen Prozesse als Zielobjekte betrachtet.

[18] Vergleiche hierzu auch Kapitel 5.8.

Wartung und Instandsetzung	TP 2.1	Wartung und Instandsetzung der für den Flugbetrieb erforderlichen elektronischen oder mechanischen Antriebskomponenten	A 03 U 02	A 05 R 04	N 05	N 06	N 07	U 01
	TP 2.2	Wartung und Instandsetzung der elektronischen oder mechanischen sonstigen Komponenten des UAS inkl. Nutzlast und Kalibrierung der Sensorik	A 03 U 01	A 05 U 02	S 02 R 04	N 05	N 06	N 07
	TP 2.3	Wartung und Instandsetzung der elektronischen oder mechanischen sonstigen Komponenten von zugehörigen Subsystemen inkl. Bediengerät, Antennensysteme, Batterieladesysteme	A 03 U 01	A 05 U 02	A 09 R 04	N 05	N 06	N 07
	TP 2.4	Aktualisierung der Flugbetriebssoftware des UAS	A 03 N 03 U 02	A 06 N 04 R 04	A 07 N 05	S 02 N 06	N 01 N 07	N 02 U 01
	TP 2.5	Aktualisierung der sonstigen Software des UAS inkl. Nutzlast	A 03 N 03 U 02	A 06 N 04 R 04	A 07 N 05	S 02 N 06	N 01 N 07	N 02 U 01
	TP 2.6	Aktualisierung aller weiteren digitalen Softwarekomponenten von zugehörigen Subsystemen inkl. Bediengerät, Antennensysteme, Batterieladesysteme	A 03 N 03 U 02	A 06 N 04 F 04	A 07 N 05 R 04	S 02 N 06	N 01 N 07	N 02 U 01
Datenhaltung der primären Sensordaten	TP 3.1	Auslesen der lokalen Datenspeicher und ggf. des zentralen Datenraums und ggf. Bereinigung der Daten gem. gesetzlicher oder sonstiger regulatorischer Vorgaben	A 06 N 07	S 01 U 01	S 02 U 02	N 03 F 01	N 04 R 05	N 05
	TP 3.2	Speicherung auf dem Zielmedium der Auswerteumgebung	A 06 N 07	S 01 R 05	S 02	N 03	N 04	N 05
	TP 3.3	Löschen der lokalen Datenspeicher und ggf. des zentralen Datenraums	A 06 R 05	N03	N 04	N 05	U 01	U 02
Auswertung der Flugbetriebsdaten	TP 4.1	Technisch-funktionale Auswertung der UAS-Flugbetriebsdaten	A 05	A 06	S 01	S 02	R 04	R 05
	TP 4.2	Qualitative Bewertung der primären Sensordaten der UAS-Nutzlast	A 05	A 06	S 01	S 02	R 04	R 05
	TP 4.3	Taktisch-Operative Auswertung des UAS-Flugbetriebs	A 05	A 06	S 01	S 02	R 03	
	TP 4.4	Einhaltung regulatorischer oder sonstiger Vorgaben während des UAS-Flugbetriebs	A 05	A 06	S 01	S 02	R 03	

Tabelle 7: Übersicht der Teilprozesse beim Betrieb von UAS in BOS.

	ID	Prozesse Anwendungen, Geräte, Netze, Infrastruktur, Akteure	Zugehörige Prozesse bzw. Zielobjekte					
Anwendungen	A 01	Flugplanung	C 01 N 05 P 04	C 02 F 01	S 01 R 03	S 02 P 01	N 03 P 02	N 04 P 03
	A 02	Geographische Informationssysteme	C 01 N 05 P 04	C 02 F 01	S 01 R 03	S 02 P 01	N 03 P 02	N 04 P 03
	A 03	Wartung und Instandhaltung	C 01 N 01 N 07 P 01	C 02 N 02 U 01 P 02	S 01 N 03 U 02 P0 3	S 02 N 04 F 01	D 01 N 05 R 04	D 02 N 06 R 06
	A 04	Fernsteuerung	D 01 U 02 P 01	D 02 F 01 P 02	N 01 F 04 P 03	N 06 R 03	N 07 R 06	U 01 R 07
	A 05	Fernüberwachung	C 01 N 01 N 07 R 05	C 02 N 02 U 01 R 06	S 01 N 03 U 02 R 07	S 02 N 04 F 01 P 01	D 01 N 05 F 04 P 02	D 02 N 06 R 03 P 03
	A 06	Datenübertragung	C 01 D 01 N 05 F 04 P 01	C 02 D 02 N 06 R 03 P 02	C 03 N 01 N 07 R 04 P 03	C 04 N 02 U 01 R 05	S 01 N 03 U 02 R 06	S 02 N 04 F 01 R 07
	A 07	UAS-Betriebssystem	D 01 P 01	D 02 P 02	N 06 P 03	N 07	R 06	R 07
	A 08	Fernsteuerung Nutzlast	C 01 N 03 F 01 P 02	C 02 N 04 F 04 P 03	D 01 N 05 R 03	D 02 N 07 R 06	N 01 U 01 R 07	N 02 U 02 P 01
	A 09	Batterieverwaltung	C 01	C 02	N 04	R 01	R 04	P 03
	A 10	BOS-Kommunikation	C 04 F 04 P 01	N 03 R 01 P 02	N 05 R 02 P 03	F 01 R 03 P 04	F 02 R 06 P 05	F 03 R 07
	A 11	Leitstelle	C 01 D 01 N 05 F 02 R 06 P 05	C 02 D 02 N 06 F03 R 07	C 03 N 01 N 07 F 04 P 01	C 04 N 02 U 01 R 01 P 02	S 01 N 03 U 02 R 02 P 03	S 02 N 04 F 01 R 03 P 04
	A 12	Luftraumüberwachung	C 03 R 03 P 05	C 04 R 06	N 03 R 07	N 04 P 01	N 05 P 02	F 01 P 04

Geräte	C 01	Arbeitsplatz-Computer	A 01 A 08 N 03 F 04 P 02	A 02 A 09 N 04 R 01 P 03	A 03 A 11 N 05 R 03 P 04	A 04 A 12 U 01 R 04 P 05	A 05 N 01 U 02 R 05	A 06 N 02 F 01 P 01
	C 02	Mobil-Computer	A 01 A 08 N 03 F 04 P 02	A 02 A 09 N 04 R 02 P 03	A 03 A 11 N 05 R 03 P 04	A 04 A 12 U 01 R 04 P 05	A 05 N 01 U 02 R 05	A 06 N 02 F 01 P 01
	C 03	Mobiltelefon	A 10 R 01 P 02	A 11 R 02 P 03	N 03 R 03 P 04	F 01 R 04 P 05	F 02 R 05	F 03 P 01
	C 04	BOS-Digitalfunkgerät	A 10 R 02 P 01	N 03 R 03 P 02	F 01 R 04 P 03	F 02 R 05 P 04	F 03 R 06 P 05	R 01 R 07
	S 01	Virtueller Datenspeicher (*Datenraum*)	A 06 P 03	N 03 P 04	N 04	N05	R 01	R 05
	S 02	Physischer Datenspeicher	A 06 P 03	N 03 P 04	N 04	N 05	R 01	R 05
	D 01	Steuergerät Bodenkontrollstation	A 04 C 02 U 02 P 02	A 05 D 02 F 04 P 03	A 06 N 01 R 01	A 07 N 02 R 02	A 08 N 05 R 03	A 09 U 01 P 01
	D 02	Steuergerät UAS (*on-board-unit*)	A 07 U 02	A 11 R 06	A 12 R 07	N 06 P 03	N 07	U 01
Netze	N 01	Leitungslose Netzwerkkomponenten (*UAS <- > Bodenkontrollstation*)	A 04 C 02 N 06 R 03	A 05 S 01 N 07 R 06	A 06 S 02 U 01 R 07	A 07 D 01 U 02 P 01	A 08 D 02 F 01 P 02	A 09 N 05 F 04
	N 02	Leitungsgebundene Netzwerkkomponenten (*UAS <- > Bodenkontrollstation*)	A 04 C 02 N 06 R 06	A 05 S 01 N 07 R 07	A 06 S 02 U 01 P 01	A 07 D 01 U 02 P 02	A 08 D 02 F 01	A 09 N 05 R 03
	N 03	Leitungslose Netzwerkkomponenten (*sonstige Verbindungen*)	A 10 S 01 R 03	A 11 S 02 R 04	A 12 F 01 R 05	C 02 F 04 P 03	C 03 R 01 P 04	C 04 R 02 P 05
	N 04	Leitungsgebundene Netzwerkkomponenten (*sonstige Verbindungen*)	A 10 S 01 R 05	A 11 S 02 P 03	A 12 R 01 P 04	C 01 R 02 P 05	C 02 R 03	C 03 R 04
	N 05	Schnittstellen zwischen Netzwerkkomponenten	A 01 A 07 C 01 R 03 P 04	A 02 A 08 C 02 R 04 P 05	A 03 A 09 S 01 R 05	A 04 A 10 S 02 P 01	A 05 A 11 F 01 P 02	A 06 A 12 F 04 P 03
	N 06	Primäre interne UAS-Netzwerkkomponenten (*Flugsicherheit*)	A 04 D 02 R 03	A 05 N 05 R 06	A 07 U 01 R 07	A 09 U 02 P 01	C 02 F 01 P 02	D 01 F 04 P 03
	N 07	Sekundäre interne UAS-Netzwerkkomponenten (*sonstige Funktionalitäten*)	A 06 U 01 R 07	A 08 U 02 P 01	C 02 F 01 P 02	D 01 F 04 P 03	D 02 R 03	N 05 R 06

Mobile und Stationäre Infrastruktur	U 01	UAS (*Multicopter*)	A 04 C 02 N 02 R 06	A 05 S 01 N 06 R 07	A 06 S 02 N 07 P 01	A 07 D 01 F 01 P 02	A 08 D 02 F 04 P 03	A 09 N 01 R 03
	U 02	UAS (*Starrflügler*)	A 04 C 02 N 02 R 06	A 05 S 01 N 06 R 07	A 06 S 02 N 07 P 01	A 07 D 01 F 01 P 02	A 08 D 02 F 04 P 03	A 09 N 01 R 03
	F 01	Bodenkontrollstation als mobiler Leitstand, Einsatzleitzentrale	A 01 A 10 C 04 N 03 F 03 P 03	A 02 A 11 S 01 N 04 F 04 P 04	A 04 A 12 S 02 N 05 R 06 P 05	A 05 C 01 D 01 U 01 R 07	A 06 C 02 N 01 U 02 P 01	A 08 C 03 N 02 F 02 P 02
	F 02	Transportfahrzeug	A 10	C 03	C 04	N 03	R 02	P 03
	F 03	Unterstützungsfahrzeug	A 03 P 03	A 10	C 03	C04	N 03	R 02
	F 04	Sonstige mobile Systeme (*z.B. Antennenanlagen*)	A 04 A 11 S 02 U 02 R 07	A 05 A 12 D 01 F 01 P 02	A 06 C 02 N 01 R 02 P 04	A 08 C 03 N 03 R 03	A 09 C 04 N 05 R 05	A 10 S 01 U 01 R 06
	R 01	Innenbereich mit Zugangskontrolle	n.N.					
	R 02	Außenbereich mit Zugangskontrolle	n.N					
	R 03	Bodenkontrollstation als stationärer Leitstand, Einsatzleitzentrale	A 01 A 10 C 04 N 03 F 02 R 07	A 02 A 11 S 01 N 04 F 03 P 01	A 04 A 12 S 02 N 05 F 04 P 02	A 05 C 01 D 01 U 01 R 04 P 03	A 06 C 02 N 01 U 02 R 05 P 04	A 08 C 03 N 02 F 01 R 06 P 05
	R 04	Werkstatt (*Wartung und Instandhaltung*)	A 03 S 01 U 01	A06 S 02 U 02	A 07 D 02 R 01	A 09 N 02 P 02	C 01 N 04 P 03	C 02 N 05
	R 05	Datenzentrum (*Administration und Management*)	A 06 N 04	C 01 N 05	C 02 F 01	S 01 R 03	S 02 P 03	N 03
	R 06	Kontrollierter Luftraum über Grund (*Übung, Erprobung und Ausbildung*)	A 04 A 10 N 02 P 02	A 05 A 11 N 06 P 03	A 06 A 12 N 07 P 04	A 07 D 01 U 01 P 05	A 08 D02 U 02	A 09 N 01 P 01
	R 07	Offener Luftraum über Grund (*Einsatz*)	A 04 A 10 N 02 P 02	A 05 A 11 N 06 P 03	A 06 A 12 N 07 P 04	A 07 D 01 U 01 P 05	A 08 D 02 U 02	A 09 N 01 P 01

Akteure	P 01	Fernpilot	A 01 A 09 C 04 N 02 U 02	A 04 A 10 S 01 N 03 F 01	A 05 A 11 S 02 N 05 F 04	A 06 A 12 D 01 N 06 R 03	A 07 C 02 D 02 N 07 06	A 08 C 03 N 01 U 01 R 07
	P 02	Betriebsüberwachung	A 01 A 09 C 04 N 02 U 02 R 07	A 04 A 10 S 01 N 03 F 01	A 05 A 11 S 02 N 05 F 04	A 06 A 12 D 01 N 06 R 02	A 07 C 02 D 02 N 07 R 03	A 08 C 03 N 01 U 01 R 06
	P 03	Betriebsunterstützung	A 01 C 04 F 01 R 04	A 02 S 01 F 02 R 05	A 03 S 02 F 03 R 06	C 01 N 03 F 04	C 02 N 04 R 01	C 03 N 05 R 03
	P 04	Leitungspersonal (*intern*)	A 01 C 03 R 01	A 02 C 04 R 02	A 10 N 03 R 03	A 11 N 04	C 01 N 05	C 02 F 01
	P 05	Leitungspersonal (*extern*)	A 01 C 03 R 01	A 02 C 04 R 02	A 10 N 03 R 03	A 12 N 04	C 01 N 05	C 02 F 01
	P 06	Unbeteiligte Dritte	n.N.					

Tabelle 8: Übersicht der Prozesse Anwendungen, Geräte, Netze, Infrastruktur und Akteure.

6. Betrachtung des Schutzbedarfs

Der Schutzbedarf der Prozesse, Komponenten und Anwendungsfälle des Informationsverbunds dieses IT-Grundschutz-Profils für den Betrieb von UAS in BOS ergibt sich aus den möglichen Auswirkungen durch die Verletzung der Grundwerte der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit). Der Schutzbedarf wird anhand der im Informationsverbund erfassten, verarbeiteten und ausgewerteten Daten sowie der zugehörigen Informationsflüsse gemäß den zugrundeliegenden Prozessen ermittelt. In dem hier vorgelegten IT-Grundschutz-Profil wird allgemein von einem normalen Schutzbedarf ausgegangen.

Die Schutzbedarfsfeststellung erfolgt durch das vom verantwortlichen Informationssicherheits-Manager (ISM) beauftragte Informationssicherheits-Managementteam (ISMT) des jeweiligen Organisationsbereichs der BOS unter Mitwirkung der Prozessverantwortlichen und der Dateneigentümer für die im Informationsverbund abgebildeten Prozesse. Im Allgemeinen sollten UAS eingesetzt werden, deren Sicherheits- und Systemarchitektur konform mit den entsprechenden europäischen und nationalen rechtlichen und technischen Normen einhergeht. Die Schutzbedarfsfeststellung sollte daher z.B. als zentrale Anforderung das Sicherheitsniveau des UAS-Herstellers und ggf. des Cloud-

Providers betrachten. Außerdem sollten entsprechend dem Stand der Technik Sicherheitseinrichtungen (z.B. secure boot)[19] verwendet werden.

BOS verfügen im Allgemeinen über eine hierarchische Organisationsstruktur mit einer räumlichen oder administrativen Gliederung sowie festgelegten Verantwortlichkeiten und Befugnissen. Die Anwendung der Empfehlungen dieses IT-Grundschutz-Profils im Rahmen einer Schutzbedarfsfeststellung und die Ableitung eines Sicherheitskonzepts sind daher erforderlichenfalls für jede Ebene unter Berücksichtigung der verfügbaren fachlichen, administrativen und sonstigen Ressourcen entsprechend anzupassen. Hierbei sollen die Führungsbereiche der Leitungsebene allgemeine und einheitliche Regelungen festlegen und die nachgeordneten Organisationsbereiche der operativen Ebenen bei der Einführung, Umsetzung und Anpassung von Maßnahmen gemäß den Zielsetzungen dieses IT-Grundschutz-Profils unterstützen.[20]

Die Schäden, die bei einer Verletzung der Grundwerte der Informationssicherheit auftreten können, werden gemäß dem Klassifikationssystem des BSI in sechs allgemeine Schadenszenarien (SZ) unterschieden:

(1) Verstoß gegen Gesetze, Vorschriften und Verträge,
(2) Beeinträchtigung des informationellen Selbstbestimmungsrechts,
(3) Beeinträchtigung der persönlichen Unversehrtheit,
(4) Beeinträchtigung der Aufgabenerfüllung,
(5) Negative Innen- oder Außenwirkung,
(6) Finanzielle Auswirkungen.

Die konkreten Auswirkungen und möglichen Schadensszenarien können je nach Anwendungsfall variieren.

---

[19] Vergleiche hierzu Kapitel 9.2 Datensicherheit.

[20] Es wird weiterhin auf die Skalierbarkeit des Informationssicherheitsmanagements gemäß den im BSI-Standard 200-2 beschriebenen Absicherungsvarianten (Standard-Absicherung, Basis-Absicherung und Kern-Absicherung) verwiesen.

Die nachfolgende Tabelle enthält mögliche Beispiele für jedes der sechs Schadenszenarien.

ID	Beispiele für Schadenszenarien
SZ 01	<u>Verstoß gegen Gesetze, Vorschriften und Verträge</u> Veränderte oder unvollständige Daten können zu Verstößen gegen gesetzliche, vertragliche und sonstige Regelungen führen (*z.B. unbeabsichtigtes Einfliegen des UAS in eine Flugverbotszone oder Überschreitung der zulässigen maximalen Flughöhe*).
SZ 02	<u>Beeinträchtigung des informationellen Selbstbestimmungsrechts</u> Personenbezogene Daten von Mitarbeitern, Kunden oder unbeteiligten Dritten werden ohne Autorisierung veröffentlicht oder unbefugten Dritten zugänglich gemacht (*z.B. unterbliebene Anonymisierung der personenbezogenen Merkmale unbeteiligter Dritter in Videoaufnahmen und Weiterleitung der Aufnahmen an Dritte.)* Unternehmenskritische bzw. -vertrauliche Daten werden ohne Autorisierung veröffentlicht oder unbefugten Dritten zugänglich gemacht (*z.B. irrtümliche Versendung von Flugplänen an unbeteiligte Dritte*).
SZ 03	<u>Beeinträchtigung der persönlichen Unversehrtheit</u> Ein unkontrollierter Absturz des UAS aufgrund eines Systemversagens führt zu einem Personenschaden eines unbeteiligten Dritten (*z.B. unbeabsichtigter Einflug in den Nahbereich eines Störsenders führt zur Überlagerung und Störung der Signalverbindung zwischen UAS und Steuerungskontrolle und resultiert in einem unkontrollierten Absturz mit Personenschaden eines unbeteiligten Dritten*).
SZ 04	<u>Beeinträchtigung der Aufgabenerfüllung</u> Aufgrund einer technischen Fehlfunktion muss ein Flug vorzeitig abgebrochen werden (*z.B. ungeplanter Leistungsverlust eines Batteriesystems bedingt den vorzeitigen Abbruch eines technischen Inspektionsflugs*).
SZ 05	<u>Negative Innen- oder Außenwirkung</u> Eine Fehlfunktion während eines UAS-Einsatzes führt zu einem Reputationsverlust der zugehörigen Organisation (*z.B. Absturz eines UAS während einer Vorführung bei einer öffentlichen Veranstaltung mit Sachschäden an geparkten Fahrzeugen*).
SZ 06	<u>Negative finanzielle Auswirkungen</u> Ein Bedienungsfehler während eines Einsatzflugs führt zu einem Schadensersatzanspruch eines unbeteiligten Dritten (*z.B. Sachschaden an einem Gebäude aufgrund von unsachgemäßen Flugmanövern des Fernpiloten*).

Tabelle 9: Übersicht von beispielhaften Schadensszenarien.

Die Eintrittswahrscheinlichkeit und die Auswirkung eines Schadens können im Vorfeld nicht konkret für jedes mögliche Schadensereignis ermittelt werden. Gemäß den Empfehlungen des IT-Grundschutzes[21] erfolgt die Klassifizierung im Rahmen der Schutzbedarfsfeststellung daher in den drei allgemeinen Kategorien normal, hoch und sehr hoch.

Die Auswirkungen eines Schadens können sich auf interne oder externe Prozesse und ihre Komponenten sowie auf beteiligte und unbeteiligte natürliche und juristische Personen beziehen.

Das Schadensereignis ist der jeweiligen Kategorie zuzuordnen, sobald mindestens eine Auswirkung erreicht wurde (z.B. wird ein überschaubarer und leicht zu behebender Schaden mit Auswirkungen auf mehrere Teilprozesse der Kategorie „hoch“ zugeordnet).

Der Schutzbedarf soll für alle Prozesse, Teilprozesse und Komponenten (z.B. Anwendungen, Geräte, Netze, stationäre und mobile Infrastruktur, Akteure) durch die jeweilige BOS für jedes mögliche Schadensereignis ermittelt werden.

Die nachfolgende Tabelle beschreibt die Auswirkungen eines Schadensereignisses für jede der drei Kategorien.

Kategorie	**Auswirkungen eines Schadens**	
normal (1)	1.1 1.2 1.3	Die Schadensauswirkungen sind überschaubar. Sie lassen sich leicht beheben. Sie sind auf einen Teilprozess begrenzt.
hoch (2)	2.1 2.2 2.3	Die Schadensauswirkungen sind erheblich. Sie lassen sich nur mit erheblichem Aufwand beheben. Sie betreffen mehrere Teilprozesse.
sehr hoch (3)	3.1 3.2 3.3	Die Schadensauswirkungen erreichen ein existenz- oder lebensbedrohliches Ausmaß. Der Schaden lässt sich eingrenzen und mindern, aber nicht vollumfänglich beheben. Sie betreffen den gesamten Prozess.

Tabelle 10: Übersicht der Schadenskategorien und mögliche Auswirkungen.

[21] Vergleiche den BSI-Standard 200-2 zur IT-Grundschutz-Methodik.

6.1 Risikobetrachtung

Im Allgemeinen ist auch bei strengster Auslegung und Berücksichtigung der ermittelten Schutzbedarfe keine vollumfängliche Betriebssicherheit im Hinblick auf eine absolute Risikominimierung des Eintritts von Schadensereignissen zu erreichen. Zielsetzung ist daher, das Bewusstsein von Akteuren und Verantwortlichen zu schärfen und das Restrisiko durch geeignete Maßnahmen und Vorgaben auf ein akzeptables und zu verantwortendes Maß zu senken.

Aufgrund der besonderen Anforderungen an den Betrieb von UAS in Behörden und Organisationen mit Sicherheitsaufgaben ist eine Risikoanalyse zur Ermittlung der allgemeinen Eintrittswahrscheinlichkeit, der Schadenshöhe und des verbleibenden Restrisikos immer dann erforderlich, wenn ein hoher Schutzbedarf ermittelt wurde, wenn kein passender IT-Grundschutz-Baustein für den zugehörigen Prozess beziehungsweise für das Zielobjekt vorliegt oder wenn ein besonderes Einsatzszenario vorliegt. Dies gilt insbesondere für Prozesse und Komponenten, die ausschließlicher Bestandteil dieses IT-Grundschutz-Profils sind und nicht über Bausteine oder Profile des IT-Grundschutz-Kompendiums des BSI abgebildet werden. Betroffen sind hiervon also alle beschriebenen Teilprozesse beim Betrieb von UAS.

Bei der Risikoanalyse sind die Empfehlungen des BSI gemäß des BSI-Standard 200-3 (Risikoanalyse auf der Basis von IT-Grundschutz) zu beachten. Hierbei sind außerdem die im IT-Grundschutz-Kompendium des BSI beschriebenen elementaren Gefährdungen für die Erstellung einer Gefährdungsübersicht zu berücksichtigen, diese sind bei Bedarf entsprechend zu ergänzen, um den Gesamtprozess inklusive aller Komponenten bei der Risikoanalyse abzubilden.

Im Rahmen der Risikoanalyse festgelegte operative oder organisatorische Sicherheitsmaßnahmen zur Risikominimierung von Schadensauswirkungen der Kategorien „hoch“ und „sehr hoch“ sollen grundsätzlich auch auf Komponenten der Kategorie „normal“ angewendet werden, sofern dies erforderlich, geeignet und verhältnismäßig erscheint.

Abbildung 9: Funktionale Komponenten können die Betriebssicherheit eines UAS in spezifischen Einsatzszenarien erhöhen und einen UAS-Verlust vermeiden (z.B. Reservebatterien, Flugabbruchsystem zur kontrollierten Notlandung und Landegestell mit Schwimmern, Greifklaue zur Bergung und Rückführung eines flugunfähigen UAS). Eine Verbesserung der Betriebssicherheit kann sich somit vorteilhaft auf die Informationssicherheit auswirken und zu einer Verminderung des Risikos beitragen.

6.2 Risikoanalyse

Die Risikoanalyse des IT-Grundschutz-Profils für den Betrieb von Uncrewed Aircraft Systems in Behörden und Organisationen mit Sicherheitsaufgaben folgt den Empfehlungen des BSI-Standard 200-3 (Risikoanalyse auf der Basis von IT-Grundschutz).

Die Risikoanalyse gliedert sich in fünf Einzelmaßnahmen:

(1) Gefährdungsübersicht,

(2) Risikoeinstufung,

(3) Risikobehandlung,

(4) Konsolidierung der Sicherheitskonzeption,

(5) Implementierung im Sicherheitsprozess.

Als Grundlage für die Risikoanalyse und die dabei durchgeführte Ermittlung des Gefährdungspotentials werden die nachfolgend aufgeführten Tabellen des vorgelegten IT-Grundschutz-Profils sowie die seitens des BSI entwickelte Risikomatrix zur Betrachtung der jeweiligen Schadensauswirkungen und Eintrittswahrscheinlichkeiten herangezogen[22].

Zur Einordnung der einzelnen Risiken wird folgende Kategorisierung verwendet:

Kategorie	**Risikobeschreibung**
gering (1)	Die bereits umgesetzten oder im Sicherheitskonzept zur Umsetzung vorgesehenen Sicherheitsmaßnahmen bieten einen ausreichenden Schutz. (*In der Praxis ist es üblich, geringe Risiken zu akzeptieren und die Gefährdung dennoch zu beobachten.*)
mittel (2)	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen reichen möglicherweise nicht aus.
hoch (3)	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. Das Risiko kann mit einer großen Wahrscheinlichkeit nicht akzeptiert werden.
sehr hoch (4)	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. Das Risiko kann mit einer sehr großen Wahrscheinlichkeit nicht akzeptiert werden. (*In der Praxis werden sehr hohe Risiken selten akzeptiert.*)

Tabelle 11: Übersicht der Risikokategorien und der zugehörigen Beschreibungen.

[22] Vergleiche den BSI-Standard 200-2 zur Risikobewertung.

Zur Betrachtung der jeweiligen Schadensauswirkungen und Eintrittswahrscheinlichkeiten wird die Risikomatrix des BSI herangezogen[23]. Im Allgemeinen ist das Eingehen von hohen und sehr hohen Risiken für Anwendungsfälle beim Betrieb eines UAS zu vermeiden.

Auswirkungen				
sehr hoch	*mittel*	*hoch*	*sehr hoch*	*sehr hoch*
hoch	*mittel*	*mittel*	*hoch*	*sehr hoch*
mittel	*niedrig*	*mittel*	*mittel*	*hoch*
niedrig	*niedrig*	*niedrig*	*mittel*	*mittel*
	unwahrscheinlich	**gering**	**mittel**	**groß**
				Eintrittshäufigkeit

Abbildung 10: Schematische Risikomatrix gemäß BSI-Standard 200-3.

[23] Siehe Tabelle 11 und Abbildung 10.

7. Anforderungen und Maßnahmen

Grundlage für die Umsetzung des IT-Grundschutzes gemäß dem IT-Grundschutz-Profil für den Betrieb von Uncrewed Aircraft Systems in Behörden und Organisationen mit Sicherheitsaufgaben sind die im IT-Grundschutz-Kompendium des BSI enthaltenen Prozess- und Systembausteine.

7.1 Prozess-Bausteine

Auf den Informationsverbund dieses IT-Grundschutz-Profils werden die im Folgenden aufgeführten übergreifenden Prozess-Bausteine angewendet. Hier werden insbesondere Aspekte der Informationssicherheit betrachtet, die allgemeingültig für die im Informationsverbund abgebildeten Prozesse sind.

Die nachfolgenden Tabellen enthalten eine Übersicht der zugrundeliegenden Prozess-Bausteine. Die nicht berücksichtigten Bausteine sind durchkreuzt, werden aber der Übersichtlichkeit halber hier aufgeführt. Weiterhin wird teilweise eine inhaltliche Eingrenzung vorgenommen oder es wird die fehlende Relevanz im Kontext des IT-Grundschutz-Profils begründet. Der Ausschluss ist nicht als verbindliche Vorgabe anzusehen, im anwendungsbezogenen Einzelfall können die hier nicht berücksichtigten Bausteine selbstverständlich als Bestandteil der jeweiligen Sicherheitskonzeption auf geeignete Weise berücksichtigt werden.

ID	**Baustein Sicherheitsmanagement**
ISMS.1	Sicherheitsmanagement

Tabelle 12: Sicherheitsmanagement.

ID	**Bausteine Organisation und Personal**
ORP.1	Organisation
ORP.2	Personal
ORP.3	Sensibilisierung und Schulung zur Informationssicherheit
ORP.4	Identitäts- und Berechtigungsmanagement
ORP.5	Compliance Management und Anforderungsmanagement

Tabelle 13: Organisation und Personal.

ID	Bausteine Konzeption und Vorgehensweise	Eingrenzung bzw. Ablehnung
CON.1	Kryptokonzept	
CON.2	Datenschutz	
CON.3	Datensicherungskonzept	
CON.6	Löschen und Vernichten	
CON.7	Informationssicherheit und Auslandsreisen	
CON.8	~~Software-Entwicklung~~	~~Kein Bestandteil des Informationsverbunds.~~
CON.9	Informationsaustausch	
CON.10	~~Entwicklung von Webanwendungen~~	~~Kein Bestandteil des Informationsverbunds.~~
CON.11.1	Geheimschutz, Verschlusssachen (VS-NfD)	

Tabelle 14: Konzeption und Vorgehensweise.

ID	Bausteine Detektion und Reaktion	Eingrenzung bzw. Ablehnung
DER.1	Detektion sicherheitsrelevanter Ereignisse	
DER.2.1	Behandlung von Sicherheitsvorfällen	
DER.2.2	Vorsorge für die IT-Forensik	
DER.2.3	Bereinigung komplexer Sicherheitsvorfälle	
DER.3.1	Audits und Revisionen	
DER.3.2	Revision auf Basis des Leitfadens IS-Revision	Ggf. gemäß Vorgabe der BOS-Fachaufsicht.
DER.4	Notfallmanagement	

Tabelle 15: Detektion und Reaktion.

ID	Bausteine Betrieb	Eingrenzung bzw. Ablehnung
OPS.1.1.1	Allgemeiner IT-Betrieb	Beschränkung auf Anwendungsfälle mit direktem Bezug zum IT-Grundschutz-Profil.
OPS.1.1.2	Ordnungsgemäße IT-Administration	
OPS.1.1.3	Patch- und Änderungsmanagement	
OPS.1.1.4	Schutz vor Schadprogrammen	
OPS.1.1.5	Protokollierung	
OPS.1.1.6	Software-Tests und Freigaben	Insbesondere bei Verwendung von Open-Source Software (z.B. UAS-Betriebssysteme).
OPS.1.1.7	Systemmanagement	
OPS.1.2.2	Archivierung	
OPS.1.2.4	~~Telearbeit~~	~~Kein Bestandteil des Informationsverbunds.~~
OPS.1.2.5	Fernwartung	
OPS.1.2.6	NTP-Zeitsynchronisation	
OPS.2.2	Cloud-Nutzung	Insbesondere dezidierte Datenräume (BOS-Cloud).
OPS.2.3	Nutzung von Outsourcing	Beschränkung auf Zusammenarbeit mit anderen BOS.
OPS.3.2	Anbieten von Outsourcing	Beschränkung auf Zusammenarbeit mit anderen BOS.

Tabelle 16: Betrieb.

7.2 System-Bausteine

Auf den Informationsverbund dieses IT-Grundschutz-Profils werden die im Folgenden aufgeführten System-Bausteine angewendet. Hier werden insbesondere Aspekte der Informationssicherheit betrachtet, die für einen oder mehrere Teilprozesse des Informationsverbunds dieses IT-Grundschutz-Profils maßgeblich sind.

Die nachfolgenden Tabellen enthalten eine Übersicht der zugrundeliegenden System-Bausteine. Die nicht berücksichtigten Bausteine sind durchkreuzt, werden aber der Übersichtlichkeit halber hier aufgeführt. Weiterhin wird teilweise eine inhaltliche Eingrenzung vorgenommen oder es wird die fehlende Relevanz im Kontext des IT-Grundschutz-Profils begründet.

Der Ausschluss ist nicht als verbindliche Vorgabe anzusehen, im anwendungsbezogenen Einzelfall können die hier nicht berücksichtigten Bausteine selbstverständlich als Bestandteil der jeweiligen Sicherheitskonzeption auf geeignete Weise berücksichtigt werden.

ID	Bausteine Anwendungen	Eingrenzung bzw. Ablehnung
APP.1.1	~~Office-Produkte~~	~~Kein Bestandteil des Informationsverbunds.~~
APP.1.2	Webbrowser	
APP.1.4	Mobile Anwendung (Apps)	
APP.2.1	Allgemeiner Verzeichnisdienst	
APP.2.2	Active Directory Domain Services	
APP.2.3	OpenLDAP	
APP.3.1	Webanwendungen und Webservices	
APP.3.2	Webserver	
APP.3.3	Fileserver	
APP.3.4	~~Samba~~	~~Kein Bestandteil des Informationsverbunds.~~
APP.3.6	~~DNS-Server~~	~~Kein Bestandteil des Informationsverbunds.~~
APP.4.2	~~SAP-ERP-System~~	~~Kein Bestandteil des Informationsverbunds.~~
APP.4.3	~~Relationale Datenbanksysteme~~	~~Kein Bestandteil des Informationsverbunds.~~
APP.4.4	~~Kubernetes~~	~~Kein Bestandteil des Informationsverbunds.~~
APP.4.6	~~SAP ABAP-Programmierung~~	~~Kein Bestandteil des Informationsverbunds.~~
APP.5.2	~~Microsoft Exchange und Outlook~~	~~Kein Bestandteil des Informationsverbunds.~~
APP.5.3	~~Allgemeiner E-Mail-Client und -Server~~	~~Kein Bestandteil des Informationsverbunds.~~
APP.5.4	~~Unified Communications und Collaboration~~	~~Kein Bestandteil des Informationsverbunds.~~
APP.6	Allgemeine Software	
APP.7	Entwicklung von Individualsoftware	Insbesondere bei Anpassung von Open-Source Software (z.B. UAS-Betriebssysteme).

Tabelle 17: Anwendungen.

ID	Bausteine IT-Systeme	Eingrenzung bzw. Ablehnung
SYS.1.1	Allgemeiner Server	
SYS.1.2.2	~~Windows Server 2012~~	~~Kein Bestandteil des Informationsverbunds.~~
SYS.1.2.3	~~Windows Server~~	~~Kein Bestandteil des Informationsverbunds.~~
SYS.1.3	~~Server unter Linux und Unix~~	~~Kein Bestandteil des Informationsverbunds.~~
SYS.1.5	Virtualisierung	
SYS.1.6	Containerisierung	
SYS.1.7	~~IBM Z~~	~~Kein Bestandteil des Informationsverbunds.~~
SYS.1.8	Speicherlösungen	
SYS.1.9	Terminal-Server	
SYS.2.1	Allgemeiner Client	
SYS.2.2.3	~~Clients unter Windows~~	~~Kein Bestandteil des Informationsverbunds.~~
SYS.2.3	~~Clients unter Linux und Unix~~	~~Kein Bestandteil des Informationsverbunds.~~
SYS.2.4	~~Clients unter macOS~~	~~Kein Bestandteil des Informationsverbunds.~~
SYS.2.5	Client-Virtualisierung	
SYS.2.6	~~Virtual Desktop Infrastructure~~	~~Kein Bestandteil des Informationsverbunds~~
SYS.3.1	Notebooks	
SYS.3.2.1	Allgemeine Smartphones und Tablets	
SYS.3.2.2	Mobile Device Management (MDM)	
SYS.3.2.3	~~iOS (for Enterprise)~~	~~Kein Bestandteil des Informationsverbunds.~~
SYS.3.2.4	~~Android~~	~~Kein Bestandteil des Informationsverbunds.~~
SYS.3.3	~~Mobiltelefon~~	~~Kein Bestandteil des Informationsverbunds.~~
SYS.4.1.	~~Drucker, Kopierer, Multifunktionssysteme~~	~~Kein Bestandteil des Informationsverbunds.~~
SYS.4.3	Eingebettete Systeme	
SYS.4.4	Allgemeines IoT-Gerät	
SYS.4.5	Wechseldatenträger	

Tabelle 18: Informationstechnik-Systeme.

ID	Bausteine Industrielle IT	Eingrenzung bzw. Ablehnung
IND.1	Prozessleit- und Automatisierungstechnik	Ausschließlich als Komponente eines UAS.
IND.2.1	Allgemeine ICS-Komponente	Ausschließlich als Komponente eines UAS.
IND.2.2	Speicherprogrammierbare Steuerung (SPS)	Kein Bestandteil des Informationsverbunds.
IND.2.3	Sensoren und Aktoren	Ausschließlich als Komponente eines UAS.
IND.2.4	Maschine	Ausschließlich als Komponente eines UAS.
IND.2.7	Safety Instrumented Systems	z.B. Anti-Kollisionssysteme, automatische Rückkehr zur Startposition bei Verbindungsabbruch…
IND.3.2	~~Fernwartung im industriellen Umfeld~~	~~Kein Bestandteil des Informationsverbunds.~~

Tabelle 19: Industrielle Informationstechnik.

ID	Bausteine Netze und Kommunikation	Eingrenzung bzw. Ablehnung
NET.1.1	Netzarchitektur und -design	z.B. als Komponente eines UAS-Betriebsnetz
NET.1.2	Netzmanagement	z.B. als Komponente eines UAS-Betriebsnetz
NET.2.1	WLAN-Betrieb	z.B. als Komponente eines UAS-Betriebsnetz
NET.2.2	WLAN-Nutzung	z.B. als Komponente eines UAS-Betriebsnetz
NET.3.1	Router und Switches	z.B. als Komponente eines UAS-Betriebsnetz
NET.3.2	Firewall	z.B. als Komponente eines UAS-Betriebsnetz
NET.3.3	VPN	z.B. als Komponente eines UAS-Betriebsnetz
NET.3.4	Network Access Control	z.B. als Komponente eines UAS-Betriebsnetz
NET.4.1	TK-Anlagen	z.B. als Komponente eines UAS-Betriebsnetz, als technische Anlagen für BOS-Digitalfunk
NET.4.2	~~VoIP~~	~~Kein Bestandteil des Informationsverbunds.~~
NET.4.3	~~Faxgeräte und Faxserver~~	~~Kein Bestandteil des Informationsverbunds.~~

Tabelle 20: Netze und Kommunikation.

ID	Bausteine Infrastruktur	Eingrenzung bzw. Ablehnung
INF.1	Allgemeines Gebäude	z.B. technischer Lagerraum
INF.2	Rechenzentrum sowie Serverraum	
INF.5	Raum für sonstige technische Infrastruktur	z.B. Werkstatt
INF.7	Büroarbeitsplatz	z.B. Arbeitsplatz Auswerter, Leitungspersonal
INF.8	~~Häuslicher Arbeitsplatz~~	~~Kein Bestandteil des Informationsverbunds.~~
INF.9	Mobiler Arbeitsplatz	
INF.10	~~Besprechungs- und Schulungsraum~~	~~Kein Bestandteil des Informationsverbunds.~~
INF.11	Allgemeines Fahrzeug	
INF.12	Verkabelung	z.B. sog. „tethered“ UAS
INF.13	~~Technisches Gebäudemanagement~~	~~Kein Bestandteil des Informationsverbunds.~~
INF.14	~~Gebäudeautomation~~	~~Kein Bestandteil des Informationsverbunds.~~

Tabelle 21: Infrastruktur.

7.3 Rollen und Rechte

Die Konzeption von Rollen und Rechten sind im Allgemeinen kein primärer Bestandteil eines IT-Grundschutz-Profils sowie des zugehörigen Informationsverbunds. Sie werden hier aus Gründen der Vollständigkeit aufgeführt und sind als Ergänzung zur Beschreibung der beteiligten Akteure anzusehen[24].

Weiterhin bildet das Rollen- und Rechtekonzept des Informationsverbunds die Grundlage für eine Rollenbasierte Eingriffs- und Zugriffskontrolle (RBAC, role-based access control) zum dokumentierten und limitierten Zugriff auf die Datenhaltungen des Informationsverbunds.

Im Folgenden werden die einzelnen Rollen und ihr Verhältnis zueinander beschrieben.

Der **Fernpilot** ist verantwortlich für die Flugsicherheit, den Flugbetrieb und die Durchführung des UAS-Einsatzes. Die Durchführung des Flugbetriebs kann durch den Fernpiloten bei Bedarf an den Co-Piloten delegiert werden (z.B. zur Gewährleistung von Pausen- und Rüstzeiten während eines längeren Einsatzzeitraums). Er koordiniert und leitet die Tätigkeiten des ihm fachlich unterstellten Personals aus den Bereichen Betriebsüberwachung und Betriebsunterstützung.

Der **Co-Fernpilot** unterstützt den Fernpiloten bei der Durchführung des Flugbetriebs und kann dabei sekundäre Funktionen (z.B. Kommunikation mit der Leitstelle) übernehmen und den Fernpiloten erforderlichenfalls bei der Durchführung des Flugbetriebs vertreten.

Der **Luftraumbeobachter** unterstützt den Fernpiloten bei der Beobachtung des Luftraums und warnt diesen beim Eintritt von Ereignissen mit Auswirkungen auf die Flugsicherheit (z.B. Einflug von anderen Luftfahrtsystemen in den Einsatzraum, einfliegende Vogelschwärme im Nahbereich des UAS, meteorologische Ereignisse). Die Ausübung dieser Rolle ist insbesondere beim Einsatz von „first-person-view“ UAS zur Gewährleistung der Flugsicherheit erforderlich.

Der **Nutzlastspezialist** überwacht die Funktionsfähigkeit von einsatzspezifischen Sensoren (z.B. sekundäre Thermalkamerasysteme) und Wirkmitteln (z.B. Scheinwerfer zur Ausleuchtung von bodengebundenen Ereignissen, Einsatz von Lautsprechersystemen) des UAS. Weiterhin überwacht und gewährleistet der Nutzlastspezialist eine hinreichende Qualität der erfassten Daten für die Erfüllung des Einsatzziels (z.B. Aufnahme von Orthofotos mit ausreichender Auflösung).

---

[24] Vergleiche hierzu auch Kapitel 5.8.

Der **Wartungstechniker** verantwortet den technischen Zustand des UAS und unterstützt den Fernpiloten bei der technischen Vor- und Nachbereitung des Flugbetriebs (z.B. Herrichtung des Start- und Landeplatzes, Einrüsten von Batterien, Durchführung von „pre-flight“ Funktionstests).

Der **Auswerter** bereitet die beim UAS-Einsatz erfassten Daten auf (z.B. Georeferenzierung und Bemaßung von Bilddaten, Zusammenfassung von Orthofotos zu einem digitalen Kartenwerk), interpretiert die Daten und führt die eigentliche Auswertung gemäß den Zielsetzungen des UAS-Einsatzes durch. Je nach Einsatzart kann die Auswertung während des Einsatzes oder nachgelagert erfolgen.

Das **interne Leitungspersonal** nimmt die Aufgaben der Einsatzleitung wahr und ist oftmals außerdem Fach- und Disziplinarvorgesetzter der am operativen UAS-Betrieb beteiligten Akteure. Weiterhin hält das interne Leitungspersonal die Verbindung zu anderen Teilbereichen der BOS oder zu Teilbereichen anderer BOS, sofern es der UAS-Einsatz erfordert.

Das **externe Leitungspersonal** nimmt Aufgaben der übergeordneten Luftsicherheit und der Luftraumüberwachung wahr (z.B. Gewährleistung der Flugsicherheit).

Grundsätzlich ist es zulässig, dass eine Person mehr als eine Rolle ausübt, sofern sich der Zeitpunkt der Ausübung nicht überlagert (z.B. kann ein Wartungstechniker gleichzeitig Aufgaben eines Luftraumbeobachters wahrnehmen) und es keine Zielkonflikte bei den tätigkeitsbezogenen Verantwortlichkeiten gibt.

Akteure
Flugbetriebsdurchführung (z.B. Fernpilot, Co-Fernpilot)
Betriebsüberwachung (z.B. Luftraumbeobachter, Nutzlastspezialist)
Betriebsunterstützung (z.B. Wartungstechniker, Auswerter)
Leitungspersonal - intern (z.B. Einsatzleiter, Fach- und Disziplinarvorgesetzte)
Leitungspersonal - extern (z.B. Luftraumüberwachungspersonal)

Tabelle 22: Akteure.

8. Restrisiken

Das verbleibende Restrisiko umfasst alle Risiken aus dem Betrieb von Uncrewed Aircraft Systems in Behörden und Organisationen mit Sicherheitsaufgaben im Kontext des vorgelegten IT-Grundschutz-Profils, die nicht durch geeignete organisatorische, technische, personelle oder sonstige Maßnahmen ausgeschlossen werden können.

Im Allgemeinen sollten durch eine BOS nach gründlichster Abwägung nur Risiken eingegangen werden, die nach Ausschöpfung aller vertretbaren und durchführbaren Maßnahmen der Risikominderung maximal mit einer geringen Eintrittshäufigkeit und einer mittleren Auswirkung bewertet werden[25].

Im Einzelfall kann ein höheres Risiko akzeptiert werden, z.B. wenn die entsprechende Gefährdung nur unter ganz speziellen Voraussetzungen zu einem Schaden führen kann oder wenn gegen die entsprechende Gefährdung aktuell keine wirksamen Gegenmaßnahmen bekannt sind und sie sich beim Betrieb von UAS kaum vermeiden lassen.

Das verbleibende Restrisiko muss durch die verantwortliche Leitungsebene der BOS getragen werden, die verbleibenden Risiken und die Verantwortlichkeiten sind revisionssicher zu dokumentieren.

9. Anwendungshinweise

Die im IT-Grundschutz-Profil beschriebenen Anwendungshinweise für den Betrieb von Uncrewed Aircraft Systems in Behörden und Organisationen mit Sicherheitsaufgaben sind für den Bereich der Informationssicherheit zu beachten, eine Umsetzung der Empfehlungen erfolgt im eigenen Ermessen der jeweiligen BOS.

Fragestellungen der Datensicherheit sind kein primärer Bestandteil des vorgelegten IT-Grundschutz-Profils. Im Rahmen der zugehörigen Anwendungshinweise wird eine elementare Berücksichtigung der Vorgaben der Datensicherheit und der zugehörigen Anforderungen des Datenschutzes dennoch als zielführend erachtet, um eine ganzheitliche, abgestimmte und ausgewogene Betrachtungsweise zu gewährleisten[26].

---

[25] Vergleiche hierzu auch die Risikomatrix in Kapitel 6.2.

[26] Siehe hierzu Kapitel 9.2 und vergleiche die Festlegung des Geltungsbereichs in Kapitel 3.

9.1 Informationssicherheit

Die bei der Anwendung des IT-Grundschutz-Profils ermittelten Anforderungen an die Informationssicherheit sind für die zugrundeliegenden Anwendungsfälle im abgeleiteten Sicherheitskonzept zu integrieren und beim UAS-Betrieb zu berücksichtigen und umzusetzen.

Weitere Informationen zu den zugrundeliegenden Anforderungen finden sich in den Umsetzungshinweisen zu den einzelnen Bausteinen im IT-Grundschutz-Kompendium des BSI.

Die ermittelten Anforderungen sind kontinuierlich anlassbezogen oder spätestens beim nächsten Prüfungsintervall des IT-Grundschutz-Profils mit der Zielsetzung der Aufrechterhaltung des angestrebten Sicherheitsstandards zu überprüfen und ggf. anzupassen. Hierbei erfolgt auch eine Berücksichtigung der zwischenzeitlich aufgetretenen weiteren technischen Entwicklung im Kontext des vorgelegten IT-Grundschutz-Profils.

Als prozessbasierter Ansatz zur Überprüfung der Anforderungen und zur Aufrechterhaltung des angestrebten Sicherheitsstandards hat sich ein iterativer Durchlauf des Zyklus von Planung, Umsetzung, Überprüfung und Anpassung (PDCA, Plan-Do-Check-Act) bewährt.

9.2 Datensicherheit

Die Datenverwaltung stellt einen elementaren Bestandteil des Betriebs eines Uncrewed Aircraft System in Behörden und Organisationen mit Sicherheitsaufgaben dar. Hieraus ergeben sich die zwei unten aufgeführten Fragestellungen:

(1) Wie können Daten auch im Falle des Verlustes des UAS gemäß der drei Schutzziele Integrität, Vertraulichkeit und Verfügbarkeit vorgehalten werden?

(2) Wie können Daten gemäß der drei Schutzziele übertragen werden?

Allgemein ist zu beachten, dass die gewählten Verfahren der Datensicherheit dem aktuellen Stand der Technik und den allgemeinen Anforderungen an den Einsatzzweck sowie den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik entsprechen. Weiterhin gelten die einschlägigen nationalen und internationalen Vorschriften und Regelungen für den Flugbetrieb mit UAS[27].

[27] Vergleiche hierzu auch die Festlegung des Geltungsbereichs in Kapitel 3.

Insbesondere die Kommunikationsprotokolle und -verfahren des UAS müssen gemäß dem aktuellen Stand der Technik verschlüsselt werden. In diesem Zusammenhang wird auf die Anforderungen an die Schutzbedarfsfeststellung unter dem Gesichtspunkt des secure boot[28] verwiesen.

Aufgrund der Vielzahl an verfügbaren Architekturen und Systemlösungen für das zugehörige Datenmanagement beim Betrieb von UAS sind unterschiedliche Lösungsvarianten zur Gewährleistung einer sicheren Datenverwaltung und -übertragung möglich. Im Allgemeinen steigert sich die technische Komplexität von ausschließlich durch den Fernpiloten gesteuerten UAS im Vergleich zu teilautonomen Systemen mit fortgeschrittenen Funktionalitäten (z.B. automatischer Rückflug zum Startpunkt nach fortbestehendem Abbruch der Verbindung zum Steuergerät, aktive Umgebungsüberwachung zur Vermeidung von Kollisionen); dieser Umstand ist entsprechend des zugrundeliegenden Anwendungsfalls zu berücksichtigten.

Das vom Fernpiloten bediente Steuerungsgerät ist in der Regel mittels einer drahtlosen Netzverbindung mit dem UAS verbunden, um den bi-direktionalen Austausch von Flugdaten (Steuerungsbefehle und Statusinformationen) und die uni-direktionale Übertragung von Sensordaten (Bewegtbilddaten, sonstige Sensordaten) zu gewährleisten. Die Interaktion und der Datenaustausch zwischen dem UAS und dem Steuerungsgerät sollte über eine abgesicherte und verschlüsselte Datenverbindung innerhalb eines geschützten Netzwerks erfolgen, es wird an dieser Stelle auf die Empfehlungen des BSI zu Kommunikationsprotokollen und kryptographischen Verfahren gemäß der Technischen Richtlinie TR-02102-1 „Kryptographische Verfahren“ verwiesen[29].

UAS beim Einsatz in BOS verfügen in der Regel über die Fähigkeit zur drahtlosen Echtzeit-Videoübertragung, um dem Fernpiloten die Überwachung der Umgebung des UAS während des Flugbetriebs zu ermöglichen. Zusätzlich werden die Aufnahmen in der Regel auf einem internen Datenträger gespeichert. Für den Fall einer Störung der Netzverbindung sollten entsprechende technische Vorkehrungen getroffen werden, Beispiele hierfür sind der Wechsel in ungestörte Frequenzbereiche und der Rückgriff auf redundante Netzverbindungen sowie die autonome Rückkehr des UAS zum Startpunkt (bzw. einer vor dem Beginn des Flugbetriebs festgelegten Position) bei fortbestehendem Verbindungsabbruch.

---

[28] Vergleiche hierzu Kapitel 6.

[29] Vergleiche hierzu Anhang 6 Quellen.

Die Daten werden üblicherweise nach dem Abschluss des UAS-Einsatzes in eine Auswerteumgebung übertragen. Die vom UAS mittels der Sensorik erfassten Daten sollen in abgesicherter und verschlüsselter Form vorgehalten und abgelegt werden. Dies gilt insbesondere für hochauflösende Videoaufnahmen oder sonstige Sensordaten, die aufgrund der zur Verfügung stehenden Bandbreite der Netzverbindung nicht oder nur anteilig in reduzierter Datenqualität während des UAS-Betriebs übertragen werden. Grundsätzlich sollte für unbefugte Dritte im Falle eines Zugriffs auf die UAS-Sensordaten keine Möglichkeit zum Rückschluss auf den Einsatzzweck oder den Betreiber ermöglicht werden (die Pflicht zur Kennzeichnung von UAS bleibt hiervon unberührt, diese Empfehlung betrifft ausschließlich die Datenhaltung).

Weiterhin ist zu gewährleisten, dass die erfassten Daten nicht in unzulässiger Weise in die Rechte von unbeteiligten Dritten eingreifen. Unbeabsichtigt erfasste Bilddaten mit unzulässigen Eingriffen in die Persönlichkeitsrechte unbeteiligter Dritter sind sicher zu löschen, es wird hier auf die entsprechenden IT-Grundschutz-Bausteine des BSI zur Verschlüsselung, Löschung und Sicherung von Daten verwiesen.

Ein weiterer relevanter Aspekt ist die Gewährleistung der manipulations- und revisionssicheren Erfassung, Speicherung und Auswertung der UAS-Sensordaten. Hier ist z.B. die Verwendung einer Streuwertfunktion denkbar, um die entsprechenden Metainformationen nachweisbar zu dokumentieren und eine unbefugte Veränderung der Daten zu einem späteren Zeitpunkt auszuschließen. Es wird auf die entsprechenden IT-Grundschutz-Bausteine des BSI für die Archivierung und Datenhaltung verwiesen.

Weiterhin sollten für die am Umgang mit den Daten beteiligten Akteure im Rahmen der zugehörigen Prozesse geeignete Kontrollebenen geschaffen werden, beispielsweise gemäß dem „Vier-Augen-Prinzip“ sowie allgemein im Rahmen der Fach- und Dienstaufsicht.

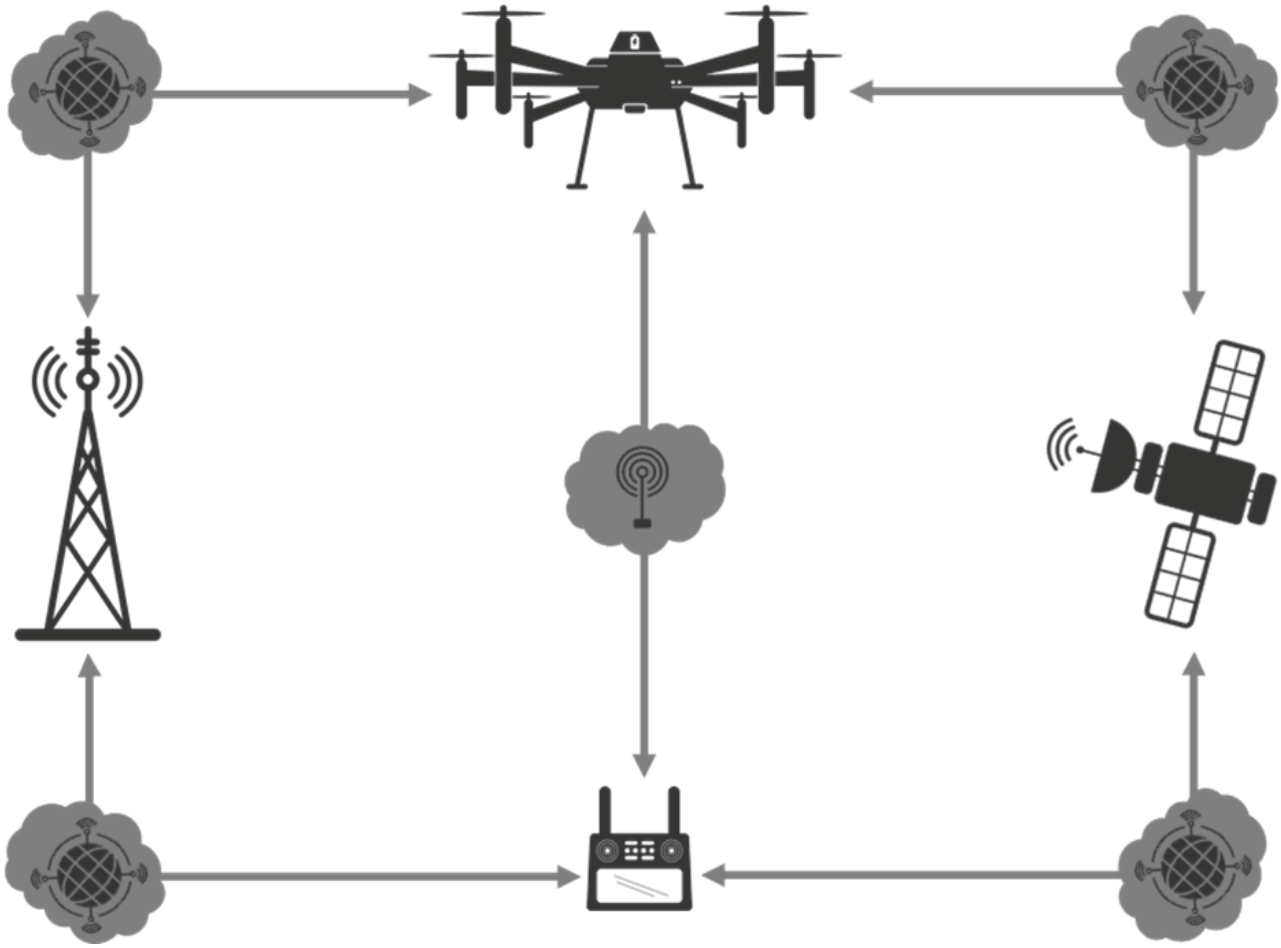

Abbildung 11: Redundante Kommunikationsverbindungen (z.B. lokales Netz, terrestrisches und orbitales Weitverkehrsnetz) ermöglichen die Aufrechterhaltung der Netzverbindung bei Ausfall oder Störung und erhöhen somit die Betriebssicherheit und reduzieren verbleibende Restrisiken. Eine Verbesserung der Betriebssicherheit kann sich daher vorteilhaft auf die Datensicherheit auswirken.

Anlage 1 – Prozesse

Die nachfolgende Tabelle führt die einzelnen Komponenten der zugrundeliegenden Prozesse auf. Die Beziehungen zwischen den Komponenten werden in den Kapiteln 5.1 und 5.10 beschrieben.

	ID	**Prozesse Anwendungen, Geräte, Netze, Infrastruktur, Akteure**
Anwendungen	A 01	Flugplanung
	A 02	Geographische Informationssysteme
	A 03	Wartung und Instandhaltung
	A 04	Fernsteuerung
	A 05	Fernüberwachung
	A 06	Datenübertragung
	A 07	UAS-Betriebssystem
	A 08	Fernsteuerung Nutzlast
	A 09	Batterieverwaltung
	A 10	BOS-Kommunikation
	A 11	Leitstelle
	A 12	Luftraumüberwachung
Geräte	C 01	Arbeitsplatz-Computer
	C 02	Mobil-Computer
	C 03	Mobiltelefon
	C 04	BOS-Digitalfunkgerät
	S 01	Virtueller Datenspeicher (*Datenraum*)
	S 02	Physischer Datenspeicher
	D 01	Steuergerät Bodenkontrollstation
	D 02	Steuergerät UAS (*on-board-unit*)
Netze	N 01	Leitungslose Netzwerkkomponenten (*UAS <-> Bodenkontrollstation*)
	N 02	Leitungsgebundene Netzwerkkomponenten (*UAS <-> Bodenkontrollstation*)
	N 03	Leitungslose Netzwerkkomponenten (*sonstige Verbindungen*)
	N 04	Leitungsgebundene Netzwerkkomponenten (*sonstige Verbindungen*)
	N 05	Schnittstellen zwischen Netzwerkkomponenten
	N 06	Primäre interne UAS-Netzwerkkomponenten (*Flugsicherheit*)
	N 07	Sekundäre interne UAS-Netzwerkkomponenten (*sonstige Funktionalitäten*)

Mobile und Stationäre Infrastruktur	D 01	UAS (*Multicopter*)
	D 02	UAS (*Starrflügler*)
	F 01	Bodenkontrollstation als mobiler Leitstand, Einsatzleitzentrale
	F 02	Transportfahrzeug
	F 03	Unterstützungsfahrzeug
	F 04	Sonstige mobile Systeme (*z.B. Antennenanlagen*)
	R 01	Innenbereich mit Zugangskontrolle
	R 02	Außenbereich mit Zugangskontrolle
	R 03	Bodenkontrollstation als stationärer Leitstand, Einsatzleitzentrale
	R 04	Werkstatt (*Wartung und Instandhaltung*)
	R 05	Datenzentrum (*Datenspeicherung und -aufbereitung*)
	R 06	Kontrollierter Luftraum (*Übung, Erprobung und Ausbildung*)
	R 07	Offener Luftraum (*Einsatz*)
Akteure	P 01	Fernpilot
	P 02	Betriebsüberwachung
	P 03	Betriebsunterstützung
	P 04	Leitungspersonal (*intern*)
	P 05	Leitungspersonal (*extern*)
	P 06	Unbeteiligte Dritte

Tabelle 23: Übersicht der Komponenten der Prozesse.

Anlage 2 – Elementare Gefährdungen

Die nachfolgende Tabelle enthält die 47 elementaren Gefährdungen gemäß den Empfehlungen der IT-Grundschutz-Methodik des BSI.

ID	Bezeichnung
G 0.01	Feuer
G 0.02	Ungünstige klimatische Bedingungen
G 0.03	Wasser
G 0.04	Verschmutzung, Staub, Korrosion
G 0.05	Naturkatastrophen
G 0.06	Katastrophen im Umfeld
G 0.07	Großereignisse im Umfeld
G 0.08	Ausfall oder Störung der Stromversorgung
G 0.09	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 oder 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- oder 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

Tabelle 24: Übersicht der Elementaren Gefährdungen.

Anlage 3 – Glossar

Das Glossar umfasst insbesondere Begriffe, deren Definition und Abgrenzung von der allgemeinen Praxis im Bereich der Informationssicherheit gemäß den Empfehlungen des BSI abweichen. Weiterhin werden die Begriffe in Bezug zum Betrieb eines UAS gesetzt.

Alle sonstigen Begrifflichkeiten sind deckungsgleich mit den im IT-Grundschutzkompendium des BSI verwendeten Definitionen.

Begriffe	**Erklärung**
Akteur	Akteure sind die am Betrieb von UAS direkt und indirekt beteiligten Angehörigen von BOS sowie das übergeordnete Leitungspersonal. Diese werden anhand ihrer spezifischen Aufgaben in funktionale Gruppen eingeteilt. Für jede dieser Gruppen und die zugehörigen Angehörigen von BOS lassen sich spezifische Rollen und Rechte ableiten. Diese können zur Erstellung eines Berechtigungskonzepts herangezogen werden.
Anwendungsfall	Ein Anwendungsfall ist ein spezifisches Einsatzszenario für den Betrieb von UAS in einer BOS (*z.B. Suche einer vermissten Person*).
Informationsverbund	Unter einem Informationsverbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten zu verstehen, die an der Aufgabenerfüllung im Anwendungsbereich der Informationsverarbeitung beim Betrieb von UAS in einer BOS direkt oder indirekt beteiligt sind. Ein Informationsverbund kann dabei als Ausprägung die gesamte Institution oder auch einzelne Bereiche, die durch organisatorische Strukturen oder zugrunde liegende Prozesse beziehungsweise durch Anwendungsfälle gegliedert sind, umfassen.
Institution	Im Sinne dieses IT-Grundschutz-Profils handelt es sich um Behörden und Organisationen mit Sicherheitsaufgaben (*BOS*). Behörden sind grundsätzlich öffentliche Institutionen, Organisationen können sowohl öffentliche als auch nicht-öffentliche Institutionen sein.
Komponenten	Eine Komponente ist eine eigenständig einsetzbare technische Einheit, die eine bestimmte Funktion erfüllt. Einzelne Komponenten sind funktionalen Gruppen zugeordnet. Die Verbindung zu anderen (*internen und externen*) Komponenten erfolgt über Schnittstellen. Gemäß dem IT-Grundschutzkompendium des BSI werden Komponenten als technische Zielobjekte bzw. Bestandteile von Zielobjekten betrachtet.

Netzplan	Ein Netzplan im Kontext der Informationssicherheit beim Betrieb von Uncrewed Aircraft Systems in Behörden und Organisationen mit Sicherheitsaufgaben ist eine grafische Darstellung von Abläufen informationstechnischer Komponenten bzw. Teilkomponenten innerhalb eines verbundenen Netzwerks. Er visualisiert Vorgänge, deren Ablauf sowie die internen und externen Beziehungen, Abhängigkeiten und Schnittstellen. Er stellt somit den Informationsfluss durch ein Netzwerk dar und zeigt auf, wie die zugehörigen Komponenten auf der technisch-funktionalen Ebene zusammenarbeiten. Die Informationsflüsse werden im Allgemeinen durch Pfeile zwischen den zugehörigen Komponenten dargestellt (sog. Vorgangspfeil-Netzplan). Einzelne Teilkomponenten eines Netzplans sind oftmals durch eine gestrichelte Linie von anderen Teilkomponenten abgegrenzt. Elemente des Netzplans sind im Allgemeinen Objekte und Geräte, Kommunikationsverfahren und -protokolle. Diese können in funktionale Komponenten bzw. Teilkomponenten untergliedert werden. Zusätzlich hat sich hier auch die Berücksichtigung der beteiligten Akteure bewährt, um die abgeleiteten Rollen- und Rechte innerhalb des Netzwerks zu berücksichtigen.
Prozesse	Prozesse sind aufeinander aufbauende und logisch miteinander verknüpfte Abfolgen von einzelnen Maßnahmen, die zur Erreichung einer Zielsetzung unternommen werden. Verwaltungsprozesse und Geschäftsprozesse beschreiben entsprechende Maßnahmen in der Verwaltung bzw. der Wirtschaft.
Streuwertfunktion	Eine Streuwertfunktion bzw. Hashfunktion wandelt einen Eingabewert in einen Hashwert um. So können unterschiedliche Informationen zu einem einzigen Wert verbunden werden. Je nach Hash- bzw. Streuwertfunktion sind Kollisionsvermeidung (unterschiedliche Eingaben führen zu unterschiedlichen Hashwerten), Chaoseffekt (ähnliche Eingaben führen zu sehr unterschiedlichen Hashwerten) und Unumkehrbarkeit (es gibt keine praktische Möglichkeit aus dem Hashwert die Eingabe zu ermitteln) wichtige funktionale Eigenschaften. Der Abgleich von zwei Hashwerten kann Auskunft über eine Veränderung des Eingabewerts geben.
Teilprozesse	Teilprozesse sind abgrenzbare Teile eines übergeordneten Prozesses.

Tabelle 25: Glossar mit Erläuterungen.

Anlage 4 – Abkürzungen

Das Abkürzungsverzeichnis beinhaltet die im vorgelegten IT-Grundschutz-Profil verwendeten Abkürzungen.

Es wird weiterhin auf das Kapitel 4.2 „Abkürzungen“ des IT-Grundschutzkompendiums des BSI verwiesen.

Abkürzung	**Erklärung**
BBK	**B**undesamt für **B**evölkerungsschutz und **K**atastrophenhilfe
BOS	**B**ehörden und **O**rganisationen mit **S**icherheitsaufgaben
BSI	**B**undesamt für **S**icherheit in der **I**nformationstechnik
FPV	**F**irst-**P**erson-**V**iew
GPS	Satellitennavigationssystem (**G**lobal **P**ositioning **S**ystem)
ISM	**I**nformations**s**icherheits-**M**anager
ISMT	**I**nformations**s**icherheits-**M**anagement-**T**eam
ISO	**I**nternational **O**rganization for **S**tandardization
IT	**I**nformations**t**echnik
PCDA	Iterativer Zyklus von Planung, Umsetzung, Überprüfung und Anpassung (**P**lan, **Do**, **C**heck, **A**ct)
RBAC	Rollenbasierte Eingriffs- und Zugriffskontrolle (**r**ole-**b**ased **a**ccess **c**ontrol)
SZ	**S**chadens**z**enarien
UAS	**U**ncrewed **A**ircraft **S**ystem, umgangssprachlich Drohne, auch Unbemanntes Luftfahrtsystem
WAN	**W**ide **A**rea **N**etwork
WLAN	**W**ireless **L**ocal **A**rea **N**etwork

Tabelle 26: Abkürzungsverzeichnis mit Erläuterungen.

Anlage 5 – Vorlagen

Die nachfolgende Vorlage kann zur Anpassung von Prozessen, Teilprozessen und der jeweils referenzierten Prozesse beziehungsweise der Zielobjekte verwendet werden.

	ID	Teilprozesse							
Bezeichnung Prozess	TP #.#	Bezeichnung Teilprozess							
		☐ A 01	☐ A 02	☐ A 03	☐ A 04	☐ A 05	☐ A 06	☐ A 07	☐ A 08
		☐ A 09	☐ A 10	☐ A 11	☐ A 12	☐ C 01	☐ C 02	☐ C 03	☐ C 04
		☐ S01	☐ S 02	☐ D 01	☐ D 02	☐ N 01	☐ N 02	☐ N 03	☐ N 04
		☐ N 05	☐ N 06	☐ N 07	☐ U 01	☐ U 02	☐ F 01	☐ F 02	☐ F 03
		☐ F 04	☐ R 01	☐ R 02	☐ R 03	☐ R 04	☐ R 05	☐ R 06	☐ R 07
		☐ P 01	☐ P 02	☐ P 03	☐ P 04	☐ P 05	☐ X ##	☐ X ##	☐ X ##
	TP #.#	Bezeichnung Teilprozess							
		☐ A 01	☐ A 02	☐ A 03	☐ A 04	☐ A 05	☐ A 06	☐ A 07	☐ A 08
		☐ A 09	☐ A 10	☐ A 11	☐ A 12	☐ C 01	☐ C 02	☐ C 03	☐ C 04
		☐ S01	☐ S 02	☐ D 01	☐ D 02	☐ N 01	☐ N 02	☐ N 03	☐ N 04
		☐ N 05	☐ N 06	☐ N 07	☐ U 01	☐ U 02	☐ F 01	☐ F 02	☐ F 03
		☐ F 04	☐ R 01	☐ R 02	☐ R 03	☐ R 04	☐ R 05	☐ R 06	☐ R 07
		☐ P 01	☐ P 02	☐ P 03	☐ P 04	☐ P 05	☐ X ##	☐ X ##	☐ X ##
	TP #.#	Bezeichnung Teilprozess							
		☐ A 01	☐ A 02	☐ A 03	☐ A 04	☐ A 05	☐ A 06	☐ A 07	☐ A 08
		☐ A 09	☐ A 10	☐ A 11	☐ A 12	☐ C 01	☐ C 02	☐ C 03	☐ C 04
		☐ S01	☐ S 02	☐ D 01	☐ D 02	☐ N 01	☐ N 02	☐ N 03	☐ N 04
		☐ N 05	☐ N 06	☐ N 07	☐ U 01	☐ U 02	☐ F 01	☐ F 02	☐ F 03
		☐ F 04	☐ R 01	☐ R 02	☐ R 03	☐ R 04	☐ R 05	☐ R 06	☐ R 07
		☐ P 01	☐ P 02	☐ P 03	☐ P 04	☐ P 05	☐ X ##	☐ X ##	☐ X ##
	TP #.#	Bezeichnung Teilprozess							
		☐ A 01	☐ A 02	☐ A 03	☐ A 04	☐ A 05	☐ A 06	☐ A 07	☐ A 08
		☐ A 09	☐ A 10	☐ A 11	☐ A 12	☐ C 01	☐ C 02	☐ C 03	☐ C 04
		☐ S01	☐ S 02	☐ D 01	☐ D 02	☐ N 01	☐ N 02	☐ N 03	☐ N 04
		☐ N 05	☐ N 06	☐ N 07	☐ U 01	☐ U 02	☐ F 01	☐ F 02	☐ F 03
		☐ F 04	☐ R 01	☐ R 02	☐ R 03	☐ R 04	☐ R 05	☐ R 06	☐ R 07
		☐ P 01	☐ P 02	☐ P 03	☐ P 04	☐ P 05	☐ X ##	☐ X ##	☐ X ##
	TP #.#	Bezeichnung Teilprozess							
		☐ A 01	☐ A 02	☐ A 03	☐ A 04	☐ A 05	☐ A 06	☐ A 07	☐ A 08
		☐ A 09	☐ A 10	☐ A 11	☐ A 12	☐ C 01	☐ C 02	☐ C 03	☐ C 04
		☐ S01	☐ S 02	☐ D 01	☐ D 02	☐ N 01	☐ N 02	☐ N 03	☐ N 04
		☐ N 05	☐ N 06	☐ N 07	☐ U 01	☐ U 02	☐ F 01	☐ F 02	☐ F 03
		☐ F 04	☐ R 01	☐ R 02	☐ R 03	☐ R 04	☐ R 05	☐ R 06	☐ R 07
		☐ P 01	☐ P 02	☐ P 03	☐ P 04	☐ P 05	☐ X ##	☐ X ##	☐ X ##

Tabelle 27: Vorlage zur Anpassung von Prozessen und Teilprozessen durch den Anwender.

Anlage 6 – Quellen

Die nachfolgende Übersicht referenziert auf die insbesondere in Kapitel 3 verwiesenen externen Dokumente über Internetlinks.

Für die Inhalte der angegebenen externen Internetlinks sind die jeweiligen Inhaber der Urheberrechte verantwortlich[30].

Der Aufruf der Links und die Hinterlegung im Dokument erfolgte am 01.12.2025.

Quellenbeschreibung	**Aufruf**
BSI IT-Grundschutz-Profil „Strukturbeschreibung“ (*Bundesamt für Sicherheit in der Informationstechnik, Version 1.0*)	(Link)
BSI IT-Grundschutzkompendium „Edition 2023“ (*Bundesamt für Sicherheit in der Informationstechnik, Edition 2023*)	(Link)
BSI-Standard 200-2 „IT-Grundschutz-Methodik“ (*Bundesamt für Sicherheit in der Informationstechnik, Version 1.0*)	(Link)
BSI-Standard 200-3 „Risikoanalyse auf der Basis von IT-Grundschutz“ (*Bundesamt für Sicherheit in der Informationstechnik, Version 1.0*)	(Link)
BSI-Empfehlung CS-125 „Absicherung von Telemediendiensten“ (*Bundesamt für Sicherheit in der Informationstechnik, Version 1.0*)	(Link)
BSI-Empfehlung „Overview of drone-based cyber threats and aspects of defence“ (*Bundesamt für Sicherheit in der Informationstechnik, Version 1.0*)	(Link)
BSI-Richtlinie TR-02102-1 „Kryptographische Verfahren“ *(Bundesamt für Sicherheit in der Informationstechnik, Version 1.0)*	(Link)
BSI-Information „Cyber Resilience Act“ *(Bundesamt für Sicherheit in der Informationstechnik)*	(link)
BBK-Empfehlung EGRED-2 „Empfehlungen für Gemeinsame Regelungen zum Einsatz von Drohnen im Bevölkerungsschutz“ (*Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Version 2.0*)	(Link)
BBK-Empfehlung STS-BOS „BOS-Standardszenarien zu den EGRED-2“ (*Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Version 1.0*)	(link)
ISO/IEC 27001:2022 „Information security, cybersecurity and privacy protection - Information security management systems - Requirements“ (*International Organization for Standardization, Edition 3, 2022*)	(Link)
UAV DACH e.V. „IT-Grundschutz-Profil für den Betrieb von UAS Band 1: UAS-Betriebskategorie Open (Offen)“ (*UAV DACH e.V. – Association for Unmanned Aviation, Version 1.1*)	(Link)

Tabelle 28: Übersicht der als Quellen herangezogenen externen Dokumente.

[30] Vergleiche hierzu auch Kapitel 1.1.

Anlage 7 – Abbildungsverzeichnis

Die im IT-Grundschutz-Profil verwendeten Piktogramme zur Visualisierung von Netzplänen und Informationsverbünden wurden durch EVERS DESIGN (www.evers-design.de, info@evers-design.de) nach Vorgabe der Autoren gestaltet.

Der Inhaber des Nutzungsrechts ist Herr Gunnar Korte[31].

Die Verwendung der Piktogramme zur Visualisierung von Netzplänen und Informationsverbünden im Kontext der Informationssicherheit durch Dritte ist ausdrücklich erlaubt, Voraussetzung ist dabei die Angabe des Herausgebers.

Piktogramme: UAV DACH e.V. - Verband für Unbemannte Luftfahrt | E-Mail: info@uavdach.org

Die Bildmarke auf dem Titelbild des Dokuments ist Eigentum des UAV DACH e.V. – Verband für Unbemannte Luftfahrt (info@uavdach.org).

Der Inhaber des Urheberrechts der Abbildung 8 auf Seite 24 (Darstellung eines Quadcopter-UAS) ist die Donaustahl GmbH (info@donaustahl.com).

[31] Siehe hierzu auch Kapitel 1.2.