SYSTEMARCHITEKTUR FÜR UNBEMANNTE FLUGSYSTEME MIT COTS-KOMPONENTEN UNTER ZERTIFIZIERUNGSRANDBEDINGUNGEN

M. Gruber, H. Flühr, K. Kainrath, E. Knoll, A. Gruber*, M. Artner*
Studiengang Luftfahrt, FH JOANNEUM, Alte Poststr. 149, Graz, Österreich
*TTTech Computertechnik AG, Schönbrunner Str. 7, Wien, Österreich

Zusammenfassung

Im Rahmen eines aktuellen Luftfahrtprojekts wird ein Konzept für die drahtlose Datenkommunikation mit unbemannten Flugsystemen erarbeitet. Dieses System besteht aus Fluggerät, Bodenstation und Datenlink. In diesem Beitrag wird eine mögliche Architektur für ein hochverfügbares, echtzeitfähiges Gesamtsystem vorgestellt. Zur Anwendung kommt dabei ein zeitgesteuerter Datenbus, der mit den über die Luftschnittstelle hinweg verteilten Rechnerknoten ein skalierbares System bildet. Die eingesetzte Hard- und Software ist kommerziell verfügbar und erfüllt im Hinblick auf eine mögliche Zertifizierung die Anforderungen der in der Luftfahrt derzeit anwendbaren Richtlinien. Die Beurteilung des Architekturvorschlags hinsichtlich Ausfallwahrscheinlichkeit erfolgt anhand der Fehlerbaumanalyse. Die Ergebnisse zeigen die grundsätzliche Einsetzbarkeit des Systems, Gefahren- und Verbesserungspotentiale werden aufgezeigt.

1. EINLEITUNG

Unbemannte Flugsysteme (UAS), bestehend aus unbemanntem Fluggerät (UAV), Bodenkontrollstation (GCS) und Luft-Boden-Datenlink gewinnen im militärischen, als auch im zivilen Anwendungsbereich stark an Bedeutung. Das Gesamtsystem muss im Hinblick auf die Flugsteuerung, die Flugsicherung, die Kollisionsverhinderung und für die Mission selbst hohe Sicherheitsansprüche erfüllen. Im Rahmen des nationalen Luftfahrtprojekts „CertLink“ wird erforscht, wie die Systemarchitektur eines UAS unter Verwendung von kommerziell verfügbaren Komponenten ausgelegt werden muss, um auch über die Luftschnittstelle hinweg ein hochverfügbares Gesamtsystem zu erhalten.

2. SYSTEMKONZEPTION

2.1. Systemanforderungen

Die Zertifizierung eines UAS ist derzeit nicht einheitlich geregelt. Die Vorbereitung auf eine mögliche zukünftige Zertifizierung soll jedoch durch nachweisliche Robustheit erfolgen. Diese „Zertifizierbarkeit“ soll durch Einhaltung folgender standardisierter Entwicklungsprozesse gewährleistet sein [1]-[5]:

- ARP 4754/ED-79
  (System Development Process)
- ARP 4761/(ED-135)
  (Safety Assessment Process)
- DO-254/ED-80
  (Design Assurance Guidance for Airborne Electronic Hardware)
- DO-178B/ED-12B
  (Software Considerations in
  Airborne Systems and Equipment Certification)

In Anlehnung an die Functional Hazard Analysis (FHA) nach SAE ARP 4754/EUROCAE ED-79 wird eine Gesamtarchitektur konzipiert, die im Hinblick auf Design Assurance Level (DAL) A eine geforderte Ausfallwahrscheinlichkeit von $<10^{-9}$ pro Flugstunde erfüllt.

2.2. Systemarchitektur

Für die Vernetzung der Systemkomponenten wurde eine im Luftfahrtbereich etablierte, zeitgesteuerte Technologie gewählt [7]. Der TTP-Datenbus (Time Triggered Protocol) findet unter anderem bereits Anwendung im Kabinendrucksystem des Airbus A380, im Energieversorgungssystem der Boeing 787, oder auch in der Triebwerksreglung der Lockheed Martin F-16. Er ermöglicht eine zuverlässige und deterministische Kommunikation, sowie die Integration von sicherheitsrelevanten und nicht sicherheitsrelevanten Systemen im Netzwerk. Boden- als auch luftseitig ist die Verwendung von kommerziell verfügbaren Computern mit einem PowerPC und integriertem TTP-Controller vorgesehen, beispielsweise im PMC-Formfaktor (BILD 1). Der TTP-Chip erfüllt dabei die Anforderungen aus DO-254 und DO-178B.

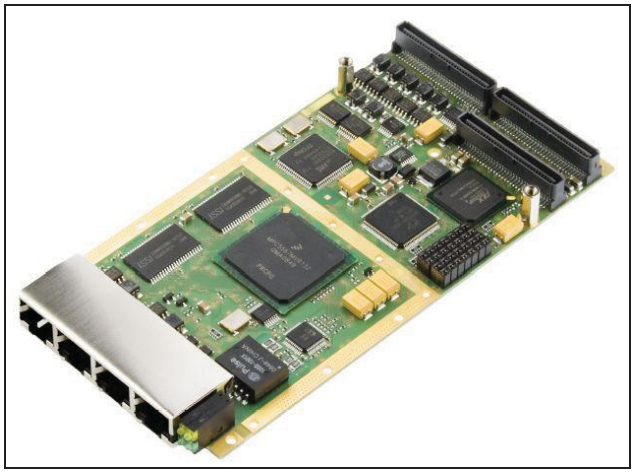

BILD 1. TTP PMC Karte von TTTech [8]

Für den Datenlink kommt ein derzeit in Entwicklung befindliches Modem zum Einsatz. Mittels Software Defined Radio (SDR) wird für die Signalübertragung ein Orthogonales Frequenzmultiplexverfahren (OFDM) auf einem FPGA (Field Programmable Gate Array) implementiert.

Unter diesen Randbedingungen werden mögliche Systemarchitekturen betrachtet. Bei einer linearen Busstruktur lassen sich die beiden Enden des bodenseitigen Busses mit zwei redundanten, drahtlosen Datenlinks erweitern. So kann der Bus über die Luftschnittstelle hinweg mit bis zu zwei weiteren Ästen mit bordseitigen Rechnereinheiten fortgeführt werden. Bei Verwendung von nur einem Datenlink ergibt sich ein Gesamtsystem wie in BILD 2 dargestellt.

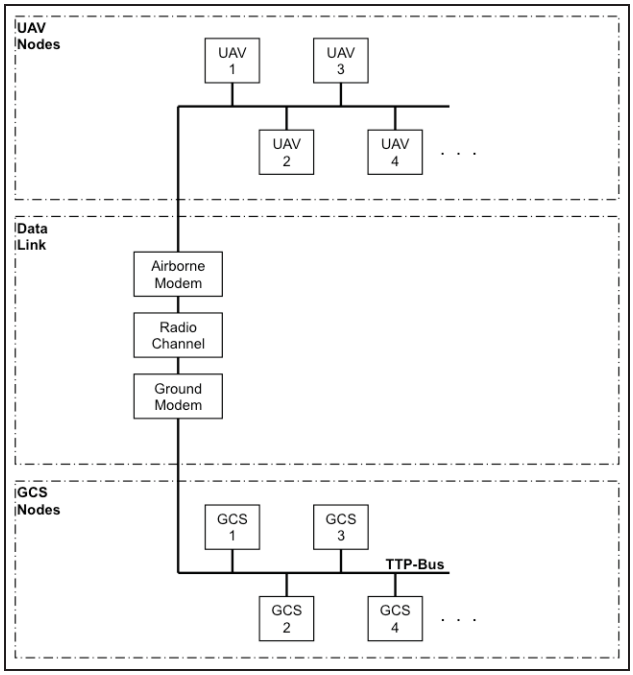

BILD 2. Gesamtarchitektur in Bus-Topologie mit einer Luftschnittstelle

Werden hingegen zwei Luftschnittstellen verwendet ergibt sich eine U-förmige Struktur, wie in BILD 3 ersichtlich. Eine Skalierbarkeit des Systems ist durch Variation der Anzahl von Rechnerknoten gegeben.

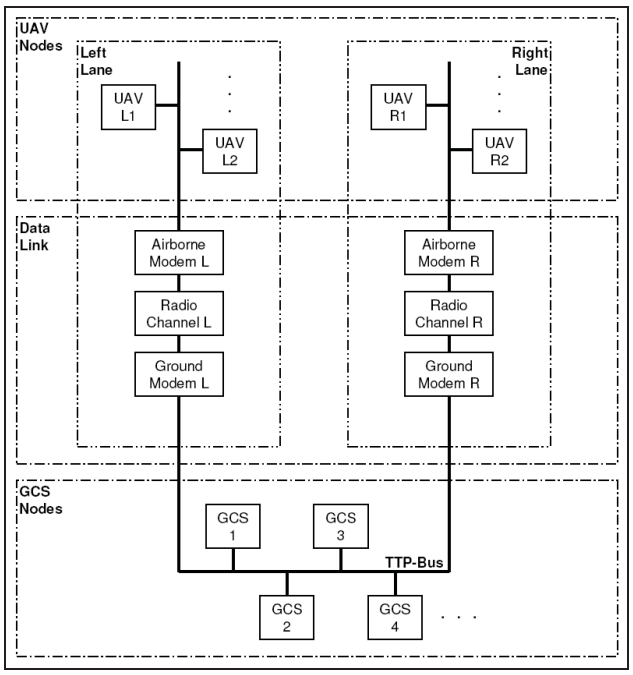

BILD 3. Gesamtarchitektur in Bus-Topologie mit zwei Luftschnittstellen

2.3. Systemanalyse

Der Architekturvorschlag wird mittels Fehlerbaumanalyse (FTA) verifiziert. Die Methode ist in mehreren Standards beschrieben, wie in SAE ARP 4761 für die Zivilluftfahrt oder in MIL-HDBK-338B (Electronic Reliability Design Handbook) für militärische Systeme. Auch in zahlreichen Softwareprodukten wird diese Vorgehensweise für die Zuverlässigkeitsbewertung herangezogen. Auf das vorliegende System angewendet ergibt sich BILD 4 für die Gesamtbetrachtung. Ein Systemausfall tritt bei Versagen der Bodenkontrollstation oder bei Verlust aller Luftschnittstellen auf.

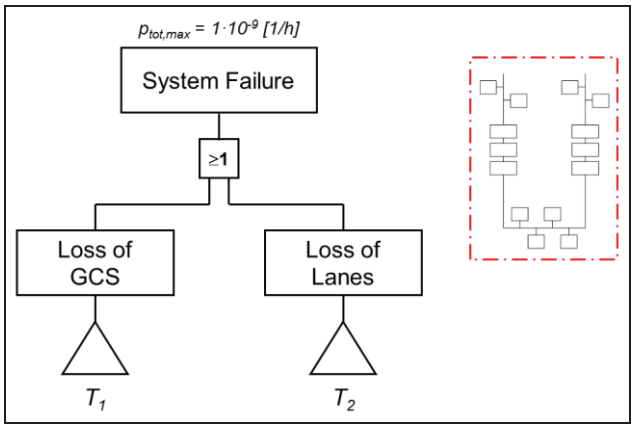

BILD 4. Fehlerbaumanalyse, Gesamtsystem

Ein Ausfall der Bodenkontrollstation kommt durch Versagen sämtlicher GCS-Rechner zustande (BILD 5).

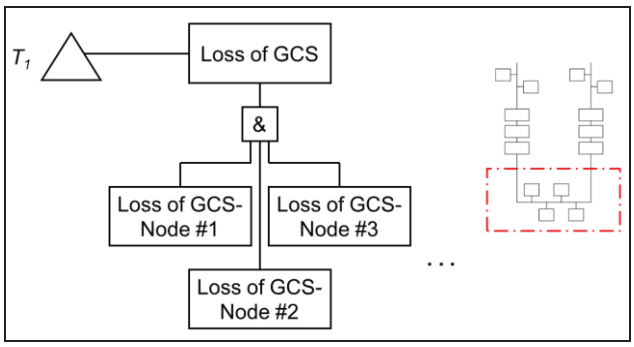

BILD 5. Fehlerbaumanalyse, Bodenkontrollstation

Fällt ein Datenlink oder ein bordseitiges System aus, so hat dies das Versagen einer Luftschnittstelle zur Folge (BILD 6).

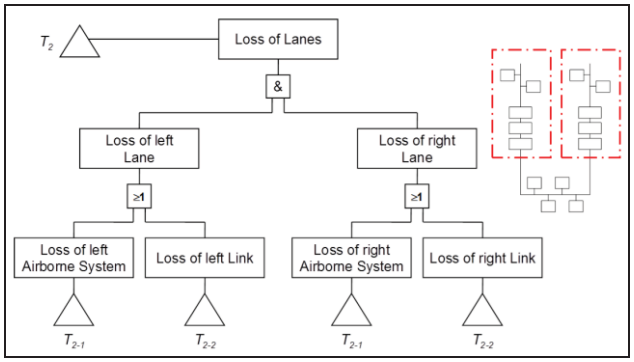

BILD 6. Fehlerbaumanalyse, Luftschnittstellen

Wenn an Bord des UAV's alle Knoten einer Lane versagen, bedeutet dies den Ausfall der jeweiligen Luftschnittstelle (BILD 7).

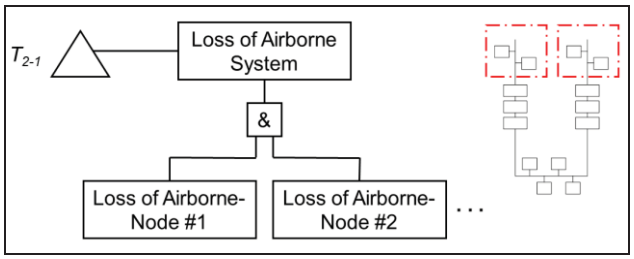

BILD 7. Fehlerbaumanalyse, UAV-Rechner

Für den fehlerfreien Betrieb eines Datenlinks sind zwei funktionstüchtige Modems, eine bestehende Funkverbindung und ausreichender Empfang notwendig (BILD 8).

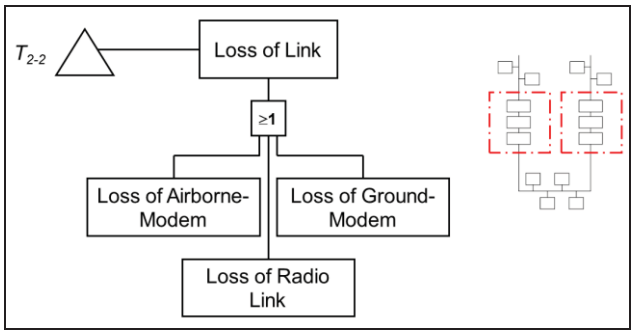

BILD 8. Fehlerbaumanalyse, Datenlinks

Für die Abschätzung der maximal zulässigen Fehlerraten der Einzelkomponenten wird zunächst die Annahme getroffen, dass alle Systemelemente aus BILD 3 und BILD 3 dieselbe Ausfallwahrscheinlichkeit besitzen:

(1) $p = p_{GCS\text{-}Node} = p_{UAV\text{-}Node} = p_{Modem} = p_{Channel}$.

Mit Hilfe der logischen Verknüpfungen aus BILD 4 bis BILD 8 ergibt sich dadurch für das Gesamtsystem:

(2) $p_{tot} = p^g + (p^u + 3p)^l$

Wobei gilt:

– g… Anzahl der GCS-Knoten
– u… Anzahl der UAV-Knoten pro Luftschnittstelle
– l… Anzahl der Luftschnittstellen (Lanes)

Als Anforderung aus 2.1 gilt weiters:

(3) $p_{tot} \leq 10^{-9} \cdot 1/h$

Durch Auflösen der Gleichungen (2) und (3) erhält man somit je nach Konstellation unterschiedliche Maximalwerte für die zulässige Ausfallwahrscheinlichkeit p.

3. ERGEBNISSE

Aus der Berechnung der maximalen Fehlerraten und MTBF-Werte (mittlere Betriebsdauer zwischen Ausfällen) der Einzelkomponenten nach 2.3 gehen für eine Luftschnittstelle folgende Forderungen hervor:

Anzahl der			Max. Fehlerrate p [10^{-9}·1/h]	Min. MTBF [10^{9}·h]
Lanes l	UAV-Knoten pro Lane u	GCS-Knoten g		
1	1	1	0,2	5
	1	2	0,25	4
	2	1	0,25	4
	2	2	0,333	3
	2	4	0,333	3
	4	2	0,333	3
	4	4	0,333	3

TAB 1. Ergebnis der Fehlerratenabschätzung für eine Luftschnittstelle

Es wird deutlich, dass bei Verwendung von nur einer Luftschnittstelle jede Komponente des Datenlinks einen Single Point of Failure (SPOF) darstellt. Fällt eine solche Komponente aus, so hat dies den Ausfall des Gesamtsystems zur Folge. Anders formuliert müsste die Einzelkomponente eine geringere Ausfallwahrscheinlichkeit als das Gesamtsystem besitzen, oder im Falle einer einzigen solchen Stelle zumindest die gleiche. Dies widerspricht natürlich dem Redundanzgedanken bei einem hochverfügbaren System. Solche Konstellationen sind daher nicht zweckmäßig anwendbar und in den Tabellen ausgegraut.

Die Fehlerbaumanalyse zeigt damit, wie in TAB 2 ersichtlich, als realistische Mindestanforderung für die Einhaltung der geforderten Ausfallwahrscheinlichkeit des Gesamtsystems: 2 Luftschnittstellen (Left/Right Lane), 1 luftseitiger Rechner pro Schnittstelle (UAV L1/R1) und 2 bodenseitige Rechner (GCS 1/2).

Anzahl der			Max. Fehlerrate p [10^{-9}·1/h]	Min. MTBF [10^{9}·h]
Lanes l	UAV-Knoten pro Lane u	GCS-Knoten g		
2	1	1	1	1
	2	1	1	1
	1	**2**	**7.669,65**	**0,000130**
	2	**2**	**9.999,97**	**0,000100**
	2	**4**	**10.540,89**	**0,000095**

TAB 2. Ergebnis der Fehlerratenabschätzung für zwei Luftschnittstellen

Unter der Annahme von identen Fehlerraten sämtlicher Komponenten (Rechner, Modem und Kanal) erfordert diese Minimalkonfiguration eine durchschnittliche, fehlerfreie Betriebsdauer jeder einzelnen Komponente von etwa $1{,}3 \cdot 10^5$ Stunden. Verglichen mit der Fehlerratenabschätzung vorliegender COTS-Hardware (TTTech PMC Karte, BILD 1) wird bereits diese Mindestdauer rund 30-fach übertroffen.

4. DISKUSSION

Als Engstelle für die Erweiterbarkeit des Systems zur Erhöhung der Zuverlässigkeit geht in der Bus-Topologie die begrenzte Anzahl von Datenlinks hervor. Ein Zusatzgewinn würde etwa durch Interfaces erreicht, welche weitere Buspfade aktiv oder inaktiv schalten. Im Hinblick auf die Vernetzung mehrerer Bodenstationen und UAVs bringt aber vor allem der Einsatz einer Stern-Topologie große Vorteile mit sich (BILD 9).

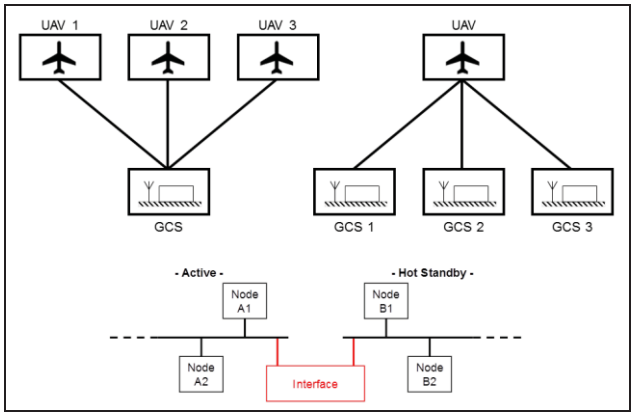

BILD 9. Stern-Topologie, Bus-Interfaces

Sämtliche Abschätzungen beziehen sich auf idente Fehlerraten der Komponenten. Im realen System muss Gleichung (2) anhand des Fehlerbaum-Modells korrigiert werden.

Eine erhöhte Zuverlässigkeit des Systems wird durch den Einsatz von zwei redundanten TTP-Kanälen erreicht. Durch das in den Modems verwendete OFDM-Schema werden beide TTP-Kanäle nochmals in unterschiedlichen Frequenzbereichen übertragen, wodurch nicht nur der Datenbus, sondern auch ein einzelner Datenlink bereits ein gewisses Maß an Redundanz aufweist. Bei lediglich schmalbandigen Störungen der Funkverbindung bliebe das Gesamtsystem operabel, was sich wiederum positiv auf die Ausfallwahrscheinlichkeit auswirkt. Aufgrund nicht vollständig getrennter Hardware für die Kanäle werden diese Zugewinne aber in der allgemeinen Betrachtung nicht explizit berücksichtigt, sondern den einzelnen Komponenten zugerechnet.

Eine wesentliche technische Herausforderung im vorgeschlagenen System stellt auch die Kommunikation des TTP-Bussystems über die Luftschnittstelle hinweg dar. Verbindungsausfälle oder Latenzzeiten der Modems sind dabei mit der Protokollspezifikation in Einklang zu bringen.

DANKSAGUNG

Die vorliegende Arbeit wurde im Rahmen des Projekts „CertLink“ (Certifiable Data Link in Time Triggered-Architecture for Remote Control of Unmanned Aerial Vehicles) durchgeführt und wird von der Österreichischen Forschungsförderungsgesellschaft (FFG) im Rahmen des Programms TAKE OFF unterstützt.

GLOSSAR

ARP	Aerospace Recommended Practices
COTS	Commercial Off-The-Shelf
DAL	Design Assurance Level
DO	RTCA-Dokument
ED	EUROCAE-Dokument
EUROCAE	European Organisation for Civil Aviation Equipment
FHA	Functional Hazard Analysis
FPGA	Field-Programmable Gate Array
FTA	Fault Tree Analysis
GCS	Ground Control Station
MIL-HDBK	Defense Handbook, United States Military Standard
MTBF	Mean Time Between Failures
OFDM	Orthogonal Frequency-Division Multiplexing
PCI	Peripheral Component Interconnect
PMC	PCI Mezzanine Card
RTCA	Radio Technical Commission for Aeronautics
SAE	Society of Automotive Engineers
SDR	Software-Defined Radio
SPOF	Single Point of Failure
TTP	Time-Triggered Protocol
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle

LITERATUR

[1] SAE ARP 4754 (System Development Process). SAE International Inc.
[2] SAE ARP 4761 (Safety Assessment Process). SAE International Inc.
[3] DO-254/ED-80 (Design Assurance Guidance for Airborne Electronic Hardware). RTCA, Inc./EUROCAE.
[4] DO-178B/ED-12B (Software Considerations in Airborne Systems and Equipment Certification). RTCA, Inc./EUROCAE.
[5] MIL-HDBK-338B (Electronic Reliability Design Handbook). Department of Defense, USA.
[6] H. Kopetz, G. Bauer. The Time-Triggered Architecture. Proceedings of the IEEE Special Issue on Modeling and Design of Embedded Software, Jan 2003.

[7] H. Kopetz. Real-Time Systems, Design Principles for Distributed Embedded Applications, Seventh printing 2003. 1997, Boston: Kluwer Academic Publishers.
[8] TTP PMC Card User Manual. TTTech Computertechnik AG, Wien, 2009.
[9] S. Hesse, R. Reichel, S. Görke, L. Dalldorff. Eine skalierbare Plattform für sicherheitskritische, automatische Flugsteuerungssysteme der allgemeinen Zivilluftfahrt. Deutscher Luft- und Raumfahrtkongress 2009.
[10] Y.C. (Bob) Yeh. Triple-Triple Redundant 777 Primary Flight Computer, Boeing Commercial Airplane Group, 1996, IEEE.