Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Ausarbeitung - Anwendung 1

Mosawer Ahmad Nurzai

Technisch sichere Systeme in UAV

Fakultät Technik und Informatik
Studiendepartment Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Mosawer Ahmad Nurzai

Technisch sichere Systeme in UAV

Ausarbeitung - Anwendung 1 eingereicht im Rahmen von Anwendung 1

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

Gutachter: Prof. Dr. Kai von Luck
Gutachter: Prof. Dr. Bettina Buth

Betreuer: Prof. Dr. Thomas Lehmann

Eingereicht am: 06. März 2014

Mosawer Ahmad Nurzai

Thema der Arbeit
Technisch sichere Systeme in UAV

Stichworte
Sicherheit, Safety, UAV, UAS, Unmanned Aerial Vehicle, Unbemanntes Luftfahrzeug, technische Sicherheit, Funktionale Sicherheit, Safety Critical Computer System

Mosawer Ahmad Nurzai

Title of the paper
Technical safe systems in UAV

Keywords
Safety, UAV, UAS, Unmanned Aerial Vehicle, Functional Safety, Safety Critical Computer System

Inhaltsverzeichnis

1 Einführung

1.1 Einleitung

> *„**Safety** can be described as a characteristic of the system of not endangering, or cousing harm to, human lives or the environment in which the equipment or plant operates. [...] safety evaluates system operation in terms of freedom from occurrence of catastrophic failures.“ -Bozzano und Villafiorita [2010]*

In komplexen technischen Systemen spielt die Sicherheit (Safety (1.1) eine wichtige Rolle, denn der Begriff Safety sagt aus, dass weder Menschen noch Umgebung durch dieses System geschädigt bzw. gefährdet werden sollen. Die Prozesse die notwendig sind um Safety zu erlangen, folgen bestimmten Richtlinien und vorgeschriebenen Verfahren, jedoch gibt es nicht für jeden Bereich Normen und Verfahren.
In dieser Arbeit geht es um technisch sichere Systeme in UAV (Drohnen), dabei soll, wie der Titel schon verrät, die Sicherheit (Safety) in Vordergrund treten. In Kapitel 2 werden die Grundlagen zu Safety eingeführt. Kapitel 3 stellt den Hauptteil der Arbeit dar, es werden aus verschiedenen Blickwinkel Safety in UAV/technischen System vorgestellt. Zum Schluss, in Kapitel 4, gibt es eine Zusammenfassung und einen Ausblick.

1.2 Motivation

Abbildung 1: Nurflügler
Quelle: http://www.ac2030.de

In der hochschulinternen Forschungsgruppe BWB-AES (Airborne Embedded Systems) arbeiten viele Departments unter anderem Fahrzeug- und Flugzeugbau und Informatik am Großraumflugzeug/Drohne BWB 20.30 Nurflügler (1). Hauptmotivation ist der spätere Einsatz für den Katastrophenschutz.
Neben den hochschulinternen Aktivitäten und Interessen bieten Drohnen, abseits vom militärischen Kontext, weitere interessante Einsatzgebiete. Die Nutzung von UAV im zivilen und staatlichen Räumen findet immer mehr Anklang (DeGarmo [2004]):

- **Landwirtschaft und Wildnis:** Erntebeobachtung, Bekämpfung von Waldbränden.
- **Erdwissenschaft:** Messung der Erde, Geographische Prozesse bei Naturkatastrophen.
- **Heimatschutz:** Grenzschutzüberwachung (Drogenschmuggler, Spionage).
- **Zivilbevölkerung / staatliche Interesse:** Überwachung zivile Bevölkerung in kritischen Orten/Situationen, Rettungsaktionen (Hilfe für Polizei).
- **Kommerziell:** Filmindustrie, Nachrichtenerstattung, Fischjagd.

Es entstehen durch diese verschiedenen Einsatzgebiete, verschiedene Anforderungen an technische Systeme für UAV. Der Aspekt von Safety bzw. funktionaler Sicherheit/Anforderung soll betrachtet werden.
Am Fall des Jungfernflugs der Ariane 5 am 04.06.1996, kann festgestellt werden, wie wichtig der Safety-Aspekt in technischen Systemen ist. Wenige Sekunden nach dem Startflug explodierte die Ariane 5. Das Problem war die Nutzung der alten Software der Ariane 4 (Ariane5 [2013]). Durch ordnungsmäßige Sicherheitsverfahren wäre ein Fehler im Zusammenspiel von Hard- und Software entdeckt wurden. Aus diesen Gründen ist es wichtig bei technisch kritischen Systemen den Safety-Aspekt nicht zu vernachlässigen.

2 Grundlagen

In diesem Kapitel sollen einige Grundlagen bzgl. Safety aufgezeigt werden, der Bezug zu UAV wird ebenfalls gestellt.

2.1 Begriffe

- **UAS:** UAS steht für *Unmanned Aerial System* und besteht aus dem UAV (*Unmanned Aerial Vehicle*) und zusätzlichen Elementen, wie z.B. der Bodenstation. Das Zusammen-

spiel zwischen UAV und den zusätzlichen Elementen, die für ordnungsmäßigen Ablauf notwendig sind, beschreiben also das UAS.

- **Safety:** Safety ist die Freiheit von unvertretbaren Risiken (nach DIN EN 61508-4). Siehe auch 1.1.
- **Safety-Critical/Related Computer System:** Ein Safety-Critical/Related Computer System ist ein System welches die Sicherheit der Ausstattung/Geräte und des Betriebs, im Sinne von Safety, garantiert. Critical und Related im Begriff werden oft als Synonyme verwendet, jedoch in einigen Fällen, wird zur Unterscheidung, ein System welches hoch kritisch ist, Safety-Critical Computer System genannt (Storey [1996]).
- **Funktionale Sicherheit:** „Teil der Gesamtsicherheit, bezogen auf das EUC [..], die von der korrekten Funktion des elektrischen/elektronischen/programmierbaren elektronischen-sicherheitsbezogenen Systems, [..] zur Risikominderung abhängt (Storey [1996])."

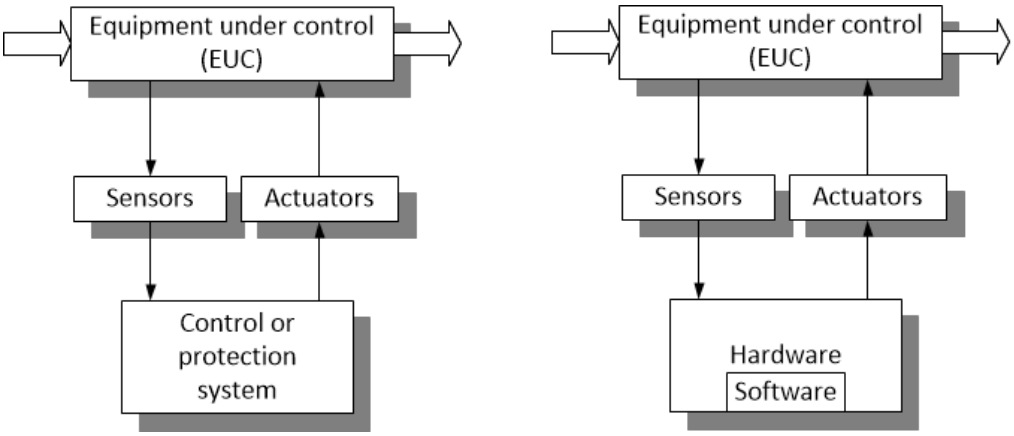

Abbildung 2: EUC Sicherheit
Quelle: Storey [1996]

In Abbildung 2 sieht man eine die (Sicherheits-)Kontrolle eines sogenannten „Equipment under control (EUC)". Das EUC kann abstrakt gesehen, alles mögliche Technische sein, ein einfacher Schalter bis hin zu einer komplexen Nuklearanlage. Durch Sensoren werden Eingaben des EUC aufgenommen und an ein Kontroll- oder Schutzsystem weitergeleitet. Je nach Eingabe wird entschieden ob Aktoren individuelle Aktionen durchführen müssen, um die Sicherheit im Sinne von Safety zu gewährleisten. Das Kontroll- oder Schutzsystem kann ebenfalls durch Hard- und Software gesteuert werden.

2.2 Safety-Critical Computer Systems

Ein UAV ist ein Safety-Critical Computer System, denn es verfügt über mehrere Komponenten, die bei einer nicht korrekten Ausführung dazu führen können, dass das UAV mit hoher Wahrscheinlichkeit seine Umgebung inklusive Menschen verletzten könnte (2.1).
Eines der Ziele von Safety-Critical Computer Systems ist das Erlangen von Safety und Reliability (Zuverlässigkeit) des Systems mit seinen Komponenten. Zuverlässigkeit ist die Wahrscheinlichkeit des Funktionieren eines Systems, einer Komponente über einen gegebenen Zeitraum unter einer gegebenen Menge von Bedingungen (nach Spezifikation) (Storey [1996]). Es herrscht jedoch ein Konflikt zwischen Safety und Reliability, möchte man mehr Safety, so müssen Abstriche in Reliability getan werden und umgekehrt. Das Finden eines Mittelmaßes zwischen Safety und Reliability ist eines der Kernaufgaben von Hazard und Risiko Analysen (Storey [1996]). Nach De Garmo kann Zuverlässigkeit durch zwei essentielle Wege erreicht werden: Verbessern der Integrität der Komponenten und des Systems und/oder Redundanzen für Komponenten einbauen (DeGarmo [2004]). Es folgt eine Auflistung von Hazard-Analysen und im Hauptteil der Arbeit wird auf die Erhöhung der Zuverlässigkeit eingegangen.

Hazard Analysen

Um kurz auf die Hazard Analysen einzugehen muss erklärt werden was ein Hazard ist. **Hazard** ist die tatsächliche oder potentielle Gefahr für Mensch oder Umgebung (Storey [1996]). Hazard Analysen dienen zur Identifikation von Gefahren (Storey [1996]):

- **FMEA (Failure modes and effects analysis):** Textuelle Methode, betrachtet Störung von jeder Komponente im System und verfolgt Auswirkung dieser Störung um die Folge/Konsequenz zu bestimmen.
- **HAZOP (Hazard and operability studies):** Textuelle Methode, durch Nutzung von sogenannten „Guide Words“ werden Effekte bei Abweichung vom normalen Betriebszustand untersucht.
- **ETA (Event tree analysis):** Grafische Methode, eventbasierte Methode: Events werden aufgestellt, um Auswirkung bzw. Einflüsse des System zu bestimmen.
- **FTA (Fault tree analysis):** Grafische Methode, eventbasierte Methode: Ähnlich wie ETA, jedoch arbeitet es rückwärts, in dem es alle Hazard identifiziert, um mögliche Ursache zu bestimmen.

Die textuellen Methodiken dienen (oft) als Input für die grafischen Methodiken. Im Hauptteil erfolgt eine Veranschaulichung einer Hazard-Analyse.

3 Technisch sichere Systeme in UAV

In diesem Kapitel wird der Zusammenhang zwischen Safety und technischen Systemen/UAV hergestellt, dabei wird der Safety-Aspekt aus verschiedenen Blickwinkel betrachtet: hardware-nah, software-nah, Safety in UAV und eine konkrete Nutzung einer Analyse-Methodik, um Safety zu erhöhen.

3.1 Hardware-nah

In technischen Systemen werden häufig Mikrocontroller eingesetzt. Um Mikrocontroller in sicherheitskritischen Applikationen benutzen zu können gibt es verschiedene Methodiken diese vorzubereiten. Durch Derating (Lastminderung) können Mikrocontroller so vorbereitet werden, dass sie in kritischen bzw. „rauen“ Umgebungen (Bedingungen) arbeiten können. Derating ist: „eine Komponente in seinen Leistungsgrenzen im Betrieb zu nehmen, um die Ausfallrate zu reduzieren“ oder „eine Komponente in so einer Weise zu benutzen, dass die angewandten Belastungen kleiner sind als die maximale Ausfallrate“ (Forsberg und Manefjord [2007]). Ziel des Derating ist es die Zuverlässigkeit der Komponenten zu erhöhen, außerdem kann durch Derating die Robustheit von Komponenten getestet und in Erfahrung gebracht werden. Es gibt verschiedene Derating-Parameter die verändert werden können, um Zuverlässigkeit zu garantieren und Robustheit zu prüfen.

- **Spannung:** Robustheit der Komponente erhöhen. Spannung nach Spezifikation im minimalen und maximalen Bereich halten, sonst Hardware-Fehler.
- **Frequenz:** Robustheit der Komponente erhöhen.
- **Temperatur:** Kontroverser Parameter, jedoch oft Überschreitung in rauen Umgebungen. Maximum-Temperatur darf nicht überschritten werden.
- **Stromstärke:** Zuverlässigkeit der Komponente wird erhöht.
- **Zeit:** Robustheit der Komponente erhöhen. Beispielsweise ein Signal ist stabil nach 5 ns, so soll je nach Spezifikation eine gewisse Zeit gewartet werden bis das Signal gelesen werden soll.

In Mikroprozessor-Umgebungen ist noch zusätzlich auf die Spezifikation der einzelnen Komponenten zu achten, da beispielsweise oft niedrige und unterschiedliche Spannungen herrschen. Die Hersteller liefern Parametereinstellungen für ihre Komponenten, dies ist zu berücksichtigen, um die Komponenten sicher, im Sinne von Safety, zu halten (Forsberg und Manefjord [2007]).

3.2 Software-nah

Die Nutzung von Pattern ermöglicht es eine (einfache und schnelle) Lösung für häufig auftretende Design-Probleme in Applikationen zu finden. In Safety-Critical Computer Systemen können ebenfalls verschiedene Pattern genutzt werden, um Safety, Zuverlässigkeit, Robustheit etc. zu garantieren. In Kumar u. a. [2011] wurde bei einem Vier-Finger-Roboter, welches ein Safety-Critical System ist, nach Anwendung von Hazard- und Risiko-Analysen verschiedene Software-Pattern eingesetzt. Die Pattern sollen dafür sorgen, die Hazards und Risiken welche im Analyseverfahren entdeckt wurden zu mildern oder zu tilgen.

3.2.1 N-Version Programming Pattern

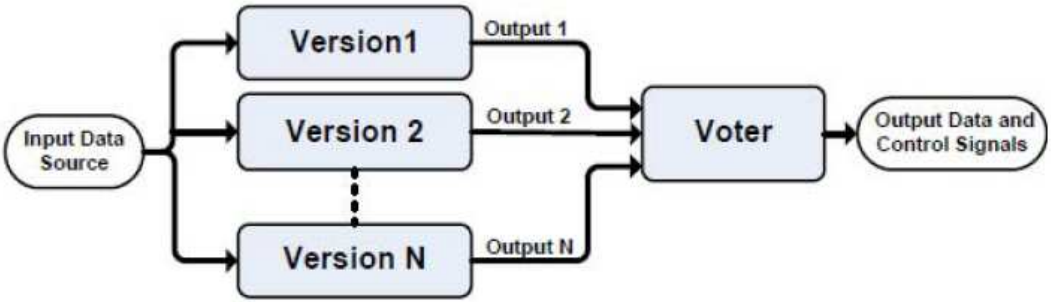

Abbildung 3: N-Version Programming Pattern
Quelle: Kumar u. a. [2011]

In Abbildung 3 ist das N-Version Programming Pattern zu sehen. Ziel dieses Pattern ist es die Zuverlässigkeit und Safety einer Komponente im System zu erhöhen. Verschiedene Programmierteams entwickeln unabhängig von einander N-Versionen (anhand von Spezifikationen) einer Applikation. Bester Output wird einem sogenannten Voter übergeben. Der Voter wählt korrektesten dieser Outputs anhand von Voting Techniken aus. Nachteile dieser Methodik ist, dass es zusätzliche Kosten entstehen. Es werden N-unabhängige Hardware benötigt und bei Modifizierung müssen alle Versionen modifiziert werden.

3.2.2 Protected Single Channel Pattern

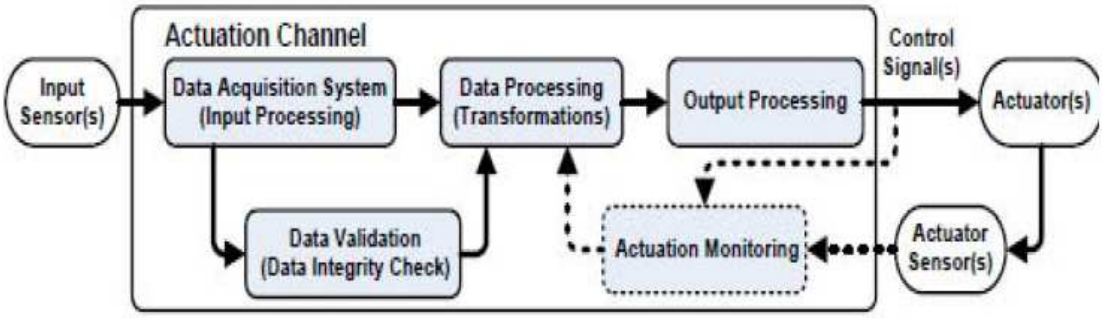

Abbildung 4: Protected Single Channel Pattern
Quelle: Kumar u. a. [2011]

In Abbildung 4 ist das Protected Single Channel Pattern abgebildet. Durch dieses Pattern soll Safety bei Fehlererkennung erhöht werden. Eintreffende Input-Daten werden verarbeitet und beispielsweise durch CRC validiert. Es ist möglich den Output/die Output-Befehle zusätzlich zu validieren, sind die Output-Daten korrekt, so können diese an Aktoren weitergeschickt werden. Für Re-Konfiguration werden Aktionen des Aktor durch Aktorsensoren erfasst. Die Ergebnisse der Sensoren werden an ein Actuation Monitoring weitergegeben, der die Daten auswertet und Aktorenoutputs ggf. (re)konfiguriert. Nachteil dieser Methodik sind erhöhte Kosten, da zusätzlich Sensoren und verschiedene Validationeinheiten benötigt werden, außerdem ist das Pattern nicht geeignet für persistente Fehler, also Fehler die ständig auftauchen und nicht behoben werden können, denn bei so einem Fehler kann das System nicht Safety weiter operieren.

3.3 Safety in UAV

Safety und Zuverlässigkeit zu garantieren ist in der Konstruktion eines UAV zu berücksichtigen. In Uhlig u. a. [2006] wird explizit auf diese Thematik eingegangen. Studien haben ergeben, dass UAV signifikant höhere Ausfallraten als bemannte Fluggeräte haben (Uhlig u. a. [2006]). Ursache ist der mangelnde Einsatz von Safety-Analysen. Diese werden aus Kostengründen nur sporadisch/oberflächig durchgeführt.
In der Konstruktion von UAV kann man auf die Benutzung von Komponenten, die auf den freien Markt (COTS: Commercial off-the-shelf) erhältlich sind zugreifen. Sie verschaffen einem Vorteile, jedoch entstehen auch Nachteile. Vorteile von Benutzung solcher Komponenten sind, dass sie weniger kosten, sie verfügen über verschiedene Schnittstellen um Eingaben vorzubereiten/einzugeben und liefern somit auch Ausgaben, die nach Spezifikation gedeutet werden

können. Die Benutzung solcher Komponenten ist auch zeitsparend, da sie nicht erst neu entwickelt werden muss. Die Komponente kann auch wiederverwendet werden. Nachteile von solchen Komponenten sind, dass man eine Art Blackbox hat, denn man kennt nicht das Innenleben und die exakte Arbeitsweise im Gegensatz zu einem FPGA oder Mikrocontroller. Da das genaue Verhalten nicht exakt bestimmt werden kann, sind viele Tests notwendig. Firmen wie Cloud Cap Technology (http://www.cloudcaptech.com, Athena Controls (http://www.athenacontrols.com/) und Micropilot (http://www.micropilot.com/) bieten solche Hard-/Software an.
In Uhlig u. a. [2006] ist eines der Hauptbestandteile des UAV der Piccolo SL von Cloud Cap Technology.

Abbildung 5: Piccolo SL
Quelle: http://www.cloudcaptech.com

Der Piccolo SL ist ein Autopilot, welcher 14 konfigurierbare GPIOs, Flugsensoren, Navigationssystem und Wireless Kommunikation besitzt. Die UAV kann durch eine Bodenstation koordiniert werden.
In Uhlig u. a. [2006] wurden mit Hilfe von Hazard-Analysen die Safety Critical Komponenten ermittelt, somit können Hazard-Analysen als einer der erste Schritte genutzt werden, um Safety zu garantieren. Folgende Komponenten werden als kritisch betrachtet: Steuerfläche, Backup Board, die Piccolo-Funkverbindung, Flugwerk und Flugtests. Drei Schritte wurden festgelegt, um Safety und Zuverlässigkeit zu gewährleiten.

- **Operative Verfahren zur Sicherheitsmaßnahme:** In diesen Verfahren werden hauptsächlich operative Maßnahmen getätigt. In der Regel werden keine technischen Mittel benutzt, sondern es werden verschiedene Ablaufpläne abgearbeitet und deren Ergebnisse aufgezeichnet. Beispiele: Checklisten (für Verbindungen von Komponenten), detaillierte Flugpläne.

- **Sicherheitsmaßnahmen für Design und Einrichtung:** Bei dieser Sicherheitsmaßnahme spielt der Einsatz von technischen Mittel auch eine Rolle. Einheiten, Komponenten bzw. Geräte werden zusätzlichen nach Vorschriften und Standards gesichert. Zusätzlich kann der Einsatz von Checklisten den Grad der Sicherheit erhöhen. Beispiele: Sicherheitsgurte, Isolationen.
- **Redundanz:** Bei dieser Maßnahme werden Redundanzen eingesetzt, sprich es werden zusätzliche, meist identische Geräte eingesetzt. Beim Ausfall der Hauptkomponente wird durch verschiedene Mechanismen die redundante Komponente eingeschaltet und benutzt. Hauptnutzen dieser Maßnahme ist die Erhöhung der Zuverlässigkeit des Systems.

Durch Kombination dieser Verfahren kann ein besserer, intensiver Effekt auftreten. Die Nutzung der Verfahren kann in der Konstruktion des eigenen sicheren UAV eine wichtige Rolle spielen. Eines der Ziele, die in Uhlig u. a. [2006] angestrebt wird ist eine Flight-Time to Failure (MFTF) von 30 Stunden.

Anwendung: Nutzung von FTA

Aus der gleichen Arbeitsgruppe, die das Paper Uhlig u. a. [2006] verfasst hat, stammt eine Thesis bezüglich der Milderung von UAV Bodenstoß Gefahr durch Fault-Tree Analyse (FTA) (Bhamidipati [2007]). Es soll aufgezeigt werden, wie durch FTA eine Sicherheitsanalyse statt finden kann. Die Nutzung von Komponenten, die auf den freien Markt erhältlich sind, spielen bei der Thesis eine Rolle. Der Piccolo SL wird genutzt (5) in einer vorhandenen Testumgebungsplattform im Labor. Vorteil ist das Testen ohne tatsächlichen Einsatz, um schwer auftretende Schäden zu vermeiden. Nachteil hingegen ist das Testen in verschiedenen Umgebungen.

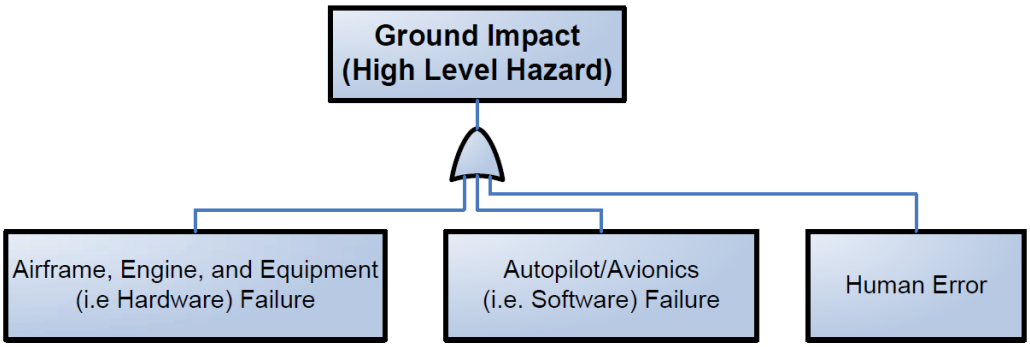

Abbildung 6: FTA - Hazard - Analyse
Quelle: Bhamidipati [2007]

In der Abbildung 6 sieht man ein Fault-Tree. Er beschreibt abstrakt den „Ground-Impact-Hazard“. Jeder der Kästen beschreibt ein Event. An höchster Stelle steht das Hauptevent, welches den Hazard beschreibt. Es werden weitere Events jeweils mit „und“ oder „oder“ verbunden. In diesem Beispiel findet ein Bodenstoß statt, wenn es ein „Airframe, Engine, and Equipment (i.e. Hardware) Failure“-, „Autopilot/Avionics (i.e. Software) Failure“- oder „Human Error“-Event statt findet. Die einzelnen Events bilden jeweils einen Unter(-Fault)-Baum. Beispielsweise wurde durch die Analyse ermittelt, dass die Piccolo SL Funkverbindung ein Single-Point-of-failure ist, welches durch eine Redundanz gelöst werden konnte, jedoch im weiteren Verlauf wurde die Redundanz entfernt, da die Zuverlässigkeit der jeweiligen Software nicht bestimmt werden kann. Die Software-Komplexität erhöht sich und daraus könnten sich weitere gravierende Fehler entwickeln.

4 Schluss

Diese Arbeit hat einen Einblick über technisch sichere Systeme verschaffen, dabei wurden einige Grundlagen zu Safety dargestellt. Grundlage für die Arbeit dienten hauptsächlich die Arbeiten von Uhlig u. a. [2006], Bhamidipati [2007], Forsberg und Manefjord [2007] und Kumar u. a. [2011].
Technische Systeme wurden aus der Hardware- und der Software-Perspektive betrachtet. Aus der HW-Perspektive wurden verschiedene physikalische Parameter betrachtet. In der SW-Perspektive wurden zwei Pattern betrachtet, die jeweils eingesetzt werden um Safety von Komponenten zu erhöhen. Der Einsatz von sicheren Systemen in UAV wird anhand eines Beispiels beschrieben, dabei werden verschiedene Sicherheitsmaßnahmen beschrieben, die in der Konstruktion des UAV notwendig sein können, um die Safety und Zuverlässigkeit zu erhöhen.

Ausblick

Die Arbeit kann als Einstieg für die Konstruktion von sicheren Systemen (in UAV) dienen. Für die Entwicklung einer Sicherheitsarchitektur im UAV können die Kenntnisse in dieser Arbeit als erste Grundlage dienen. Für die Entwicklung der Sicherheitsarchitektur muss ebenfalls geklärt werden was für technische Komponenten ausgewählt werden. Die technischen Komponenten müssen bewertet werden. Welche Vor- und Nachprozesse sind notwendig für die Entwicklung der Sicherheitsarchitektur. Standardisierte Sicherheitsanalyseverfahren (ISO 26262) können beispielsweise als Vorprozess dienen. Verschiedene Testverfahren können als Nachprozesse dienen. Inwieweit spielt die Betrachtung des UAS (Unmanned Aerial System) bei der Konstruktion der Sicherheitsarchitektur des UAV eine Rolle? Die Frage muss nach

Analyse-Verfahren beantwortet werden.
Einige Probleme sind nicht vermeidbar, die Anzahl von verfügbaren Material zu UAV bezüglich Safety ist gering. Aus Sicherheits- und Konkurrenzgründen wird kaum Material von Staaten und Industrie zur Verfügung gestellt. Alternativen bieten Safety-Standards aus anderen Branchen, beispielsweise der Industriebranche oder es wird ausgewichen auf universitäre Arbeitsgruppen.

Literatur

[Ariane5 2013] : *Ariane 5 Absturz*. 2013. – URL http://www.wikiservice.at/dse/wiki.cgi?Ariane5Absturz

[Bhamidipati 2007] Bhamidipati, K.K.: *Mitigating the UAV Ground Impact Hazard Using Fault-tree Analysis and a Fuel Consumption Model*. University of Illinois at Urbana-Champaign, 2007. – URL http://books.google.de/books?id=6zdaXwAACAAJ

[Bozzano und Villafiorita 2010] Bozzano, Marco ; Villafiorita, Adolfo: *Design and Safety Assessment of Critical Systems*. CRC Press Taylor & Francis Group, 2010

[DeGarmo 2004] DeGarmo, Matthew T.: Issues Concerning Integration of Unmanned Aerial Vehicles in Civil Airspace. (2004). – URL http://www.mitre.org/sites/default/files/pdf/04_1232.pdf

[Forsberg und Manefjord 2007] Forsberg, H. ; Manefjord, T.: Derating concerns for microprocessors used in safety critical applications. In: *Digital Avionics Systems Conference, 2007. DASC '07. IEEE/AIAA 26th*, 2007, S. 2.C.2–1–2.C.2–8

[Kumar u. a. 2011] Kumar, S. P. ; Ramaiah, P. S. ; Khanaa, V.: Architectural patterns to design software safety based safety-critical systems. In: *Proceedings of the 2011 International Conference on Communication, Computing & Security*. New York, NY, USA : ACM, 2011 (ICCCS '11), S. 620–623. – URL http://doi.acm.org/10.1145/1947940.1948069. – ISBN 978-1-4503-0464-1

[Storey 1996] Storey, Neil R.: *Safety Critical Computer Systems*. Boston, MA, USA : Addison-Wesley Longman Publishing Co., Inc., 1996. – ISBN 0201427877

[Uhlig u. a. 2006] Uhlig, D. ; Bhamidipati, K. ; Neogi, N.: Safety and Reliability Within UAV Construction. In: *25th Digital Avionics Systems Conference, 2006 IEEE/AIAA*, 2006, S. 1–9

Abbildungsverzeichnis