Bachelorarbeit

Arne Maximilian Richter

Konzept und Einführung von Safety-Analysen bei Mikrocontroller-basierten Anwendungen in UAVs

Fakultät Technik und Informatik
Studiendepartment Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Arne Maximilian Richter

Konzept und Einführung von Safety-Analysen bei Mikrocontroller-basierten Anwendungen in UAVs

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung

im Studiengang Bachelor of Science Technische Informatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Thomas Lehmann
Zweitgutachter: Prof. Dr. Bettina Buth

Eingereicht am: 30. September 2013

Arne Maximilian Richter

Thema der Arbeit
Konzept und Einführung von Safety-Analysen bei Mikrocontroller-basierten Anwendungen in UAVs

Stichworte
Safety-Analyse, unbemannte Luftfahrzeuge, autonomes Fliegen, Sicherheit, Notfallszenarien, Fehlerbehandlung, Fehlerausbreitung

Kurzzusammenfassung
Gegenstand dieser Arbeit ist das Erarbeiten von Safety-Analysen für unbemannte Luftfahrzeuge. Teil dieser Arbeit ist das Analysieren auf Fehlerquellen und das darstellen der Auswirkungen dieser möglichen Fehler. Dabei sollen Gegenmaßnahmen analysiert werden, welche mögliche Fehlerquellen beseitigen oder mit den Fehlern umgehen. Am Ende soll die Arbeit als Leitfaden für die Entwicklung unbemannter Flugobjekte fungieren.

Arne Maximilian Richter

Title of the paper
Concept and introduction of safety analysis for microcontroller-based applications in UAV's

Keywords
Safety analysis, unmanned aerial vehicles, autonomously flying, safety, emergency scenarios, error handling, error spreading

Abstract
The subject of this thesis is the development of safety analysis for unmanned aerial vehicles. Part of this work is the analysis of failure-sources and the representation of the failure impact. Thereby counteraction shout be analyzed, which should eliminate failures-sources or handle the failures. At the end this work should act as guideline for the development of unmanned aerial vehicles.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Die Abkürzung UAV steht für den englischen Begriff Unmanned Aerial Vehicle. Dieser Begriff lässt sich wiederum in den deutschen Begriff unbemanntes Luftfahrzeug übersetzen. Doch was steht hinter dem Begriff, der den Kern dieser Arbeit ausmacht?

Grundsätzlich sollte sich jeder etwas unter dem Begriff vorstellen dürfen. So dürfte jeder militärische Drohnen und Raketen mit unbemannten Luftfahrzeugen in Verbindung bringen. In der Technik ist es jedoch üblich, feste Definitionen für Begriffe festzulegen. Aus diesem Grund werden zuerst die Begriffe Flugobjekt und Luftfahrzeug betrachtet und für das Umfeld dieser Arbeit definiert.

> Ein **Flugobjekt** ist ein physischer Körper, welcher sich zeitweise durch die Luft bewegt und den Boden nicht berührt.

Mit dieser recht freien Definition für Flugobjekt, kann nahezu alles als Flugobjekt definiert werden. So fallen sowohl Flugzeuge, als auch Tennisbälle und Papierflieger in die Kategorie. Aufbauend darauf kann nun das Luftfahrzeug definiert werden.

> **Luftfahrzeuge** sind eine echte Teilmenge der Flugobjekte und erweitern diese um die Fähigkeit, ihre Flugbahn während des Fluges mittels Aktorik zu verändern.

Diese neue Definition schränkt die Gruppe weiter ein und ermöglicht ein genaueres Bild auf die Luftfahrzeuge.

Weiterhin offen ist das Adjektiv “unbemannt“. Unter diesem Begriff kann man sich leicht etwas vorstellen, jedoch lässt er auch viele philosophische Diskussionen zu und wirkt dann nicht mehr so eindeutig. So kann man den Teil “mann“ im Wort mehrdeutig interpretieren und verschiedene Bedeutungen herleiten.

Die vermutlich häufigste Interpretation ist das Abwesendsein von menschlichem Leben an Bord des beschriebenen Fahrzeuges. Diese Interpretation stimmt auch mit den vorherigen Beispielen der militärischen Luftfahrzeuge überein.

Eine weitere und eher unpassende Interpretation könnte das Fehlen von Männern an Board des Fahrzeuges sein. Unter dieser Konstellation würden Frauen und Kinder nicht dazu zählen und könnten sich an Board des Fahrzeuges befinden. So unpassend diese Beschreibung auch ist, so hilfreich ist der Ansatz, um eine Interpretation zu finden, die den Kern dieser Arbeit beschreibt.

Betrachtet man die alte Seefahrt mit Segelschiffen, so stellt man fest, dass es ein klassischer Männerberuf war. Frauen und Kinder wurden höchstens als Passagiere mit an Bord genommen und wurden in die Abläufe für die Fahrt nicht integriert. Somit waren die Männer für die Fahrt zuständig. Diese Gruppe wurde dann als Mannschaft bezeichnet. Hatte die Mannschaft, bzw. die Männer das Schiff verlassen, so war es unbemannt und somit nicht fahrtüchtig.

In der heutigen Zeit würde man den Begriff Mannschaft nicht zwangsläufig mit Männern in Verbindung bringen. So können auch Frauen und Kinder teile der Mannschaft sein und ein Fahrzeug betreiben und steuern. Auf der Basis dieser Beschreibung lässt sich nun eine passende Definition für den Begriff unbemannt suchen.

> Ein **unbemanntes** Fahrzeug ist ein Fahrzeug, welches über keine Mannschaft verfügt, die Einfluss auf das System nehmen kann.

Diese Definition lässt es zu, dass ein Mensch oder eine andere Lebensform an Bord des Fahrzeuges ist. Sie verdeutlicht dafür noch mehr, dass das System selbstständig mit Fehlern umgehen muss.

Ein Beispiel aus dem Wasserfahrzeugbereich ist ein Motorboot und ein ferngesteuertes Motorboot. Fällt das Motorboot aus, kann die Mannschaft die Fehlerquelle suchen und gegebenenfalls auf den Fehler reagieren. Im Zweifelsfall könnten sie mit Rudern versuchen, das Motorboot zu bewegen. Bei dem ferngesteuerten Motorboot fehlen diese Möglichkeiten. Die Mannschaft, die nicht an Bord des Bootes ist, kann weder den Fehler direkt suchen und beheben, noch kann sie das Boot aus der Ferne bewegen.

1.1 Motivation und Zielsetzung

Die Gruppe der unbemannten Luftfahrzeuge lässt sich mit der vorherigen Definition in eine Vielzahl von Untergruppen unterteilen. So bilden militärische Drohnen und Raketen nur einen Anteil der unbemannten Luftfahrzeuge. Eine weitere Untergruppe bilden die Modellflugzeuge und Modell-Quadrocopter.

Durch massive Entwicklungen im Bereich der Embedded-Systeme wurde es möglich, dass sich die unbemannten Luftfahrzeuge und besonders die Modellflugzeuge und Modell-Quadrocopter weiterentwickelten. So ergeben sich heute völlig neue Möglichkeiten, durch Kombinationen aus unbemannten Luftfahrzeugen und moderner Computertechnik. Dabei werden die Computer immer kleiner, leistungsstärker und günstiger. So stellt der Computer Raspberry Pi ein Beispiel für kleine, leistungsstarke Technik, die wenig kostet und nicht viel größer als eine Kreditkarte ist ([5]).

Diese Kombination stellt dem Anwender eine Vielzahl von Möglichkeiten zur Verfügung. So ist es leicht Möglich, Luftaufnahmen von Veranstaltungen zu erstellen oder die Lebensräume von Tieren zu überwachen und zu beobachten. Als konkretes Beispiel kann man die Suche nach Ölfeldern nehmen. So setzt Norwegen unbemannte Luftfahrzeuge ein, um in entlegenen Regionen nach Öl zu suchen ([6]).

Der große Vorteil der unbemannten Luftfahrzeuge ist, dass bei den Missionen keine Menschen an Bord sein müssen. Somit sind die Risiken und Kosten viel geringer, als z.B. bei bemannten Missionen. So kann ein unbemanntes Luftfahrzeug während einer Mission in einem unbewohnten Gebiet abstürzen und es muss nicht sofort ein Rettungsteam geschickt werden. Die Verantwortlichen für die Mission und das Gerät können einen passenden Moment auswählen und müssen somit nicht weitere Personen einer Gefahr aussetzen, wenn dies nicht notwendig ist.

Auch wenn die Risiken für unbewohnte Gebiete viel geringer sind, so trifft diese Aussage nur gegenteilig bei bewohnten Gebiet zu. Greift man an dieser Stelle das Beispiel mit dem Motorboot und dem ferngesteuerten Motorboot auf, so fällt einem auf, dass man im Fehlerfall nur schwer bis überhaupt nicht reagieren kann. Nimmt man beispielsweise einen ferngesteuerten Quadrocopter, der über einem Open-Air-Konzert automatisch, stationär fliegen soll und Aufnahmen machen soll. Fällt nun bei diesem Quadrocopter ein Propeller oder ein Teil

der Flugstabilisierung aus, so kann dieser als Folge des Ausfalls in die Menge abstürzen und Personen verletzen.

Dieses Verhalten ist nicht akzeptabel. Daher müssen Maßnahmen während der Entwicklung getroffen werden, die Fehler erkennen, abfangen und lösen. Um dies zu erreichen werden Safety-Analysen durchgeführt, die sich mit möglichen Fehlern und ihren Auswirkungen beschäftigen. Sind die möglichen Fehler und ihre Auswirkungen bekannt, so können Maßnahmen ins System integriert werden, die die Fehler erkennen und mit ihnen umgehen.

Ziel dieser Arbeit ist es daher, sich mit den Grundlagen der Safety-Analysen und dem Umgang mit Fehlern zu beschäftigen. Die Arbeit soll später als Leitfaden für Safety-Analysen dienen, die von der Arbeitsgruppe BWB-AES an der Hochschule für Angewandte Wissenschaften Hamburg im Rahmen eines Projektes durchgeführt werden sollen. Dabei sollen die Analysen auf der modellierten Architekturebene eines UAVs ansetzen und mehrere Flugmodi berücksichtigen.

1.2 Randbedingungen der Arbeit

Dieser Abschnitt soll einleitend zur Arbeit die Randbedingungen vorstellen, unter denen die vorliegende Arbeit erstellt wurde.

Die Arbeit läuft im Rahmen des Projektes der Arbeitsgruppe BWB-AES, welche aus der Arbeitsgruppe BWB und der Projektgruppe AES bestehen. Die Arbeiten sind in den Gruppen soweit eingeteilt, dass die BWB-Gruppe sich mit dem Flugmodell beschäftigt und dieses zur Verfügung stellt. Die AES-Gruppe kümmert sich hingegen um den Bordcomputer, welcher Messdaten während des Fluges aufnehmen soll und später eine Flugstabilisierung durchführen soll. Diese Arbeit läuft parallel zu den beiden Gruppen und betrachtet safety-relevante Aspekte des Gesamtprojektes.

BWB

Das BWB-Team wurde im Jahr 2001 an der Hochschule für Angewandte Wissenschaften Hamburg im Department für Fahrzeug- und Flugzeugbau gegründet. Die Aufgabe des Teams ist es, sich mit dem Konzept der Blended Wing Body Bauform für Flugzeuge zu beschäftigen. Diese Bauform ist eine Zwischenstufe von Nurflüglern und eine klassischen Passagierflugzeugen.

In Rahmen dieses Projektes konstruierte das Team einen derartigen Blended Wing Body.

Diese von der Gruppe konstruierte Konstellation wurde AC20.30 getauft. Um diese Konstellation zu testen, wurde ein Versuchsträger gebaut, der in einem 1:30 Maßstab einer möglichen Passagiermaschine der Bauform entspricht. Dieses Modell wird in der Abbildung 1.1 gezeigt.

Abbildung 1.1: 1:30 Modell des AC2030 bei einem Flugtag im Jahr 2013.

Der Versuchsträger hat dabei eine Spannweite von 3,24m, eine Länge von 2,12m und eine Startmasse von 20 Kg ([7]).

Im Jahr 2013 wurde aus der BWB-Arbeitsgruppe dann der Verein “Neues Fliegen e.V.“ gegründet. Dieser Verein beschäftigt sich mit der Weiterentwicklung des Versuchsträgers und der Weiterentwicklung des Passagierflugzeugmodells. So werden beispielsweise mögliche Konstellationen für das Kabinen-Design erforscht und analysiert. Zusätzlich beschäftigt sich der Verein mit neuen Versionen des Modells, so wurde im Jahr 2013 eine Fräse angeschafft, mit deren Hilfe Modelle im 1:60 Maßstab gebaut werden sollen. Diese Modelle sollen mittels der Fräse in möglichst kurzen Zeitabständen gefertigt werden können und sollen es dem Verein ermöglichen besser neue Designs und Anpassungen zu testen.

Um Ergebnisse aus den Flügen zu bekommen, wird aber ein Messsystem benötigt, welches Sensorwerte während des Fluges aufnimmt, abspeichert und möglichst auch in Echtzeit an den Boden übertragt. Um dies zu bewältigen nahmen die damaligen Mitglieder des Projektes BWB im Jahr 2012 Kontakt mit dem Department für Informatik an der Hochschule für Angewandte Wissenschaften Hamburg auf. Als Ergebnis dieser Kontaktaufnahme entstand 2013 die Projektgruppe “Airborne Embedded Systemms“.

AES

Die Projektgruppe “Airborne Embedded Systemms“ oder abgekürzt AES, entstand aus Studenten der Technischen Informatik, die sich mit autonomen und geregelten Luftfahrzeugen beschäftigen wollten. In diesem Rahmen wird von ihnen ein Messsystem für den Versuchsträger des Vereins Neues Fliegen e.V. entwickelt.

Aufbauend auf dem Messsystem soll dann eine Steuerung entwickelt werden, welche einen Versuchsträger zu einem autonomen UAV umrüstet. Die Abbildung 1.2 zeigt dabei ein erstes

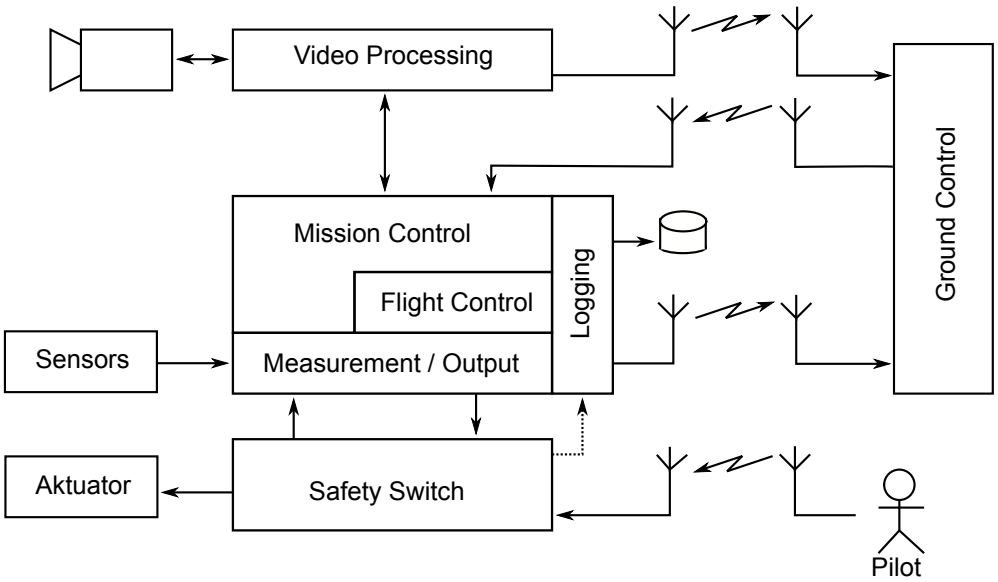

Abbildung 1.2: Erstes Konzept der AES Architektur aus Beständen der Projektgruppe.

Architekturkonzept der Projektgruppe.

Als Ziel für den Einsatz des UAVs wählte man den Katastrophenschutz aus. So soll das UAV im späteren Stadium selbstständig über Katastrophengebiete fliegen und in Echtzeit eine 3D-Karte des Gebietes für ein Krisenteam erstellen. Dies soll es den Einsatzkräften beispielsweise nach Erdbeben, Überschwemmungen oder bei Flächenbränden ermöglichen, eine Übersicht zu bekommen, um sich somit optimiert zu koordinieren. An diesem Ziel arbeiten nun die Gruppen AES und BWB seit dem Sommersemester 2013.

Um diese Aufgabe zu bewältigen, versucht die Projektgruppe Verfahren und Arbeitsmethoden aus der Industrie zu erlernen und anzuwenden. So sollen gängige Verfahren wie das V-Modell,

als auch Hardware in the Loop Simulation angewandt werden. Bei der Betrachtung der zu lösenden Aufgaben fiel dabei auch Safety-Analysen auf. So darf das UAV nicht im Fehlerfall über einem Krisengebiet abstürzen, da es Menschen verletzten könnte oder die Umgebung im nicht angemessenen Rahmen beschädigen könnte. Die Einleitung dieser Analysen wurde daraufhin vom Projekt getrennt und in diese Arbeit gesteckt. Daher lief die Arbeit parallel zum AES-Projekt und zu der Arbeit des Vereins.

1.3 Gliederung der Arbeit

Die Arbeit wurde in 6 Kapitel unterteilt. Die Kapitel sind dabei wie folgt gegliedert:

Im **1. Kapitel** wird das Thema vorgestellt. Es dient als Einstieg in den Themenbereich "unbemannte Luftfahrzeuge" und soll wichtige Projekthintergründe und Randbedingungen vermitteln.

Das **2. Kapitel** soll als Einführung in die Grundlagen und Grundbegriffe der Safety-Analysen dienen. Es soll Grundlagen für die Vorgehensweise bilden, sodass auf dieser Basis erste Analysen möglich sind.

Im **Kapitel 3** werden die Anforderungen an das System vorgestellt und analysiert. Auf deren Basis kann dann das System betrachtet werden.

Kapitel 4 liefert die Safety-Analysen an einer Beispielarchitektur auf funktionaler Ebene. Dies geschieht in Verbindung mit den verwendeten Modi. Dabei wird das Kapitel in fünf Unterkapitel unterteilt. Jedes Unterkapitel betrachtet dabei das System auf der Basis, eines eigenen Funktionssets von unterstützen Modi.

Im **Kapitel 5** werden die gewonnenen Kenntnisse zusammengefasst und eine Aussicht auf zukünftige Arbeiten gewährt.

Im **6. Kapitel** wird abschließend ein persönliches Fazit getroffen.

2 Grundlagen der Safety-Analyse

Bevor die ersten Safety-Analysen durchgeführt werden können, werden Grundlagen für deren Durchführung benötigt. Die Aufgabe dieses Kapitels ist es, die wichtigsten Grundlagen zu schaffen und den Leser auf die späteren Kapitel vorzubereiten.

So werden im ersten Abschnitt grundlegende Begriffe aus dem Bereich der Safety-Analysen geklärt. Der zweite Abschnitt arbeitet die Grundlagen der Modellierung auf und soll damit ein grundlegendes Verständnis für das Zielobjekt der Analysen schaffen. Sind diese Grundlagen geschaffen, so werden in Abschnitt drei und vier die Hintergründe von Safety-Analysen und ihre Kategorien beschrieben. Im fünften Abschnitt werden dann gängige Verfahren für Safety-Analysen vorgestellt. Die Abschnitte sechs und sieben beschäftigen sich danach mit den Grundlagen des sogenannten System Health Managements und somit mit der Konsequenz aus den zuvor durchgeführten Analysen. Dabei erklärt der Abschnitt sechs die Erkennung von Fehlern zur Laufzeit des Systems und der Abschnitt sieben den vorbeugenden Umgang mit zuvor identifizierten Fehlerquellen. Abschließend wird im achten Abschnitt die in der Arbeit verwendete Vorgehensweise vorgestellt und erläutert.

2.1 Grundlegende Begriffe

Um den Einstieg in den Bereich Safety-Analysen zu bekommen, müssen zuerst grundlegende Begriffe geklärt werden. In diesem Abschnitt werden folglich neue Begriffe eingeführt und definiert und bekannte Begriffe genau definiert. Als Grundlage für die Begriffe wird die Arbeit von Neil Storey ([8]) und die DIN EN 61508-4 (VDE 0803-4): 2011-02 verwendet.

Anmerkung zur IEC 61505

Die DIN EN 61508 (VDE 0803) ist die deutsche Fassung der IEC 61508: “Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme“. Sie gehört zu den grundlegenden Normen im Bereich der funktionalen Sicherheit. Im Abschnitt

vier dieser Norm werden wichtige Begriffsdefinitionen getroffen, die im Rahmen dieser Arbeit verwendet werden.

Schaden

Als ein Schaden wird die Verletzung von Menschen und anderen Lebewesen definiert. Zusätzlich fällt unter den Begriff des Schadens die Schädigung von Gütern und der Umwelt.

Gefährdung

Eine Gefährdung wird als eine potentielle Schadensquelle definiert.

Risiko

Ein Risiko wird gemäß der IEC 61508-4 wie folgt definiert:

> **Risiko** Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens

Bruce Douglass beschreibt das Risiko hingegen konkreter mit der Formel 2.1 ([9]).

$$Risiko_{\text{Gefahr}} = Wahrscheinlichkeit_{\text{Gefahr}} * Schweregrad_{\text{Gefahr}} \tag{2.1}$$

Restrisiko

Das Restrisiko wird als das verbleibende Risiko definiert, welches überbleibt, nachdem Schutzmaßnahmen ergriffen wurden.

Tolerierbares Risiko

Als tolerierbares Risiko wird ein Risiko definiert, welches auf den aktuellen gesellschaftlichen Wertvorstellungen in einem gegebenen Zusammenhang akzeptiert wird.

Sicherheit

Das deutsche Wort “Sicherheit“ lässt sich in zwei englische Wörter übersetzen. Dabei handelt es sich um die Wörter “Safety“ und “Security“. Da sich beide Wörter in der Bedeutung massiv unterscheiden, muss an dieser Stelle eine Unterscheidung stattfinden. Die Begriffe werden im folgenden Abschnitt unterschieden. Im Rahmen dieser Arbeit wird das Wort Sicherheit nur im Rahmen, der Bedeutung von “Safety“ verwendet. Wird im Rahmen der Arbeit von “Security“

gesprochen, so wird explizit der Begriff “Security“ verwendet und nicht das deutsche Wort “Sicherheit“.

Safety

Die Norm-Definition für Safety lässt sich übersetzt aus der IEC 61508-4 entnehmen:

> **Sicherheit** Freiheit von unvertretbarem Risiko

Daraus lässt sich eine neue Beschreibung herleiten. So kann man Sicherheit als “Sicherheit“ vor der Verletzung von Menschen und anderen Lebewesen, sowie als “Sicherheit“ vor der Schädigung von Gütern und der Umwelt beschreiben.

Security

Durch die klare Trennung von Safety und Security, wird der Begriff Security weder von Neil Storey ([8]), noch durch die DIN EN 61508-4 abgedeckt. Aus diesem Grund wird auf die Beschreibung aus [10] zurückgegriffen. Andrew Tannenbaum beschreibt darin Security, als eine Kombination aus vier Aspekten im Bezug auf Informationen und Nachrichten. Dabei handelt es sich um die Aspekte Geheimhaltung, Authentifizierung, Nachweisbarkeit und Unversehrtheit.

Funktionale Sicherheit

Neben den Begriffen Sicherheit, Safety und Security muss auch der Begriff der funktionalen Sicherheit geklärt werden. So ist die Definition der IEC 61508-4:

> **funktionale Sicherheit** Teil der Gesamtsicherheit, bezogen auf die EUC und das EUC-Leit- oder Steuerungssystem, der von der korrekten Funktion des sicherheitsbezogenen E/E/PE-Systems und anderer risikomindernder Maßnahmen abhängt

Dabei steht die Abkürzung EUC für den Englischen Begriff Equipment under Control und der Begriff E/E/PE-System für elektrisches/elektronisches/programmierbares elektronisches System.

Fail-Safe

In der Veröffentlichung [11] über CPLD basierte Fail-Safe Systeme, wird der Begriff Fail-Safe kurz erläutert. Der Begriff beschreibt die Eigenschaft eines Systems, das es keine Person oder die Umgebung im Fehlerfall schadet. So muss ein Fail-Safe System garantieren, dass es

niemandem Schaden zuführen kann, selbst wenn es sich in einem Fehlerzustand befindet und keine Kontrolle mehr hat.

Single Point of Failure

Als Single Point of Failure bezeichnet man gemäß Neil Storeys ([8]) die Eigenschaft einer Systemkomponente, dass ihr Ausfall zwangsläufig zum Ausfall des kompletten Systems führt.

Safety Integrity Level

Ein Begriff, der im Rahmen von Sicherheitsanalysen häufiger auftaucht, ist das Safety Integrity Level, kurz SIL. Auch wenn das SIL nicht in dieser Arbeit weiter verwendet wird, sollte es zumindest einmal erwähnt werden. Eine passende Beschreibung für SIL findet man in [12]. Auch wenn die Quelle sich auf Automobile bezieht, so arbeitet sie bei der Erklärung auch mit der IEC 61508 und beschreibt das SIL als ein Maß für die erforderte Risikoreduzierung. Das SIL wird dabei durch Werte der Tabelle 2.1 bestimmt.

So wird zuerst die Ausfallwahrscheinlichkeit der Komponente ermittelt und daraus das SIL

Sicherheits-integritäts-level	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde
4	$\geq 10^{-9}$ bis 10^{-8}
3	$\geq 10^{-8}$ bis 10^{-7}
2	$\geq 10^{-7}$ bis 10^{-6}
1	$\geq 10^{-6}$ bis 10^{-5}

Tabelle 2.1: SIL Grenzwerte aus der IEC 61508

der Komponente. Im Anschluss kann man dann das SIL in seine weiteren Analysen einfließen lassen und kann über das Level die Menge an Maßnahmen ermitteln, die in das System integriert werden müssen.

System Health Management

In [13] wird die Tatsache beschrieben, dass Systeme im Laufe der Zeit ausfallen können. Diese Tatsache ist für den Begriff System Health Management, kurz SHM bedeutend. So steht der Begriff des SHM nicht für eine generelle Betrachtung der Sicherheit, sondern für den Umgang mit Fehlern und den Erhalt der Sicherheit und der Funktion im System.

2.2 Systemmodellierung

Um eine Sicherheitsanalyse an einem entsprechenden System durchführen zu können, benötigt man entweder das fertige System oder ein Modell des Systems. Die Aufgabe des Modells ist es das Verhalten und den Aufbau des Systems zu beschreiben. So wird in [14] ein Modell wie folgt definiert:

> Ein **Modell** ist eine abstrakte Beschreibung der Realität.

Das Modell kann folglich ein System unterschiedlich detailliert beschreiben. Im Rahmen der modellgetriebenen Entwicklung wird daher zuerst ein grobes Modell gebaut und dieses nach und nach erweitert. Dabei werden nach und nach immer mehr Komponenten und Subsysteme beschrieben und modelliert. Dieser Prozess wird Modellierung genannt. Während dieser Modellierung werden unterschiedliche Arten von Artefakten erstellt, die das System und dessen Komponente beschreiben. Diese Artefakte können aus reinem Text bestehen, aber auch aus grafischen Abbildungen, die das System abbilden.

In dieser Arbeit wird davon ausgegangen, dass das System als ein Modell vorliegt. Daher zielen alle Beschreibungen auf eine Sicherheitsanalyse mit einem Modell ab. Die Analyse an einem fertigen System wird daher nicht beschrieben.

Im folgenden Abschnitt werden vier bedeutende Verfahren vorgestellt, die für die Modellierung von Systemen verwendet werden können und die eine Bedeutung für diese Arbeit haben.

Textuelle Beschreibung

Die textuelle Beschreibung ist vermutlich das ursprüngliche Verfahren der Systemmodellierung. Bei diesem Verfahren wird in einem Text beschrieben, wie ein System funktioniert und arbeitet. Details oder Unterkomponenten können beispielsweise mit einer Unterteilung in Kapitel strukturiert und organisiert werden. Im Vergleich zu grafischen Arten der Modellierung kann die textuelle Beschreibung alle möglichen Details und Zusammenhänge beschreiben, selbst die, die sich schlecht bis nicht grafisch darstellen lassen. Dafür haben textuelle Beschreibungen oft den Nachteil, dass Zusammenhänge, die sich leicht grafisch Darstellen lassen, in textueller Form viel Text benötigen und nicht so schnell zu verstehen sind.

Die textuelle Beschreibung kann für Sicherheitsanalysen dazu verwendet werden, dass sich

der Analyst mittels der textuellen Beschreibung ein Bild des Systems macht und darauf seine Analysen anwendet. Darüber hinaus kann die textuelle Beschreibung als Erweiterung für grafische Modelle verwendet werden. Dies bietet sich besonders an, wenn sich Eigenschaften eines Modells schlecht grafisch darstellen lassen.

UML

Die Unified Modeling Language, kurz UML, ist eine grafische Notation für die Darstellung von Systemmodellen und wurde von der Object Management Group, kurz OMG entwickelt. Die UML wurde entwickelt, um die Entwicklung von Software zu vereinfachen und Entwicklungsfehler zu verhindern. Somit hat sich die UML zu einem wertvollen Werkzeug für das Software Engineering entwickelt.

Auf der Seite der OMG ([15]) wird beschrieben, dass mit der UML mehrere Perspektiven auf ein Projekt möglich sind und sich mit UML darstellen lassen. So unterstützt die UML mehrere Arten von Diagrammen, welche wiederum unterschiedliche Bereiche der Modellierung abdecken. In diesem Rahmen unterstützt die UML beispielsweise strukturelle Diagramme wie die Paket- und Klassendiagramme, welche entweder eine Paket- oder Klassenstruktur im Softwareprojekt darstellen können. Zusätzlich unterstützt die UML aber auch Verhaltensdiagramme, welche das Verhalten von Elementen und Systemen grafisch darstellen soll.

Die Abbildung 2.1 zeigt eine Übersicht der Diagramme, die von der UML unterstützt werden. Die UML befindet sich in der Abbildung in der Version 2.2. Dabei ist zu beachten, dass die UML sich in ständiger Weiterentwicklung befindet und der Inhalt der Sprache sich von Version zu Version verändern kann.

Bei Sicherheitsanalysen hat die UML die Aufgabe, dem Analysten ein Bild des Systems zu liefern. Dabei kann der Analyst seine Analysen direkt auf den Elementen der Diagramme anwenden . Ein Beispiel dafür liefert Bruce P. Douglass, indem er seine UML-Modelle mit einem Metamodell erweiterte und auf dem Ergebnis eine automatisierte FTA-Analyse anwandte ([9]).

SysML

Während die UML für das Software Engineering entwickelt wurde, entwickelte die OMG eine weitere Modellierungssprache, die Systems Modeling Language, kurz SysML. In [14] werden die Ursprünge der SysML beschrieben. So baut die SysML auf Teilen der UML auf und erweitert diese in Richtung System Engineering. Dabei werden neue Diagrammtypen hinzugefügt, die

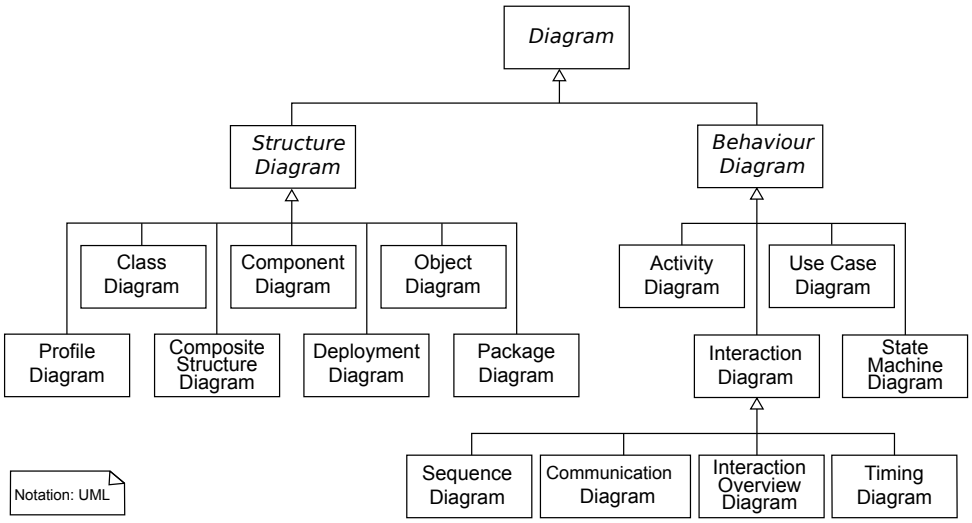

Abbildung 2.1: Hierarchie von Diagrammen in UML 2.2, die wie ein Klassendiagramm dargestellt wurden ([1]).

in der UML nicht enthalten sind.

Die Elemente der SysML werden in der Abbildung 2.2 dargestellt. Vergleicht man diese Abbildung mit der Abbildung 2.1, so fällt einem auf, dass die UML über mehr Diagrammtypen verfügt. Dies hat den Grund, dass nicht alle Diagrammtypen von der SysML übernommen wurden. Somit ist die SysML keine Erweiterung der UML im mathematischen Sinne.

Einen Einstieg in die SysML bildet dabei das Buch [16]. Im Rahmen des Buches werden die Blockdefinitionsdiagramme erklärt, die in den weiteren Abschnitten verwendet werden. Eine genaue Definition des aktuellen Standes der SysML findet man zusätzlich unter [17].

Ebenso wie die UML, kann die SysML für Sicherheitsanalysen am Modell verwendet werden. Anders als bei der UML lassen sich aber mit der SysML technische Zusammenhänge und Signalflüsse besser darstellen und können direkt vom Diagramm übernommen werden und in die Analyse einfließen.

Mathematische Formeln

Ein weiteres Verfahren zum Beschreiben von Systemen sind mathematische Formeln. Diese Formeln bilden formale Modelle des Systems. Das Ziel der Formeln ist es, ein Systemverhalten

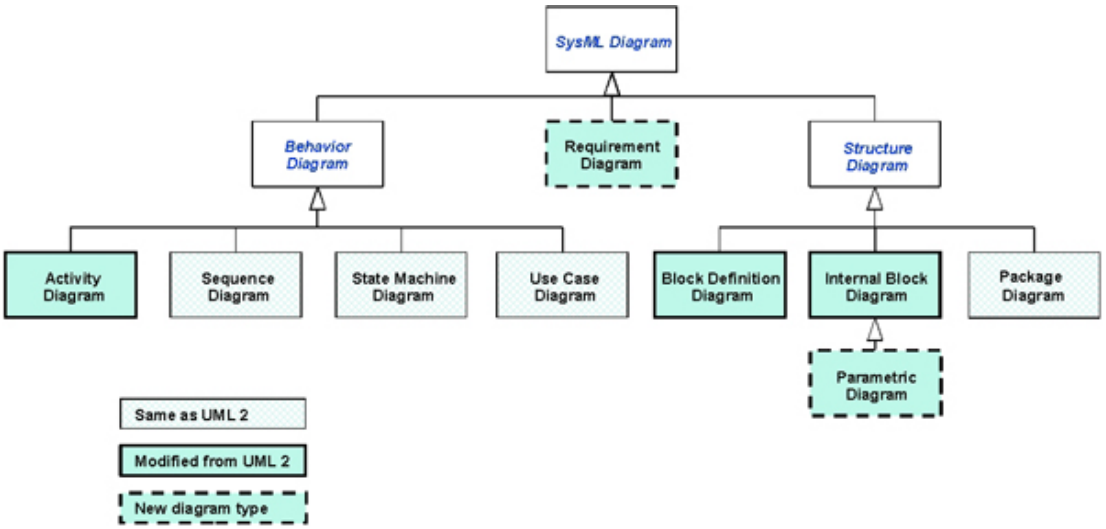

Abbildung 2.2: SysML Diagrammtypen ([2]).

mathematisch zu beschreiben. So wird beispielsweise das Verhalten eines Reglers mit einer Formel modelliert. Diese Beschreibung kann klassisch mit textuellen Formeln geschehen, aber auch mit Formeln, die in Funktionsblöcke verpackt sind. So kann das Tool Simulink mathematische Ausdrücke in Blöcken darstellen und das Verhalten des Systems beschreiben.

Für die Sicherheitsanalyse sind diese Formeln eher uninteressant. Da sie das Verhalten des Systems beschreiben, lässt sich durch sie nicht der Aufbau des Systems ermitteln. Somit sind sie für die Analyse, die sich mit dem Systemaufbau und den daraus ergebenen Verhalten bezogen auf die Sicherheit beschäftigen, uninteressant. Wiederum bieten sich die Formeln dafür an, Ergebnisse von Sicherheitsanalysen zu beschreiben. Kombiniert man die mathematischen Formeln mit einer anderen Modellierungstechnik, so kann man das Verhalten des Systems und seiner Komponenten bezogen auf die Sicherheit beschreiben. So lässt sich eine binäre Formel aufstellen, die beschreibt, unter welchem Umstand ein System eine spezifische Funktion erfüllt. Als Beispiel für den Zusammenhang werden die Formeln 2.2 und 2.3 verwendet.

$$(A \vee B) \wedge C \Rightarrow System_{\mathrm{X}} \tag{2.2}$$

$$A \wedge B \wedge C \Rightarrow System_{\mathrm{Y}} \tag{2.3}$$

In dem Beispiel wird die Funktion eines Systems beschrieben, welches von drei Komponenten abhängt. Das System erfüllt dabei zwei Funktionen, X und Y, die mit Buchstaben als Indexe an die Komponente, bzw. das System gesetzt werden. Die Funktionen hängen dabei von der

Funktion der Komponenten A, B und C ab. Dabei hat jede Funktion eine andere Abhängigkeit zu den Komponenten.

2.3 Kreativitäts-basierte und systematische Analyseverfahren

Steht ein Modell des Systems, so kann man mit dem Analysieren beginnen. Jedoch muss man sich bei der Sicherheitsanalyse für ein Vorgehen entscheiden. Bei dem Vorgehen kann man die Verfahren in zwei größere Verfahrensgruppen unterteilen. Die erste Gruppe basiert auf der Kreativität des Anwenders. Ein Beispiel, für ein Verfahren dieser Gruppe ist das bekannte Brainstorming. Bei diesem Verfahren versucht der Anwender durch Sammeln von zufälligen Gedanken eine Übersicht zu erstellen. Aufgrund der Art und Weise dieser Verfahren, sind die Ergebnisse nicht deterministisch und können von Anwender zu Anwender stark variieren. Darüber hinaus können wichtige Aspekte, durch beispielsweise fehlende Erfahrungen oder Kreativität, übersehen werden.

Aus diesem Grund wurden systematische Verfahren entwickelt, die dem Anwender helfen sollen, bessere Ergebnisse zu erhalten. Das Ziel der systematischen Verfahren ist es, so wenig Kreativität wie möglich in die Analyse einfließen zu lassen. Dadurch sollen die Ergebnisse deterministisch werden und sich unabhängig von dem Analysten ermitteln lassen. Zusätzlich sollen die Verfahren Ergebnisse aufdecken, die bei kreativen Verfahren übersehen werden können.

2.4 Quantifizierende Verfahren

Eine weitere Unterteilung, der man sich bewusst sein muss, ist die Unterteilung in quantifizierende und nicht quantifizierende Verfahren. Bei den quantifizierenden Verfahren geht es darum, dass man unter anderem Wahrscheinlichkeiten und Schweregrade von Gefahren mit konkreten Zahlen betitelt und diese in die Analyse einfließen lässt. Dieses Vorgehen kann hauptsächlich bei mechanischen und elektrischen Elementen angewandt werden, die einen Verschleiß haben oder über die man Statistiken zu deren Ausfallwahrscheinlichkeiten erstellt hat. Auch wird das Vorgehen zum Teil bei Software angewandt. Bei dem Zusammenhang mit Software sollte man jedoch bedenken, dass Software sich deterministisch verhalten muss und über keinen Verschleiß verfügt. Folglich resultieren die Fehler in der Software auf einer anderen Basis und lassen sich nur schwer mit sinnvollen Zahlen betiteln. In dieser Arbeit wird daher nicht mit quantifizierenden Verfahren gearbeitet. Systeme und Komponenten werden

rein auf der Basis betrachtet, dass diese ausfallen können und nicht mit welcher konkreten Wahrscheinlichkeit sie ausfallen können.

Auch wenn keine quantifizierenden Verfahren genutzt werden, so muss sich der Analyst bewusst sein, dass er im Moment einer Entscheidung ein quantifizierendes Verfahren nutzt. So können keine Entscheidungen getroffen werden, ohne dass man die Auswahlmöglichkeiten auf irgendeine beliebige Technik gewichtet. So werden beispielsweise selbst bei der Auswahl des Essens die Möglichkeiten auf kreativer Basis unterbewusst quantifiziert. Da im Anschluss einer Sicherheitsanalyse konsekutiv Maßnahmen gegen die Fehler überprüft werden sollten, werden bei Überprüfung zwangsläufig quantifizierende Verfahren angewandt.

2.5 Gängige Analyseverfahren

Hat man sich für ein eine grobe Richtung bei den Analyseverfahren entschieden, so muss man noch ein konkretes Verfahren auswählen. Zur Auswahl stehen mehrere unterschiedliche Analyseverfahren. Dabei haben die unterschiedlichen Verfahren stark variierende Herangehensweisen und unterschiedliche Perspektiven auf das System. So gibt es Verfahren, die einen Fehler und seine Auswirkungen auf das System betrachten. Andere Verfahren betrachten beispielsweise ein Element und betrachten die Fehler, die passieren müssen, damit das Element ausfällt. Ausgehend von der Situation bieten sich somit unterschiedliche Verfahren an. Diese Verfahren können dann abhängig von den Umständen kombiniert werden und somit ein neues Bild von der Situation erzeugen.

In diesem Abschnitt werden ein paar gängige Verfahren vorgestellt. Die Auflistung erhebt nicht den Anspruch auf Vollständigkeit. Sie bildet lediglich eine Grundlage für Analysen. Die Beschreibung der Verfahren bassiert auf der Grundlage von Neil Storeys Beschreibungen ([8]). Eine weitere Auflistung dieser und anderer Verfahren bietet [13]. Dabei werden die Verfahren mit Zweck, Hintergrund und Vorgehen vorgestellt.

HAZOP

Eine HAZOP-Studie oder englisch HAZard and OPerability studies, ist ein Verfahren, welches in der Chemieindustrie entwickelt wurde und sich zu einem gängigen Verfahren für Sicherheitsanalysen entwickelt hat. Der Kern des Verfahrens ist eine Expertenrunde, die aus Fachkräften besteht, die sich mit den einzelnen Komponenten des zu analysierenden Systems gut auskennen. Ein Diskussionsleiter versucht dann in dieser Runde mit Hilfe von geeigneten

Leitworten die Funktion von Systemelementen zu analysieren. Wobei das Verfahren auf der Frageart “Was passiert, wenn ...?“ basiert. So ergeben sich Fragen wie “Was passiert, wenn die Funkverbindung abbricht?“, die an die Expertenrunde gestellt werden. Antworten und Vorschläge auf die Fragen werden dann dokumentiert und später weiter verarbeitet.

Neil Storey schreibt zusätzlich über die HAZOP-Studie, dass dieses Verfahren sehr effektiv sein kann. Er erwähnt aber auch, dass das Verfahren für die Beteiligten auch sehr anstrengend sein kann und es viel Zeit in Anspruch nehmen kann.

FMEA

Die Failure Mode and Effects Analysis, kurz FMEA betrachtet das Fehlverhalten einer jeden Systemkomponente und die Auswirkungen dieses Fehlers. Bei dem Verfahren wird zwischen potenziellen Fehlern, potenziellen Fehlerfolgen und potenziellen Fehlerursachen unterschieden. Diese Angaben werden meistens in Tabellen sortiert und lassen sich aber auch zu Graphen kombinieren. Auf diese Weise kann verfolgt werden, wie ein Fehler ausgehend von einer Komponente sich weiter ausbreitet und wie er sich dann auf das ganze System auswirkt.

Eine Konsequenz aus der Vorgehensweise beim FMEA-Verfahren ist, dass selbst unkritische Elemente und Fehler analysiert werden. So schreibt Neil Storey, dass das Verfahren aufgrund der detaillierten Analyse sehr teuer und aufwändig ist.

FTA

Die Fault Tree Analysis, kurz FTA oder zu Deutsch Fehlerbaumanalyse ist ein Analyseverfahren, welches darauf aufbaut, dass mögliche Fehler eines Systems bekannt sind. Bei dem Verfahren wird das zu betrachtende Element als Wurzel eines Baumes, bzw. Graphen betrachtet. Ausgehend von der Wurzel wird der Baum dann mit Fehlern erweitert. Die hinzukommenden Fehler werden dabei mit booleschen Operatoren verknüpft. Dabei bildet jeder neue Knoten einen neuen Zweig, der weiter betrachtet wird. Das Ziel ist es am Ende einen logischen Baum zu erhalten, der die Abhängigkeiten für den Ausfall einer Hauptkomponente beschreibt. Das Vorgehen beim Erstellen dieses Baumes wird in der DIN 25424-2 vorgestellt und standardisiert.

Ein Beispiel für einen Fehlerbaum stellt die Abbildung 2.3 dar. Bei der vereinfachten Darstellung geht es um die Analyse eines Aufzuges und dessen Fahrtüchtigkeit. Dabei erfüllt der Aufzug seine Tätigkeit nicht, wenn er ausgefallen ist oder in Wartung ist. Das Ausfallen des Aufzuges kann wiederum mehrere Gründe haben, die sich auch wieder in mehreren Zweigen

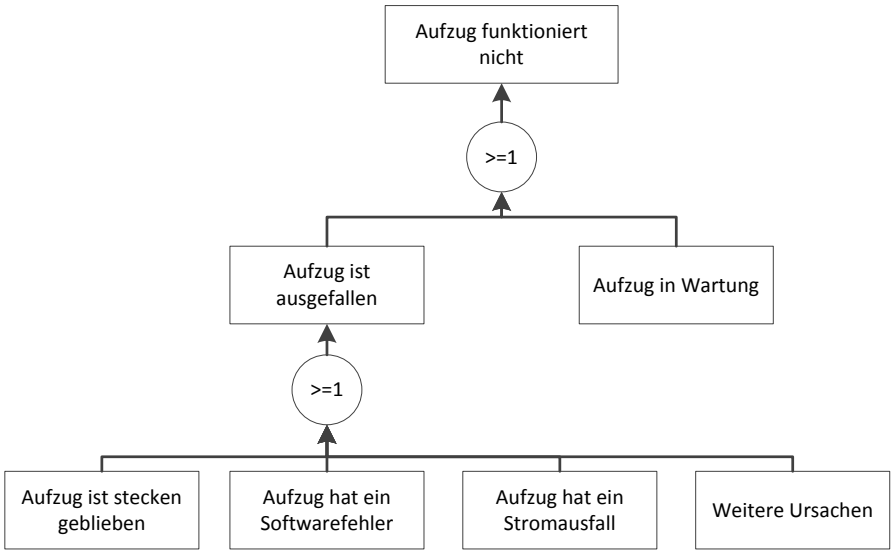

Abbildung 2.3: Beispiel eines Fehlerbaums für den Ausfall von Aufzügen.

darstellen.

Neil Storey verweist explizit darauf, dass die möglichen Fehler bekannt sein müssen. Somit müssen zuvor Analysen stattfinden, die mögliche Fehler aufdecken, bevor diese in den Fehlerbaum einfließen können.

Best Practice Maßnahmen

Ein weniger analytisches Verfahren ist die Suche nach “Best Practice“ Maßnahmen. In diesem Rahmen wird nicht das eigene System analysiert, sondern man greift auf bestehende Systeme zurück, die man betrachtet und analysiert. Das Ziel dieses Vorgehens ist es, bereits vorhandene Probleme, Ansätze und Lösungen zu entdecken und diese dann später zu integrieren. So wird bei diesem Verfahren ein Blick über den Tellerrand getätigt, um ein möglichst umfangreiches Bild zu erhalten.

2.6 Fehlererkennung zur Laufzeit

Sind mögliche Fehlerursachen, -quellen und -ausbreitungen identifiziert, so ist der nächste Schritt der Umgang mit den Fehlern. Dieser Abschnitt gehört zum System Health Management. Damit das System mit diesen Fehlern umgehen kann und auf diese reagieren kann, muss es diese zuvor erkennen. Dieser Abschnitt des Kapitels beschäftigt sich daher mit der Erkennung von Fehlern zur Laufzeit.

Totmanneinrichtung

Die Totmanneinrichtung ist ein System zum Überwachen von Personen. Die zu überwachende Person muss dabei in einer vorgegebenen Zeit einen Schalter, Taster oder Ähnliches bedienen, um dem System mitzuteilen, dass er in Kontrolle über das System ist. Dieses Verfahren lässt sich in vielerlei Arten und Weisen einsetzen. Das Ziel ist, festzustellen, ob ein Teilsystem (unter anderem eine Person) noch aktiv ist und seine Funktion erfüllt. Meldet die Person sich nicht beim System, so können Maßnahmen ergriffen werden. Ein Beispiel dafür ist der Lokführer in Zügen ([18]). Dieser meldet sich in einem regelmäßigen Abstand beim System über einen Totmannschalter. Wird dieser Schalter nicht rechtzeitig betätigt, so wird der Zug automatisch gestoppt. Dies soll sicherstellen, dass der Zug nicht weiter fährt, wenn der Fahrer ausgefallen ist.

Watchdog

Neil Storey beschreibt ein Watchdog als eine Maßnahme, mit der man einen Prozessor, bzw. einen Programmablauf zurück setzen kann ([8]). Das in der Praxis weit verbreitete System arbeitet auf der gleichen Basis, wie die Totmanneinrichtung. Eine Umsetzung dieser Maßnahme findet man schon in den meisten Mikrocontrollern. Dabei sendet ein Zähler im System in einem festen Zeitabstand ein Signal an den sogenannten Watchdog. Erhält der Watchdog nicht das Signal, so startet er das System neu. Diese Technik wird im Bereich Software eingesetzt und der Watchdog besteht entweder aus einer Software- oder Hardwareeinheit. Der Hintergrundgedanke ist dabei, dass ein Fehler in der Software die Ausführung manipuliert und das System nicht mehr regulär weiter arbeiten kann. In diesem Fall, kann das System nicht mehr sein Signal an den Watchdog senden. Der Watchdog versucht daraufhin, den Fehler durch einen Neustart zu beseitigen.

Neil Storey beschreibt aber auch wesentliche Nachteile dieses Verfahrens ([8]). Zwar ist das Verfahren leicht zu implementieren, jedoch erkennt es Fehler erst nach dem Ablauf der

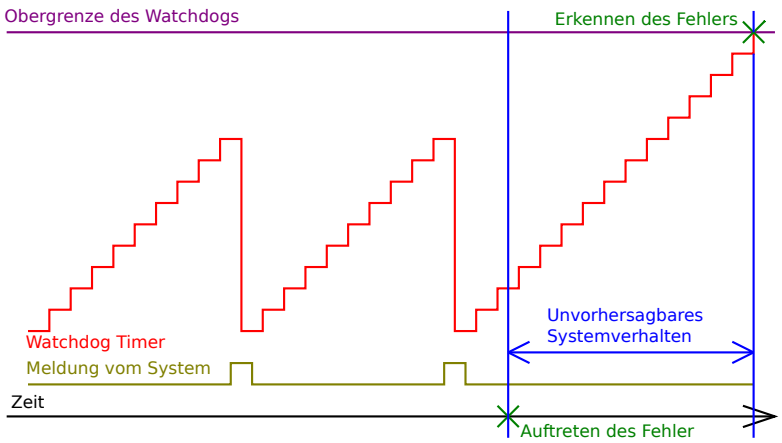

Abbildung 2.4: Beispiel der Problematik in von Watchdogs überwachten Systemen.

zeitlichen Periode. Zwischen dem Auftreten des Fehlers und dessen Erkennung ist das Verhalten des Systems nicht vorhersagbar. Somit kann das System gegebenen Falls nicht auf eingehende Signale reagieren, noch kann garantiert werden, dass das System nicht irgendeinen Schaden anrichtet. Dabei ist die Zeit, die ein Fehler unerkannt anliegen kann, abhängig von der zeitlichen Periode des Watchdogs. Die Abbildung 2.4 stellt diese Problematik bildlich dar und markiert den gefährlichen Bereich mit unvorhersagbaren Systemverhalten.

Systemverhalten beobachten

Die zuvor vorgestellten Verfahren ließen sich leicht umsetzen, jedoch sind diese auch mit gewissen Nachteilen verbunden. Ein alternativer Ansatz ist die Beobachtung der steuernden Elemente. So können zusätzliche Elemente das Verhalten und die Ergebnisse der ursprünglichen Elemente beobachten und auswerten. Ein Beispiel dafür ist der Einbau von n gleichen Systemen, wobei n eine natürliche Zahl größer gleich zwei ist. Dabei können die Ergebnisse der einzelnen Elemente ausgewertet und verglichen werden. Dieses Verfahren wird im Abschnitt 2.7 an dem Beispiel von redundanten Systemen erklärt. Es ist jedoch zu bedenken, dass eine gewisse Komplexität für dieses Verfahren benötigt wird.

2.7 Maßnahmen im Fehlerfall

Mit der Fähigkeit einen Fehler zu erkennen, gewinnt das System die Möglichkeit auf einen Fehler zu reagieren. Dieser Abschnitt, der sich ebenfalls mit dem System Health Management

beschäftigt, hat die Aufgabe auf einen Fehler zu reagieren und somit einen Schaden abzuwenden. So kann man entweder auf einen Fehler reagieren, indem man versucht den Betrieb aufrechtzuerhalten oder in dem man versucht das System in einen sicheren Zustand zu bringen.

Es ist zu bedenken, dass das Hinzufügen von Maßnahmen das System und sein Verhalten

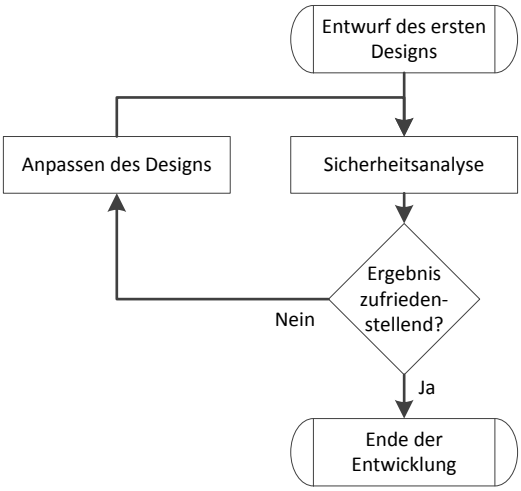

Abbildung 2.5: Abstrakter Ablauf der Entwicklung von sicherheitskritischen Systemen mit iterativen Vorgehen.

verändert. Somit wird bei keiner gewählten Maßnahme das System auf dem alten Stand bleiben. Durch den neuen Stand im System werden folglich neue Analysen des Systems benötigt. Die Abbildung 2.5 zeigt dabei abstrakt den Ablauf der Entwicklung. Dabei wird das System so oft angepasst und neu analysiert, bis es einen akzeptablen Stand erhalten hat.

Mitigations

Die Mitigations oder zu Deutsch Schadensbegrenzungmaßnahmen beschäftigt sich mit einem Fehler im System, indem sie das System in einem neuen Modus setzt und somit das Verhalten ändert. Um dieses Vorgehen zu verdeutlichen kann man erneut auf das Beispiel mit dem Totmannschalter und den Zug aus Abschnitt 2.6 zurückgreifen. Fällt der Lokführer aus, dann erkennt das System diesen Ausfall über das zuvor beschriebene Verfahren. Im Anschluss wechselt das System sein Verhalten und reagiert somit auf die neue Situation. In diesem Beispiel stoppt es den Zug, als Reaktion auf die Situation. Für dieses Vorgehen werden neue

Elemente, bzw. Funktionen im System benötigt, die nach der Auswahl der Mitigation in das System integriert werden müssen.

Redundante Systeme

Eine Alternative zu den Mitigations ist der Einsatz von redundanten Systemen. Neil Storey beschreibt dabei die Grundlagen für die Verwendung von redundanten Systemen ([8]). Auch definiert die IEC 61508-4 den Begriff:

> **Redundanz** das Vorhandensein von mehr als einem Mittel zum Ausführen einer geforderten Funktion oder zur Darstellung von Informationen

So wird die Funktion einer Komponente redundant, bzw. in mehreren Modulen umgesetzt. Dabei kann ein Modul ausfallen und die Aufgabe wird weiterhin gelöst, da ein weiteres Modul die Aufgabe weiterhin lösen kann. Dieses klassische Verfahren wird in vielen Bereichen und Verfahren ein- und umgesetzt. Abbildung 2.6 stellt ein Beispiel für dieses Verfahren dar. In einem nicht redundanten System ist der Verlauf, dass eine Signalquelle einen Input für das System generiert. Ein Modul empfängt den Input und ermittelt ein Ergebnis. Dieses Ergebnis wird dann ausgegeben. Das redundante System arbeitet auf einer anderen Basis. Die Signalquelle generiert weiterhin einen Input für das System. Dieser Input wird an zwei oder mehrere Module geliefert. Diese Module ermitteln dann ihre Ergebnisse. Danach gibt es n Ergebnisse, wobei n der Anzahl der Module entspricht. Da am Ende nur ein Ergebnis weiterverarbeitet werden kann, muss ein einheitliches Ergebnis ermittelt werden. Um dieses Ergebnis zu erhalten, wird ein zusätzliches Element hinzugefügt. Dieses zusätzliche Element wird Voter genannt. Dieser Voter hat die Aufgabe, die Ergebnisse von fehlerhaften Modulen rauszufiltern und einheitliche, richtige Ergebnisse weiterzuleiten.

Weiterhin stellen redundante Systeme nicht eine problemlose Lösung dar. So muss das Voter-Element sicher feststellen können, welches arbeitende Element fehlerhaft ist. Dabei können byzantinische Fehler auftauchen, die es dem Voter erschweren, das fehlerhafte Modul zu identifizieren. Weiterhin entsteht bei der einfachen Betrachtung ein Single-Point-Of-Failure. Fällt das Voter-Element aus, so kann der Ablauf nicht weiter durchgeführt werden.

Eine detaillierte Erklärung der byzantinischen Fehler wird in der Veröffentlichung [19] gemacht. Dabei wird erklärt, welche Herausforderung an die beteiligten Elemente gestellt wird. Zusätzlich werden Lösungsansätze präsentiert und erläutert.

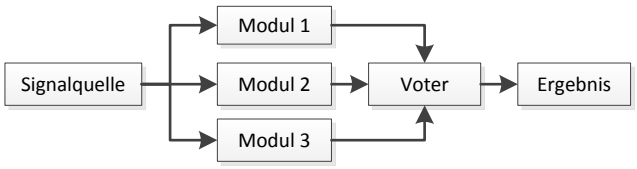

Abbildung 2.6: Beispielstruktur eines redundanten Systems (nach Neil Storey).

2.8 Verwendete Verfahren und Vorgehensweisen

In den vorhergehenden Abschnitten wurden die notwendigen Grundlagen erörtert. In diesem Abschnitt werden die ausgewählten Verfahren und Vorgehensweisen präsentiert und die Auswahl erörtert.

Für die Modellierung des Systems wird eine angepasste SysML-Notation verwenden, die eine textuelle Beschreibung für Details und Beschreibungen verwendet. Diese Notation verwendet angepasste SysML Blockdefinitionsdiagramme. Während die Blockdefinitionsdiagramme der SysML alle Signale zwischen den einzelnen Blöcken betitelt werden, wird in der angepassten Notation darauf verzichtet. So werden nur die Signale beschriftet, die über Blockgrenzen hinaus gehen. Dies soll ermöglichen, dass der Betrachter einen Bezug zu den nicht abgebildeten Blocken bekommt und auf der anderen Seite die Darstellung nicht mit zu viel Text ausgefüllt wird und übersichtlich bleibt. Darüber hinaus werden die Ports der Blöcke von der Position her nicht bewegt. So behält ein Block die Position der inneren Ports, wenn er in einem neuen Diagramm in einer neuen Ansicht dargestellt wird. Dies Maßnahmen soll es ermöglichen Diagramme in der Arbeit als Bilder zu präsentieren, die nicht den Rahmen einer übersichtlichen Ansicht überschreiten.

In der Modellierung werden sowohl physikalische Architektur, als auch funktionale Architektur in Diagrammen kombiniert. Da feste Elemente aus dem Modellflugbau einfließen, werden diese als physikalische Elemente, bzw. Komponenten in die Architektur integriert. Dabei erfüllen sie die Funktion und die Eigenschaften von handelsüblichen Komponenten des Modellflugbaus.

Der Grund für die Auswahl der SysML ist, dass die SysML es einen ermöglicht Signalver-

läufe, sowohl aus elektrotechnischer, als auch aus der Informationssicht zu beschreiben. Dabei werden durch die Blockdefinitionsdiagramme klare Verläufe und Zusammenhänge dargestellt, die es Möglich machen die funktionalen Abhängigkeiten eines Blockes festzustellen. Für dieses Ziel müssen nur die Verläufe vom Ziel der Signalkette aus betrachtet werden und es bilden sich dann automatisch die funktionalen Abhängigkeiten der Blöcke.

Die Bedingungen, die die funktionalen Abhängigkeiten der Blöcke beschreiben, werden wie in Abschnitt 2.2 beschrieben verwendet. Die Formel 2.4 greift dabei das vorherige Beispiel auf.

$$(A \vee B) \wedge C \Rightarrow System_{\mathrm{X}} \tag{2.4}$$

$$(\neg(A) \wedge \neg(B)) \vee \neg(C) \Rightarrow Ausfall\_System_{\mathrm{X}} \tag{2.5}$$

Durch die Verwendung von boolscher Logik ist es möglich, aus der Formel 2.4 die neue Formel 2.5 zu generieren. Die Formel 2.5 betrachtet dabei den Zusammenhang aus negierter Sicht und beschreibt somit die Bedingungen für den Ausfall der Funktion im System. Dieser Aufbau ermöglicht es einen aus den Werten einen Fehlerbaum zu generieren. Ähnlich wie in der Arbeit von Bruce P. Douglass wird dann aus den Beschreibungen, bzw. Metadaten der Modellkomponenten ein Fehlerbaum generiert ([9]).

Die Formeln werden verwendet, weil sie es dem Leser ermöglichen, möglichst schnell die Zusammenhänge klar zu erfassen. Im Gegensatz zu einer textuellen Beschreibung sind sie eindeutig für den Leser, leicht zu erfassen und lassen sich gut weiterverarbeiten. Ein weiterer Vorteil ist die automatische Generierung eines Fehlerbaumes.

Die Fehlerbaumanalyse wurde ausgewählt, weil sie hervorragend mit der formel-basierten Modellierung zusammen arbeitet. Zusätzlich bildet die Fehlerbaumanalyse eines der grundlegenden Verfahren der Sicherheitsanalysen und ermöglicht es dem Anwender sich auf die beteiligten Elemente zu konzentrieren und nicht auf jedes Element und jeden möglichen Fehler.

Nach dem Abschluss der Analyse werden die Formeln betrachtet und auf Aspekte des System Health Management analysiert. Das Ziel dieser Maßnahme ist es, auf die entdeckten Schwachstellen im System einzugehen und mögliche Risiken zu mindern. Wird eine Maßnahme getroffen, die die Struktur des Modells verändert, so wird und muss ein neuer Iterationszyklus mit neuen Analysen gestartet.

3 Anforderungsanalyse

In dem vorhergehenden Kapitel wurden die Grundlagen für Sicherheitsanalysen gelegt. Bevor diese Analysen angewandt werden können muss das System ausgewählt und spezifiziert werden. In diesem Rahmen müssen die Anforderungen an das System und sein verhalten definiert werden. Dies ist notwendig, damit die Sicherheitsanalysen im nächsten Schritt konkrete Funktionen überprüfen können.

In diesem Rahmen werden in diesen Kapitel zuerst die gewünschten Flugmodi vorgestellt und analysiert. Diese Flugmodi werden getrennt betrachtet, da an das UAV mehrere Anforderungen variierend zu dem Flugmodus gestellt werden und unterschiedliches Verhalten des UAVs verlangen. So soll das UAV auf unterschiedliche Arten gesteuert werden und das jeweilige Vorgehen bei der Steuerung soll variieren. So sind die Anforderungen an ein UAV, welches wie ein Modellflugzeug gesteuert wird stark abweichend von den Anforderungen, die an ein UAV gestellt werden, welches autonom eine Strecke abfliegen soll.

Im zweiten Abschnitt werden zwei zuvor ausgewählte Mitigations vorgestellt und analysiert. Zwar werden Mitigations erst als Ergebnis von zuvor durchgeführten Analysen ausgewählt und eingesetzt, jedoch wurden zuvor mehrere Maßnahmen im Rahmen des Projektes besprochen. Zusätzlich lässt sich aufgrund der Tatsache, dass es sich um ein Luftfahrzeug handelt davon ausgehen, dass kein Fail-Safe-State erreicht werden kann. Aus diesem Grund wird davon ausgegangen, dass Fehler auftauchen und Mitigations ergriffen werden müssen. Folglich werden aus den zuvor besprochenen Maßnahmen zwei Maßnahmen ausgewählt, vorgestellt und in diesem Kapitel analysiert.

3.1 Flugmodi

An Flugmodi sollen die Modi “Safemode - Reines Messsystem“, “Begrenzter Steuerungsmodus“, “Stabilisierter Flugmodus“ und der “Autonome Flugmodus“ unterstützt werden. Aus diesen unterschiedlichen Flugmodi soll später der Pilot einen Modus auswählen, nachdem sich dann das UAV verhält. Diese Flugmodi werden in diesem Abschnitt vorgestellt.

Im Laufe des Projektes stellen die Flugmodi zusätzliche Milestones dar, die nach und nach den Funktionsumfang erweitern. So bauen die späteren Modi auf Teilen der vorherigen Modi auf. Im folgenden Kapitel 4 werden dann die Modi in Funktionssets kombiniert, die jeweils einen Entwicklungsstand darstellen.

Die rechtlichen Grundlagen für den Flug in Deutschland werden in der Luftverkehrsordnung (LuftVO) [20] geregelt. Gemäß § 4a fallen UAVs unter diese Regelung, wenn aufgrund der Art des Gerätes keine gesonderte Freistellung besteht. Aus diesem Grund muss darauf geachtet werden, dass das UAV jederzeit diese Ordnung einhält.

3.1.1 Safemode - Reines Messsystem

Im Rahmen dieses Modus muss das UAV so sicher wie möglich fliegen. Um dies zu erreichen, sollen alle Steuersignale direkt und unbeeinflusst vom Piloten kommen. Alle Steuersignale sollen von einer Funkfernsteuerung aus dem Modellflugbereich kommen (siehe Beispielabbildung 3.1). Kein Signal darf durch zusätzliche Logik manipuliert werden und somit das Flugverhalten beeinflussen.

Zusätzlich soll ein Messsystem betrieben werden. Dieses Messsystem soll während des Fluges

Abbildung 3.1: Beispiel einer Funkfernsteuerung ([3]).

unterschiedliche Daten aufnehmen und dokumentieren. Die Daten sollen im Flugzeug auf einem Speichermedium abgelegt werden. Zusätzlich sollen ausgewählte Datensätze im Rahmen

der Möglichkeit an die Bodenstation übertragen werden.

An das UAV werden danach folgende Anforderungen gestellt:

- Eine direkte Steuerung vom Piloten muss garantiert werden.
- Es sollen unterschiedliche Messdaten während des Fluges dokumentiert werden.
- Ein Teil der dokumentierten Messdaten sollen an die Bodenstation gesendet werden.

3.1.2 Begrenzter Steuerungsmodus

Der begrenzte Steuermodus erweitert das System mit einer Begrenzung für die Aktoren. Das Ziel soll dabei sein, dass die Aktoren des Systems keine Stellpositionen annehmen, bei denen die Aktoren beschädigt werden. Dabei werden die Steuersignale wie beim messenden System an das UAV übertragen. Danach werden sie aber nicht direkt an die Aktorik übergeben, sondern zuerst ausgewertet. Liegt ein Wert außerhalb des akzeptierten Wertebereiches vor, so wird der Wert auf den maximal erlaubten Stellwert begrenzt.

An das UAV werden in diesem Modus folgende Anforderungen gestellt:

- Das UAV soll wie ein Modellflugzeug gesteuert werden.
- Steuerwerte sollen so manipuliert werden, sodass diese die Aktorik des UAVs nicht beschädigen können.
- Es sollen unterschiedliche Messdaten während des Fluges dokumentiert werden.
- Ein Teil der dokumentierten Messdaten sollen an die Bodenstation gesendet werden.

3.1.3 Stabilisierter Flugmodus

Der stabilisierte Flugmodus erweitert das System mit einer Regelung für die Fluglage. Um einen autonomen Flug durchzuführen, muss das UAV in der Lage sein einen Vektor, im Raum stabilisiert abzufliegen, dieser Modus ist ein Schritt in diese Richtung. Dabei soll das UAV unabhängig von Windstärke und -richtung den Vektor abfliegen. Die Werte sollen von dem Piloten oder einem zusätzlichen Anwender an das UAV übergeben werden. Das System soll dann aus den Vorgaben neue Stellwerte für die Aktorik errechnen und diese dann übergeben.

Um dies zu erreichen, wird das System im dritten Schritt mit einer passenden Regelung

erweitert. Die benötigten Werte für den Regler sollen über das Messsystem gewonnen werden. Das Messsystem soll folglich benötigte Werte zeitlich diskretisiert an den Regler übertragen. Die neu errechneten Stellwerte sollen weiterhin vom System begrenzt werden und dürfen den akzeptablen Wertebereich nicht verlassen.

Der Punkt, dass sich das Steuerverhalten beim Wechsel in diesen Modus stark verändert wird nur am Rande betrachtet. Generell muss man aber bedenken, dass sich das Steuerverhalten des UAVs massiv verändert, sobald man von einem der vorherigen Modi in den stabilisierten Flug schaltet. Da sich das Steuerverhalten der Eingabequelle stark verändert, wird an diesem Punkt davon ausgegangen, dass ein zusätzlicher Anwender im stabilisierten Flug die Steuerung übernehmen kann. Somit kann im Zweifelsfall ein Anwender übernehmen, der beim Eingeben seiner Steuerbefehle ein stabilisiertes Verhalten erwartet und nicht versucht die Stabilisierung selbstständig durchzuführen.

Somit ergeben sich folgende Anforderung an das UAV:

- Ein Pilot muss Steuerwerte in Form von neuen Lagevektoren an das UAV übertragen können.
- Ein Anwender soll alternativ in der Lage sein, Steuerwerte in Form von Lagevektoren an das UAV übertragen zu können.
- Das Messsystem muss zeitlich diskretisierte Messwerte für eine Regelung zur Verfügung stellen.
- Ein Regler muss die Steuerwerte als Vektoren im Raum interpretieren und in Verbindung mit den Messwerten neue Steuerwerte für die Aktorik generieren.
- Steuerwerte sollen so manipuliert werden, sodass diese die Aktorik des UAVs nicht beschädigen können.
- Es sollen unterschiedliche Messdaten während des Fluges dokumentiert werden.
- Ein Teil der dokumentierten Messdaten sollen an die Bodenstation gesendet werden.

3.1.4 Autonomer Flugmodus

Der letzte angedachte Flugmodus ist der autonome Flug. Im Rahmen dieses Entwicklungsschrittes soll nicht mehr ein Vektor im Raum vorgegeben werden, sondern eine konkrete Position

im Raum. Das UAV muss dann autonom aus der Ausgangs- und Zielposition, einen Vektor im Raum bestimmen, den es dann abfliegt.

Die Zielposition wird von einem Anwender an der Basisstation vorgegeben. Die Ausgangsposition wird über zeitlich diskretisierte Messwerte des Messsystems vorgegeben. Der daraus errechnete Vektor wird weiter an einen Regler weitergegeben. Dieser Regler basiert auf der Basis des stabilisierten Flugmodus. Somit erweitert der autonome Flug die Funktionen des stabilisierten Fluges.

Die sich daraus resultierenden Anforderungen an das UAV sind folgende:

- Ein Anwender soll eine Zielposition an das System vorgeben können.
- Das UAV muss aus seiner Ausgangs- und Zielposition einen Vektor im Raum bestimmen können.
- Das Messsystem muss zeitlich diskretisierte Messwerte für die Positionsbestimmung liefern.
- Das Messsystem muss zeitlich diskretisierte Messwerte für eine Regelung zur Verfügung stellen.
- Ein Regler muss die Vektoren im Raum interpretieren und in Verbindung mit den Messwerten Steuerwerte für die Aktorik generieren.
- Steuerwerte sollen so manipuliert werden, sodass diese die Aktorik des UAVs nicht beschädigen können.
- Es sollen unterschiedliche Messdaten während des Fluges dokumentiert werden.
- Ein Teil der dokumentierten Messdaten sollen an die Bodenstation gesendet werden.

3.2 Mitigations

Als nächstes werden die ausgewählten Mitigations analysiert. Die Mitgigations haben die Aufgabe, einen möglichst sicheren Zustand im Fehlerfall zu erzeugen. Um dieses Ziel zu erreichen wurden im Vorfeld die Mitigations “Akustischer Signalgeber“ und “Gezielter Aufstieg“ ausgewählt. Diese Maßnahmen haben den Vorteil, dass sie grundlegend in der Anwendung,

als auch in den Anforderungen verschieden sind und unterschiedliche Fehlerklassen abdecken. Somit bieten beide Maßnahmen einen guten Einblick in die dazugehörigen Analysen und Anforderungen. Darauf aufbauend können dann andere Maßnahmen analysiert und ins System integriert werden. Eine kurze Auflistung alternativer Maßnahmen wird im Kapitel 5 vorgestellt. Diese werden in der Arbeit nicht betrachtet, können aber aufbauend auf den folgenden Analysen auch analysiert werden.

3.2.1 Akustische Signalgeber

Ein im Projekt diskutierter Ansatz, ist der Einsatz von akustischen Signalgebern. Im Rahmen des Modellflugs werden akustische Signale für die Überwachung der Spannungsversorgung eingesetzt ([21]). Das Ziel dieser Technologie ist es Personen in der Umgebung auf das UAV aufmerksam zu machen und auf den Missstand hinzuweisen. Tritt ein Fehler im System auf und wird dieser erkannt, dann soll die entsprechende Systemkomponente darauf reagieren und die Maßnahme auslösen. Infolgedessen sollen Personen am Boden in der Lage sein einen abstürzenden UAV auszuweichen.

Die Anforderungen, die sich an den Signalgeber ergeben sind folgende:

- Der Signalgeber muss feststellen, ob die Funkverbindung verloren gegangen ist.
- Er muss feststellen, ob Aktorik ausgefallen ist.
- Er muss Fehler erkennen, die einen geplanten Betrieb des UAVs verhindern.
- Ist eines der angegebenen Elemente ausgefallen, so muss der akustische Signalgeber sich aktivieren.
- Der Pilot sollte in der Lage sein die Maßnahme zu aktivieren.

3.2.2 Gezielter Aufstieg

Eine Maßnahme, die für ein fortgeschrittenes Projekt diskutiert wurde, ist ein gezielter Aufstieg des UAVs. Bei dieser Maßnahme versucht das UAV in einem Kreisflug an Höhe zu gewinnen. Hat das UAV die obere Grenze ihres Luftraumes erreicht (siehe [20]), dann soll dieses dort in einer Kreisbewegung die Position für einen gewissen Zeitraum halten.

Diese Maßnahme findet Einsatz bei beispielsweise lokalen Störquellen am Boden und bei Funkabschattung durch etwaige Gebäude oder geografische Gegebenheiten. Durch die erhöhte

Lage soll das UAV aus dem negativen Einflussbereich entfernt werden. Ist eine Verbindung wieder hergestellt, so kann ein Anwender oder Pilot das UAV wieder übernehmen. Ist es nicht möglich eine neue Verbindung zwischen UAV und Bodenstation herzustellen, dann können weitere Maßnahmen ergriffen werden. Steht beispielsweise ein Fallschirm zur Verfügung, so kann eine Landung mit Fallschirm angepeilt werden. Stehen keine weiteren Maßnahmen zur Verfügung, geht das UAV beim Fehlschlag in einen Absturz über.

Folgende Anforderungen ergeben sich für das System:

- Fällt die Funkverbindung aus, dann muss das System dies erkennen.
- Ist keine Verbindung von Bodenstation und UAV vorhanden, so muss Steuerung des UAVs die Kontrolle übernehmen.
- Besteht eine neue Verbindung zwischen Bodenstation und UAV, so muss die Kontrolle zurückgegeben werden.

4 Analyse der Funktionssets

Im Rahmen dieses Kapitels werden die im Kapitel 3 beschriebenen Flugmodi zu Funktionssets zusammengefasst und funktional analysiert. Ein Funktionsset kombiniert dabei ein oder mehrere Flugmodi zu einem Set von Modi. Um dies zu erreichen, hat ein jedes Funktionsset eine eigene Architektur und Komponentenmodell, die die benötigten Elemente enthalten.

Die Funktionssets sollen dabei nach einem natürlichen Entwicklungsablauf gebildet werden. So soll zuerst ein Messsystem erstellt werden. Dieses soll dann nach und nach mit neuen Flugmodi erweitert werden und neue Funktionssets ergeben, welche ein System beschreiben, welches im letzten Stadium, bzw. letzten Funktionsset einen autonomen Flug unterstützt. Somit beginnt das erste Funktionsset mit nur einem Modus und wenigen Elementen. Die darauf folgenden Funktionssets haben dann jeweils einen Flugmodus mehr und dementsprechend mehr Elemente um die Systemfunktionen zu erfüllen.

Um einen ersten Eindruck des Aufbaus eines UAVs zu gewinnen, wird im ersten Abschnitt die Struktur eines Modellflugzeuges betrachtet. Danach werden die Funktionssets jeweils in einzelnen Abschnitten betrachtet. Dabei werden Funktionsblöcke in den einzelnen Architekturen betrachtet und beschrieben. Behält ein Funktionsblock seine Eigenschaften, die in dem vorherigen Funktionsset beschrieben wurden, so werden diese nicht erneut im Detail beschrieben.

4.1 Aufbau eines klassischen Modellflugzeuges

Als Beispiel für eine einfache Konfiguration wird die Konfiguration eines Modellflugzeuges verwendet. Diese Konfiguration verfügt zwar über keinen Fail-Safe-State, jedoch stellt sie ein Mindestmaß an Sicherheit dar. So dient sie als Muster für die künftigen Funktionssets und sollte für diese eine Basissicherheit darstellen.

In diesem Rahmen wird zuerst betrachtet, wie der Fluss der Steuersignale durch das Modell geht und wie die Steuerung geschieht. Im zweiten Abschnitt wird betrachtet, wie Mitigations

im System integriert werden und wie diese Maßnahmen ausgelöst werden. Dabei werden noch nicht die ausgewählten, formellen Verfahren verwendet, sondern eine einfache Betrachtung der Elemente, um eine Übersicht der verwendeten Komponenten zu bekommen.

4.1.1 Fliegen des UAVs

In der Grundkonfiguration steuert ein Pilot sein Modellflugzeug mit einer Funkfernsteuerung. Dabei behält der Pilot sein Modellflugzeug im Blickfeld, trifft Entscheidungen für den Flug und gibt diese in die Funkfernsteuerung ein. Die daraus entstehenden Daten werden über einen Funkkanal an das Modellflugzeug übertragen. Dort werden diese Daten in elektrische Steuersignale überführt, die dann von den Aktoren in Bewegungen umgesetzt werden.

Die Abbildung 4.1 zeigt den Verlauf in der angepassten SysML-Notation. Der Pilot erstellt seine

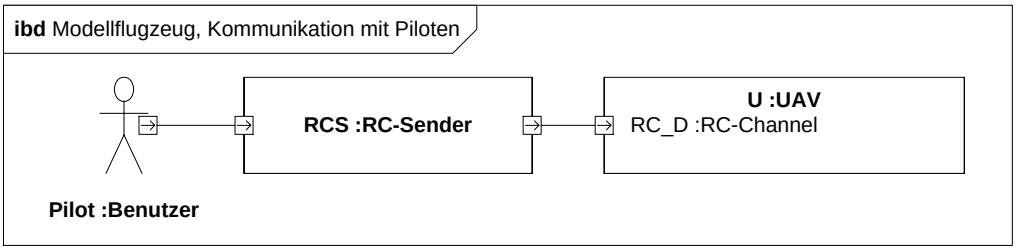

Abbildung 4.1: Modellflugzeug, Kommunikation mit Piloten.

Entscheidung und übergibt diese an die Funkfernsteuerung RCS. Die Verbindung ist dabei nur in eine Richtung und ermöglicht keine Rückmeldung von der Funkfernsteuerung an den Piloten. Die Funkfernsteuerung gibt dann in einem gerichteten Signal, ohne Rückmeldung, die Informationen an das Modellflugzeug weiter. Die optische Rückmeldung des Modellflugzeuges U an den Piloten wird in diesem Modell hingegen nicht dargestellt. Auch wird in diesem Modell der Funkkanal und die tragende Luft nicht modelliert.

$$Pilot_{\mathrm{f}} \wedge RCS_{\mathrm{f}} \wedge U_{\mathrm{f}} \Rightarrow Funktion_{\mathrm{f}} \tag{4.1}$$

Formel 4.1 stellt dabei die Bedingung für die Flugfunktion des UAVs dar und verwendet den Buchstaben klein F als Index für die Symbolisierung der Flugfunktion. Alle Komponenten in der Kette müssen ihre Funktion erfüllen, damit das UAV fliegen kann. Fällt eine Komponente

aus, so kann das UAV seine Funktion nicht mehr erfüllen und gerät außer Kontrolle (siehe Formel 4.2).

$$\neg(Pilot_{\mathrm{f}}) \vee \neg(RCS_{\mathrm{f}}) \vee \neg(U_{\mathrm{f}}) \Rightarrow Kontrollverlust_{\mathrm{f}} \tag{4.2}$$

Pilot

Der Pilot wird vorerst nicht weiter betrachtet. Grundsätzlich muss man davon ausgehen, dass der Pilot ausfallen kann. Dies kann verschiedene Gründe haben, wobei das Feststellen dieser Gründe nicht Inhalt dieser Arbeit ist. Es ist jedoch zu bedenken, dass der Pilot eine Schwachstelle im Gesamtsystem ist und keine Funktionsgarantie gibt.

Funkfernsteuerung

Bei der Funkfernsteuerung wird davon ausgegangen, dass es sich um eine handelsübliche Funkfernsteuerung aus dem Modellflugbereich handelt. Diese Fernsteuerungen bestehen aus einer Kombination von Sender und Empfänger. Der entsprechende Empfänger wird im Modellflugzeug untergebracht und setzt die Funksignale des Senders in elektrische Steuersignale für die Aktoren um. Diese Funksignale werden auf einem zuvor konfigurierten Funkkanal gesendet, welcher in einem speziell reservierten Frequenzbereich liegt. Der Frequenzbereich ist soweit ausgelegt, dass mehrere Piloten mit ihren Modellflugzeugen auf einem Flugplatz fliegen können und sich nicht gegenseitig blockieren. Dabei müssen sich jedoch die Piloten gegenseitig absprechen, welche Kanäle von welchem Piloten genutzt werden. Diese Absprache ist notwendig um Kollisionen zu vermeiden.

Die Spannungsversorgung geschieht jeweils einzeln bei Sender und Empfänger. Während der Sender eine eigene Spannungsversorgung benötigt, greift der Empfänger auf die Spannungsversorgung des Modellflugzeuges zurück (siehe nächsten Abschnitt Abbildung 4.2). Die Spannungsversorgung des Senders ist in die Funkfernsteuerung integriert und läuft entweder über eine Batterie oder über einen Akkumulator.

Eine Beispielumsetzung der Funkfernsteuerung wird in dem Projektdokument [22] beschrieben. Dabei wird eine Funkfernsteuerung der Firma Spektrum beschrieben, wie sie im Modellflugbereich eingesetzt wird.

UAV

Der Aufbau des Modellflugzeugs wird in Abbildung 4.2 dargestellt. Das Modellflugzeug hat

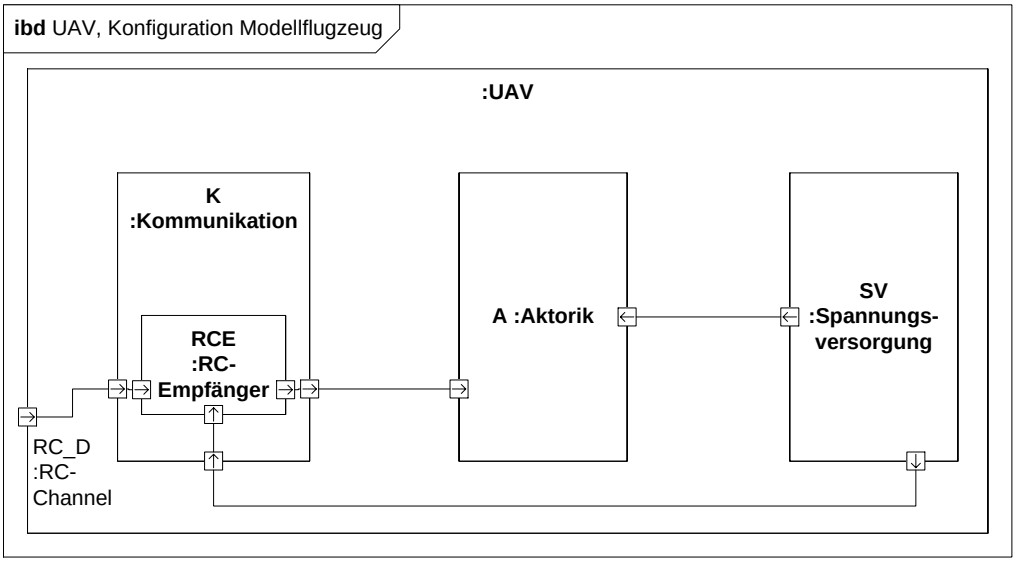

Abbildung 4.2: UAV, Konfiguration Modellflugzeug.

einen eingehenden Funkkanal RC_D, über den die Steuerdaten für das Modell kommen. Intern besteht das Modell aus drei Blöcken. Der Block K kümmert sich um die Kommunikation mit den außen stehenden Elementen und bereitet die Steuersignale auf. Der Aktorik-Block A stellt die verwendete Aktorik dar und setzt die Steuersignale in Bewegungen des Modells um. Der letzte Block ist die Spannungsversorgung SV, die das System und ihre Teilkomponenten versorgt. Betrachtet man diese Elemente abstrakt ohne eine eine detaillierte Betrachtung, so kann man eine Wirkkette aus der Abbildung entnehmen. Aus dieser Wirkkette lässt sich die Formel 4.3 bilden, welche dann die Flugfunktion des Modellflugzeuges beschreibt.

$$RC\_D_{\mathrm{f}} \wedge K_{\mathrm{f}} \wedge A_{\mathrm{f}} \wedge SV_{\mathrm{f}} \Rightarrow UAV_{\mathrm{f}} \tag{4.3}$$

$$\neg(RC\_D_{\mathrm{f}}) \vee \neg(K_{\mathrm{f}}) \vee \neg(A_{\mathrm{f}}) \vee \neg(SV_{\mathrm{f}}) \Rightarrow Kontrollverlust\_UAV_{\mathrm{f}} \tag{4.4}$$

Die Formel 4.4 beschreibt hingegen die Bedingungen für den Ausfall der Flugfunktion des Modellflugzeuges. Die konkreten Teilkomponenten und ihre Abhängigkeiten werden im folgenden Abschnitt beschrieben und betrachtet.

Die **Spannungsversorgung** wird nicht im Detail modelliert. Sie enthält eine beliebige Spannungsquelle (LiPo-Akkumulator, Brennstoffzelle, etc.) und mehrere Ausgangsports. Die Ausgangsports stellen unterschiedliche Spannungen für die Teilsysteme zur Verfügung. Unterschiedliche Ports können aber auch die gleiche Spannung zur Verfügung stellen. Intern besteht eine Abhängigkeit zwischen allen ausgehenden Ports. So stellt der Block entweder allen Ports Spannung zur Verfügung oder fällt komplett aus. Dabei wird zuerst davon ausgegangen, dass die Komponenten einen festen Strombedarf haben. Wird dieser Bedarf überschritten, so wird er von der Spannungsversorgung begrenzt. Eine detaillierte Betrachtung der Problematik eines Kurzschlusses in einer Komponente sollte erst mit einer expliziten Komponentenarchitektur durchgeführt werden. Daher werden die ausgehenden Spannungen in der SysML-Notation als gerichtet betrachtet und ohne Rückwirkungen durch Kurzschlüsse oder entstehende Überspannung in einer Komponente. Dies hat den Grund, dass in diesem Abschnitt noch Funktions- und Komponentenblöcke kombiniert werden. Das Ziel ist es erstmal die funktionalen Abhängigkeiten zu betrachten. Später, wenn alle Funktionen auf konkrete Komponenten abgebildet werden können die Interaktionen der Komponenten im Detail betrachtet werden.

Von außen hat die Spannungsversorgung keine eingehenden Ports. Daher bestehen keine zusätzlichen Abhängigkeiten für den Betrieb. Somit wird die Spannungsversorgung als ein Block betrachtet, der nur aufgrund interner Fehler ausfallen kann.

Die Spannungsversorgung kann intern redundant aufgebaut sein. So kann sie beispielsweise über zwei gespiegelte Akkumulatoren verfügen. Diese Konstellation ist jedoch abhängig von der Bauform und den Einbaumöglichkeiten. Aus diesem Grund wird der Block an dieser Stelle nur abstrakt betrachtet und unter einem Ausfall wird ein Ausfall des kompletten Blocks verstanden.

Eine genaue Betrachtung der Abhängigkeiten für die Spannungsversorgung muss jeweils im Detail für das entsprechende UAV durchgeführt werden. Somit lässt sich allein durch den Einsatz einer Brennstoffzelle eine komplett neue Situation für die Sicherheit erzeugen.

Der **Kommunikation**-Block stellt die Schnittstelle nach außen bereit. Er nimmt die Signale des Piloten auf und bereitet diese für die Aktorik auf. Dieser Block besteht in der klassischen Modellflugzeug-Konstellation aus einem Empfänger (RCE) für die Funkfernsteuerung. Dieser Empfänger nimmt die Funksignale der Funkfernsteuerung RC_D auf und wandelt sie in elektrische Steuersignale für die Aktorik um. Um diese Aufgabe zu bewältigen benötigt, der

Empfänger eine anliegende Spannung. Daraus ergibt sich die Formel 4.5, die die Abhängigkeiten für den Block K beschreibt.

$$RC\_D_{\mathrm{f}} \wedge SV_{\mathrm{f}} \wedge RCE_{\mathrm{f}} \Rightarrow K_{\mathrm{f}} \tag{4.5}$$

Dabei ist zu beachten, dass der Empfänger-Block RCE die gleichen Abhängigkeiten nach außen hat. Jedoch kann der Block RCE auch aufgrund von internen Fehlern ausfallen. Daher ist die Funktionalität von RC_D und SV kein Garant dafür, dass der Kommunikationsblock seine Funktion erfüllt.

Der **Aktorik**-Block bündelt alle vorhandenen Aktoren zu einem Block. Er besteht aus Antrieben, Leitwerken, Bremsen und weiteren Komponenten, die entweder für den Flug von Bedeutung sind oder nicht. Der Inhalt dieses Blocks kann sich generisch an das vorliegende Flugmodell anpassen. So kann ein Modell über zwei Antriebe oder über nur einen Antrieb verfügen. Dabei kann der Ausfall des Antriebes bei einer Ein-Antrieb-Lösung zum Versagen des Modells führen. Bei einem Modell mit zwei Antrieben kann unter Umständen ein Antrieb ausfallen. Wird dieser Ausfall rechtzeitig vom Piloten erkannt, so kann dieser unter Umständen die Kontrolle behalten. Auch kann das Modell unterschiedliche Leitwerke, an variierenden Positionen haben. Dabei haben die Leitwerke jeweils unterschiedliche Gewichtungen. So können gewisse Funktionen eines Leitwerks bei einigen Modellen von anderen Leitwerken übernommen werden. Andere Funktionen von speziellen Leitwerken lassen sich hingegen nicht ersetzen und sind für die Funktion des Modells unabdingbar.

Aus diesen Gründen werden die Aktoren erst einmal als eine abstrakte Einheit gesehen, die eine gewisse Funktion erfüllt. Infolgedessen wird dieser Block nicht im Detail betrachtet. Unterstützt das verwendete Modell eine Konstellation der Aktorik, die einen teilweisen Ausfall der Aktoren unterstützt, so muss dies explizit betrachtet werden. Dazu gehört eine genaue Betrachtung der Aktoren und eine Analyse der technischen Notwendigkeit dieser. Um diese Betrachtung durchzuführen, werden spezielle Kenntnisse im Flugzeugbau benötigt. Daher sollte diese Aufgabe in einer Expertenrunde gelöst werden. Da der Gegenstand dieser Arbeit die Analyse im Bereich Elektrotechnik und Informatik ist, wird diese Analyse nicht weiter verfolgt. Dies stimmt auch mit dem Ziel überein, eine möglichst generische Lösung für die Probleme zu finden. In einer konkreten Umsetzung sollte aber betrachtet werden, in welchem Rahmen Aktorik teilweise ausfallen kann und welche Elemente der Aktorik die ausgefallenen Elemente, wie ersetzen können.

Letztendlich lassen sich mit der Formel 4.6 die Bedingungen für den Aktorik-Block bestimmen.

So müssen die einzelnen Aktoren funktionieren, das Kommunikationsmodul K muss Steuersignale liefern und die Spannungsversorgung SV muss eine Versorgung für die Aktoren und den Kommunikationsblock bereitstellen.

$$K_{\mathrm{f}} \wedge SV_{\mathrm{f}} \wedge Aktoren_{\mathrm{f}} \Rightarrow A_{\mathrm{f}} \tag{4.6}$$

Nach einer Betrachtung der Komponenten ergibt sich weiterhin die Formel 4.3. Die Funkverbindung wird als Teil der Funkfernsteuerung gesehen. Jedoch ergibt sich, dass die übrigen Elemente alle notwendige Glieder der Wirkkette sind und nicht ausfallen dürfen.

Da es sich in diesem Abschnitt um eine Betrachtung des aktuellen Zustandes handelt, wird an dieser Stelle keine Empfehlung und weitere Beurteilung getätigt.

4.1.2 Schadensbegrenzung

Die rechtlichen Grundlagen für den Flug werden in der Luftverkehrsordnung (LuftVO) [20] definiert. Im Rahmen dieser Ordnung befindet sich der § 16 “Erlaubnisbedürftige Nutzung des Luftraums“. Gemäß dieser Ordnung dürfen Modellflugzeuge nicht ohne Sondergenehmigung in der Nähe von Wohngebieten fliegen. Daher handelt es sich bei einem jeden Risiko, welches eingegangen wird um ein tolerierbares Restrisiko, welches in diesem Rahmen akzeptiert wird. Aus diesem Grund besteht im normalen Modellflug kein Bedürfnis für Mitigations. Infolgedessen sind keine Maßnahmen für die Schadensbegrenzung eingeplant.

4.2 Messsystem

Das Messsystem stellt das erste Funktionsset dar. Es kombiniert die Aspekte des Modellflugzeug aus Kapitel 4.1, mit den im Kapitel 3.1.1 beschriebenen Messsystem und den im Kapitel 3.2.1 beschriebenen akustischen Signalgeber. Um die gestellten Anforderungen zu erfüllen, wird das System um eine Bodenstation erweitert. Die Bodenstation BS hat die Aufgabe, die aktiven Messwerte entgegenzunehmen und einen aktuellen Status des UAVs an einen Anwender zu übermitteln. Die Abbildung 4.3 stellt die Erweiterung des Systems dar. So verfügt das UAV

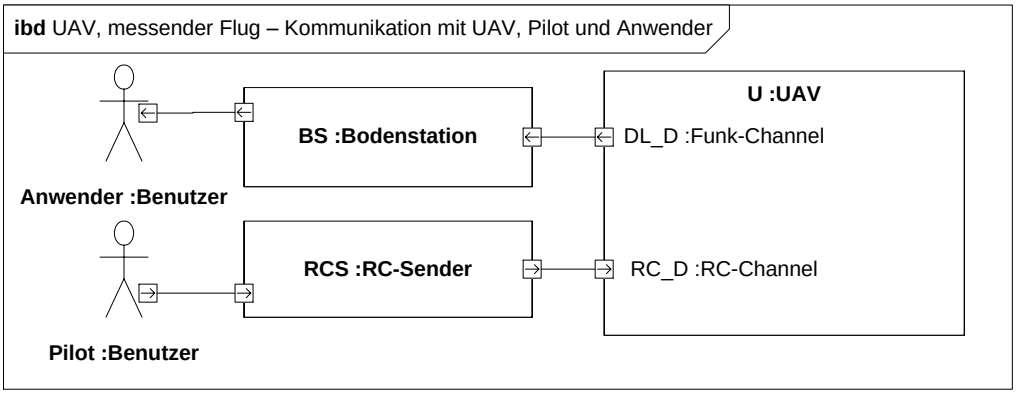

Abbildung 4.3: UAV, messender Flug – Kommunikation mit UAV, Pilot und Anwender.

in der erweiterten Konstellation über einen zusätzlichen Kanal weg von dem UAV hin zu der Bodenstation BS. Diese Bodenstation BS stellt ihre Informationen einem Anwender zur Verfügung, der die Daten ablesen und auswerten kann.

4.2.1 Fliegen des UAVs

Dieser Abschnitt betrachtet die notwendigen Bedingungen, die für den Flug des angepassten UAVs erfüllt sein müssen. In diesem Rahmen stellt die Abbildung 4.4 die neue interne Struktur des UAVs dar. In Abbildung 4.2 im Kapitel 4.1 wurde zuvor ein Einblick in den Aufbau eines UAVs gewährt. An dieser Stelle wurde das UAV um mehrere Elemente erweitert, um die hinzukommenden Ansprüche zu erfüllen.

Im Vergleich der Abbildungen 4.2 und 4.4 stellt sich schnell ein Problem der Sicherheitsanalysen heraus. Die gestiegene Komplexität in Abbildung 4.4 erschwert eine Analyse auf

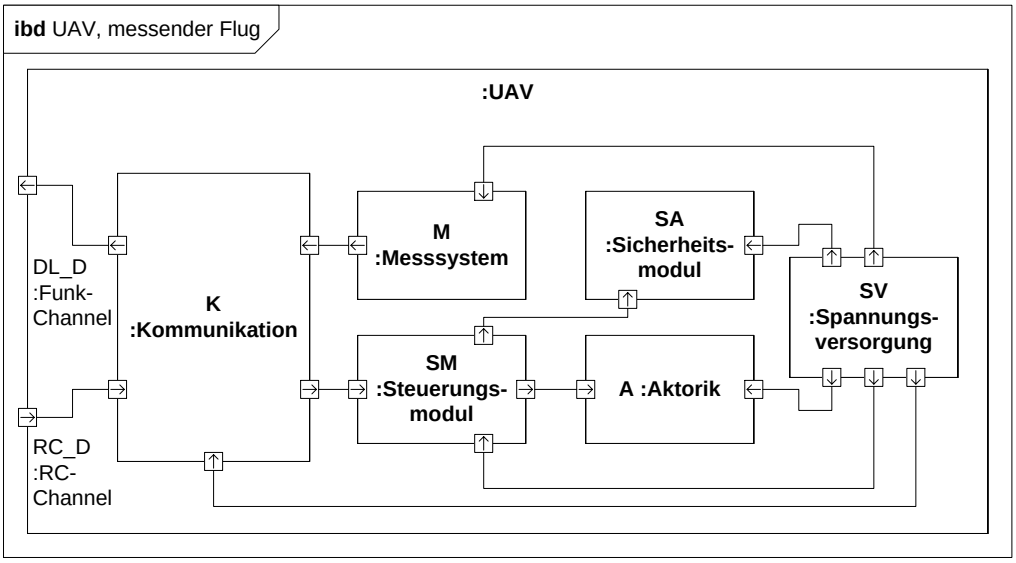

Abbildung 4.4: UAV, messender Flug.

den ersten Blick. So konnte man noch in Abbildung 4.2 leicht die benötigten Abhängigkeiten erkennen. Im aktuellen System ist dies durch hinzugewonnene Verbindungen und Elemente nicht mehr so leicht. Aus diesem Grund wird bei der Analyse der Abhängigkeiten für den Flug beim letzten Element der Wirkkette begonnen. Als das letzte Element in der Wirkkette, wurde im Kapitel 4.1 das Aktorik-Element festgestellt. Dieses Element setzt die Entscheidungen am Ende um und ist das entscheidende Element für das Einhalten des Fluges.

Im folgenden Abschnitt werden die Blöcke des UAVs ausgehend von dem Aktorik-Block betrachtet. Blöcke die in der aktuellen Konstellation keinen Einfluss auf den Aktorik-Block haben, werden vorerst nicht betrachtet und werden erst in späteren Abschnitten betrachtet. Das Ziel dieser Vorgehensweise ist es, nach und nach eine Formel für die funktionale Abhängigkeit zu gewinnen. Zusätzlich kann auf der Basis dieses Vorgehens ein Fehlerbaum (siehe Kapitel 2.5) generiert werden. Dabei wird der Aktorik-Block als Wurzel betrachtet und die Knoten werden sukzessive hinzugefügt. Das Ergebnis ist dann ein fertiger Fehlerbaum, in dem nichtbeteiligte Elemente nicht angeben werden. Dadurch müssen Elemente, die keine Auswirkung auf das betrachtete System haben, nicht analysiert werden. Auf der anderen Seite muss der Baum in

einem Zweig bei dem Piloten, bzw. bei der Verbindung zum Piloten ankommen, wodurch er dann die Wirkkette anzeigt.

Aktorik

Wie zuvor in Kapitel 4.1.1 beschrieben, ist der Aktorik-Block A eine Blackbox, die für die Umsetzung der Flugbefehle des UAVs zuständig ist. Dieser Block kann aufgrund von internen Fehlern ausfallen. Diese internen Fehler werden an dieser Stelle nicht weiter betrachtet.

Nach außen hin hat dieser Block zwei Ports. Beide Ports sind eingehende Signale und müssen dahingehend betrachtet werden, ob die eingehenden Signale notwendig für die Funktion von A sind.

Auf der rechten Seite des Blocks befindet sich ein Port, welcher mit der Spannungsversorgung SV verbunden ist. Wie schon zuvor betrachtet, stellt der Block SV eine Grundlage für den Block A zur Verfügung, ohne der er nicht arbeiten kann. Aus diesem Grund ist die Funktion der Spannungsversorgung SV unabdingbar für die Funktion der Aktorik A.

Auf der linken Seite des Aktorik-Blocks A befindet sich ein eingehender Port des Steuerungsmoduls SM. Aus dem Block SM kommen die Steuerungssignale für die Aktorik. Da die Aktoren ihre Funktion nur mit sinnvollen Steuerungssignalen erfüllen können, wird dieser Block auch zu einen unverzichtbaren Eingang.

Aus diesen Informationen lässt sich eine Formel für die funktionalen Abhängigkeiten der Aktorik beschreiben. Die Formel 4.7 beschreibt diese direkten Abhängigkeiten für den Aktorik-Block A. Dabei verwendet sie erneut den Index klein F für die verwendete Funktion des Fluges.

$$SM_{\mathrm{f}} \wedge SV_{\mathrm{f}} \wedge Aktoren_{\mathrm{f}} \Rightarrow A_{\mathrm{f}} \tag{4.7}$$

Spannungsversorgung

Als erster Knoten im Fehlerbaum wird die Spannungsversorgung SV betrachtet. Die Spannungsversorgung wurde schon einmal im Kapitel 4.1.1 betrachtet und hat sich seitdem nicht verändert. Weiterhin wird sie als ein generischer Block betrachtet, der aufgrund von internen Problemen ausfallen kann.

Steuerungsmodul

Der zweite Knoten des Fehlerbaums besteht aus dem Steuerungsmodul SM. Die Abbildung 4.5 zeigt den internen Aufbau des Steuerungsmoduls in dieser Architekturstufe. Dieses Modul

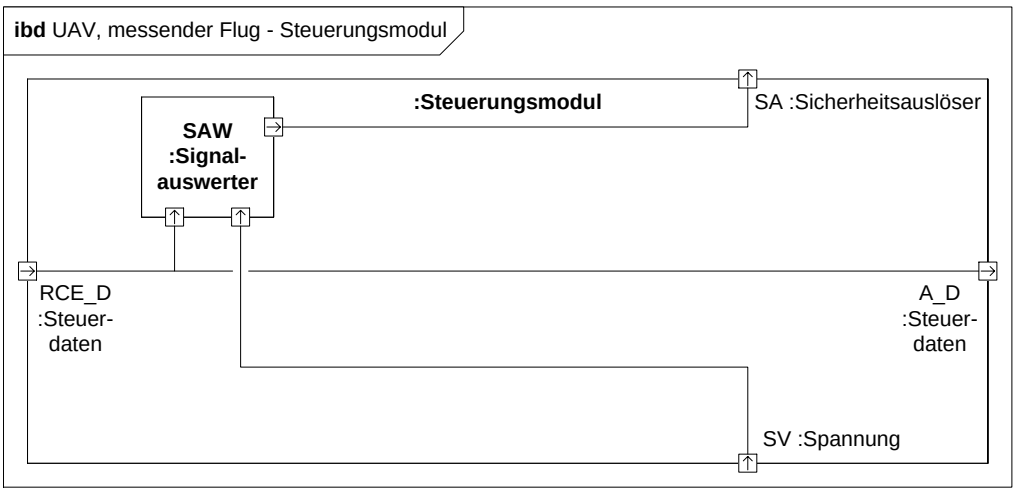

Abbildung 4.5: UAV, messender Flug - Steuerungsmodul.

wurde präventiv in das System aufgenommen. Seine Funktion wird sich erst mit erweiterten Architekturen ergeben. In der ersten Fassung Stellt es einen Auslöser für die Sicherheitsfunktionen zur Verfügung und ein Kanal mit Steuerdaten für die Aktorik.

Bei einer detaillierten Betrachtung des Modells fällt auf, dass die Verbindung mit den Steuerdaten für die Aktorik eine durchgehende Leitung ist. Somit hat dieser eingeschobene Block keinen besonderen Einfluss auf die Aktoren. Der eingehende Port liefert diese Signale (RCE_D) und leitet sie direkt weiter. Die Steuerdaten A_D gehen dann direkt an die Aktorik und versorgen diese mit Befehlen.

Der interne Signalauswerter-Block SAW kann an dieser Stelle ignoriert werden, da er kein Teil der Wirkkette für die betrachtete Funktion ist. Er liegt parallel zu dem Signalverlauf, der aktuell betrachtet wird. Infolgedessen kann auch der eingehende Port mit der Spannung SV ignoriert werden. Die Spannung SV versorgt nur den Block SAW und hat daher keinen Einfluss auf die aktuelle Betrachtung für den Flug des UAVs.

Da das einzig relevante Element für die Funktion des Steuerungsmodul das eingehende Steuersignal ist, kann auf der höheren Architekturebene die Formel 4.8 aufgestellt werden. Folglich erweitert sich der Fehlerbaum in diesem Zweig mit einem neuen Knoten zum Kommunikations-Block K. Somit folgt die spezifische Funktion von SM nur dann, wenn K seine Funktion erfüllt.

$$K_{\mathrm{f}} \Rightarrow SM_{\mathrm{f}} \tag{4.8}$$

Kommunikation

Der Kommunikations-Block K wird in der Abbildung 4.6 detailliert dargestellt. Der Kommunikations-Block wurde dabei erweitert und verfügt nun über mehr Elemente als die Version im Modellflugzeug. Vergleicht man wieder die alte Abbildung 4.2 mit der aktuellen Abbildung 4.6, so stellt

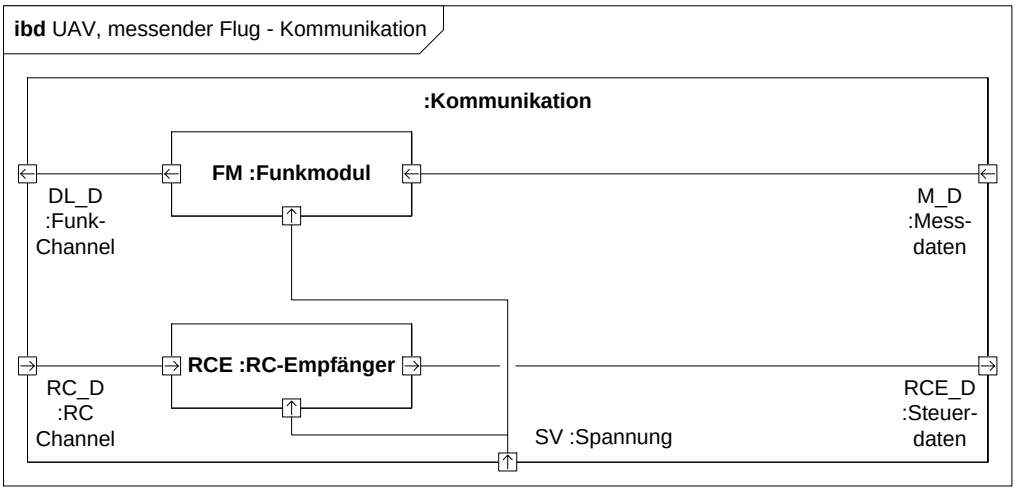

Abbildung 4.6: UAV, messender Flug - Kommunikation.

man fest, dass sich kein wesentlicher Teil für die Funktion verändert hat. Dieser Block wurde nur mit einem Elemente erweitert, welches für den Flug nicht relevant ist. Der hinzugefügte Block ist ein Funkmodul, welches für das Messsystem Daten an die Bodenstation sendet. Somit ergibt sich für den Kommunikations-Block die Formel 4.9, für die funktionale Abhängigkeit im Bereich des Empfangs und Weiterleitens der Steuerdaten.

$$RCE_{\mathrm{f}} \wedge RC\_D_{\mathrm{f}} \wedge SV_{\mathrm{f}} \Rightarrow K_{\mathrm{f}} \tag{4.9}$$

Pilot und Funkfernsteuerung

Die **Funkfernsteuerung** ist weiterhin ein gekauftes System, welches mit den Kriterien aus Kapitel 4.1.1 geliefert wird. Sie kann aus verschiedenen Gründen ausfallen und hat eine vorgegebene Reichweite vom Piloten aus. Der **Pilot** ist ebenso eine Schwachstelle, die weiterhin nicht betrachtet wird.

4.2.2 Zusammenfassung und Analyse des Flugs

Kombiniert man nun die Formeln 4.7 bis 4.9, so kann man für die Abhängigkeiten im UAV eine neue Formel generieren. So lassen sich die Formeln 4.7 und 4.8 zur Formel 4.10 kombinieren.

$$K_{\mathrm{f}} \wedge SV_{\mathrm{f}} \wedge Aktoren_{\mathrm{f}} \Rightarrow A_{\mathrm{f}} \tag{4.10}$$

Bindet man dann noch die Formel 4.9 ein, so erhält man die Formen 4.11, welche alle Abhängigkeiten für die Funktion der Aktorik und den daraus folgenden Flug enthält.

$$(RCE_{\mathrm{f}} \wedge RC\_D_{\mathrm{f}} \wedge SV_{\mathrm{f}}) \wedge SV_{\mathrm{f}} \wedge Aktoren_{\mathrm{f}} \Rightarrow A_{\mathrm{f}} \tag{4.11}$$

Kürzt man nun noch die Formel, so ergibt sich die vereinfachte Formel 4.12.

$$RCE_{\mathrm{f}} \wedge RC\_D_{\mathrm{f}} \wedge SV_{\mathrm{f}} \wedge Aktoren_{\mathrm{f}} \Rightarrow A_{\mathrm{f}} \tag{4.12}$$

An dieser Stelle kann man zusätzlich die Formel 4.13 bilden, welche den Ausfall des UAVs beschreibt.

$$\neg(RCE_{\mathrm{f}}) \vee \neg(RC\_D_{\mathrm{f}}) \vee \neg(SV_{\mathrm{f}}) \vee \neg(Aktoren_{\mathrm{f}}) \Rightarrow Ausfall\_UAV_{\mathrm{f}} \tag{4.13}$$

Mit diesen Formeln kann man alle benötigten Elemente des Systems erkennen. Darüber hinaus kann man aus den Daten nun einen Fehlerbaum generieren, welcher eine Übersicht über die Abhängigkeiten darstellt. Die Abbildung 4.7 zeigt dabei exemplarisch diesen Fehlerbaum.

Betrachtet man diesen Baum im Detail, so kann man erkennen, dass alle Zusammenhänge mit Oder-Funktionen verbunden sind. Somit kann der Ausfall einer jeden Komponente zum Ausfall des Systems führen. Jede Komponente bildet somit einen Single Point of Failure.

Ein Ansatz, dieses Problem zu lösen, ist das Hinzufügen von Redundanzen. Lässt sich ein Element dieser Formel durch zwei Elemente ersetzen, die im Fehlerbaum mit einem Und

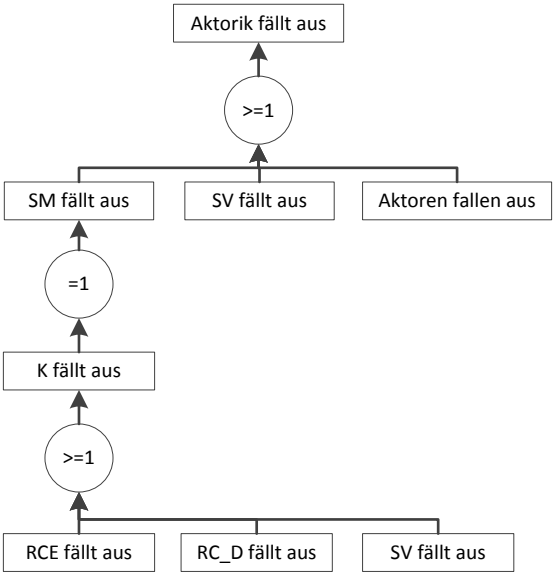

Abbildung 4.7: Fehlerbaum für das UAV mit Messsystem unter Betrachtung der Flugfunktion.

verknüpft sind, so wäre die Konsequenz, dass eines dieser Elemente ausfallen kann und das System weiterhin seine Funktion erfüllen kann. Um festzustellen, welche Elemente durch Redundanzen optimiert werden können, wird nun jedes Element der Formel betrachtet und analysiert, inwiefern das System erweitert werden kann um das Element redundant zu gestalten.

Bei dieser Betrachtung muss jedoch bedacht werden, dass es sich bei dem Modell um eine Kombination von Funktions- und Komponentenblöcken handelt. So können Blöcke, die konkrete Komponenten vertreten auf Redundanzen geprüft werden. Hingegen können funktionale Blöcke nicht auf konkrete Redundanzen geprüft werden. Jedoch kann schon im Vorfeld geprüft werden, ob man funktionale Abhängigkeiten von Blöcken entfernen kann. Zeichnet sich beispielsweise ab, dass ein funktionaler Block später in eine Komponente mit einem geringen Strombedarf kommt, könnte betrachtet werden inwiefern der Einsatz von Redundanzen Abhängigkeiten auflöst oder neu strukturiert.

Sowohl **RCE**, als auch **RC_D** kümmern sich um die direkte Kommunikation. Die Verbindung RC_D kann aufgrund mehrerer Ereignisse ausfallen. So kann der Pilot ausfallen und deshalb keine neuen Signale generieren. Die Spannungsversorgung der Funkfernsteuerung

kann ausfallen und einen Abbruch der Verbindung verursachen. Diese Probleme am Boden werden jedoch nicht betrachtet. Betrachtet werden hingegen die Probleme, die ab der Übertragung auftreten können. In der Luft kann die Übertragung durch unterschiedliche Einflüsse gestört werden. Ebenfalls kann die Verbindung auf größere Distanzen abreißen. Diese Probleme verfügen über eine Relevanz, für die Anpassung des Systems auf der Seite des UAVs.

Ein Ansatz an dieser Stelle ist, die Funkverbindung durch einen zweites Sender- und Empfängerpaar zu erweitern. Durch diese Lösung lässt sich zwar keine zusätzliche Distanz bei der Sendeleistung gewinnen, solange die gleiche Hardware verwendet wird. Auch durch Abschattung und Störungen in der Luft verursachte Probleme lassen sich somit nicht zwangsläufig lösen. Einzig das Problem mit dem Störung des Kanals lässt sich unter Umständen durch ein redundantes System lösen. In dem Dokument [22] wird jedoch die Funkfernsteuerung des Projektes betrachtet. Diese verfügt schon über redundante Kanäle. In diesem Rahmen wurde schon von Seiten des Modellflugs Maßnahmen ergriffen. Somit werden die Betrachtungen auf den Funkkanal abgeschlossen.

Die Spannungsversorgung **SV** ist eines der Kernelemente des Systems. Es wirkt sich auf mehr als nur ein Systemelement aus. Aus diesem Grund kam es in der Formel 4.11 mehr als nur ein mal vor. Folglich liegt der Schluss nahe, dass man betrachtet, inwiefern man dieses Element mit Redundanzen ausstatten kann.

Im Kapitel 4.1.1 wurde schon einmal beschrieben, dass der Block an sich intern mit Redundanzen arbeiten kann. Für die aktuelle Betrachtung bietet es sich aber nicht an, generell über eine Redundanz nachzudenken. Dies liegt an mehreren Faktoren. Einer der wichtigen Faktoren ist die Leistung der Aktoren. Die Aktoren benötigen ein leistungsstarke Spannungsversorgung. Diese benötigt eine gewisse Menge an Raum und bringt ein gewisses Gewicht mit sich. Somit kann es sein, dass eine Redundanz aufgrund von Platzmangel oder zu hohem Gewicht technisch nicht möglich ist. So kann beispielsweise eine Brennstoffzelle mit Wasserstofftank nicht einfach mit einer weiteren Brennstoffzelle und einem weiteren Wasserstofftank erweitert werden.

Auf dieser Basis wird darauf verzichtet, über eine generelle Redundanz im Bereich Spannungsquellen nachzudenken. Weiterhin ist es aber möglich, dass Teilelemente eine zusätzliche Spannungsversorgung bekommen, die redundant zur Spannungsversorgung SV ist. Dabei besteht jedoch die Anforderung, dass es sich bei dem Element um einen kleinen Verbraucher handelt, der nur eine kleine Spannungsversorgung benötigt. Unter diesem Aspekt ist es

beispielsweise möglich über eine zusätzliche Spannungsversorgung für das Kommunikationsmodul nachzudenken. Jedoch würde sich hierdurch die Formel 4.12 nur soweit umbauen, dass die Formel 4.14 erscheint.

$$(RCE_{\mathrm{f}} \wedge (SV_{\mathrm{f}} \vee RSV_{\mathrm{f}})) \wedge RC\_D_{\mathrm{f}} \wedge SV_{\mathrm{f}} \wedge Aktoren_{\mathrm{f}} \Rightarrow A_{\mathrm{f}} \tag{4.14}$$

Bei dieser neuen Formel ist das Element RSV eine redundante Spannungsversorgung für den Funkempfänger. Zwar ist eine Verknüpfung mit einem Oder dazu gekommen, jedoch lässt sich die Spannungsversorgung SV generell nicht damit ersetzen und somit würde weiterhin ein Ausfall von SV ein Ausfall des Systems bedeuten. Somit wird der Ansatz an dieser Stelle verworfen.

Die **Aktoren** sind ebenso wie die Spannungsversorgung kein Thema für eine generelle Betrachtung auf Redundanzen. Dieser Aspekt wurde zuvor in den Kapiteln 4.1.1 und 4.2.1 beschrieben. Möchte man versuchen eine Sicherheit in diesem Bereich herzustellen, beispielsweise durch den Einsatz von redundanten Aktoren, so muss dies auf einer Analyse von Ingenieuren im Bereich Mechanik geschehen.

4.2.3 Fazit bezüglich des Flugs

Letztendlich erfüllt die beschriebene Konstellation die geplanten Anforderungen und somit die angesetzte Basissicherheit. Direkt lässt sich leider noch keine Erweiterung einbringen, die Vorteile im Bereich Sicherheit mit sich bringen würde. Folglich wird diese funktionale Architektur für die Anforderungen als endgültig angesehen.

4.2.4 Mitigation ausgelöst vom Piloten

Nachdem die Betrachtungen der Flugfunktion abgeschlossen ist, steht noch die Betrachtung der Mitigations an. Dieser Abschnitt beschäftigt sich mit der Betrachtung der Mitigations des Funktionssets. Im Rahmen des Funktionssets ist nur die Umsetzung des akustischen Signalgebers als Mitigation möglich.

Der akustische Signalgeber stellt als Ziel der Wirkkette dar und soll automatisch im Fehlerfall auslösen oder manuell vom Piloten ausgelöst werden. Wobei die Analyse des manuellen und des automatischen Auslösens in zwei Abschnitte aufgeteilt wird, um eine übersichtlichere Betrachtung zu ermöglichen. Die Analyse beginnt zuerst mit dem Auslösen durch den Piloten und betrachtet dann im nächsten Abschnitt das automatische Auslösen.

Der akustische Signalgeber ist im Sicherheitsmodul SA lokalisiert, welches in der Abbildung 4.8 dargestellt ist. Das Sicherheitsmodul besteht dabei aus der Signalüberwachung SUE und

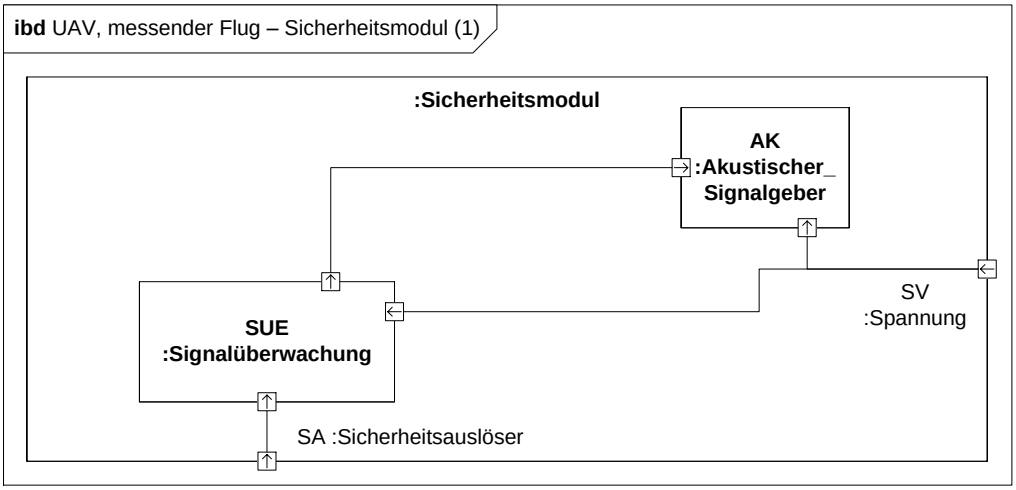

Abbildung 4.8: UAV, messender Flug - Sicherheitsmodul (1).

dem akustischen Signalgeber AK. Dabei erhält die Signalüberwachung SUE ein Signal aus dem Steuerungsmodul SM, welches den akustischen Signalgeber auslöst. Dabei reagiert die Signalüberwachung sowohl auf auslösende Signale, als auch auf einen Verbindungsabbruch. Damit muss die Verbindung des Sicherheitsauslösers SA über ein Verfahren arbeiten, welches ein auslösendes Signal senden kann aber auch einen Ausfall signalisiert. Dies kann über ein elektrisches Signal geschehene, welches einen permanenten, hohen Pegel hat, welcher beim Auslösen oder beim Ausfall nach unten gezogen wird, ähnlich wie bei einer NOT-AUS-Einrichtung. Alternativ kann ein periodisches Signal eingesetzt werden, welches von der Überwachung ausgewertet wird und beim Ausfall detektiert werden kann.

Akustischer Signalgeber

Versucht man die Abhängigkeiten für das Auslösen durch den Piloten in einer Formel darzustellen, so wird von dem Ziel erneut ausgegangen um die Formel zu bilden. So wird in diesem Fall von dem akustischen Signalgeber ausgegangen. Für den Signalgeber kann man dann die Formel 4.15 erstellen, in der der akustische Signalgeber als Signalgeber aufgelistet

wird, welcher aufgrund von internen Fehlern ausfallen kann. Bei der Formel steht der Index klein S für die Sicherheitsfunktion und der Index klein P für das Auslösen durch den Piloten.

$$SUE_{\mathrm{s,\,p}} \wedge Signalgeber \wedge SV_{\mathrm{s,\,p}} \Rightarrow AK_{\mathrm{s,\,p}} \tag{4.15}$$

Signalüberwachung

Ausgehend von der Formel 4.15 wird die Spannungsversorgung SV nicht betrachtet. Jedoch wird das neue Element der Signalüberwachung weiter betrachtet. Während die Funktion zuvor schon beschrieben wurde, so ergeben sich die Abhängigkeiten der Formel 4.16.

$$SM_{\mathrm{s,\,p}} \wedge Signalueberwachung \wedge SV_{\mathrm{s,\,p}} \Rightarrow SUE_{\mathrm{s,\,p}} \tag{4.16}$$

In dieser Formel vertritt die Signalüberwachung ihre Ausfallmöglichkeit. Zusätzlich ist der Block von der Spannungsversorgung SV und dem Steuerungsmodul SM abhängig, über welches die Überwachung das auslösende Signal bekommt.

Steuerungsmodul

Das Steuerungsmodul, welches in der Abbildung 4.5 beschrieben wird, erfüllt für die Mitigations eine neue Funktion und hat damit neue Abhängigkeiten. In der Abbildung wird der Signalauswerter SAW aufgelistet, welcher die Steuerdaten RCE_D empfängt. Dieser Block leitet ein Signal an das Sicherheitsmodul weiter und sendet somit einen Auslöseauftrag an die Mitigation. Es kann ein Auslösesignal empfangen und auswerten, sowie einen Verbindungsabbruch feststellen. Durch die Wirkkette, die in der Abbildung dargestellt wird ergibt sich die Formel 4.17 für die Funktion des Steuerungsmoduls SM.

$$K_{\mathrm{s,\,p}} \wedge Signalauswerter_{\mathrm{s,\,p}} \wedge SV_{\mathrm{s,\,p}} \Rightarrow SM_{\mathrm{s,\,p}} \tag{4.17}$$

Im Rahmen der Formel muss das Kommunikationsmodul Steuerdaten zur Verfügung stellen, der Signalauswerter muss funktionieren und die Spannungsversorgung muss eine Spannung zur Verfügung stellten.

Kommunikation

Ausgehend vom Steuerungsmodul SM muss das Kommunikationsmodul K betrachtet werden. Das in Abbildung 4.6 beschriebene Modul verfügt dabei über die gleichen Abhängigkeiten, wie für den Flug und stellt damit die Formel 4.18 zur Verfügung.

$$RCE_{\mathrm{s,\,p}} \wedge RC\_D_{\mathrm{s,\,p}} \wedge SV_{\mathrm{s,\,p}} \Rightarrow K_{\mathrm{s,\,p}} \tag{4.18}$$

Zusammenfassung und Fazit

Wie auch schon bei der Flugfunktion zuvor lassen sich nun die Abhängigkeiten zu einer übergreifenden Formel zusammenfassen. So kommt man durch sukzessives Einsetzen auf die Formel 4.19, welche die Abhängigkeiten enthält. Daraus lässt sich direkt die gekürzte Formel 4.20 erstellen.

$$\begin{aligned}&(((RCE_{\mathrm{s,\,p}} \wedge RC\_D_{\mathrm{s,\,p}} \wedge SV_{\mathrm{s,\,p}}) \wedge Signalauswerter_{\mathrm{s,\,p}} \wedge SV_{\mathrm{s,\,p}})\\ &\wedge Signalueberwachung \wedge SV_{\mathrm{s,\,p}}) \wedge Signalgeber \wedge SV_{\mathrm{s,\,p}} \Rightarrow AK_{\mathrm{s,\,p}}\end{aligned} \tag{4.19}$$

$$\begin{aligned}&RCE_{\mathrm{s,\,p}} \wedge RC\_D_{\mathrm{s,\,p}} \wedge Signalauswerter_{\mathrm{s,\,p}}\\ &\wedge Signalueberwachung \wedge Signalgeber \wedge SV_{\mathrm{s,\,p}} \Rightarrow AK_{\mathrm{s,\,p}}\end{aligned} \tag{4.20}$$

Vergleicht man diese Formel mit der Formel für den Flug 4.21, so fällt einem auf, dass ähnliche Abhängigkeiten zwischen den Formeln bestehen.

$$RCE_{\mathrm{f}} \wedge RC\_D_{\mathrm{f}} \wedge SV_{\mathrm{f}} \wedge Aktoren_{\mathrm{f}} \Rightarrow A_{\mathrm{f}} \tag{4.21}$$

So müssen die Elemente RCE, RC_D und SV für beide Funktionen ordnungsgemäß operieren. Man kann nun überprüfen inwiefern Maßnahmen auf Basis von Redundanzen anwendbar sind. Dabei bietet es sich an zu betrachten inwieweit man die Spannungsversorgungen separieren kann. Die Aktoren benötigen zwar eine starke Spannungsversorgung, die nur abstrakt betrachtet werden kann, jedoch kann der akustische Signalgeber mit einer eigenen Spannungsversorgung ausgestattet werden. Dies wird in der Praxis auch gemacht, da diese für

die Überwachung der Spannungsversorgung eingesetzt werden und bei einem Ausfall der Spannungsversorgung auslösen ([21]).

$$\begin{aligned} &RCE_{\mathrm{s,\,p}} \wedge RC\_D_{\mathrm{s,\,p}} \wedge Signalauswerter_{\mathrm{s,\,p}} \\ &\wedge Signalueberwachung \wedge Signalgeber \\ &\wedge (SV_{\mathrm{s,\,p}} \vee N\_SV_{\mathrm{s,\,p}}) \Rightarrow AK_{\mathrm{s,\,p}} \end{aligned} \tag{4.22}$$

Die Formel 4.22 verfolgt dabei diesen Ansatz und wird mit der zusätzlichen Spannungsversorgung N_SV ausgestattet, welche mit allen Komponenten in der Kette als zusätzliche Spannungsversorgung verbunden ist. Dabei wird davon ausgegangen, dass alle Komponenten soweit abgesichert sind, dass der Strom nicht zu den nicht erwähnten Komponenten fließt und sich somit die Spannungsversorgung N_SV ruckartig über der Aktorik entlädt. Weiterhin wird Problematik des Wechsels von einer zur anderen Spannungsversorgung an dieser Stelle nicht betrachtet.

Vergleicht man nun die Formel 4.22 mit der Formel 4.21 für den Flug, so fällt auf, dass eine größere Schwachstelle durch Redundanzen teilweise aufgelöst wurde und der Pilot nach dem Ausfall der Spannungsversorgung SV weiterhin den akustischen Signalgeber einschalten kann. Jedoch ist der Ausfall der Spannungsversorgung SV ein schwerer Fehler, der zu einem Absturz des UAVs führen wird. Somit muss der akustische Signalgeber automatisch auslösen und ohne das explizite Auslösen durch den Pilot. Aus diesem Grund wird das Ergebnis insofern Verworfen, das eine Notfallspannungsversorgung an dieser Stelle nicht auf diese Art und Weise eingeplant wird.

Zusätzlich müssen die Elemente **Signalauswerter SAW** und die **Signalüberwachung SUE** betrachtet werden. Diese Elemente lassen sich noch keiner Komponente zuordnen. Es lässt sich jedoch sagen, dass diese Elemente eine wichtige Funktion für die Sicherheit erfüllen und daher bei einer Umsetzung auf eine konkrete Komponente sollte überprüft werden, inwiefern diese Komponente redundant aufgebaut werden kann. Ausgehend davon, dass der akutische Signalgeber nur ein einfaches elektrisches Signal basierend auf einem hohen Spannungspegel benötigt, wird an dieser Stelle kein aufwendiges Konstrukt benötigt. Das Voting-Element kann in dem Fall die Leitung zum Signalgeber sein und auf das Signal einer jeden physikalischen Komponente reagieren.

Der **akustische Signalgeber AK** hingegen lässt sich direkt einer physikalischen Kompo-

nente zuordnen und kann abhängig von der Bauform und den benötigten Platz redundant in das System eingebaut werden.

Abschließend kann man über das Auslösen des akustischen Signalgebers durch den Piloten sagen, dass der Aufbau durch den Einsatz von Redundanzen sich sicherer gestaltet lässt. Jedoch besteht weiterhin eine große Abhängigkeit zu der Spannungsversorgung SV. So führt ein Ausfall des Systems zum Ausfall der Funktion, die es dem Piloten ermöglicht die Mitigation zu aktivieren. In diesem Rahmen wird im nächsten Abschnitt betrachtet, wie das Sicherheitsmodul auf den Ausfall der restlichen Komponenten im System reagieren kann.

4.2.5 Automatisches auslösen der Mitigation

Basierend auf der Abbildung 4.8 und den zuvor beschriebenen Zusammenhängen wird nun betrachtet, inwiefern das System automatisch den akustischen Signalgeber für den Fall eines Fehlers auslösen kann.

Akustischer Signalgeber

Um das Auslösen zu betrachten wird erneut vom akustischen Signalgeber ausgegangen und eine Formel gebildet. Die Formel 4.23 beschreibt dabei die Zusammenhänge und arbeitet mit dem zweiten Index klein S für die Auslösung durch das System.

$$SUE_{\mathrm{s,\,s}} \wedge Signalgeber \wedge SV_{\mathrm{s,\,s}} \Rightarrow AK_{\mathrm{s,\,s}} \tag{4.23}$$

Signalüberwachung

Die Signalüberwachung SUE erfüllt dabei weiterhin die zuvor beschriebene Funktion. Fallen die Signale vom Piloten aus, so ist es zwar die Aufgabe des Steuerungsmoduls dies zu detektieren, jedoch löst die Signalüberwachung auf der Basis dieser Erkenntnis den Signalgeber aus. Damit hat sie die Abhängigkeiten der Formel 4.24.

$$SM_{\mathrm{s,\,s}} \wedge Signalueberwachung \wedge SV_{\mathrm{s,\,s}} \Rightarrow SUE_{\mathrm{s,\,s}} \tag{4.24}$$

Steuerungsmodul

Das Steuerungsmodul SM wertet die Steuersignale aus und löst im Fall von fehlenden neuen Signalen das Sicherheitsmodul aus. Dabei bestehen die in Kapitel 4.2.4 beschriebenen Abhängigkeiten und Verbindungen zwischen den Modulen. Folglich kann das Steuerungsmodul auch

intern Ausfallen und würde aufgrund dieses Fehlers die Signalüberwachung auslösen. Damit ergibt sich die Formel 4.25 für die Abhängigkeiten, in der der boolsche Wert true eingetragen ist, welcher ausdrücken soll, dass dieses Modul keine negative Abhängigkeit für die Funktion hat.

$$true \Rightarrow SM_{\mathrm{s,\,s}} \tag{4.25}$$

Dieser Zusammenhang lässt sich basierend auf den vorherigen Formeln leicht veranschaulichen. So fällt du den Ausfall der Funkverbindung RC_D automatisch der Empfänger RCE aus. Den Ausfall kann das Steuerungsmodul erkennen und entsprechend die Maßnahme auslösen. Fällt der Empfänger RCE aufgrund von internen Fehler aus, so kann dies wieder vom Steuerungsmodul erkannt werden. Fällt hingegen das Steuerungsmodul aus, so erhält das Sicherheitsmodul kein Signal mehr und erkennt dadurch den Ausfall. Auf Basis dieser Abhängigkeiten in einer Kette, bei der jeder Ausfall detektiert werden muss, ist das erkennen eines Fehlers kein Problem und das ganze Modul kann ausfallen.

Zusammenfassung und Fazit

Die neuen Formeln lassen sich erneut zu einer großen Formel 4.26 zusammenfassen, in der das true jedoch direkt raus gekürzt wird.

$$(Signalueberwachung \wedge SV_{\mathrm{s,\,s}}) \wedge Signalgeber \wedge SV_{\mathrm{s,\,s}} \Rightarrow AK_{\mathrm{s,\,s}} \tag{4.26}$$

Die Signalüberwachung und der Signalgeber wurden zuvor schon auf Redundanzen überprüft und mit ihren Abhängigkeiten beschrieben. Die Spannungsversorgung wurde auch schon betrachtet und der Ansatz mit einer redundanten Spannungsquelle für die manuelle Auslösung wurde dabei verworfen. Mit den Anforderungen an eine automatische Auslösen verändert sich jedoch die Situation und eine erneute Betrachtung wird für die neue Funktion notwendig. So ist das Ziel des akustischen Signalgebers auf Fehler im System zu reagieren, indem er sich auslöst. Das Ausfallen der Spannungsversorgung SV ist ein derartiger Fehler. Jedoch ist die Spannungsversorgung SV ein wesentliches Element in der Liste der Abhängigkeiten.

So wird der Ansatz mit der Notfallspannungsversorgung erneut aufgegriffen und es wird einen zusätzliche, redundante Spannungsversorgung an die Blocke der Formel 4.26 angeschlossen. Die Abbildung 4.9 zeigt dieses neue Element mit der Bezeichnung N_SV, welches vom Typ Spannungsversorgung ist und nur mit der Signalüberwachung SUE und dem akustischen Signalgeber AK verbunden ist. Dabei müssen die Blöcke so gebaut werden, dass der Strom

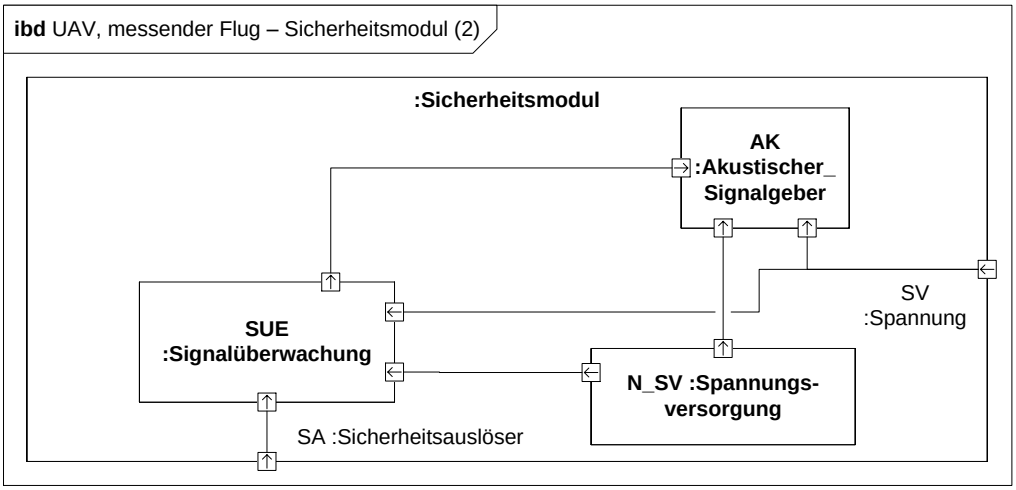

Abbildung 4.9: UAV, messender Flug - Sicherheitsmodul (2).

nicht von der N_SV zurück zur regulären Spannungsversorgung SV fließen kann. Es wird zusätzlich davon ausgegangen, dass die Elemente regulär auf die Spannungsversorgung SV zugreifen und bei einem Ausfall direkt ohne Komplikationen zu der Spannungsversorgung N_SV wechseln.

Bei reellen Komponenten muss davon ausgegangen werden, dass der Wechsel nicht fehlerfrei geschieht oder das die Komponenten kurzzeitig einen Spannungsverlust oder andere Komplikationen haben. Verwendet man keine Steuerung zum Umschalten der Spannungsquellen und schließt beide Quellen direkt an der Komponente an, so kann es geschehen, dass die Komponente nur auf die Ersatzspannungsversorgung N_SV zugreift und diese zum Fehlerzeitpunkt leer ist.

$$Signalueberwachung \wedge Signalgeber \wedge (SV_{\mathrm{s,\,s}} \vee N\_SV_{\mathrm{s,\,s}}) \Rightarrow AK_{\mathrm{s,\,s}} \tag{4.27}$$

Basierend auf diesem Ansatz ergibt sich die neue Formel 4.27, welche es ermöglicht den Fehlerfall der ausgefallenen Spannungsversorgung SV abzufangen und somit die beschriebene Anforderung an die Funktionalität des akustischen Signalgebers erfüllt.

Abschließend lässt sich über das automatische Auslösen des akustischen Signalgebers sagen,

dass die Architektur in diesem Rahmen zwangsläufig um ein zusätzliches Element erweitert werden muss. Ohne die zusätzliche Spannungsversorgung ist die Mitigation nicht in der Lage auf einen einzelnen Fehler zu reagieren, wenn dieser der Ausfall der Hauptspannungsversorgung SV ist. Folglich muss die zusätzliche Spannungsversorgung in die spätere Architektur übernommen werden.

4.3 Begrenzende Steuerung

Die begrenzende Steuerung wird in einem neuen Funktionsset angewandt. Dieses Funktionsset

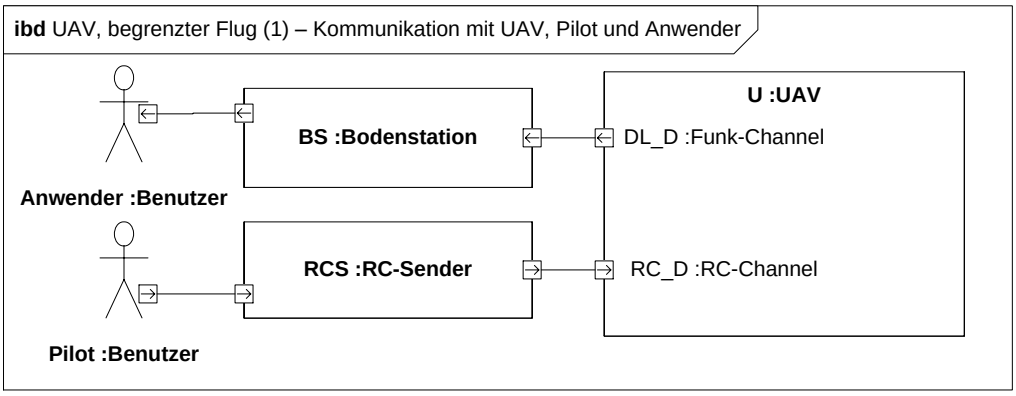

Abbildung 4.10: UAV, begrenzter Flug (1) – Kommunikation mit UAV, Pilot und Anwender.

baut auf den Entwicklungen aus dem Kapitel 4.2 auf und fügt den Flugmodi des begrenzten Fliegens aus dem Kapitel 3.1.2 hinzu. Dabei bleibt der Aufbau bezüglich der Kommunikation zwischen Anwender, Piloten und UAV der gleiche. Die Abbildung 4.10 stellt diesen Sachstand dar.

4.3.1 Fliegen des UAVs

Wie schon zuvor in Kapitel 4.2.1, wird in diesem Kapitel betrachtet, welche Bedingungen für den Flug benötigt werden. Dabei wird eine neue Architektur als Grundlage verwendet, welche auf der Architektur aus Kapitel 4.2 aufbaut. Die Abbildung 4.11 zeigt dabei die Struktur auf der oberen Ebene. Im Vergleich mit der alten Architektur stell man fest, dass auf dieser Ebene aktuell noch keine Änderungen vorliegen. Jedoch muss eine erneute Analyse durchgeführt werden. Diese beginnt erneut bei der Aktorik. Dabei werden zwei Flugmodi betrachtet. Einmal wird der alte Flugmodus des messenden Flugs betrachtet und zusätzlich der Modus mit der begrenzten Flugsteuerung. Um einen unterschied in den Abhängigkeiten darzustellen werden die Formeln, die sich mit dem messenden Flug beschäftigen mit dem Index klein M versehen und die Formeln, die den Flug mit einer begrenzten Flugsteuerung als Modus beschreiben mit dem Buchstaben klein B. Generell werden die Formeln mit den Index klein F für den Flugmodus markiert.

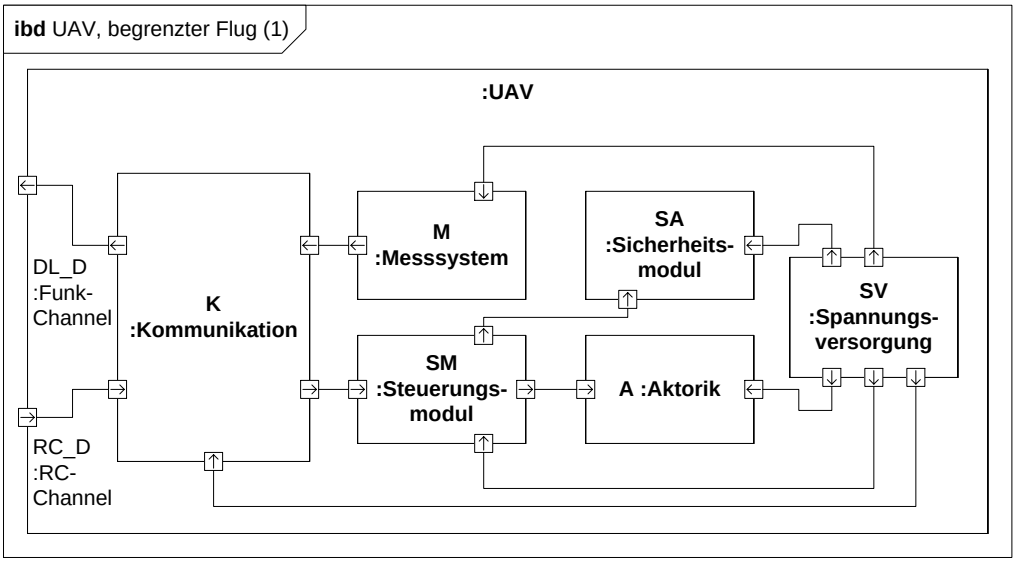

Abbildung 4.11: UAV, begrenzter Flug (1).

Der Flugmodus des messenden Fluges wird erneut betrachtet um Unterschiede und dadurch neue Einflüsse zu betrachten. Aus diesem Grund startet die Analyse erneut bei der Aktorik und arbeitet sich dann erneut in alle Richtungen vor. Bleiben Elemente unverändert, so bleibt die alte Beschreibung gültig.

Aktorik

Die Aktorik hat sich in diesem Schritt nicht verändert. Daraus resultieren weiterhin gleich bleibende Abhängigkeiten, die die Formel 4.28 bilden. Zusätzlich wird die Formel 4.29 gebildet, welche die gleichen Eigenschaften für den begrenzten Flug darstellt.

$$SM_{\text{f, m}} \wedge SV_{\text{f, m}} \wedge Aktoren_{\text{f, m}} \Rightarrow A_{\text{f, m}} \tag{4.28}$$

$$SM_{\text{f, b}} \wedge SV_{\text{f, b}} \wedge Aktoren_{\text{f, b}} \Rightarrow A_{\text{f, b}} \tag{4.29}$$

Spannungsversorgung

Die Spannungsversorgung SV wird weiterhin nicht genauer betrachtet. Da sie auch keine Elemente für die Formeln beiträgt, wird sie in den nächsten Abschnitten nicht mehr zusätzlich aufgelistet.

Steuerungsmodul

Das Steuerungsmodul erfährt in diesem Schritt eine wesentliche Erweiterung. So wurde es um einen Begrenzer BG und einen Schalter SW erweitert. Die Abbildung 4.12 zeigt diese Erweiterung. Der Schalter SW hat die Aufgabe, die ausgewählten Steuerdaten an das nächste

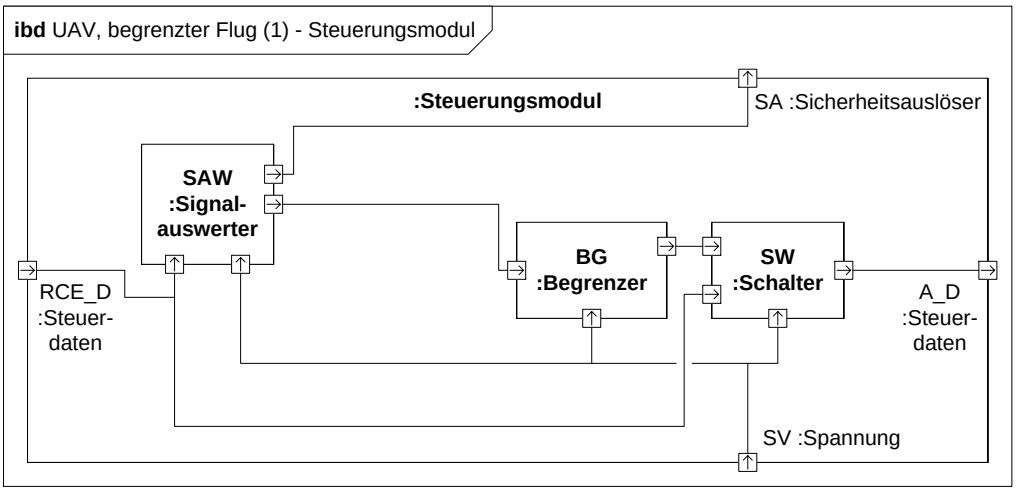

Abbildung 4.12: UAV, begrenzter Flug (1) - Steuerungsmodul.

Element in der Kette weiterzuleiten. Dabei muss er von dem vorrangigen Steuersignalen eine Quelle vorgegeben bekommen und dieses Steuersignal von der ausgewählten Quelle sicher weiterleiten. Welches Steuersignal dabei das vorrangige sein soll muss in dem Signal kodiert sein. Im Fall von SW muss das Steuersignal direkt vom Piloten vorgegeben werden, wenn es dominant ist. Aus diesem Grund müssen die eingehenden Steuerdaten RCE_D dominant sein. Damit SW die Steuerdaten A_D für die Aktorik zur Verfügung stellen kann, müssen folglich die Abhängigkeiten der Formel 4.30 erfüllt sein.

$$RCE\_D_{\mathrm{f,\,m}} \wedge SV_{\mathrm{f,\,m}} \Rightarrow SW_{\mathrm{f,\,m}} \tag{4.30}$$

Der Schalter SW muss dabei sicher gegen störende Einflüsse des Begrenzers sein. Darüber hinaus ergibt sich dann die Formel 4.31 für die Funktion des messenden Fluges für das Steuerungsmoduls.

$$K_{\mathrm{f,\,m}} \wedge SV_{\mathrm{f,\,m}} \wedge SW_{\mathrm{f,\,m}} \Rightarrow SM_{\mathrm{f,\,m}} \tag{4.31}$$

Um die Formel für den begrenzten Flug aufzustellen müssen die weiteren Elemente in dem Modul betrachtet werden. So müssen die Steuerdaten im begrenzten Flugmodus über das Begrenzer-Element BG geleitet werden. Dabei muss der Begrenzer Steuerdaten aufnehmen, auf einen maximal zulässigen Wert begrenzen und dann erneut in Steuerdaten für die Aktorik umsetzen.

Für die Steuersignale wird in Modellflugzeugen Pulsweitenmodulation eingesetzt, welche mit der Abkürzung PWM des englischen Begriffes Pulse-width modulation bezeichnet werden. Diese Signale müssen für den Begrenzer erst aufgenommen und in einen Zahlenwert umgesetzt werden, den der Begrenzer mit Computeroperationen auswerten kann. Erst dann kann der Begrenzer die Werte begrenzen. Danach muss er die Werte zurück in PWM-Signale umsetzen. Die Hintergründe für das Aufzeichnen und Herstellen von neuen PWM-Signalen werden in den Projektdokumenten [23] und [24] beschrieben.

Ausgehend von dieser Situation wird der Signalauswerter SAW für das Einlesen der PWM-Signale verwendet. Dieser Block hat schon vorher die Aufgabe bekommen um die Signale für den akustischen Signalgeber auszuwerten. Die Erzeugung neuer PWM-Signale wird hingegen als Teil des Begrenzerblocks angesehen.

$$K_{\mathrm{f,\,b}} \wedge SV_{\mathrm{f,\,b}} \wedge SAW_{\mathrm{f,\,b}} \wedge BG_{\mathrm{f,\,b}} \wedge SW_{\mathrm{f,\,b}} \Rightarrow SM_{\mathrm{f,\,b}} \tag{4.32}$$

Als Ergebnis dieser Betrachtung steht am Ende die Formel 4.32 für die Funktion des begrenzten Fluges im Steuerungsmodul SM.

Kommunikation

Die Abbildung 4.13 zeigt den Aufbau des Kommunikationsblocks K. Dabei hat sich der Aufbau des Blocks zu der vorherigen Version aus Kapitel 4.2.1 nicht verändert. So bleibt die Formel

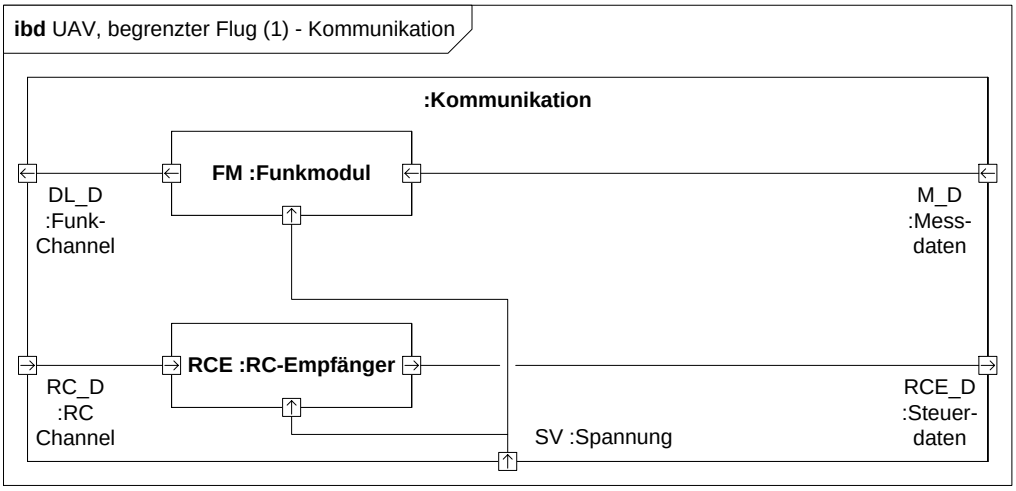

Abbildung 4.13: UAV, begrenzter Flug (1) - Kommunikation.

aus dem vorherigen Kapitel erhalten und wird mit der Formel 4.33 nur aus Übersichtlichkeit wiederholt. Zusätzlich wird die Formel 4.34 erstellt, welche den begrenzten Flug beschreibt.

$$RCE_{\mathrm{f,\,m}} \wedge RC\_D_{\mathrm{f,\,m}} \wedge SV_{\mathrm{f,\,m}} \Rightarrow K_{\mathrm{f,\,m}} \tag{4.33}$$

$$RCE_{\mathrm{f,\,b}} \wedge RC\_D_{\mathrm{f,\,b}} \wedge SV_{\mathrm{f,\,b}} \Rightarrow K_{\mathrm{f,\,b}} \tag{4.34}$$

4.3.2 Zusammenfassung und Analyse

Wie auch zuvor lassen sich die Formeln nun kombinieren um eine Übersicht zu gewinnen. So werden zuerst die Formeln für die Aktorik und das Steuerungsmodul kombiniert.

$$(K_{\mathrm{f,\,m}} \wedge SV_{\mathrm{f,\,m}} \wedge SW_{\mathrm{f,\,m}}) \wedge SV_{\mathrm{f,\,m}} \wedge Aktoren_{\mathrm{f,\,m}} \Rightarrow A_{\mathrm{f,\,m}} \tag{4.35}$$

$$(K_{\mathrm{f,\,b}} \wedge SV_{\mathrm{f,\,b}} \wedge SAW_{\mathrm{f,\,b}} \wedge BG_{\mathrm{f,\,b}} \wedge SW_{\mathrm{f,\,b}}) \wedge SV_{\mathrm{f,\,b}} \wedge Aktoren_{\mathrm{f,\,b}} \Rightarrow A_{\mathrm{f,\,b}} \tag{4.36}$$

Im zweiten Schritt werden dann die Formeln für das Kommunikationsmodul eingesetzt.

$$((RCE_{\text{f, m}} \wedge RC\_D_{\text{f, m}} \wedge SV_{\text{f, m}}) \\ \wedge SV_{\text{f, m}} \wedge SW_{\text{f, m}}) \wedge SV_{\text{f, m}} \wedge Aktoren_{\text{f, m}} \Rightarrow A_{\text{f, m}} \tag{4.37}$$

$$((RCE_{\text{f, b}} \wedge RC\_D_{\text{f, b}} \wedge SV_{\text{f, b}}) \wedge SV_{\text{f, b}} \wedge SAW_{\text{f, b}} \wedge BG_{\text{f, b}} \wedge SW_{\text{f, b}}) \\ \wedge SV_{\text{f, b}} \wedge Aktoren_{\text{f, b}} \Rightarrow A_{\text{f, b}} \tag{4.38}$$

Die daraus resultierenden Formeln 4.37 und 4.38 beschreiben dann die internen Abhängigkeiten im UAV.

Vergleicht man nun die Formel 4.37 mit der Formel 4.12 aus dem Kapitel 4.2.2, so fällt auf, dass bei gleicher Funktionalität eine zusätzliche Abhängigkeit hinzu gekommen ist.

Da zuvor bis auf den SW-Block alle Elemente auf Redundanzen geprüft wurden, wird an dieser Stelle nur der SW-Block noch einmal betrachtet.

Der Schalter SW ist kein Standardelement und muss daher selber in das System integriert werden. Um seine Arbeit zu bewältigen muss der Block sicher die Signalquelle auswählen können. Dieses Problem erzeugt eine gewisse Komplexität. Im Rahmen des HAW Projektes FAUST, würde diese Thematik schon einmal betrachtet. Für ein Modellfahrzeug sollte eine sichere Umschaltung von autonomen Computer zu einer Funkfernsteuerung entwickelt werden. Enrico Hensel beschrieb den Ansatz in seiner Bachelorarbeit ([25]) und entwickelte in diesem Rahmen ein Modul, welches mittels zwei CPLDs eine Auswahl erzeugt und welches dabei redundant ist.

Unter diesen Umständen sollte ein sicheres Modul verwendet werden, welches mindestens die Anforderungen des Moduls aus der Arbeit [25] erfüllt.

Die Betrachtung einer getrennten Spannungsversorgung für diese Modul wird verworfen, da gemäß der Formel für den Ausfall des Systems ein Ausfall von SV das komplette System ausfallen lassen würde. Hätte SW eine eigene Spannungsversorgung, so könnte SW weiterhin operieren. Jedoch hätte seine Arbeit keine Auswirkung auf das UAV und könnte somit keinen Absturz oder Kontrollverlust verhindern.

Weiterhin müssen noch die Abhängig für den begrenzten Flugmodus geprüft werden. Um dies zu erreichen werden zuerst die Formeln 4.37 und 4.38 mit einander verglichen. Dabei fällt auf, dass die Blöcke SAW und BG nicht beim messenden Flug betrachtet wurden und daher noch nicht analysiert wurden. Bei der Analyse der Funktionalität fällt auf, dass beide Blöcke später in einer Komponente kombiniert werden sollten, da sie einen direkten Arbeitsablauf von Digitalisierung, Auswertung und Umsetzung durchführen. Je nachdem sollte dann geprüft werden, inwiefern diese Komponente redundant aufgebaut werden kann. Zusätzlich sollte jedoch betrachtet werden, dass die Funktionalität ausfallen kann. So sollte bei einem Ausfall der Pilot informiert werden, damit dieser einen Modiwechsel durchführen kann.

Um den Ausfall zu detektieren kann eine Totmanneinrichtung ins System integriert werden, welche das System überwacht und versucht Fehler zu detektieren. Wird ein Fehler detektiert, so löst es den akustischen Signalgeber aus. In Abbildung 4.14 wird das erweiterte Sicherheitsmodul dargestellt. Dies Verfügt nun über den Block Totmanneinrichtungen TM.

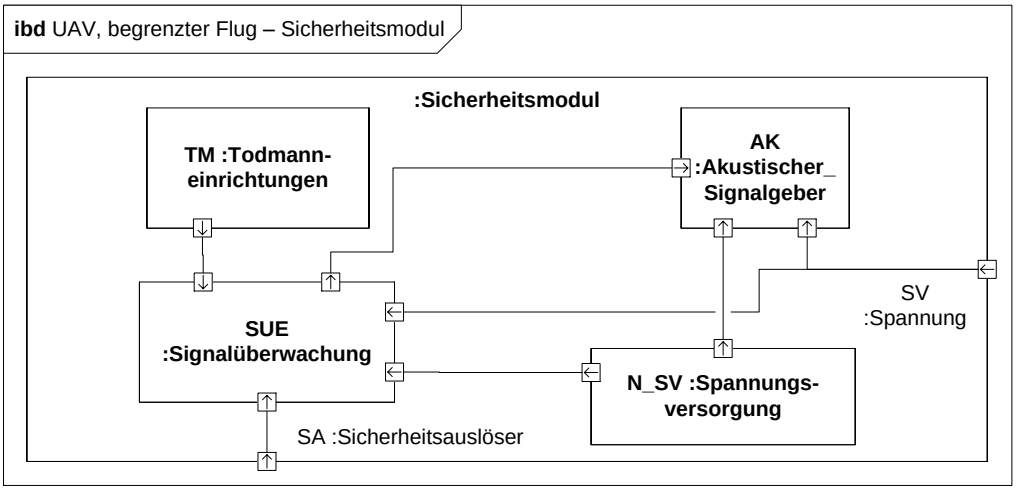

Abbildung 4.14: UAV, begrenzter Flug - Sicherheitsmodul.

Der Block symbolisiert die Verbindung zu den beteiligten Komponenten. Somit bestehen die Totmanneinrichtungen aus Zählern und den nicht dargestellten Verbindungen. Läuft eine der Totmanneinrichtungen ab, so löst diese ein Signal aus, welches die Signalüberwachung SUE anspricht und den akustischen Signalgeber auslöst.

Eine zusätzliche Erweiterung, die in Betracht gezogen werden kann, ist das Steuern des UAVs über eine weitere Funkverbindung. Dabei kann der Datenkanal zur Bodenstation in eine bidirektionale Verbindung umgebaut werden. Der Vorteil dieser Erweiterung ist, dass die Datenverbindung zur Bodenstation schon im Kommunikationsblock in digitale Daten umgesetzt wird. Zusätzlich kann die Kommunikation zur Bodenstation über einen andere Funkübertragungsgrundlage geschehen. So könnte beispielsweise ein GSM-Modul verwendet werden, welches Daten über das Mobilfunknetz überträgt und einen größeren Radius ermöglicht, als eine Funkfernsteuerung für den Modellflugbereich.

Es ist an dieser Stelle zu bedenken, dass der Pilot mit der Funkfernsteuerung noch die Hauptverantwortung hat und seine Steuerung somit dominant sein muss. Jedoch bietet die zusätzliche Erweiterung auf ein weiteres Funksystem ein neues Maß an Sicherheit bezüglich der Übertragung. Die Abbildung 4.15 zeigt dabei die neue Konstellation in der Verbindungsübersicht. So

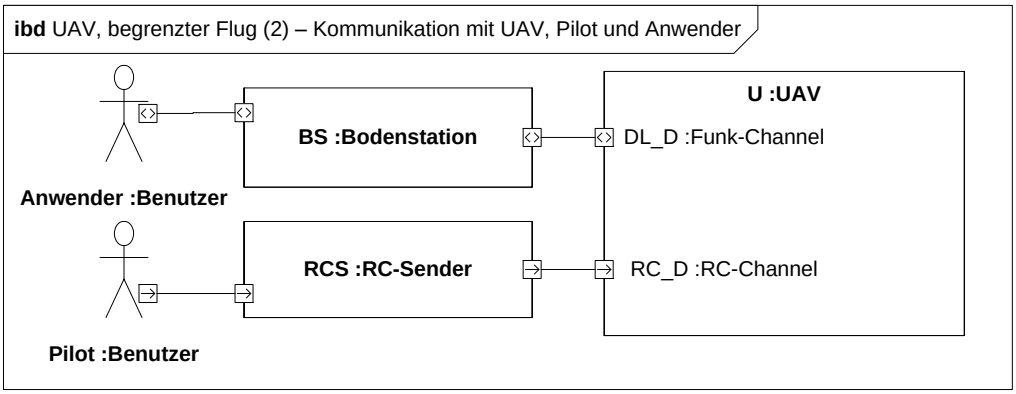

Abbildung 4.15: UAV, begrenzter Flug (2) – Kommunikation mit UAV, Pilot und Anwender.

können in der neuen Version sowohl Pilot, als auch Anwender Daten an das UAV senden und dieses somit steuern.

Der Kommunikationsblock des UAVs wird dabei mit einem neuen Datenausgang ausgestattet, welcher in der Abbildung 4.16 dargestellt wird. Dabei sendet der Kommunikationsblock mit dem Ausgang FM_D digitale Steuerdaten, welche nicht zuvor ausgewertet werden müssen.

Auf der obersten Architekturebene des UAV ergibt sich somit die neue Abbildung 4.17. Somit

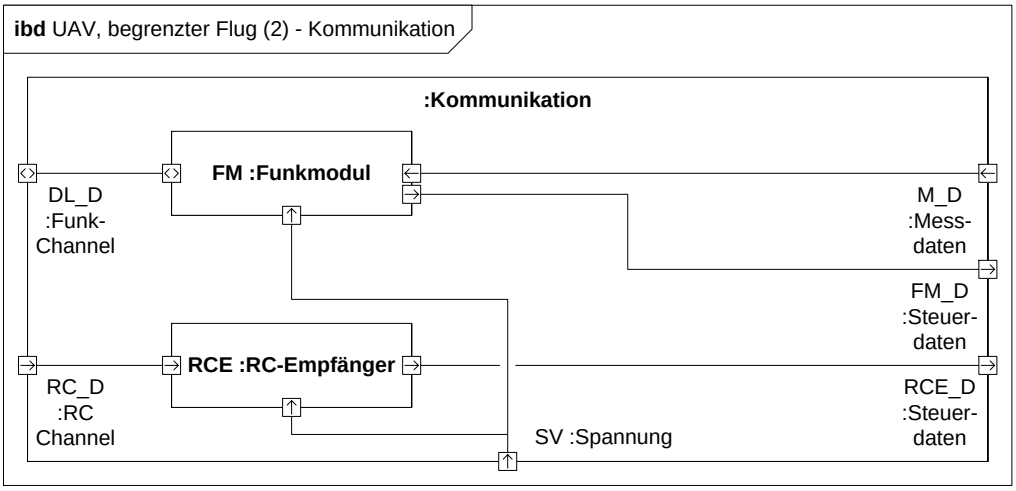

Abbildung 4.16: UAV, begrenzter Flug (2) - Kommunikation.

steht ein weiterer Kanal an das Steuerungsmodul zur Verfügung.

Die Abbildung 4.18 stellt das neue Steuerungsmodul dar. Im Rahmen des Moduls werden die Signale von der Signalauswertung SAW aufgenommen, bevor sie begrenzt werden und dann über den Schalter SW an die Aktorik geleitet werden. Dabei muss der Signalauswerter SAW intern die eingehenden Signale durchschalten können und auch wie ein Schalter funktionieren.

$$\begin{aligned}((RCE_{\text{f, b1}} \wedge RC\_D_{\text{f, b1}} \wedge SV_{\text{f, b}}) \wedge SV_{\text{f, b}} \wedge SAW_{\text{f, b1}} \wedge BG_{\text{f, b1}} \wedge SW_{\text{f, b1}}) \\ \wedge SV_{\text{f, b1}} \wedge Aktoren_{\text{f, b1}} \Rightarrow A_{\text{f, b1}}\end{aligned} \tag{4.39}$$

$$\begin{aligned}(((RCE_{\text{f, b2}} \wedge RC\_D_{\text{f, b2}} \wedge SV_{\text{f, b2}}) \vee (FM_{\text{f, b2}} \wedge DL\_D_{\text{f, b2}} \wedge SV_{\text{f, b2}})) \\ \wedge SV_{\text{f, b2}} \wedge SAW_{\text{f, b2}} \wedge BG_{\text{f, b2}} \wedge SW_{\text{f, b2}}) \\ \wedge SV_{\text{f, b2}} \wedge Aktoren_{\text{f, b2}} \Rightarrow A_{\text{f, b2}}\end{aligned} \tag{4.40}$$

Die Formel 4.40 stellt die neue Kombination dar, welche mit der alten Kombination aus Formel 4.39 verglichen werden kann. Bei der Betrachtung ist zu erkennen, dass ein wesentlicher Teil der Abhängigkeiten in eine neue Beziehung gerutscht ist und ein kompletter Kommunika-

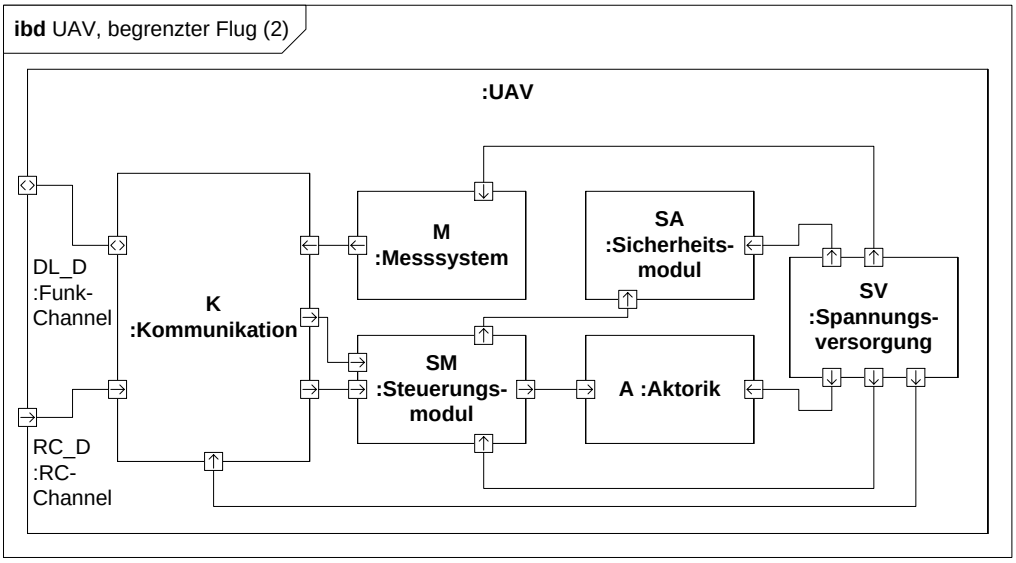

Abbildung 4.17: UAV, begrenzter Flug (2).

tionskanal ausfallen kann. Da jedoch die Abhängigkeiten zum Teil auf der Funkverbindung basieren, muss beachtet werden, dass beide Funkkanäle vor Ort zur Verfügung stehen müssen, damit der Vorteil der doppelten Kopplung zur Geltung kommen kann.

Weiterhin wurde der Aspekt der Security nicht beachtet. So muss dieser Aspekt bei einer konkreten Umsetzung analysiert werden, da beispielsweise eine Fernsteuerung über den zweiten Kanal IP-basiert sein kann und jemand über den Kanal das UAV gekapert kann, um einen Schaden anzurichten.

Zusätzlich muss aus formellen Gründen die Formel für den messenden Flugmodus erstellt werden. Dabei werden die Signalverläufe in der neuen Architektur erneut verfolgt. Ist dies ge-

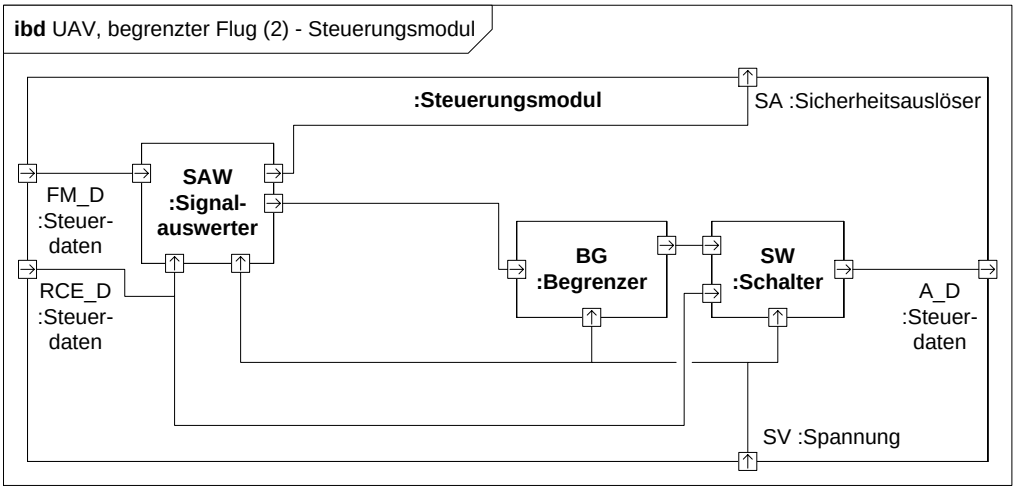

Abbildung 4.18: UAV, begrenzter Flug (2) - Steuerungsmodul.

schehen, so kann man die alte Formel 4.41 mit der dann neu erstellten Formel 4.42 vergleichen. Bei dem Vergleich fällt jedoch auf, dass sich die Zusammenhänge nicht geändert haben.

$$((RCE_{\text{f, m1}} \wedge RC\_D_{\text{f, m1}} \wedge SV_{\text{f, m1}}) \wedge SV_{\text{f, m1}} \wedge SW_{\text{f, m1}}) \wedge SV_{\text{f, m1}} \wedge Aktoren_{\text{f, m1}} \Rightarrow A_{\text{f, m1}} \tag{4.41}$$

$$((RCE_{\text{f, m2}} \wedge RC\_D_{\text{f, m2}} \wedge SV_{\text{f, m2}}) \wedge SV_{\text{f, m2}} \wedge SW_{\text{f, m2}}) \wedge SV_{\text{f, m2}} \wedge Aktoren_{\text{f, m2}} \Rightarrow A_{\text{f, m2}} \tag{4.42}$$

Dies liegt daran, dass beim messenden Flug die Signale über die Funkfernsteuerung des Piloten kommen müssen und er nur die eine Übertragungsart zur Verfügung hat.

4.3.3 Fazit bezüglich des Flugs

Die neue Architektur liefert einen möglichen Vorteil bezüglich der Reichweite. Jedoch erfüllt die Architektur nicht die Basissicherheit für den messenden Flug. So kommt das zusätzliche Element des Schalters SW in die Wirkkette, welches für den Flugmodus keine notwendige Funktion erfüllt, jedoch eine neue Schwachstelle in die Wirkkette hinzufügt. Zwar lässt sich durch den Einsatz von Redundanzen diese Schwachstelle absichern, doch hat auch die redun-

dante Lösung nicht die Sicherheit einer einfachen Leitung.

Der begrenzte Flugmodus kann aufgrund seiner Definition nicht als Basissicherheit dienen. Dadurch, dass die Steuersignale verarbeitet werden müssen, kann nur der messende Flug bezüglich der Basissicherheit betrachtet werden. Der begrenzte Flugmodus bietet dafür aber interessante Perspektiven bezüglich der Ausfallsicherheit an. So können die Elemente im Steuerungsmodul SM redundant aufgebaut werden, mit einer Totmanneinrichtung kann der Ausfall der Elemente detektiert werden und es kann ein zweiter Weg für die Übertragung der Steuerdaten verwendet werden. Somit kann dieser Flugmodus mit der aktuellen Architektur unter Umständen selbst dann operieren, wenn das System mit dem ersten Funktionsset ausfallen würde. Jedoch ist dies stark von den verwendeten Komponenten abhängig und bei der Betrachtung wurde auch nicht analysiert, wie sich der Ausfall beider logischer Komponenten oder des Voters auf das System auswirkt.

4.3.4 Mitigations

Als letzte Betrachtung für das Funktionsset steht noch die Betrachtung der Mitigations an. Während bei der Analyse im letzten Funktionsset beide Auslösewege aus Übersichtlichkeitsgründen getrennt betrachtet wurden, so findet in diesem Abschnitt eine gemeinsame Betrachtung statt. Dies hat den Grund, dass die Details und Hintergründe der Maßnahmen zuvor komplett unbekannt waren. In diesem Abschnitt sind die Hintergründe und Zusammenhänge jedoch bekannt und müssen nur noch mit der aktuellen Architektur überprüft werden. In diesen Rahmen werden erneut Formeln gebildet, bei denen der Index klein S für die Mitigation akustischer Signalgeber steht und die Indexe klein P und klein S für jeweils das manuelle Auslösen vom Boden und das autonome Auslösen durch das System.

Ausgegangen wird bei der Analyse beim akustischen Signalgeber AK im Sicherheitsmodul SA. Die Abbildung 4.14 zeigt das aktuelle Sicherheitsmodul, welches im vorherigen Abschnitt aktualisiert wurde. In dem Rahmen wird ausgehend von dem akustischen Signalgeber AK die Analyse gestartet.

Akustischer Signalgeber

Wie zuvor beschrieben ist der Aufbau des akustischen Signalgebers mit den folgenden Abhängigkeiten versehen, die mit den Formeln 4.43 und 4.44 beschrieben werden.

$$SUE_{\mathrm{s,\,p}} \wedge Signalgeber \wedge (SV_{\mathrm{s,\,p}}\ lorN\_SV_{\mathrm{s,\,p}}) \Rightarrow AK_{\mathrm{s,\,p}} \tag{4.43}$$

$$SUE_{\mathrm{s,\,s}} \wedge Signalgeber \wedge (SV_{\mathrm{s,\,s}} \vee N\_SV_{\mathrm{s,\,s}}) \Rightarrow AK_{\mathrm{s,\,s}} \tag{4.44}$$

Signalüberwachung

Für das Auslösen durch den Piloten bleiben die Abhängigkeiten gleich und so wird die Formel 4.45 gebildet. Bezüglich des Auslösen durch das System ändern sich sich die Abhängigkeiten. So entsteht die neue Abhängigkeit zu den Totmanneinrichtungen TM. Diese neuen Abhängigkeiten werden in der Formel 4.46 dargestellt.

$$SM_{\mathrm{s,\,p}} \wedge Signalueberwachung \wedge (SV_{\mathrm{s,\,p}}\ lorN\_SV_{\mathrm{s,\,p}}) \Rightarrow SUE_{\mathrm{s,\,p}} \tag{4.45}$$

$$TM_{\mathrm{s,\,s}} \wedge SM_{\mathrm{s,\,s}} \wedge Signalueberwachung \wedge (SV_{\mathrm{s,\,s}}\ lorN\_SV_{\mathrm{s,\,s}}) \Rightarrow SUE_{\mathrm{s,\,s}} \tag{4.46}$$

Totmanneinrichtungen

Die im vorherigen Abschnitt beschriebenen Totmanneinrichtungen gehören zu den jeweiligen Komponenten, die in die Steuerung eingreifen. Fällt eine Komponente aus, so sendet sie kein Signal mehr an die Signalüberwachung. Daraufhin wird der Fehler detektiert. Aus diesem Grund wird davon ausgegangen, dass die Totmanneinrichtung ausfallen kann und muss, damit die Funktion automatisch ausgelöst werden kann. Somit besteht die beschreibende Formel 4.47 nur aus einem true.

$$true \Rightarrow TM_{\mathrm{s,\,s}} \tag{4.47}$$

Steuerungsmodul

Für das automatische Auslösen durch das System haben sich die Anforderungen nicht geändert. So löst in diesem Zusammenhang das System automatisch aus und bildet somit keine direkte Abhängigkeit, was in der Formel 4.49 mit einem true beschrieben wird.

Beim manuellen Auslösen kommt der zweite Weg über den Anwender hinzu. Ebenso wie bei der Steuerung über den begrenzten Flugmodus, kann die Ansteuerung des akustischen

Signalgebers über den zweiten Kanal angesprochen werden. So kann der Signalauswerter SAW Auslösesignale von beiden Eingängen empfangen, auswerten und weiterleiten.

$$(RCE\_D_{\mathrm{s,\,p}} \vee FM\_D_{\mathrm{s,\,p}}) \wedge Signalauswerter_{\mathrm{s,\,p}} \wedge SV_{\mathrm{s,\,p}} \Rightarrow SM_{\mathrm{s,\,p}} \tag{4.48}$$

$$true \Rightarrow SM_{\mathrm{s,\,s}} \tag{4.49}$$

Kommunikation

Im Kommunikationsmodul K ergeben sich für beide Signale die folgenden Formeln, welche äquivalent zu den Formeln für das begrenzte Fliegen sind.

$$RCE_{\mathrm{s,\,p}} \wedge RC\_D_{\mathrm{s,\,p}} \wedge SV_{\mathrm{s,\,p}} \Rightarrow RCE\_D_{\mathrm{s,\,p}} \tag{4.50}$$

$$FM_{\mathrm{s,\,p}} \wedge DL\_D_{\mathrm{s,\,p}} \wedge SV_{\mathrm{s,\,p}} \Rightarrow FM\_D_{\mathrm{s,\,p}} \tag{4.51}$$

Zusammenfassung und Fazit

Abschließend lassen sich die Formeln erneut zusammenfassen. So lassen sich die Formeln 4.43 und 4.45 zu der Formel 4.52 für das manuelle Auslösen zusammenfassen. Ebenso lassen sich die Formeln 4.44 und 4.46 für das automatische Auslösen zu der Formel 4.53 zusammenfassen.

$$\begin{aligned}&(SM_{\mathrm{s,\,p}} \wedge Signalueberwachung \wedge (SV_{\mathrm{s,\,p}} \wedge N\_SV_{\mathrm{s,\,p}}))\\ &\wedge Signalgeber \wedge (SV_{\mathrm{s,\,p}} \vee N\_SV_{\mathrm{s,\,p}}) \Rightarrow AK_{\mathrm{s,\,p}}\end{aligned} \tag{4.52}$$

$$\begin{aligned}&(TM_{\mathrm{s,\,s}} \wedge SM_{\mathrm{s,\,s}} \wedge Signalueberwachung \wedge (SV_{\mathrm{s,\,s}} \vee N\_SV_{\mathrm{s,\,s}}))\\ &\wedge Signalgeber \wedge (SV_{\mathrm{s,\,s}} \wedge N\_SV_{\mathrm{s,\,s}}) \Rightarrow AK_{\mathrm{s,\,s}}\end{aligned} \tag{4.53}$$

Die Formel 4.53 lässt sich dabei direkt mit der Formel 4.47 erweitern. Zwar besteht die Erweiterung nur aus der Erweiterung true, doch wird diese aus Vollständigkeitsgründen in die Formel übernommen.

$$\begin{aligned}&(true \wedge SM_{\mathrm{s,\,s}} \wedge Signalueberwachung \wedge (SV_{\mathrm{s,\,s}} \vee N\_SV_{\mathrm{s,\,s}}))\\ &\wedge Signalgeber \wedge (SV_{\mathrm{s,\,s}} \wedge N\_SV_{\mathrm{s,\,s}}) \Rightarrow AK_{\mathrm{s,\,s}}\end{aligned} \tag{4.54}$$

Darauf aufbauend lassen sich die letzten Formeln für beide Auslösemodi mit den Formeln 4.48 und 4.49 erweitern, welche die Abhängigkeiten für das Steuerungsmodul SM hinzufügen.

$$\begin{aligned}(((RCE\_D_{\mathrm{s,\,p}} \vee FM\_D_{\mathrm{s,\,p}}) \wedge Signalauswerter_{\mathrm{s,\,p}} \\ \wedge SV_{\mathrm{s,\,p}}) \wedge Signalueberwachung \wedge (SV_{\mathrm{s,\,p}} \wedge N\_SV_{\mathrm{s,\,p}})) \\ \wedge Signalgeber \wedge (SV_{\mathrm{s,\,p}} \vee N\_SV_{\mathrm{s,\,p}}) \Rightarrow AK_{\mathrm{s,\,p}}\end{aligned} \tag{4.55}$$

$$\begin{aligned}(true \wedge true \wedge Signalueberwachung \wedge (SV_{\mathrm{s,\,s}} \vee N\_SV_{\mathrm{s,\,s}})) \\ \wedge Signalgeber \wedge (SV_{\mathrm{s,\,s}} \wedge N\_SV_{\mathrm{s,\,s}}) \Rightarrow AK_{\mathrm{s,\,s}}\end{aligned} \tag{4.56}$$

Für das automatische Auslösen bildet somit die Formel 4.56 die abschließende Formel, welche nicht weiter erweitert werden muss. Zwar lässt sich die Formel noch weiter kürzen, jedoch enthält sie die gleichen Elemente, wie die Formel aus Kapitel 4.2.5. Damit ist der Stand des letzten Abschnittes noch aktuell und die Zusammenhänge werden nicht erneut betrachtet.

Die Formel 4.55 für das manuelle Auslösen muss jedoch noch erweitert werden. So muss sie noch mit den Formeln 4.50 und 4.51 erweitert werden.

$$\begin{aligned}((((RCE_{\mathrm{s,\,p}} \wedge RC\_D_{\mathrm{s,\,p}} \wedge SV_{\mathrm{s,\,p}}) \vee (FM_{\mathrm{s,\,p}} \wedge DL\_D_{\mathrm{s,\,p}} \wedge SV_{\mathrm{s,\,p}})) \\ \wedge Signalauswerter_{\mathrm{s,\,p}} \wedge SV_{\mathrm{s,\,p}}) \wedge Signalueberwachung \\ \wedge (SV_{\mathrm{s,\,p}} \wedge N\_SV_{\mathrm{s,\,p}})) \wedge Signalgeber \wedge (SV_{\mathrm{s,\,p}} \vee N\_SV_{\mathrm{s,\,p}}) \Rightarrow AK_{\mathrm{s,\,p}}\end{aligned} \tag{4.57}$$

Die Formel 4.57 stellt somit alle Zusammenhänge für das manuelle Auslösen des akustischen Signalgeber dar. Ausgehend von der Formel kann man die neuen Zusammenhänge die der Konstellation erkennen. So ist äquivalent zum begrenzten Flugmodus, der Auslöser über zwei Übertragungswege erreichbar. Somit gewinnt man eine zusätzliche Sicherheit beim Auslösen der Maßnahme durch das Bodenpersonal. Jedoch besteht weiterhin die in Kapitel 4.2.4 beschriebene Abhängigkeit für das manuelle Auslösen, bei der die zusätzliche Spannungsversorgung N_SV keine Auswirkung auf die Funktion hat. So könnte man N_SV aus der Formel raus kürzen um den Zusammenhang zu verdeutlicht.

Abschließend lassen sich die Abhängigkeiten des akustischen Signalgebers so zusammenfassen, dass sich für das automatische Auslösen die Abhängigkeiten nicht wesentlich verändern und dass das manuelle Auslösen eine zusätzliche Verbindung zum Boden bekommt, was eine zusätzliche Sicherheit in das System bringt.

4.4 Stabilisierende Flugsteuerung

Als dritte Erweiterung des Modellflugzeugs fungiert das Funktionsset der stabilisierten Flugsteuerung. Dabei wird das vorherige Funktionsset des begrenzten Flugmodus aus Kapitel 4.3 mit dem im Kapitel 3.1.3 beschriebenen stabilisierten Flugmodus erweitert. Die Abbildung

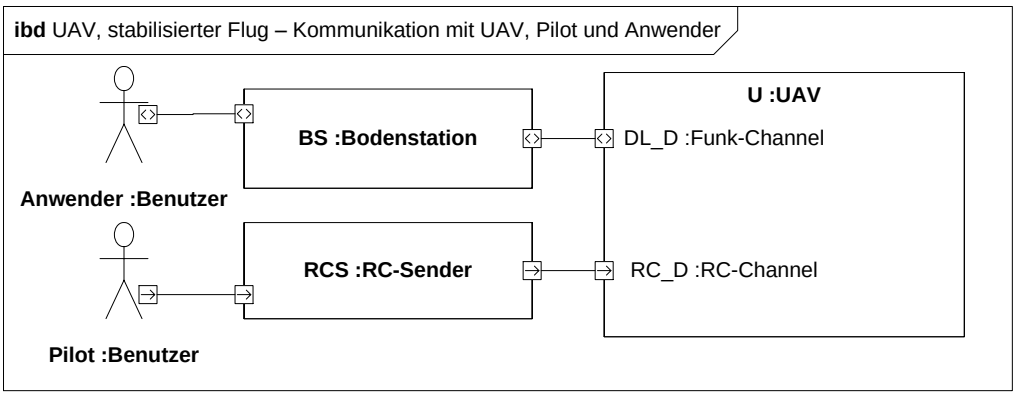

Abbildung 4.19: UAV, stabilisierter Flug – Kommunikation mit UAV, Pilot und Anwender.

4.19 stellt die Verbindungen zwischen den Systemen dar. Dabei wird der in Kapitel 3.1.3 beschriebene Punkt mit der Quelle der Steuerdaten weiterhin so gehandhabt, dass sowohl der Anwender, als auch der Pilot das UAV steuern können. Zusätzlich sollte beachtet werden, dass der Pilot und der Anwender die selbe Person sein können und der Pilot mittels einer weiteren Steuerung die Steuerdaten über die Bodenstation BS senden kann.

4.4.1 Fliegen des UAVs

Für die Analyse wird die Abbildung 4.20 verwendet. Die Architektur hat sich zu der letzten Version aus Kapitel 4.3 jedoch nicht verändert. So wird, wie bei den vorherigen Funktionssets die Analyse von dem Aktorik-Block A ausgegangen. Dabei steht der Index klein F wie zuvor für den Flug des UAVs. Die Indexe klein M, klein B und klein S stehen dabei für die Flugmodi messender, begrenzter und stabilisierter Flug.

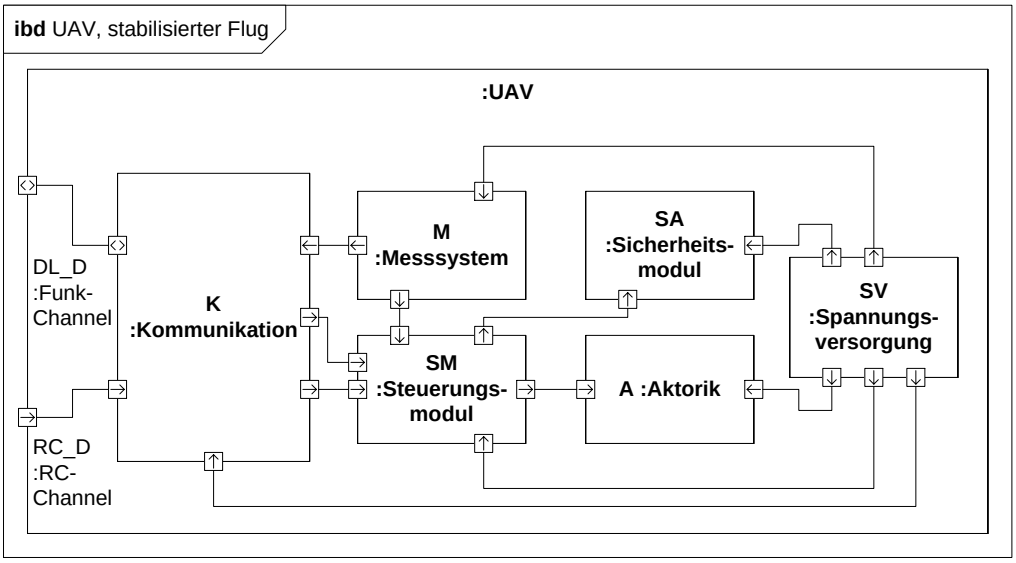

Abbildung 4.20: UAV, stabilisierter Flug.

Aktorik

Die Abhängigkeiten für den Aktorik-Block A bestehen wie bei den vorherigen Funktionssets und ergeben sich auch gleich für den stabilisierten Flugmodus.

$$SM_{\text{f, m}} \wedge SV_{\text{f, m}} \wedge Aktoren_{\text{f, m}} \Rightarrow A_{\text{f, m}} \tag{4.58}$$

$$SM_{\text{f, b}} \wedge SV_{\text{f, b}} \wedge Aktoren_{\text{f, b}} \Rightarrow A_{\text{f, b}} \tag{4.59}$$

$$SM_{\text{f, s}} \wedge SV_{\text{f, s}} \wedge Aktoren_{\text{f, s}} \Rightarrow A_{\text{f, s}} \tag{4.60}$$

Steuerungsmodul

Das Steuerungsmodul SM bildet erneut den Kern des steuernden Systems. Dabei bildet die Abbildung 4.21 erneut das Steuerungsmodul ab, welches die Aufgaben des Funktionssets bewältigt. In diesen Rahmen beschreibt die Formel 4.61 die Abhängigkeiten für den messenden Flugmodus.

$$K_{\text{f, m}} \wedge SV_{\text{f, m}} \wedge SW_{\text{f, m}} \Rightarrow SM_{\text{f, m}} \tag{4.61}$$

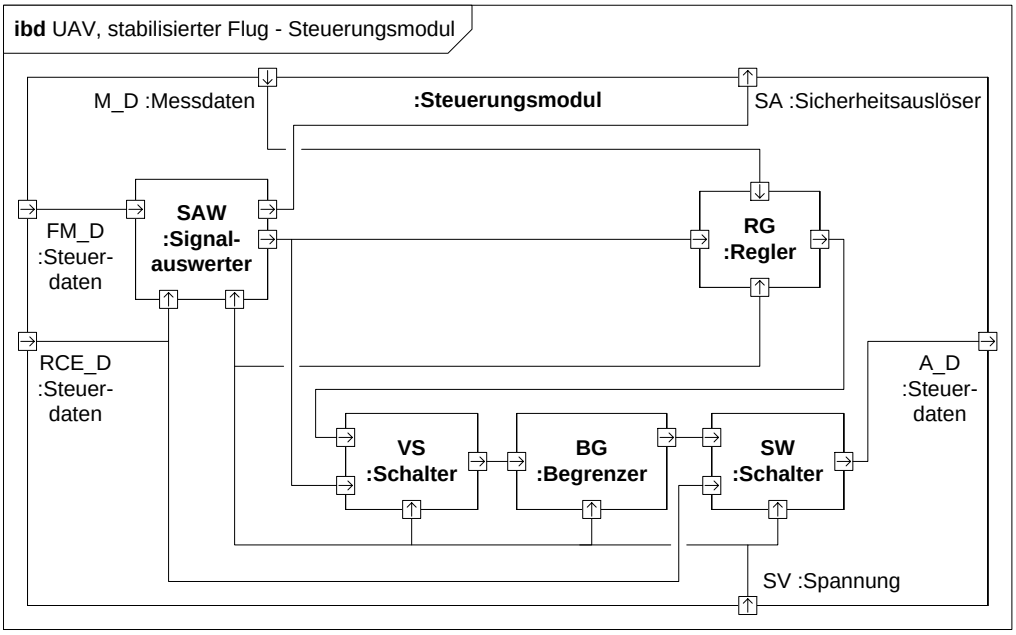

Abbildung 4.21: UAV, stabilisierter Flug - Steuerungsmodul.

So haben sich die Abhängigkeiten für den messenden Flug nicht verändert. Durch die sukzessive Erweiterungen mit den Funktionssets und der schrittweisen Erweiterung des Systems ändert sich der Aufbau der Architektur für ein Flugmodus nur beim Hinzufügen des nächsten Flugmodus. Danach ändert sich der Flugmodus durch die Art der Erweiterung nicht. Dies liegt jedoch nur daran, dass die Erweiterungen so ausgewählt wurden, dass sie das System auf eine bestimmte Art und Weise erweitern. Aus diesem Grund muss bei einer Änderung im System das ganze System mit seinen Funktionen überprüft werden.

Gemäß den Beobachtung müssen die Abhängigkeiten für den begrenzten Flugmodus neu analysiert werden. So fügt sich in die Wirkkette des begrenzten Fluges ein neuer Schalter hinzu. Der Schalter VS verhalt sich dabei wie der Schalter SW, welcher zuvor in Kapitel 4.3.1 beschrieben wurde. Der Schalter VS hat einzig die Erneuerung, dass er im Rahmen der beschriebenen Signalkette vermutlich rein mit digitalen Steuersignalen arbeiten muss. Durch das Hinzufügen des Schalters entsteht dabei die Formel 4.62.

$$K_{\mathrm{f,\,b}} \wedge SV_{\mathrm{f,\,b}} \wedge SAW_{\mathrm{f,\,b}} \wedge VS_{\mathrm{f,\,b}} \wedge BG_{\mathrm{f,\,b}} \wedge SW_{\mathrm{f,\,b}} \Rightarrow SM_{\mathrm{f,\,b}} \tag{4.62}$$

Mit dieser Formel ist die Betrachtung für den begrenzten Flug und das Steuerungsmodul SM abgeschlossen.

Ein weiteres neues Element ist der Regler RG. Dieses Element wird für eine Regelung des UAVs benötigt. Dafür werden Messdaten des Messsystems M benötigt. Somit benötigt das verwendete Element die Messdaten M_D des Messsystems, eine Spannung SV und Steuerdaten über den Signalauswerter SAW. Die Zusammenhänge werden beispielhaft in der Formel 4.63 dargestellt.

$$SV_{\mathrm{f,\,s}} \wedge SAW_{\mathrm{f,\,s}} \wedge RG_{\mathrm{f,\,s}} \wedge M\_D_{\mathrm{f,\,s}} \Rightarrow Regler \tag{4.63}$$

Die Formel 4.63 wird dabei nicht weiter verwendet, sie soll lediglich die Zusammenhänge darstellen. Im Rahmen der Formel stellt das Element RG die Ausfallmöglichkeit des Reglers dar.

Basierend auf den vorherigen Betrachtungen lässt sich somit eine Gesamtformel für das Steuerungsmodul und den stabilisierten Flugmodus bilden. In der Formel 4.64 werden diese Zusammenhänge kombiniert und dargestellt.

$$K_{\mathrm{f,\,s}} \wedge SV_{\mathrm{f,\,s}} \wedge SAW_{\mathrm{f,\,s}} \wedge RG_{\mathrm{f,\,s}} \wedge M_{\mathrm{f,\,s}} \wedge VS_{\mathrm{f,\,s}} \wedge BG_{\mathrm{f,\,s}} \wedge SW_{\mathrm{f,\,s}} \Rightarrow SM_{\mathrm{f,\,s}} \tag{4.64}$$

Kommunikation

Das in Abbildung 4.22 dargestellte Kommunikationsmodul hat sich zur vorherigen Version nicht verändert. Folglich haben sich die Anforderungen für den messenden und den begrenzten Flugmodus nicht verändert und somit bleiben die Formeln 4.65 und 4.66 für beide Flugmodi inhaltlich auf dem vorherigen Stand.

$$RCE_{\mathrm{f,\,b1}} \wedge RC\_D_{\mathrm{f,\,b1}} \wedge SV_{\mathrm{f,\,b}} \Rightarrow K_{\mathrm{f,\,m}} \tag{4.65}$$

$$(RCE_{\mathrm{f,\,b}} \wedge RC\_D_{\mathrm{f,\,b}} \wedge SV_{\mathrm{f,\,b}}) \vee (FM_{\mathrm{f,\,b}} \wedge DL\_D_{\mathrm{f,\,b}} \wedge SV_{\mathrm{f,\,b}}) \Rightarrow K_{\mathrm{f,\,b}} \tag{4.66}$$

Einzig die Formel 4.67 für den stabilisierten Flugmodus kommt als neue Formel hinzu, welche die gleichen Abhängigkeiten wie der begrenzte Flugmodus hat. Somit lässt sich wie in den Anforderungen beschrieben, eine Steuerung über die Funkverbindung des Anwenders, als auch über die Funkfernsteuerung des Piloten realisieren.

$$(RCE_{\mathrm{f,\,s}} \wedge RC\_D_{\mathrm{f,\,s}} \wedge SV_{\mathrm{f,\,s}}) \vee (FM_{\mathrm{f,\,s}} \wedge DL\_D_{\mathrm{f,\,s}} \wedge SV_{\mathrm{f,\,s}}) \Rightarrow K_{\mathrm{f,\,s}} \tag{4.67}$$

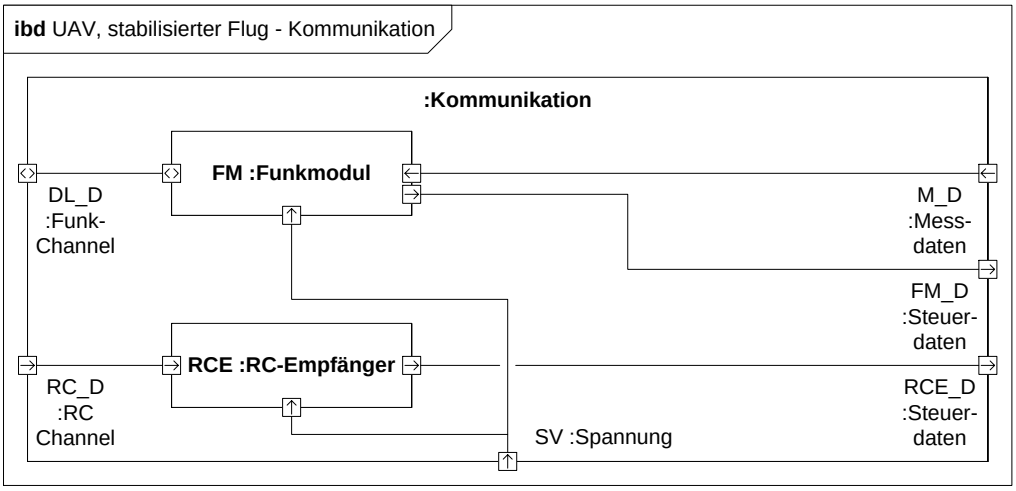

Abbildung 4.22: UAV, stabilisierter Flug - Kommunikation.

Messsystem

Das Messsystem M hat die hat die Aufgabe Messdaten von Sensoren zu sammeln und diese dem System zur Verfügung zu stellen. Der dafür verwendete Aufbau wird in der Abbildung 4.23 dargestellt. Die darauf abgebildete Messdatenaufnahme MA zeichnet die Sensorwerte zeitlich diskretisiert auf und stellt diese anderen Systemkomponenten zur Verfügung. Dafür benötigt sowohl die Messdatenaufnahme, als auch die einzelnen Sensoren eine Spannungsversorgung. Zusätzlich werden die Sensoren in zwei Sensorgruppen unterteilt. Die erste Gruppen der Sensoren S1 stellt dabei die Sensoren dar, welche für eine Regelung benötigt werden. Dabei wird die Gruppe abstrakt betrachtet. So können unter umständen einzelne Sensoren ausfallen und eine Regelung kann immer noch gewährleistet werden. Ein Ansatz, der diese Problematik behandelt ist die Sensorfusion. Bei der Sensorfusion werden die Wert mehrerer Sensoren kombiniert und daraus neue Werte errechnet. Aus diesem Grund werden die Sensoren auch nur abstrakt betrachtet. So kann erst für konkrete Sensoren und eine konkrete Regelung eine Betrachtung im Detail gemacht werden, was zuvor auf der abstrakten Ebene nicht möglich ist.

Die zweite Gruppe von Sensoren, welche mit Sensoren S2 betitelt wird, stellt Sensoren dar, welche nicht für eine Regelung verwendet. So werden die Sensoren zwar am System ange-

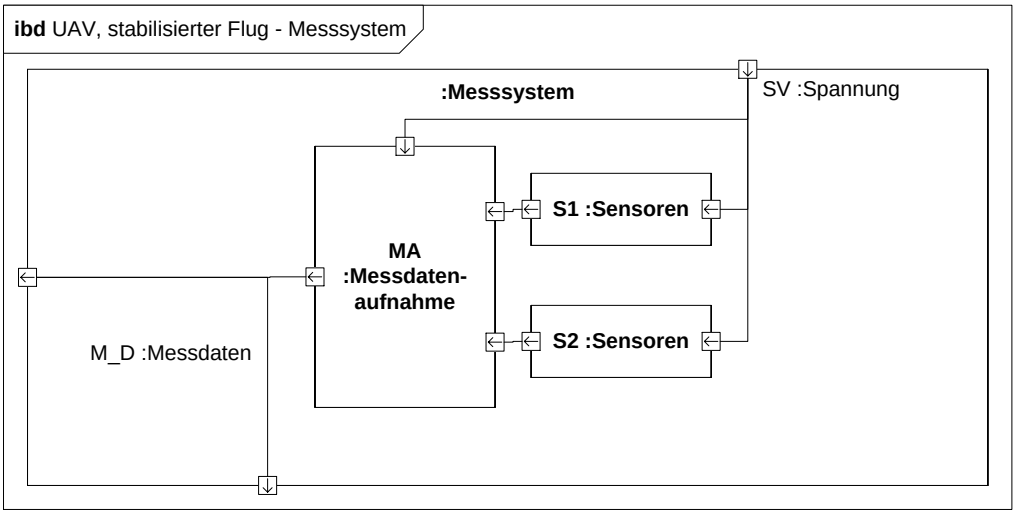

Abbildung 4.23: UAV, stabilisierter Flug - Messsystem.

schlossen, haben aber keine Auswirkung auf die Flugfunktionen. Dementsprechend ergibt sich für das Messsystem M die Formel 4.68 für den stabilisierten Flug.

$$MA_{\mathrm{f,\,s}} \wedge S1_{\mathrm{f,\,s}} \wedge SV_{\mathrm{f,\,s}} \Rightarrow M_{\mathrm{f,\,s}} \tag{4.68}$$

4.4.2 Zusammenfassung und Analyse

Abschließend werden wieder die Formeln zusammengefasst. Als erstes werden erneut die Formeln für die Aktorik und das Steuerungsmodul kombiniert.

$$(K_{\mathrm{f,\,m}} \wedge SV_{\mathrm{f,\,m}} \wedge SW_{\mathrm{f,\,m}}) \wedge SV_{\mathrm{f,\,m}} \wedge Aktoren_{\mathrm{f,\,m}} \Rightarrow A_{\mathrm{f,\,m}} \tag{4.69}$$

$$\begin{aligned}(K_{\mathrm{f,\,b}} \wedge SV_{\mathrm{f,\,b}} \wedge SAW_{\mathrm{f,\,b}} \wedge VS_{\mathrm{f,\,b}} \wedge BG_{\mathrm{f,\,b}} \wedge SW_{\mathrm{f,\,b}}) \\ \wedge SV_{\mathrm{f,\,b}} \wedge Aktoren_{\mathrm{f,\,b}} \Rightarrow A_{\mathrm{f,\,b}}\end{aligned} \tag{4.70}$$

$$\begin{aligned}(K_{\mathrm{f,\,s}} \wedge SV_{\mathrm{f,\,s}} \wedge SAW_{\mathrm{f,\,s}} \wedge RG_{\mathrm{f,\,s}} \wedge M_{\mathrm{f,\,s}} \wedge VS_{\mathrm{f,\,s}} \wedge BG_{\mathrm{f,\,s}} \wedge SW_{\mathrm{f,\,s}}) \\ \wedge SV_{\mathrm{f,\,s}} \wedge Aktoren_{\mathrm{f,\,s}} \Rightarrow A_{\mathrm{f,\,s}}\end{aligned} \tag{4.71}$$

Danach werden die Formeln für den Kommunikationsblock integriert.

$$((RCE_{\text{f, b1}} \wedge RC\_D_{\text{f, b1}} \wedge SV_{\text{f, b}}) \wedge SV_{\text{f, m}} \wedge SW_{\text{f, m}}) \\ \wedge SV_{\text{f, m}} \wedge Aktoren_{\text{f, m}} \Rightarrow A_{\text{f, m}} \tag{4.72}$$

$$(((RCE_{\text{f, b}} \wedge RC\_D_{\text{f, b}} \wedge SV_{\text{f, b}}) \vee (FM_{\text{f, b}} \wedge DL\_D_{\text{f, b}} \wedge SV_{\text{f, b}})) \\ \wedge SV_{\text{f, b}} \wedge SAW_{\text{f, b}} \wedge VS_{\text{f, b}} \wedge BG_{\text{f, b}} \wedge SW_{\text{f, b}}) \wedge SV_{\text{f, b}} \wedge Aktoren_{\text{f, b}} \Rightarrow A_{\text{f, b}} \tag{4.73}$$

$$(((RCE_{\text{f, s}} \wedge RC\_D_{\text{f, s}} \wedge SV_{\text{f, s}}) \vee (FM_{\text{f, s}} \wedge DL\_D_{\text{f, s}} \wedge SV_{\text{f, s}})) \\ \wedge SV_{\text{f, s}} \wedge SAW_{\text{f, s}} \wedge RG_{\text{f, s}} \wedge M_{\text{f, s}} \wedge VS_{\text{f, s}} \wedge BG_{\text{f, s}} \wedge SW_{\text{f, s}}) \\ \wedge SV_{\text{f, s}} \wedge Aktoren_{\text{f, s}} \Rightarrow A_{\text{f, s}} \tag{4.74}$$

Die daraus resultierenden Formeln für den messenden und den begrenzten Flug sind danach endgültig. So stellt die Formel 4.72 die Zusammenhänge für den messenden Flug dar. Dabei haben sich die Zusammenhänge und Abhängigkeiten zu dem vorherigen Funktionsset nicht verändert.

Die Formel 4.73 hat sich hingegen verändert und enthält einen neuen Schalter in der Wirkkette und somit in den Abhängigkeiten. Jedoch wird das neue Element VS vermutlich auf der gleichen Komponente abgelegt, wie der Signalauswerter SAW und der Begrenzer BG. Dieser Zusammenhang wurde schon zuvor im Kapitel 4.3.2 beschrieben.

Die dritte Formel ist die Formel 4.74 für den stabilisierten Flugmodus. Wobei die Formel noch um die Formel 4.68 für das Messsystem M erweitert werden muss. Die daraus resultierende Formel ist die Formel 4.75.

$$(((RCE_{\text{f, s}} \wedge RC\_D_{\text{f, s}} \wedge SV_{\text{f, s}}) \vee (FM_{\text{f, s}} \wedge DL\_D_{\text{f, s}} \wedge SV_{\text{f, s}})) \\ \wedge SV_{\text{f, s}} \wedge SAW_{\text{f, s}} \wedge RG_{\text{f, s}} \wedge (MA_{\text{f, s}} \wedge S1_{\text{f, s}} \wedge SV_{\text{f, s}}) \\ \wedge VS_{\text{f, s}} \wedge BG_{\text{f, s}} \wedge SW_{\text{f, s}}) \wedge SV_{\text{f, s}} \wedge Aktoren_{\text{f, s}} \Rightarrow A_{\text{f, s}} \tag{4.75}$$

Basierend auf diesen Formeln lässt sich die Architektur analysieren. Jedoch wurden fast alle möglichen Komponenten für die Funktionen schon auf Redundanzen und weitere Möglichkeiten geprüft. So stehen noch die Elemente RG, MA, S1 und VS auf der Liste der zu betrachtenden Elemente.

Die Sensoren S1 wurden schon zuvor so beschrieben, dass sie erst bei konkreten Komponenten und einer konkreten Regelung bezüglich möglicher Redundanzen geprüft werden können. Die zu den Sensoren gehörende Messdatenaufnahme MA wird vermutlich auf der selben Komponente abgebildet, wie der Regler. Der Regler RG und der dazu gehörige Schalter VS werden vermutlich mit dem Begrenzer BG auf einer Komponente abgebildet, da sie einen direkten Signalfluss abbilden. So bietet es sich an die steuernden Funktionen auf einer Komponente abzubilden. Dies basiert auf den Beschreibungen aus Kapitel 4.3.2. Somit kann diese Komponente redundant in das System integriert werden.

Ein Punkt, der bisher ignoriert wurde und an dieser Stelle immer wichtiger wird ist die Validierung und Verifikation des Systems. So wird beispielsweise das steuernde Modul vermutlich in Software umgesetzt. Während des Entwicklungsprozesses dieser Software können jedoch Fehler auftreten. Diese Fehler können dann zur Laufzeit des Systems einen Fehler im System auslösen. Im Gegensatz zu Hardwarefehlern, die auf Verschleiß basieren können, kann ein Softwarefehler theoretisch im Vorfeld gefunden werden. So kann basierend auf dem deterministischen Verhalten der Fehler schon im Vorfeld entdeckt und beseitigt werden. So lassen sich mit den passenden Verfahren die Fehler finden und beseitigen. Somit sollte es möglich sein Software-basierte Fehler komplett zu vermeiden.

Jedoch steigt mit der Komplexität eines Systems auch die Schwierigkeit einen Fehler zu finden. So ist es noch leicht mögliche Fehler im System für das Funktionsset des begrenzten Fluges zu finden. Doch steigt der Schwierigkeitsgrad einen Fehler zu finden mit der Komplexität. So steigt der Schwierigkeitsgrad mit dem aktuellen Funktionsset massiv an.

Das Finden dieser möglichen Fehler ist jedoch nicht Stand dieser Arbeit. Es sollte jedoch bei der Entwicklung beachtet werden, so sollten dementsprechend Verfahren für die Validierung und Verifikation des Systems angewandt werden und man sollte auf zertifizierte Testverfahren zurückgegriffen.

4.4.3 Fazit bezüglich des Flugs

Das Funktionsset erweitert die vorherige Architektur zwar mit neuen Funktionsblöcken, jedoch basiert die Erweiterung im Wesentlichen auf Logik. Somit lassen sich die Erweiterungen auch kaum auf Redundanzen und ähnliche Maßnahmen überprüfen.

Auf der anderen Seite ist das Funktionsset eine wesentliche Erweiterung in Richtung eines autonomen Fluges. Zusätzlich ermöglicht die Erweiterung eine leichtere Steuerung des UAVs.

4.4.4 Mitigations

Im Rahmen der Mitigations wird weiterhin auf den akustischen Signalgeber zurückgegriffen. Die dazugehörige Architektur wird in Abbildung 4.24 dargestellt. Dabei hat sich die Architektur

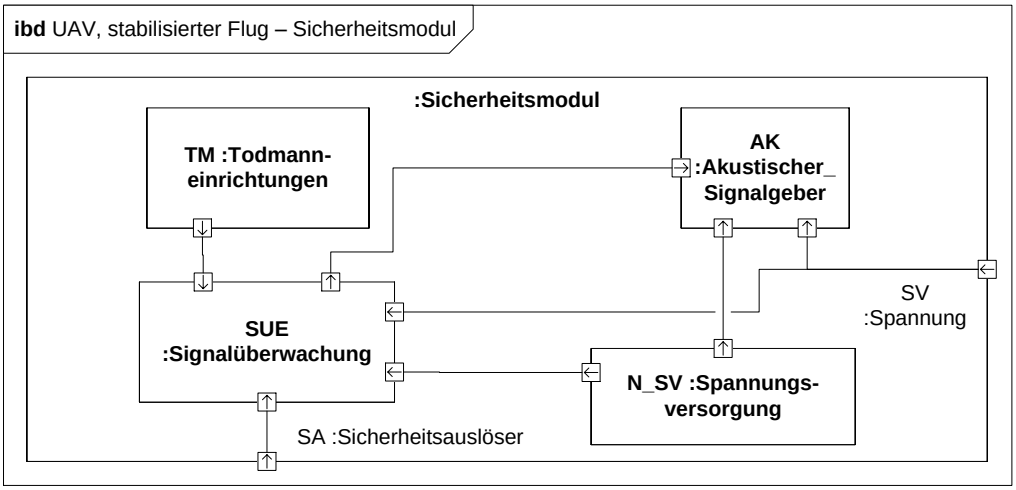

Abbildung 4.24: UAV, stabilisierter Flug - Sicherheitsmodul.

und die Abhängigkeiten nicht verändert. Aus diesem Grund wird auf eine erneute Analyse verzichtet. Jedoch sollte beachtet werden, dass bei einem konkreten System und konkreten Komponenten bei einer Änderung im System das komplette System neu analysiert werden sollte, um sicherzustellen, dass man keine verdeckten Abhängigkeit übersehen hat.

4.5 Autonome Flugsteuerung

Die autonome Flugsteuerung stellt das letzte Funktionsset dar, welches betrachtet wird. Es erweitert das Funktionsset der stabilisierten Flugsteuerung aus Kapitel 4.4. Dabei wird das Funktionsset mit dem im Kapitel 3.1.4 beschriebenen Flugmodus und der im Kapitel 3.2.2 beschriebenen Mitigation erweitert.

Um den neuen Flugmodus für den autonomen Flug durchzuführen wird eine Steuerung durch den Anwender benötigt. Dies hat den Grund, dass der Pilot über die Funkfernsteuerung keine

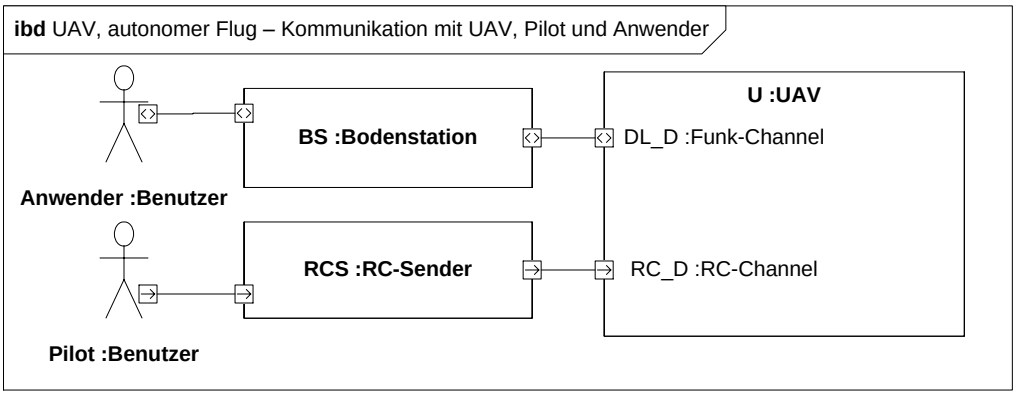

Abbildung 4.25: UAV, autonomer Flug – Kommunikation mit UAV, Pilot und Anwender.

Koordinaten oder Ziele eingeben kann. Der Zusammenhang wird in der Abbildung 4.25 dargestellt. Bei der Abbildung besteht jedoch weiterhin eine Verbindung vom Piloten zum UAV. Dies ist notwendig, da der Pilot jederzeit die Kontrolle übernehmen können muss.

4.5.1 Fliegen des UAVs

Im Rahmen dieser Analyse wird auf die Architektur der Abbildung 4.26 zurückgegriffen. Weiterhin wird bei der Analyse vom Funktionsblock der Aktorik A ausgegangen. Dabei steht der Index klein F erneut für den Flug des UAVs. Die Indexe klein M, klein B, klein S und klein A stehen für die Flugmodi messender, begrenzter, stabilisierter und autonomen Flug.

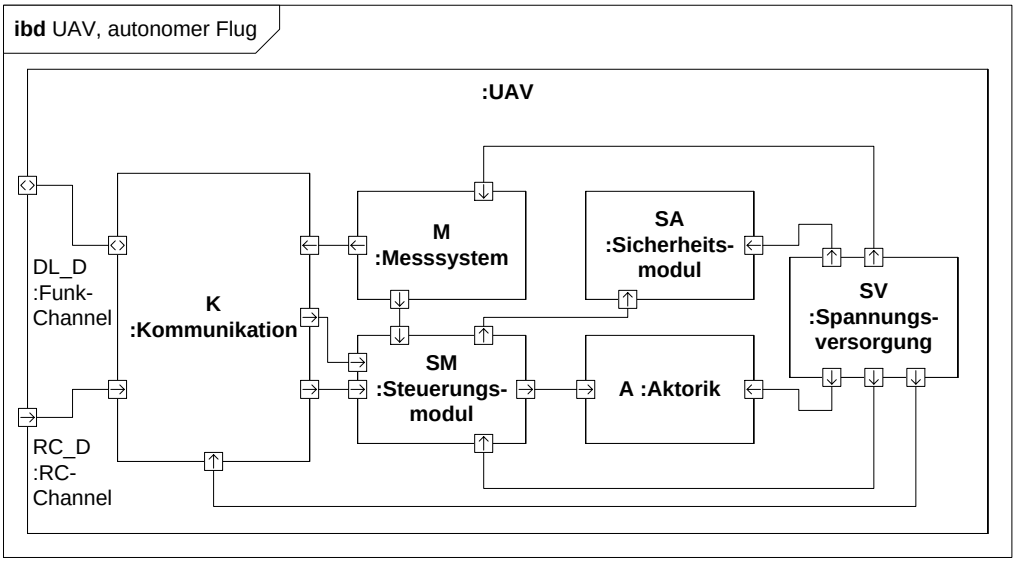

Abbildung 4.26: UAV, autonomer Flug.

Aktorik

Als Ausgangspunkt wird erneut die Formel für die Aktorik A aufgestellt, welche bei allen Flugmodi gleich ist und die gleichen Abhängigkeiten hat.

$$SM_{\text{f, m}} \wedge SV_{\text{f, m}} \wedge Aktoren_{\text{f, m}} \Rightarrow A_{\text{f, m}} \tag{4.76}$$

$$SM_{\text{f, b}} \wedge SV_{\text{f, b}} \wedge Aktoren_{\text{f, b}} \Rightarrow A_{\text{f, b}} \tag{4.77}$$

$$SM_{\text{f, s}} \wedge SV_{\text{f, s}} \wedge Aktoren_{\text{f, s}} \Rightarrow A_{\text{f, s}} \tag{4.78}$$

$$SM_{\text{f, a}} \wedge SV_{\text{f, a}} \wedge Aktoren_{\text{f, a}} \Rightarrow A_{\text{f, a}} \tag{4.79}$$

Steuerungsmodul

Der Kern der Analyse ist erneut das Steuerungsmodul SM, welches die Funktionen für den jeweiligen Flugmodus enthält. Dabei wird die auf der Abbildung 4.27 abgebildete Architektur verwendet. Aufbauend auf der Abbildung werden zuerst die Formeln für die Flugmodi messen-

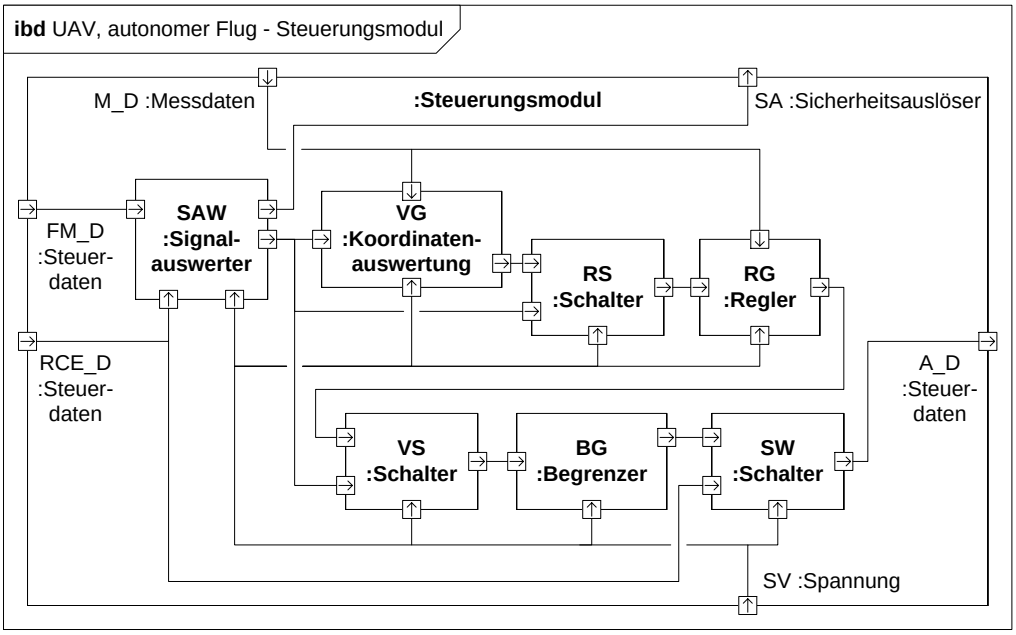

Abbildung 4.27: UAV, autonomer Flug - Steuerungsmodul.

der und begrenzter Flug aufgestellt, welche sich zu der vorherigen Architektur nicht verändert haben.

$$K_{\mathrm{f,\,m}} \wedge SV_{\mathrm{f,\,m}} \wedge SW_{\mathrm{f,\,m}} \Rightarrow SM_{\mathrm{f,\,m}} \tag{4.80}$$

$$K_{\mathrm{f,\,b}} \wedge SV_{\mathrm{f,\,b}} \wedge SAW_{\mathrm{f,\,b}} \wedge VS_{\mathrm{f,\,b}} \wedge BG_{\mathrm{f,\,b}} \wedge SW_{\mathrm{f,\,b}} \Rightarrow SM_{\mathrm{f,\,b}} \tag{4.81}$$

Die neue Formel für den stabilisierenden Flugmodus wird hingegen um den Schalter RS erweitert. Beim Verhalten des Schalters wird wieder auf die Beschreibungen der Schalter VS und SW zurückgegriffen. Die darauf resultierende Formel 4.82 stellt somit einen neuen Stand für den Flugmodus dar.

$$\begin{aligned} &K_{\mathrm{f,\,s}} \wedge SV_{\mathrm{f,\,s}} \wedge SAW_{\mathrm{f,\,s}} \wedge RS_{\mathrm{f,\,s}} \wedge RG_{\mathrm{f,\,s}} \\ &\wedge M_{\mathrm{f,\,s}} \wedge VS_{\mathrm{f,\,s}} \wedge BG_{\mathrm{f,\,s}} \wedge SW_{\mathrm{f,\,s}} \Rightarrow SM_{\mathrm{f,\,s}} \end{aligned} \tag{4.82}$$

Neben den Schalter RS kommt das zusätzliche Element der Koordinatenauswertung VG hinzu, welche aus Messdaten Koordinaten bildet und mittels einer vorgegebenen Koordinate

einen Vektor im Raum zu der vorgegebenen Koordinate berechnet. Das Vorgehen des Elementes entspricht dabei einer Regelung. So kann man die beispielhafte Formel 4.84 für die Koordinatenauswertung aufstellen, welche zu der Regler-Formel aus Kapitel 4.4.1 äquivalent ist.

$$SV_{\mathrm{f,\,a}} \wedge SAW_{\mathrm{f,\,a}} \wedge VG_{\mathrm{f,\,a}} \wedge M\_D_{\mathrm{f,\,a}} \Rightarrow Koordinatenauswertung \tag{4.83}$$

Auf dieser Grundlage lässt sich für den autonomen Flug die abschließende Formel 4.5.1 aufstellen.

$$\begin{aligned} &K_{\mathrm{f,\,a}} \wedge SV_{\mathrm{f,\,a}} \wedge SAW_{\mathrm{f,\,a}} \wedge VG_{\mathrm{f,\,a}} \wedge RS_{\mathrm{f,\,a}} \wedge RG_{\mathrm{f,\,a}} \\ &\wedge M_{\mathrm{f,\,a}} \wedge VS_{\mathrm{f,\,a}} \wedge BG_{\mathrm{f,\,a}} \wedge SW_{\mathrm{f,\,a}} \Rightarrow SM_{\mathrm{f,\,a}} \end{aligned} \tag{4.84}$$

Kommunikation

Für die Kommunikation K, welche in der Abbildung 4.28 dargestellt wird, ergeben sich für die Flugmodi messender, begrenzter und stabilisierter Flug keine Änderungen.

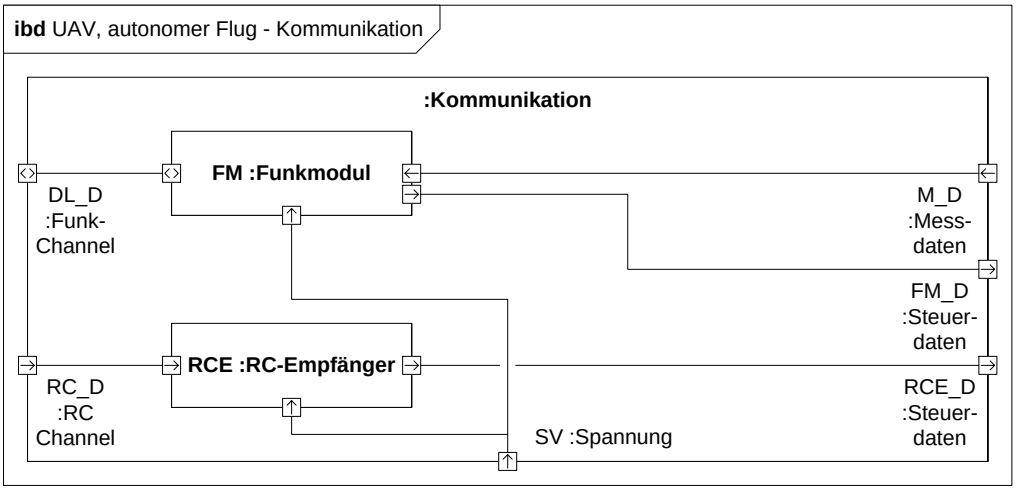

Abbildung 4.28: UAV, autonomer Flug - Kommunikation.

$$RCE_{\mathrm{f,\,m}} \wedge RC\_D_{\mathrm{f,\,m}} \wedge SV_{\mathrm{f,\,m}} \Rightarrow K_{\mathrm{f,\,m}} \tag{4.85}$$

$$(RCE_{\mathrm{f,\,b}} \wedge RC\_D_{\mathrm{f,\,b}} \wedge SV_{\mathrm{f,\,b}}) \vee (FM_{\mathrm{f,\,b}} \wedge DL\_D_{\mathrm{f,\,b}} \wedge SV_{\mathrm{f,\,b}}) \Rightarrow K_{\mathrm{f,\,b}} \tag{4.86}$$

$$(RCE_{\mathrm{f,\,s}} \wedge RC\_D_{\mathrm{f,\,s}} \wedge SV_{\mathrm{f,\,s}}) \vee (FM_{\mathrm{f,\,s}} \wedge DL\_D_{\mathrm{f,\,s}} \wedge SV_{\mathrm{f,\,s}}) \Rightarrow K_{\mathrm{f,\,s}} \tag{4.87}$$

Jedoch muss eine neue Formel für den autonomen Flug aufgestellt werden. Dabei ist zu Bedenken, dass die Steuerung dabei nicht über eine Funkfernsteuerung geschehen kann und daher auf diesen Übertragungsweg verzichtet werden muss. Somit bildet die Formel 4.88 die Zusammenhänge für den autonomen Flug, bei dem die Zielkoordinate vom Anwender vorgegeben wird.

$$FM_{\mathrm{f,\,a}} \wedge DL\_D_{\mathrm{f,\,a}} \wedge SV_{\mathrm{f,\,a}} \Rightarrow K_{\mathrm{f,\,a}} \tag{4.88}$$

Messsystem

Als letzter Punkt für die Funktionsblockanalyse steht erneut das Messsystem M an. Dieser Block wird in der Abbildung 4.29 dargestellt und wurde an das neue Funktionsset angepasst. So wurden die Sensoren der Gruppe 1, welche für die Regelung notwendig sind in zwei neue

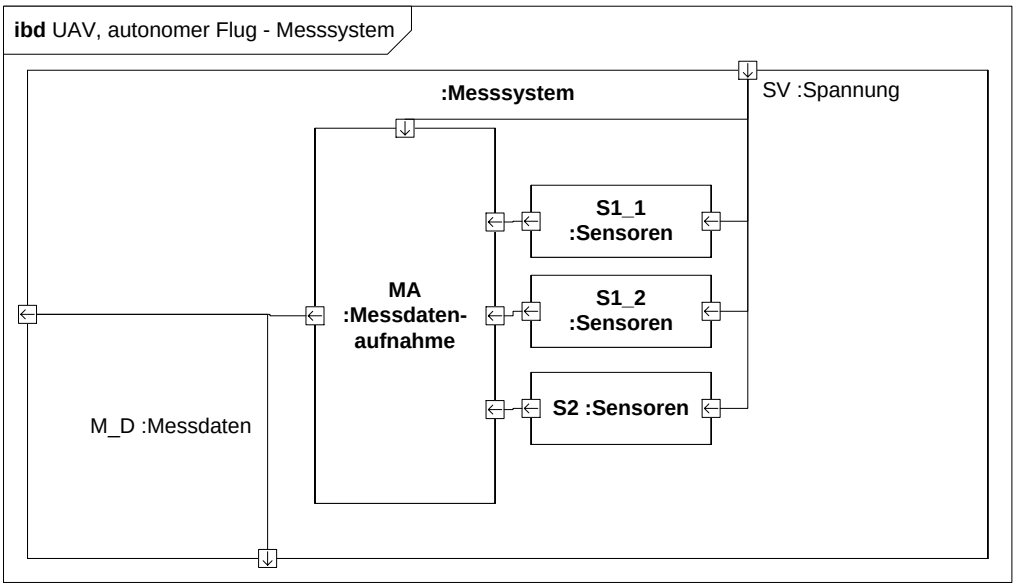

Abbildung 4.29: UAV, autonomer Flug - Messsystem.

Gruppen aufgeteilt. Die erste Gruppe S1_1 stellt dabei die Sensoren dar, welche für einen

einfachen stabilisierten Flug des Systems benötigt werden. Die Sensoren der zweiten Gruppe S1_2 stellt die Sensoren dar, welche zusätzlich für die erweiterte Regelung des autonomen Fluges benötigt werden und nicht für einen rein stabilisierten Flug benötigt werden.

Darauf aufbauend lässt sich die Formel für den stabilisierten Flugmodus neu aufstellen und ergibt die Formel 4.89.

$$MA_{\text{f, s}} \wedge S1\_1_{\text{f, s}} \wedge SV_{\text{f, s}} \Rightarrow M_{\text{f, s}} \tag{4.89}$$

Für den autonomen Flug werden hingegen sowohl die Sensoren der Gruppe S1_1 benötigt, als auch die Sensoren der Gruppe S1_2. Dabei ist zu beachten, dass die Gruppe S1_2 auch leer sein kann. Wenn die Regelung für den autonomen Flug rein mit den Sensoren auskommt, die auch für den einfachen stabilisierten Flug benötigt werden, kann die Gruppe S1_2 leer sein. Dies ist jedoch abhängig von der konkreten Regelung und den konkreten Sensoren, die Verwendet werden sollen. So kann in der Formel 4.90 für den autonomen Flug das Element S1_2 unter Umständen mit einem true ersetzt werden und könnte somit aus der Formel gestrichen werden.

$$MA_{\text{f, a}} \wedge S1\_1_{\text{f, a}} \wedge S1\_2_{\text{f, a}} \wedge SV_{\text{f, a}} \Rightarrow M_{\text{f, a}} \tag{4.90}$$

4.5.2 Zusammenfassung und Analyse

Im ersten Schritt der Zusammenfassung werden wieder die Formeln für die Aktorik und das Steuerungsmodul zusammengefasst.

$$(K_{\text{f, m}} \wedge SV_{\text{f, m}} \wedge SW_{\text{f, m}}) \wedge SV_{\text{f, m}} \wedge Aktoren_{\text{f, m}} \Rightarrow A_{\text{f, m}} \tag{4.91}$$

$$\begin{aligned}(K_{\text{f, b}} \wedge SV_{\text{f, b}} \wedge SAW_{\text{f, b}} \wedge VS_{\text{f, b}} \wedge BG_{\text{f, b}} \wedge SW_{\text{f, b}}) \\ \wedge SV_{\text{f, b}} \wedge Aktoren_{\text{f, b}} \Rightarrow A_{\text{f, b}}\end{aligned} \tag{4.92}$$

$$\begin{aligned}(K_{\text{f, s}} \wedge SV_{\text{f, s}} \wedge SAW_{\text{f, s}} \wedge RS_{\text{f, s}} \wedge RG_{\text{f, s}} \wedge M_{\text{f, s}} \wedge VS_{\text{f, s}} \wedge BG_{\text{f, s}} \wedge SW_{\text{f, s}}) \\ \wedge SV_{\text{f, s}} \wedge Aktoren_{\text{f, s}} \Rightarrow A_{\text{f, s}}\end{aligned} \tag{4.93}$$

$$\begin{aligned}(K_{\text{f, a}} \wedge SV_{\text{f, a}} \wedge SAW_{\text{f, a}} \wedge VG_{\text{f, a}} \wedge RS_{\text{f, a}} \wedge RG_{\text{f, a}} \wedge M_{\text{f, a}} \wedge VS_{\text{f, a}} \\ \wedge BG_{\text{f, a}} \wedge SW_{\text{f, a}}) \wedge SV_{\text{f, a}} \wedge Aktoren_{\text{f, a}} \Rightarrow A_{\text{f, a}}\end{aligned} \tag{4.94}$$

Im zweiten Schritt werden erneut die Formeln für die Kommunikation integriert.

$$((RCE_{\text{f, m}} \wedge RC\_D_{\text{f, m}} \wedge SV_{\text{f, m}}) \wedge SV_{\text{f, m}} \wedge SW_{\text{f, m}}) \\ \wedge SV_{\text{f, m}} \wedge Aktoren_{\text{f, m}} \Rightarrow A_{\text{f, m}} \tag{4.95}$$

$$(((RCE_{\text{f, b}} \wedge RC\_D_{\text{f, b}} \wedge SV_{\text{f, b}}) \vee (FM_{\text{f, b}} \wedge DL\_D_{\text{f, b}} \wedge SV_{\text{f, b}})) \\ \wedge SV_{\text{f, b}} \wedge SAW_{\text{f, b}} \wedge VS_{\text{f, b}} \wedge BG_{\text{f, b}} \wedge SW_{\text{f, b}}) \wedge SV_{\text{f, b}} \wedge Aktoren_{\text{f, b}} \Rightarrow A_{\text{f, b}} \tag{4.96}$$

$$(((RCE_{\text{f, s}} \wedge RC\_D_{\text{f, s}} \wedge SV_{\text{f, s}}) \vee (FM_{\text{f, s}} \wedge DL\_D_{\text{f, s}} \wedge SV_{\text{f, s}})) \\ \wedge SV_{\text{f, s}} \wedge SAW_{\text{f, s}} \wedge RS_{\text{f, s}} \wedge RG_{\text{f, s}} \wedge M_{\text{f, s}} \wedge VS_{\text{f, s}} \wedge BG_{\text{f, s}} \wedge SW_{\text{f, s}}) \\ \wedge SV_{\text{f, s}} \wedge Aktoren_{\text{f, s}} \Rightarrow A_{\text{f, s}} \tag{4.97}$$

$$((FM_{\text{f, a}} \wedge DL\_D_{\text{f, a}} \wedge SV_{\text{f, a}}) \wedge SV_{\text{f, a}} \wedge SAW_{\text{f, a}} \wedge VG_{\text{f, a}} \wedge RS_{\text{f, a}} \\ \wedge RG_{\text{f, a}} \wedge M_{\text{f, a}} \wedge VS_{\text{f, a}} \wedge BG_{\text{f, a}} \wedge SW_{\text{f, a}}) \wedge SV_{\text{f, a}} \wedge Aktoren_{\text{f, a}} \Rightarrow A_{\text{f, a}} \tag{4.98}$$

Die Formeln 4.95 und 4.96 sind damit die abschließenden Formeln für den messenden und den begrenzten Flugmodus. Diese Formeln haben sich auch zu den Ergebnis aus dem Kapitel 4.4.2 nicht verändert und werden daher nicht weiter betrachtet.

Die Formeln 4.97 und 4.98 für den stabilisierten und den autonomen Flugmodus müssen hingegen noch mit den Formeln für das Messsystem erweitert werden.

$$(((RCE_{\text{f, s}} \wedge RC\_D_{\text{f, s}} \wedge SV_{\text{f, s}}) \vee (FM_{\text{f, s}} \wedge DL\_D_{\text{f, s}} \wedge SV_{\text{f, s}})) \\ \wedge SV_{\text{f, s}} \wedge SAW_{\text{f, s}} \wedge RS_{\text{f, s}} \wedge RG_{\text{f, s}} \wedge (MA_{\text{f, s}} \wedge S1\_1_{\text{f, s}} \wedge SV_{\text{f, s}}) \\ \wedge VS_{\text{f, s}} \wedge BG_{\text{f, s}} \wedge SW_{\text{f, s}}) \wedge SV_{\text{f, s}} \wedge Aktoren_{\text{f, s}} \Rightarrow A_{\text{f, s}} \tag{4.99}$$

$$((FM_{\text{f, a}} \wedge DL\_D_{\text{f, a}} \wedge SV_{\text{f, a}}) \wedge SV_{\text{f, a}} \wedge SAW_{\text{f, a}} \wedge VG_{\text{f, a}} \\ \wedge RS_{\text{f, a}} \wedge RG_{\text{f, a}} \wedge (MA_{\text{f, a}} \wedge S1\_1_{\text{f, a}} \wedge S1\_2_{\text{f, a}} \wedge SV_{\text{f, a}}) \\ \wedge VS_{\text{f, a}} \wedge BG_{\text{f, a}} \wedge SW_{\text{f, a}}) \wedge SV_{\text{f, a}} \wedge Aktoren_{\text{f, a}} \Rightarrow A_{\text{f, a}} \tag{4.100}$$

Aus dieser Erweiterung resultieren die Formeln 4.99 und 4.100. Bei der Betrachtung dieser Formeln fällt jedoch der Zusammenhang auf, der schon in Kapitel 4.4.2 beschrieben wurde. So

ist die Koordinatenauswertung eine Erweiterung der Regelung und wird somit vermutlich auf der gleichen Komponente realisiert, die zuvor schon mehrfach analysiert wurde.

4.5.3 Fazit bezüglich des Flugs

Dieses letzte Funktionsset bringt dem System einen wichtigen Milestone, mit dessen Hilfe das System für mehrere Anwendungen eingesetzt werden kann. So kann mit dem Stand die Zielaufgabe des BWB-AES Teams vorerst bewältigt werden.

Auf der anderen Seite bestehen die Erweiterungen jedoch nur noch im Bereich der Logik und unter den Betrachtungen möglicher Ausfälle von Komponenten kommt keine Erweiterung zum vorherigen Funktionsset dazu. Lediglich die verwendeten Sensoren müssen erneut geprüft werden und die Anforderungen an die Stabilität der Logik steigt. Somit muss basierend auf einer Software-Lösung ein größeres Augenmerk auf die Entwicklung dieser Software gelegt werden und nicht auf elektronische Komponenten.

4.5.4 Mitigations

Als letzter wichtiger Punkt für das Funktionsset steht die Betrachtung der Mitigations an. So wird unter anderem wieder auf den akustischen Signalgeber zurückgegriffen, welcher in Abbildung 4.30 abgebildet ist. Jedoch hat sich die Architektur für den akustischen Signalgeber

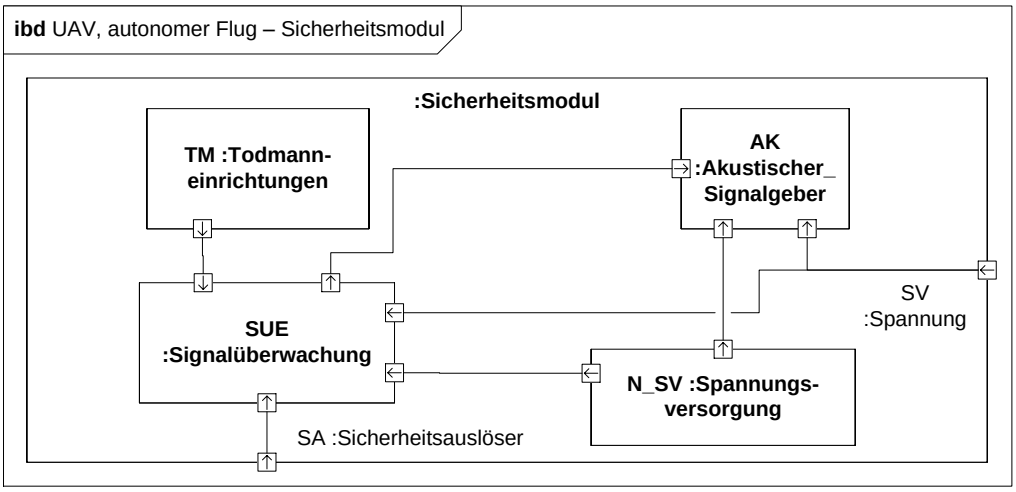

Abbildung 4.30: UAV, autonomer Flug - Sicherheitsmodul.

erneut nicht verändert und somit wird auf eine Analyse dieser Maßnahme verzichtet.

Im Rahmen dieses Funktionssets kommt aber eine weitere Maßnahme hinzu. Der im Kapitel 3.2.2 beschriebene gezielte Aufstieg soll neben dem akustischen Signalgeber eingreifen, wenn beide Funkverbindungen ausgefallen sind und keine neuen Steuerdaten empfangen werden können oder wenn der Flug nicht weiter vom Boden aus überwacht werden kann. Um dies zu erreichen muss erneut auf das Steuerungsmodul SM von der Abbildung 4.27 zurückgegriffen werden. So muss der Signalauswerter SAW und die Koordinatenauswertung VG soweit erweitert werden, dass der Signalauswerter nicht nur dem Sicherheitsmodul einen Sicherheitsauslöser-Signal sendet, sondern auch der Koordinatenauswertung die Anweisung gibt eine erhöhte Position über der aktuellen Position stationär einzunehmen.

Um diese Zusammenhänge darzustellen kann die Formel 4.100 für den autonomen Flug soweit abgeändert werden, dass die Abhängigkeiten zur Kommunikation wegfallen. Dabei wird der Index klein S für die Sicherheitsfunktion verwendet und der Index klein A für das automatische Aufsteigen und das Halten der Position.

$$(SV_{\text{s, a}} \wedge SAW_{\text{s, a}} \wedge VG_{\text{s, a}} \wedge RS_{\text{s, a}} \wedge RG_{\text{s, a}} \wedge (MA_{\text{s, a}} \wedge S1\_1_{\text{s, a}} \wedge S1\_2_{\text{s, a}} \wedge SV_{\text{s, a}}) \\ \wedge VS_{\text{s, a}} \wedge BG_{\text{s, a}} \wedge SW_{\text{s, a}}) \wedge SV_{\text{s, a}} \wedge Aktoren_{\text{s, a}} \Rightarrow A_{\text{s, a}} \tag{4.101}$$

Die resultierende Formel 4.101 enthält nun alle Abhängigkeiten für die Maßnahme. Jedoch wurden alle Komponenten schon bezüglich Ausfall geprüft werden. Dies geschah im Rahmen der Analyse für den Flug. Somit wird in diesem Rahmen von weiteren Analysen abgesehen und somit enden die Analyse an der funktionalen Architektur.

5 Zusammenfassung und Aussicht

Basierend auf den zuvor geleisteten Analysen auf der funktionalen Ebene, sollten im Anschluss Analysen auf der Komponentenebene stattfinden. Da jedoch diese Arbeit als Vorleistung für die Projektgruppe BWB-AES erstellt wurde und die Arbeiten der Projektgruppe noch am Anfang stehen, steht noch keine Architektur auf Komponentenebene zur Verfügung, die man analysieren kann. In diesem Rahmen enden die Analysen an dieser Stelle. Dieses Kapitel soll noch eine kurze Zusammenfassung der bisherigen Arbeit und einen Aussicht auf zukünftig anstehende Arbeiten geben.

5.1 Entwicklung des Systems

Durch die sukzessive Weiterentwicklung des Systems wurde die Wirkkette von der Entscheidung bis zum Resultat immer länger. Während in der Ausgangssituation ein System mit einer kurzen Wirkkette und überschaubaren Schwachstellen zur Verfügung stand, so wurde das System immer Komplexer und entwickelte neue Abhängigkeiten. Daraus resultierten neue Schwachstellen und Fehlermöglichkeiten, wodurch die Anforderungen an die verwendeten Komponenten nach und nach stiegen und sowohl robuste, als auch alternative Elemente benötigt wurden. Jedoch ließen sich leider nicht alle Elemente auf Maßnahmen und Möglichkeiten überprüfen. Da keine festen Komponenten vorlagen war dies nicht möglich. So konnten zwar mögliche Empfehlungen und Hinweise ausgesprochen werden aber keine maßgebende Architekturentscheidung. Ebenso konnte aufgrund von fehlenden Komponenten keine Auswirkungen auf Nachbarn im System analysiert werden. So musste für die Analyse davon ausgegangen werden, dass die Spannungsversorgung unbeeinflusst von den Abnehmern ist. In einer konkreten Implementierung mit Komponenten kann eine Komponente jedoch einen Kurzschluss haben und beeinfluss dann die Spannungsversorgung. Auch wurden Fehler wie Leiterschlüsse in der Elektronik und Pointerfehler in der Software nicht beachtet, welche bei konkreten Komponenten auftreten können und Fehler verursachen würden.

Zusammenfassend lässt such über die Entwicklung nur sagen, dass die bisherige Arbeit ein

Einstieg war. Folglich steht noch eine Vielzahl von Arbeiten an, welche noch bis zum fertigen Produkt bewältigt werden müssen.

5.2 Ausstehende Arbeiten

Ein wesentlicher Punkt, der während der Erstellung der Arbeit aufgefallen ist, ist die Bedeutung der Architekturmodelle. So basierten die Sicherheitsanalyse auf Modellen, welche mit einer wohldefinierten Notation beschrieben wurden. Dieser Ansatz der modellgetriebenen Entwicklung sollte als Grundlage für weitere Arbeiten im Projekt ausgewählt werden und dann die Durchführung von Sicherheitsanalysen erleichtern, bzw. ermöglichen. So sollte dies geschehen bevor eine Komponente entwickelt wird und dann mittels Reverse Engineering ein Modell erzeugt werden muss, welches erst dann analysiert werden kann.

Neben der modellgetriebenen Entwicklung stehen aber noch weitere Aufgaben aus, von denen die einige Hauptaufgaben in diesem Abschnitt vorgestellt werden.

5.2.1 Sicherheitsschalter

Das in [25] beschriebene Modul für das sichere Umschalten von Steuersignalen sollte analysiert werden, an das System angepasst werden und dann in das System integriert werden. Das Ziel soll es sein eine äquivalente Sicherheit beim Auswählen einer Steuersignalquelle zu erhalten und folglich den Piloten als letzte Sicherheitsinstanz einzusetzen für den Fall, dass die komplexe Logik einen Fehler aufweist und ausfällt.

5.2.2 Redundante Mikrocontroller

Als eine grundlegende Komponente wurde die steuernde Logik identifiziert. Durch sie werden wichtige Entscheidungen im System getroffen und ein Ausfall hätte verheerende Folgen für die meisten Flugmodi. Folglich sollte versucht werden ein ausfallsicheres System aus der Steuerung zu entwickeln, welches mittels Redundanzen eine sichere Funktion zur Verfügung stellt.

Da in den ersten Projekttagen sich rausstellte, dass ein durchschnittlicher Mikrocontroller von der Anzahl der Peripherie des Chips nicht ausreicht, wurden zwei Mikrocontroller eingeplant. Das Ziel sollte es sein, dass eine Konstellation von Mikrocontrollern, Software und Voting-Verfahren entwickelt wird, welche es ermöglicht, dass mindestens einer der Mikrocontroller ausfallen kann und die Funktion weiterhin gegeben ist.

5.2.3 Funkverbindung

Ein wichtiger Punkt für die Detailanalyse ist die Analyse der zweiten Funkstrecke zur Bodenstation. Da die Funkfernsteuerung des Piloten als Basissicherheit gilt kann diese vorerst so betrachtet werden, wie sie ist. Jedoch bildet die zweite Funkverbindung eine neue Grundlage und die dazu ausgewählte Komponente muss auf mehrere Aspekte hin analysiert werden. So müssen beispielsweise Ausfallsicherheit, Reichweite und Datenübertragung überprüft werden und es muss analysiert werden, inwiefern diese die Anforderungen erfüllen, die den gewünschten Betrieb ermöglichen und diesen sicherstellen.

5.2.4 Regelung, Sensoren und Sensorfusion

Für das Fortführen der Entwicklung wird eine konkrete Regelung benötigt, auf der der stabilisierte und der autonome Flugmodus aufbauen können. Wurde dies geleistet kann man sich mit den Konzepten der Sensoren und der Sensorfusion beschäftigen. Somit ist eine konkrete Regelung notwendig für die Sicherheitsanalysen bezüglich der Sensoren und der Sensorfusion.

5.2.5 Weitere Mitigations

Zwar wurden im Rahmen der Analysen zwei Mitigations betrachtet, jedoch doch stehen noch weitere Maßnahmen zur Verfügung, die analysiert und eingesetzt werden können und somit das UAV sicherer machen könnten. In diesem Abschnitt werden noch kurz mögliche Maßnahmen vorgestellt, welche es nicht in die Arbeit geschafft haben aber interessant für eine Umsetzung oder Betrachtung sein könnten.

Fallschirm

Fallschirme sind hauptsächlich aus dem Personenbereich bekannt. Darüber hinaus werden aber auch Fallschirme im Modellflugbereich eingesetzt. So setzen Modellraketen Fallschirme ein, um sicher zurück zum Boden zu kommen. In diesem Rahmen können die Fallschirme auch für Drohnen eingesetzt werden. Am Beispiel 5.1 kann man eine Drohne mit einem Fallschirm landen sehen. So setzt die Deutsche Bundeswehr Fallschirme bei ihren KZO Drohnen ein ([4]).

Der Vorteil einer Fallschirmlandung liegt in einer relativ sicheren Landung. Dafür steigen die Anforderungen an die Steuerung. So müssen beispielsweise die Antriebe deaktiviert werden, sobald sich der Fallschirm öffnet. Dieser und andere Aspekte müssen im Detail analysiert werden.

Abbildung 5.1: Fallschirmlandung einer Bundeswehr Drohne ([4]).

Zerlegen des Flugkörpers

Werden Objekte in der Raumfahrt nicht mehr benötigt, so werden diese teilweise in einem Wiedereintritt in die Atmosphäre zerstört. Dabei werden größere Objekte an Sollbruchstellen zerlegt, um kleiner Teile zu ergeben, die dann verglühen können oder zumindest keinen großen Schaden anrichten können. Unter diesen Aspekt kann man die Drohne vor einem Absturz gezielt explodieren lassen.

Da eine Drohne in voller Größe einen massiven Schaden an der Umgebung ausüben kann, könnte mit diesem Verfahren der Schaden minimiert werden. Zusätzlich könnte in einer Konfiguration mit Wasserstoffantrieb, eine mögliche Explosion beim Aufprall auf den Boden verhindert werden.

Da dieser Ansatz den Einsatz von Sprengstoff erfordert sollte er mit Bedacht analysiert werden. Zusätzlich müsste betrachtet werden, wie die Umgebungsschäden sich verhalten würden. So müsste geprüft werden, wodurch größere Schäden entstehen, kleine Überreste oder eine komplette Drohne mit mehreren Kilogram Gewicht und einer möglichen explosiven Ladung.

Autonomer Rückflug

Ein Ansatz um einen Absturz zu verhindern ist der autonome Rückflug zu einer vorgegebenen Position oder zu der Position, an der der letzte Funkkontakt bestand. Diese Maßnahme sollte zwar nicht über bewohnten Gebiet eingesetzt werden und ist im deutschen Luftraum auch nicht erlaubt. Dies hat den Grund, dass keine Person den Flug überwachen kann und die Gefahr einer Kollision besteht. So gibt es das Beispiel der Beinahe-Kollision einer deutschen Bundeswehrdrohne mit einem Personenflugzeug, bei dem die Drohne beinahe ein Personenflugzeug mit ca. 100 Menschen an Bord getroffen hat ([26]).

Auch wenn der autonome Rückflug eine große Gefahr birgt, so bietet er gewisse Möglichkeiten über unbewohnten Gebieten, wie z.B. Meeren, Ozeanen und Urwäldern, bei denen sichergestellt ist, dass keine Gefahr entsteht.

Gezielter Absturz

Aus der Raumfahrt kann man einen weiteren Lösungsansatz für die Mitigations entnehmen. Alte Flugobjekte in der Raumfahrt werden oftmals in einem gezielten Absturz zur Erde gebracht. So wurde 2001 die Raumstation Mir gezielt über dem Pazifischen Ozean in die Umlaufbahn gebracht, um mögliche Schäden durch nicht verglühte Teile zu minimieren. Unter diesem Aspekt kann versucht werden die Drohne in einem gezielten Absturz zum Boden zu bringen. So könnte man versuchen den Boden nach einer passenden Stelle abzusuchen und dort das UAV abstürzen lassen.

Autonomes Landen

Ein weiterer Ansatz, welcher sich in der aktiven Forschung befindet ist das autonome Landen von UAVs. So wird beispielsweise in [27] ein Einstieg in die Thematik geliefert und eine grobe Übersicht an die Anforderungen für eine Lösung der Problematik geliefert.

Dieser Ansatz ist jedoch erst für ein sehr spätes Projektstadium interessant, da die Anforderungen an die Technik immens sind und das UAV soweit sicher fliegen können muss.

5.3 Aussicht

Neben den direkt anstehenden Arbeiten gibt es auch weitere Arbeiten, die in weiterer Zukunft umgesetzt werden können und das System wesentlich erweitern können. So setzen einige der

möglichen Mitigations wesentliche technische Erweiterungen voraus. Dabei basieren einige Maßnahmen auf der Auswertung von Bilddaten und der Entwickeln von Entscheidungen aus diesen Ergebnissen.

So stehen für die Zukunft Themen an, wie Systeme mittels Umgebungskarten und Kommunikationssystemen sich frei, kollisionsfrei und autonom im Raum bewegen können. So wäre ein Ziel, dass Flugzeuge zukünftig autonom Fliegen können, ohne dass ein direkter Überwacher für jedes Flugzeug notwendig ist.

Auch wäre eine automatisierte Analyse bei der Entwicklung sehr hilfreich. So könnte man zukünftig die Architekturmodelle soweit erweitern, dass Tools ein Übersicht über die sicherheitskritischen Komponenten erstellt, auf deren Basis Maßnahmen eingeplant werden können.

Diese Beispielthemen bilden nur einen Einstieg in die mögliche Themen der Sicherheitsanalyse und der unbemannten Luftfahrt. So wurde schon in [27] erwähnt, dass die unbemannte Luftfahrt früher oder später in den zivilen Bereich eintreten wird und den normalen Luftraum nutzen darf. Bevor diese Tage jedoch kommen, werden vermutlich noch einige Arbeiten und Entwicklungen anstehen.

6 Fazit

An diesem Punkt möchte ich noch einmal mein persönliches Fazit zur Arbeit und dem dazugehörigen Projekt treffen.

Die Arbeit war mein persönlicher Einstieg in systematische Analyseverfahren, Sicherheitsanalysen im Allgemeinen und UAVs. Dabei stand ich vor mehreren komplexen und interessanten Themenbereichen, bei denen mir klar wurde, dass bis zum Erreichen des Projektzieles noch viel Arbeit geleistet werden muss. Jedoch sind die möglichen Ergebnisse im Rahmen UAVs auch sehr interessant und ich bin sehr gespannt auf die Zukunft und darauf, wie UAVs später eingesetzt werden.

Bei den Sicherheitsanalysen griff ich zwar auf die Fehlerbaumanalyse zurück, jedoch wären auch noch andere Verfahren interessant, die bei den komplexen System UAV sicherlich angebracht wären. Auch konnte ich während der Arbeit nur begrenzt auf Normen zurückgreifen. Somit könnte ich leider nicht nach den Vorgaben arbeiten, was bei einem späteren System jedoch gemacht werden sollte. Dieses Problem mit den Normen liegt leider an den hohen Kosten und an der fehlenden Verfügbarkeit für Studenten.

Auch ist es unbefriedigend gewesen, aus der Sicht eines Informatikers auf Ausfallmöglichkeiten von Aktoren und andere Elemente zu schauen, an denen man als Informatiker keine Verbesserungen durchführen kann. So würde ich aber auch gerne später mit Leuten aus anderen Themengebieten das System betrachten und analysieren. Daraus würde ich mir eine bessere und detailliertere Sicht auf das System erhoffen, bei der auch andere Aspekte besser betrachtet werden können.

Zusammenfassend muss ich sagen, dass ich die Arbeit nur als Einstieg in den Bereich sehe und ich noch viel Arbeit in dem Bereich sehe.

Literaturverzeichnis

[1] Derfel73 and Pmerson. UML diagrams overview. http://en.wikipedia.org/wiki/File:UML_diagrams_overview.svg, September 2011. abgerufen am 14.08.2013.

[2] Object Management Group. OMG Systems Modeling Language. http://www.omgsysml.org/. abgerufen am 14.08.2013.

[3] Michael32710. Sender einer programmierbaren Funkfernsteuerung. http://commons.wikimedia.org/wiki/File:Remote-control-mc12.jpg, March 2006. abgerufen am 14.08.2013.

[4] Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr. Erprobung des Aufklärungsdrohnensystems „Kleinfluggerät Zielortung“ KZO. http://www.baain.de/, August 2012. abgerufen am 26.08.2013.

[5] The Raspberry Pi Foundation. Raspberry Pi - FAQs. http://www.raspberrypi.org/faqs. abgerufen am 19.08.2013.

[6] Ben Schwan. Drohnen spüren Ölfelder auf. *Technology Review*, July 2013. http://heise.de/-1885458.

[7] Neues Fliegen e.V. Project BWB AC20.30 - Der Versuchsträger. http://ac2030.de/about/. abgerufen am 14.08.2013.

[8] Neil Storey. *Safety Critical Computer Systems.* Addison-Wesley, August 1996.

[9] Bruce Powel Douglass. *Build Safety-Critical Designs with UML-based Fault Tree Analysis.* IBM/Rational, April 2009. https://www.ibm.com/developerworks/community/blogs/BruceDouglass/entry/safety_analysis_with_the_uml8?lang=en.

[10] Andrew S. Tanenbaum. *Computer Networks.* Prentice Hall PTR, fourth edition, 2003.

[11] Gerhard Grießnig, Roland Mader, Christian Steger, and Reinhold Weiss. Design and Implementation of Safety Functions on a Novel CPLD-Based Fail-Safe System Architecture. In *17th IEEE International Conference and Workshops on Engineering of Computer-Based Systems*, pages 206 – 212, March 2010.

[12] Vera Gebhardt, Gerhard M. Rieger, Jürgen Mottok, and Christian Gießelbach. *Funktionale Sicherheit nach ISO 26262 - Ein Praxisleitfaden zur Umsetzung*. dpunkt.verlag GmbH, firsth edition, July 2013.

[13] Stephen B. Johnson, Thomas J. Gormley, Seth S. Kessler, Charles D. Mott, Ann Patterson-Hine, Karl M. Reichard, and Jr. Philip A. Scandura, editors. *System Health Management: with Aerospace Applications*. John Wiley & Sons, firth edition, July 2011.

[14] Oliver Alt. *Modellbasierte Systementwicklung mit SysML*. Hanser Fachbuchverlag, March 2012.

[15] Object Management Group. Introduction To OMG's Unified Modeling Language. `http://www.omg.org/gettingstarted/what_is_uml.htm`, July 2005. abgerufen am 14.08.2013.

[16] Sanford Friedenthal, Alan Moore, and Rick Steiner. *A Practical Guide to SysML: The Systems Modeling Language*. Morgan Kaufmann, September 2009.

[17] Object Management Group. *OMG Systems Modeling Language (OMG SysML™)*, 1.3 edition, June 2012.

[18] Totmanneinrichtung. `http://de.wikipedia.org/wiki/Totmanneinrichtung`. abgerufen am 14.08.2013.

[19] Leslie Lamport and Marshall Pease amd Robert Shostak. The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*, 4:382–401, July 1982. `http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf`.

[20] Bundesministerium der Justiz. Luftverkehrs-Ordnung. `http://www.gesetze-im-internet.de/bundesrecht/luftvo/gesamt.pdf`, March 1999. abgerufen am 14.08.2013.

[21] ITG FOTOFLUG. Lipowarner – bezahlbarer Schutz für die Lipo-Akkus. `http://www.itg-fotoflug.de/lipowarner/`, April 2013. abgerufen am 14.08.2013.

[22] Henry Lorenz. Spektrum Komponenten - Informationen und Erläuterungen zu den verbauten Komponenten von Spektrum sowie zur Belegung der RC-Kanäle. Dokument aus dem AES Projekt, June 2013.

[23] Lars Harmsen and René Büscher. Konzept PWM einlesen - Beschreibung eines Konzeptes zum einlesen der Steuer-PWMs. Dokument aus dem AES Projekt, June 2013.

[24] Henry Lorenz. PWM Erzeugung - Beschreibung der Komponente zur Erzeugung der Aktorik-PWMs. Dokument aus dem AES Projekt, June 2013.

[25] Enrico Hensel. Design und Implementation eines Sicherheitskonzepts für den Betrieb eines autonomen Fahrzeuges. Bachelorarbeit, HAW Hamburg, April 2007.

[26] chs/dpa. Drohne "Luna": Bundeswehr verheimlichte Beinahe-Crash mit Airbus. http://www.spiegel.de/politik/deutschland/drohne-luna-bundeswehr-verheimlicht-beinahe-crash-mit-airbus-a-903 html, June 2013. abgerufen am 26.08.2013.

[27] Luis Mejias, Daniel Fitzgerald, Pillar Eng, and Xi Liu. Forced Landing Technologies for Unmanned Aerial Vehicles: Towards Safer Operations. In Thanh Mung Lam, editor, *Aerial Vehicles*, chapter 21. In-Tech, January 2009. http://dx.doi.org/10.5772/6481.

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, 30. September 2013 Arne Maximilian Richter