EFFIZIENTES TESTEN UND BEWERTEN VON SYSTEMFEHLERN BEI AUTOMATISCHER LANDUNG

I. Karakaya, R. Luckner
Technische Universität Berlin, Institut für Luft- und Raumfahrt, Marchstr. 12, 10587 Berlin, Deutschland

Zusammenfassung

Sicherheitskritische und komplexe Flugregelungssysteme müssen strikten Anforderungen an Funktionalität, Zuverlässigkeit und Robustheit gerecht werden. Hierfür ist eine umfangreiche und zeitaufwändige Nachweisführung notwendig, die zeigt, dass das Flugregelungssystem die Anforderungen an die Flugeigenschaften und die Flugmission erfüllt. Der Start und die Landung sind aufgrund der Bodennähe besonders kritische Flugphasen. Für die automatische Landung sind in den Acceptable Means of Compliance (AMC) der CS AWO.A.ALS.106 Richtlinien für den Aufsetzpunkt bezüglich longitudinalem Abstand zur Landebahnschwelle und lateraler Abweichung zur Landebahnmittellinie gefordert. Gemäß der Zulassungsvorschrift EASA AMC CS-25.671 müssen ein kontrollierter Flug und eine sichere Landung im Nominal- als auch im Fehlerfall sichergestellt sein. In modernen elektronischen Flugsteuerungssystemen werden zum Übertragen von Informationen zwischen einzelnen Systemkomponenten CAN-Bus-Kanäle zur Ansteuerung von Aktuatoren verwendet. Der Ausfall eines CAN-Bus-Kanals aufgrund eines Kabelbruchs kann zum Kommunikationsverlust zwischen Flugsteuerungsrechner und einer oder mehreren Stellflächen führen. Dadurch kann möglicherweise die Manövrierfähigkeit eines Flugzeugs kritisch reduziert werden. Dieser Beitrag zeigt am Beispiel einer automatischen Flugsteuerung für ein großes unbemanntes Flugzeug, wie die Anzahl der zu untersuchenden CAN-Bus-Fehlerfälle reduziert und das Worst-Case-Szenario identifiziert werden kann. Die Untersuchung mit einer nichtlinearen Simulation zeigt, dass eines der identifizierten Worst-Case-Szenarien bei der Landung nicht ausreichend ist. Die demonstrierte Methode soll erfahrene Piloten und Entwicklungsingenieure bei der Einstufung von Fehlerfällen unterstützen.

Nomenklatur

Abkürzungen

AC	Advisory Circular
AR	Average Risk
AMC	Acceptable Means of Compliance
CS	Certification Specification
CAT	Catastrophic
EAS	Equivalent Airspeed
EASA	European Aviation Safety Agency
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulations
fh	flight hours
HALE	High Altitude Long Endurance
HAZ	Hazardous
LR	Limit Risk
MSL	Mean Sea Level
MAJ	Major
MIN	Minor
MCS	Monte-Carlo-Simulation
P	Probability of Failure
TAS	True Airspeed
TCP	Treshold Crossing Point
UAV	Unmanned Aerial Vehicle

Formelzeichen (groß)

H_{gnd}	Höhe über Boden
T	Temperatur
V	Fluggeschwindigkeit

Formelzeichen (klein)

m	Masse
h_{Rwy}	Landebahnhöhe
$u_{W,10}$	x-Referenzwindgeschwindigkeit 10 m über dem Boden
$v_{W,10}$	y-Referenzwindgeschwindigkeit 10 m über dem Boden
x_{CG}	Schwerpunktlage in x-Richtung
x_{dist}	Longitudinaler Abstand zwischen Aufsetzpunkt und Landebahnschwelle
x_{max}	maximaler longitudinaler Abstand zur Landebahnschwelle
x_{min}	minimaler longitudinaler Abstand zur Landebahnschwelle
y_{dist}	Lateraler Abstand zwischen Aufsetzpunkt (Fahrwerk) und Landebahnmittellinie
y_{max}	maximaler lateraler Abstand zur Landebahnmitellinie
y_{min}	minimaler lateraler Abstand zur Landebahnmitellinie

Griechische Symbole (klein)

γ	Bahnwinkel
ξ	Querruderausschlag
ξ_i	Ausschlag des Flaperons i
η_F	Ausschlag der Hinterkantenklappen (Flaps)
η_S	Störklappenstellung (Speed Brake)

doi: 10.25967/570216

1 EINLEITUNG

Sicherheitskritische und komplexe Flugregelungssysteme müssen in allen Flugphasen robust, zuverlässig und korrekt funktionieren. Fehlerfälle im Flugregelungssystem, die nicht äußerst unwahrscheinlich sind, dürfen keine katastrophalen Auswirkungen auf das Flugzeug haben. Deshalb wird bereits in der frühen Entwicklungsphase die Kritikalität von Einfach- oder Mehrfachfehlerfällen für alle Flugphasen bewertet. Die Bewertung der Kritikalität von Fehlerfällen ist für die Nachweisführung entsprechend den Zulassungsvorschriften der EASA CS-25.1309 (*Equipment, systems, and installations*) notwendig [1].

Die gängige Nachweisführung erfolgt im *Safety Assessment Process* durch umfangreiche Analysen und Tests. Ausfallbedingungen mit katastrophalen (*catastrophic*) oder gefährlichen (*hazardous*) Auswirkungen auf das Flugzeug werden dabei nur mittels Flugsimulation und nicht im realen Flugversuch untersucht. Aber auch die Testkampagne im Flugsimulator mit Pilotenbewertung ist zeit- und kostenintensiv, da sie in Echtzeit erfolgt.

Dagegen sind PC-basierte Schnellzeitsimulationen leichter realisierbar und schneller durchzuführen. Sie können eine kostengünstige Ergänzung zu Echtzeit-Flugsimulationen darstellen, um kritische Fehlerfälle zu identifizieren. Zusätzlich kann die Entscheidung, ob die Konsequenzen eines Fehlerfalls als schwerwiegend (*major*) oder bereits als gefährlich einzustufen sind, durch Schnellzeitsimulationen mit Pilotenmodellen für die Bewertung der Fehlerfälle unterstützt werden.

In [3] wird beschrieben, wie Fehlerfälle in der Aktuatorik mittels PC-basierten Schnellzeitsimulationen automatisiert untersucht und bewertet werden können. In [4] werden auf ähnliche Weise Mehrfachfehler in der Aktuatorik hinsichtlich ihrer Auswirkungen auf flugmechanische Eigenschaften analysiert. Beide Untersuchungen wurden an bemannten Flugzeugen durchgeführt, die Methoden können aber auch auf die Analyse von Fehlerfällen einer automatischen Flugsteuerung von unbemannten Flugzeugen übertragen werden.

Gemäß den Zulassungsvorschriften der EASA CS-25.1309 muss jede Komponente eines Flugzeugs und jedes System in einem Flugzeug so konzipiert sein, dass die Auftrittswahrscheinlichkeit einer Fehlfunktion oder eines Ausfalls mit schwerwiegenden oder katastrophalen Konsequenzen äußerst selten (*extremly remote*) oder äußerst unwahrscheinlich (*extremly improbable*) ist.

Start und die Landung stellen aufgrund der Bodennähe besonders kritische Flugphasen dar. Der Flug und die Landung müssen laut AMC CS-25.671 im Nominal- und Fehlerfall kontrolliert und sicher verlaufen [1]. Für eine sichere Landung darf die longitudinale Ablage zur Landebahnschwelle sowie die laterale Ablage zur Landebahnmittellinie die Werte der AMC CS AWO.A.ALS.106 [2] Richtlinie nicht überschreiten.

Die Auftrittswahrscheinlichkeit eines katastrophalen Fehlerfalls muss kleiner 10^{-7}/fh auf Flugzeugebene und auf Systemebene kleiner 10^{-9}/fh sein. Die Annahme ist, dass in einem Flugzeug 100 Fehler mit katastrophaler Auswirkung existieren. Bei der Landung beziehen sich die Ausfallwahrscheinlichkeiten auf 1/Landungen und nicht 1/fh.

Beispielhaft werden CAN-Bus-Ausfälle (*Loss of Control of Surface*) betrachtet, die zum Verlust einer oder mehrerer Stellflächen führen. Bei den Stellflächen handelt es sich um Wölbklappen an der Flügelhinterkante, die antimetrisch zur Rollsteuerung, symmetrisch zum Beeinflussen des Auftriebsbeiwertes und gespreizt zum Erhöhen des Widerstandsbeiwertes eingesetzt werden. Die Anzahl kombinatorischer CAN-Bus-Fehlerfälle kann bei komplexer Systemarchitektur sehr groß sein. Die Untersuchung und Bewertung aller möglichen Fehlerfall-Kombinationen ist nicht immer notwendig. So haben bei einer symmetrischen Systemarchitektur Fehlerfälle auf der linken Seite ähnliche Auswirkung wie spiegelbildliche Fehler auf der rechten Seite. Auch kann intelligent reduziert werden, wenn eine Stellfläche geringere Wirkung hat als eine bereits als unkritisch identifizierte Steuerfläche.

Signifikante Fehlerfälle können bereits im Voraus durch analytische flugmechanische Berechnungen identifiziert werden. Mithilfe der Flugsimulation kann verifiziert werden, welche Auswirkungen diese Fehlerfälle generell haben. Die restlichen als sicher eingestuften Fehlerfälle können für kritische Randbedingungen (z.B starker Seitenwind oder Rückenwind) untersucht werden, um zu bestimmen, wann eine Landung noch möglich wäre.

Die Untersuchung klärt die Frage, ob diese Fehlerfälle im Grenzfall zu einer unsicheren Landung führen würden. Ziel ist es, bereits für den Einfachfehler diese Landungen zu identifizieren, die für die Mehrfachfehler nicht mehr betrachtet werden müssen.

Eine mögliche Vorgehensweise zur systematischen Untersuchung von CAN-Bus-Kanalausfällen ist in BILD 1 beschrieben. Die Bezeichnungen sind an die Abschnittsnummern in diesem Beitrag angepasst.

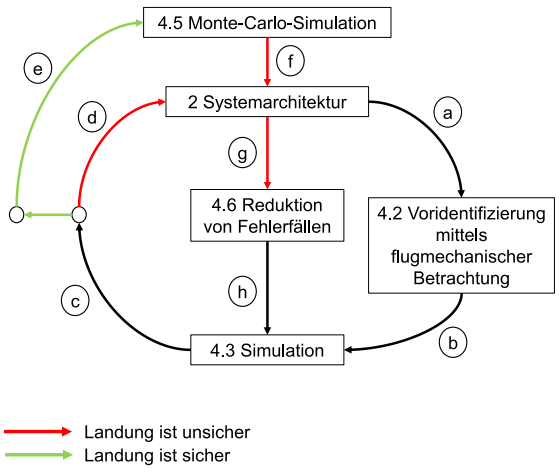

BILD 1: Prozess zur effizienten Untersuchung von Einfach- und Mehrfachfehlerfällen

Mit einer gegebenen Systemarchitektur und der bekannten CAN-Bus-Kanalordnung zu den Stellflächen werden signifikante Fehlerfälle mit den in Abschnitt 3.3 beschriebe-

nen Methoden identifiziert (a). Im Schritt (b) werden mit der Flugsimulation diese identifizierten Fehlerfälle simuliert und im Schritt (c) überprüft, ob eine sichere automatische Landung möglich ist. Ist die automatische Landung unsicher, dann wird am Flugregler oder an der Systemarchitektur eine Änderung notwendig (d). Ansonsten werden mit den Eingabeparametern aus der *limit risk* und *average risk* Monte-Carlo-Analyse mit Wind und Turbulenz untersucht, ob die als sicher eingestuften Fehler zu einer unsicheren Landung führen (f). Bei Mehrfachfehlern können die in (d) und (g) ermittelten Einzelfehlerfälle, bei der eine Landung nicht sicher ist, eliminiert werden und müssen nicht weiter betrachtet werden. Die Kritikalität der verbliebenen Mehrfachfehlerfälle kann mit der Simulation bewertet werden (h).

2 SYSTEMARCHITEKTUR DES BEISPIELFLUGZEUGS

In diesem Beitrag wird eine Flugsimulation eines hoch- und langfliegenden HALE-Flugzeugs (*high altitude long endurance*) verwendet. Charakteristisch für diese Art von Flugzeugen sind eine hohe Streckung und eine hohe Flügelspannweite. Die daraus resultierende hohe Gleitzahl ermöglicht das Fliegen in großen Höhen mit langer Flugdauer. Wegen der großen Flügelspannweite sind solche Flugzeuge träge um die Rollachse. Das Flugzeug soll nach Zulassungsvorschriften der EASA für die UAV-Kategorie "*Specific*" zugelassen werden, die noch nicht vollständig spezifiziert ist. Aus diesem Grund wird die
EASA Richtlinie CS-25 herangezogen.

Das HALE-Flugzeug besitzt multifunktionale Stellflächen. Einzelne Flügelhinterklappen, im Englischen *Flaperons* genannt, können gleichzeitig die Funktion der Auftriebshilfe (*Flaps*), die Störklappenfunktion (*Speed Brake*) oder die Funktion für das Rollen um die Längsachse mit den Querrudern (*Ailerons*) ausführen.

Das HALE-Flugzeug besitzt sechs Flaperons auf der linken und rechten Flügelhälfte, welche mit elektrischen Aktuatoren angesteuert werden. BILD 2 zeigt die Draufsicht des HALE-Flugzeugs.

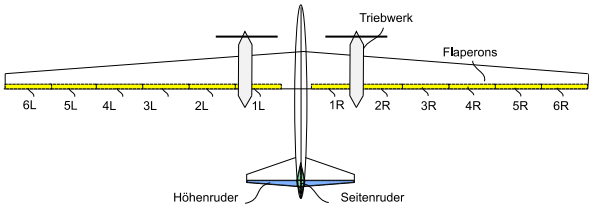

BILD 2: Draufsicht auf ein exemplarisches HALE-Flugzeug

Für die Einzelklappen ξ_{iL}, ξ_{iR} $(i = 1 \cdots 6)$ gelten in Abhängigkeit vom Querruderausschlag ξ, der Auftriebshilfe η_F und der Störklappenfunktion $\eta_{i,S}$ bei positivem Kommando ($\xi \geq 0$) die folgenden kombinierten Klappenausschläge:

$$\xi_{iL}(\eta_{i,S}) = 3 \cdot \xi + \eta_F + \eta_{i,S} \quad (1)$$

$$\xi_{iR}(\eta_{i,S}) = -\xi + \eta_F + \eta_{i,S} \quad (2)$$

Bei negativem Kommando ($\xi < 0$) folgen

$$\xi_{iL}(\eta_{i,S}) = -\xi + \eta_F + \eta_{i,S} \quad (3)$$

$$\xi_{iR}(\eta_{i,S}) = 3 \cdot \xi + \eta_F + \eta_{i,S} \quad (4)$$

Zum Übertragen von Informationen zwischen den einzelnen Systemkomponenten werden serielle Bussysteme wie beispielsweise CAN-Bus-Kanäle verwendet. Die Systemarchitektur eines Flugzeugs muss eine katastrophale Auswirkung bei einem Einfachfehler verhindern. Aus diesem Grund gilt das Redundanzkonzept und eine Stellfläche kann von mehreren CAN-Bus-Kanälen angesprochen werden. Das Problem ist deshalb die Vielfalt an kombinatorischen CAN-Bus-Stellflächen Verschaltungen, die aus einer komplexen Systemarchitektur resultieren kann.

Die fünf CAN-Bus-Kanäle (Ra, Rb, Ba, Bb, Bc) werden den 12 Stellflächen über eine Zuordnungsmatrix zugeordnet, die in TAB 1 aufgelistet ist. Diese Systemarchitektur ist nicht optimal. Sie ist ein Beispiel, welches zu Demonstrationszwecken gewählt wurde.

TAB 1: Zuordnungsmatrix zwischen CAN-Bus-Kanal und Stellfläche, die orange markierten Zellen zeigen, welche Stellflächen bei dem jeweiligen CAN-Bus-Kanalausfall ausfallen

CAN FLP	Ra	Rb	Ba	Bb	Bc
1L	1	1	1	1	0
2L	0	1	1	1	1
3L	1	1	0	1	1
4L	1	1	1	1	1
5L	1	1	1	1	0
6L	0	1	1	1	1
1R	1	1	1	1	1
2R	1	0	1	1	1
3R	1	1	1	0	1
4R	1	1	1	1	1
5R	1	1	1	1	1
6R	1	0	1	1	1

3 FEHLERBEWERTUNG UND REDUKTION

3.1 Fehlerklassifizierung

Die Bewertung und Einstufung von Fehlerfällen erfolgt in der frühen Entwicklungsphase typischerweise durch die subjektive Einschätzung von erfahrenen Entwicklungsingenieuren und Testpiloten. Eine Ausfallbedingung (*failure condition*) ist eine Bedingung, die sich auf das Flugzeug, die Arbeitsbelastung des Piloten, auf die Gesundheit der Insassen oder auf alle drei Aspekte auswirkt. Die Klassifikation aller Ausfallbedingungen und die zulässigen, maximalen Ausfallwahrscheinlichkeiten sind in EASA CS-25.1309 beschrieben (siehe TAB 2) [1].

TAB 2: Klassifizierung und Ausfallwahrscheinlichkeit (P)

Klassifizierung	Definition	P [1/h]
no safety effect	Fehlerfall hat keinen Einfluss auf die Sicherheit	–
minor	Fehlerfall mit leichter Verringerung der Sicherheitsmargen und leichter Erhöhung der Arbeitsbelastung der Besatzung	10^{-3}
major	Erhebliche Reduktion der Sicherheitsmargen und erhebliche Erhöhung der Arbeitsbelastung	10^{-5}
hazardous	Große Reduktion der Sicherheitsmargen und physische Belastung der Besatzung, die Flugmission akkurat durchzuführen	10^{-7}
catastrophic	Ausfallbedingung, die einen weiteren sicheren Flug und eine sichere Landung verhindert	10^{-9}

3.2 Reduktion von Fehlerfällen

Es gilt die Frage zu beantworten, welche Möglichkeiten existieren, kombinatorische Testfälle auf ein Minimum zu reduzieren und trotzdem die signifikanten Testfälle zu untersuchen. Im Folgenden wird eine Methode vorgestellt, mit der doppelte (z.B symmetrische) Tests eliminiert werden können.

Gegeben seien im Testraum T_1 die Variablen $\{A, B, C, D\}$, die beispielsweise CAN-Bus-Kanäle in einer Systemarchitektur darstellen.

$$\{A, B, C, D\} \in T_1 \tag{5}$$

Jeder dieser Variablen $\{A, B, C, D\}$ im Testraum T_1 sind Variablenkombinationen aus $\{a, b, c, d\}$ zugeordnet. Kombinationen der Variablen $\{a, b, c, d\}$ sind dem Testraum T_2 zugeordnet und können beispielsweise die Stellflächen sein, die von den CAN-Bus-Kanälen $\{A, B, C, D\}$ angesprochen werden (siehe TAB 3). So bedeutet beispielsweise $A \rightarrow \{a, b\}$, dass der CAN-Bus-Kanal A die Stellflächen $\{a, b\}$ ansteuert.

TAB 3: Testraum T_2

A	ab
B	bc
C	cd
D	ad

Im ersten Schritt werden doppelte und symmetrische Testfälle aus dem Testraum T_1 eliminiert (siehe TAB 4).

TAB 4: Eliminierung der doppelten und symmetrischen Testfälle aus dem Testraum T_1

	A	B	C	D
A	~~AA~~	~~AB~~	~~AC~~	~~AD~~
B	**BA**	~~BB~~	~~BC~~	~~BD~~
C	**CA**	**CB**	~~CC~~	~~CD~~
D	**DA**	**DB**	**DC**	~~DD~~

Das Zusammenführen der Zuordnung T_2 in Testraum T_1 und die erneute Reduktion der symmetrischen und doppelten Testfälle ergibt den Testraum T_3 (siehe TAB 5).

TAB 5: Testraum T_3

	A	B	C	D
A	-	-	-	-
B	abbc	-	-	-
C	abcd	bccd	-	-
D	abad	bcad	cdad	-

Mit der weiteren Reduktion doppelter- und symmetrischer Fehlerfälle aus TAB 5 folgt anschließend der zu testende Testraum $\hat{T}_3$ (siehe TAB 6)

TAB 6: Testraum $\hat{T}_3$

	A	B	C	D
A	-	-	-	-
B	**abc**	-	-	-
C	~~abcd~~	**bcd**	-	-
D	**abd**	~~abcd~~	**acd**	-

Dieses Beispiel zeigt, wie durch Eliminieren doppelter und symmetrischer Fehlerfälle bereits mehr als die Hälfte der Testfälle reduziert werden kann. Insgesamt müssen bei diesem Beispiel bei der Untersuchung von Doppelfehlern aus 16 möglichen Kombinationen nur vier Kombinationen getestet werden.

Die EASA CS-25.1309 [1] fordert, dass ein einfacher Fehlerfall nicht zu einem katastrophalen Flugzustand führen darf. Falls einer der übrig gebliebenen Fälle $\{abc, bcd, abd, acd\}$ eine katastrophale Auswirkung hat, kann dieser bei der Untersuchung von Doppelfehlern auch eliminiert werden. Allerdings muss dann entweder die Systemarchitektur oder der Flugregler geändert werden.

3.3 Identifikation signifikanter Fehlerfälle

Für die Identifizierung signifikanter Fehlerfälle wird neben der nichtlinearen Flugsimulation vereinfachend ein lineares Modell der Seitenbewegung betrachtet

$$\dot{\underline{x}} = \underline{\underline{A}} \cdot \underline{x} + \underline{\underline{B}} \cdot \underline{u} \quad . \tag{6}$$

Hierbei stellt $\underline{x} \in \mathbb{R}^n$ den Zustandsvektor, $\underline{\underline{A}} \in \mathbb{R}^{n,n}$ die Systemmatrix, $\underline{\underline{B}} \in \mathbb{R}^{n,m}$ die Eingangsmatrix und $u(t) \in \mathbb{R}^m$ die Steuergröße dar.

Die Zustandsgrößen x_i sind die Gierrate r, der Schiebewinkel β, die Rollrate p und der Hängewinkel Φ.

$$\underline{x} = [r, \beta, p, \Phi]^{\mathrm{T}} \quad . \tag{7}$$

Die Stellgrößen u_i sind die Einzel-Querruderklappen ξ_{iL}, ξ_{iR} und das Seitenruder ζ

$$\underline{u} = [\xi_{iL}, \xi_{iR}, \zeta]^{\mathrm{T}}_{i=1\ldots6} \tag{8}$$

Das Seitenruder ζ wird in diesem Beitrag nicht weiter betrachtet. Die Stellmatrix $\underline{\underline{B}}$ in Abhängigkeit der Einzelklappen ξ_{iL}, ξ_{iR} mit $i = 1 \cdots 6$ ist dann

$$\underline{\underline{B}} \cdot \underline{u} = \begin{bmatrix} B_{r,\xi_{1L}} & B_{r,\xi_{2L}} & \cdots & B_{r,\xi_{6R}} \\ B_{\beta,\xi_{1L}} & B_{\beta,\xi_{2L}} & \cdots & B_{\beta,\xi_{6R}} \\ B_{p,\xi_{1L}} & B_{p,\xi_{2L}} & \cdots & B_{p,\xi_{6R}} \\ B_{\Phi,\xi_{1L}} & B_{\Phi,\xi_{2L}} & \cdots & B_{\Phi,\xi_{6R}} \end{bmatrix} \cdot \begin{bmatrix} \xi_{1L} \\ \xi_{2L} \\ \vdots \\ \xi_{6R} \end{bmatrix} \tag{9}$$

Bei dem CAN-Bus-Kanalausfall befinden sich die ausgefallenen Stellflächen in Neutralposition. Wenn die Hinterkantenklappen (*Flaps*) ausfahren, resultiert durch die asymmetrische Auftriebsverteilung ein Roll- und ein Wendemoment. Aus diesem Grund muss die Auswirkung des Fehlers auf die Gierrate r (erste Zeile in $\underline{\underline{B}}$) und die Rollrate p (dritte Zeile in $\underline{\underline{B}}$) betrachtet werden. Das Rollmoment $\hat{L}_\xi$ mit vollem Querruderausschlag und das Wendemoment ohne Querruderausschlag $\hat{N}_\xi$ berechnen sich mit

$$\begin{bmatrix} L_\xi \\ N_\xi \end{bmatrix} \cdot \begin{bmatrix} \xi_i(\xi = 10°, \eta_F = 7°, \xi_{S,\text{full}}) \\ \xi_i(\xi = 0°, \eta_F = 7°, \xi_{S,\text{full}}) \end{bmatrix} = \begin{bmatrix} \hat{L}_\xi \\ \hat{N}_\xi \end{bmatrix} = \sum_{i=1}^{6} \begin{bmatrix} B_{p,\xi_{iL}} \cdot \xi_{iL} + B_{p,\xi_{iR}} \cdot \xi_{iR} \\ B_{r,\xi_{iL}} \cdot \xi_{iL} + B_{r,\xi_{iR}} \cdot \xi_{iR} \end{bmatrix} \quad . \tag{10}$$

Bei der Berechnung des Wendemoments wird der Querruderausschlag $\xi = 0°$ gesetzt, um das asymmetrische Wendemoment zu bestimmen, falls im Fehlerfall die Wölbklappen η_F oder die Spoiler η_S kommandiert sind. Bei der Berechnung des Rollmoments wird der volle Querruderausschlag $\xi = 10°$ verwendet, um ein Verhältnis des Rollmoments des fehlerfreien Falls (max. mögliches Rollmoment) und des fehlerhaften Falls zu berechnen.

Das HALE-Flugzeug hat auf der linken und rechten Flügelhälfte in dem Stellvektor $\underline{u}_F$ jeweils $i = 6$ linke- und rechte Stellflächen. Der Index j bezeichnet das fehlerhafte Querruder im Stellvektor $\underline{u}_F$ und ist ein Element der fehlerhaften Querruder $\mathcal{Q}_F$, dann gilt für den Stellvektor

$$u_F(i = j) = 0 \quad \forall \quad j \in \mathcal{Q}_F \tag{11}$$

$$u_F(i \neq j) = \xi_i \quad \forall \quad j \notin \mathcal{Q}_F \quad . \tag{12}$$

Das resultierende Rollmoment $\hat{L}_F$ und das Wendemoment $\hat{N}_F$ für diesen Fehlerfall berechnet sich zu

$$\begin{bmatrix} \hat{L}_F \\ \hat{N}_F \end{bmatrix} = \sum_{i=1}^{6} \begin{bmatrix} B_{p,\xi_{iL}} \cdot u_{F,iL} + B_{p,\xi_{iR}} \cdot u_{F,iR} \\ B_{r,\xi_{iL}} \cdot u_{F,iL} + B_{r,\xi_{iR}} \cdot u_{F,iR} \end{bmatrix} \quad . \tag{13}$$

Der Verlust der Steuerautorität Δ ist das Verhältnis des Rollmoments zwischen fehlerhaften und fehlerfreien Einzelstellflächen

$$\Delta = 1 - \frac{\hat{L}_F}{\hat{L}_\xi} \quad . \tag{14}$$

Die angenommenen Grenzwerte der entsprechenden Bewertungsskala aus BILD 3 müssen durch Simulationen bestätigt werden.

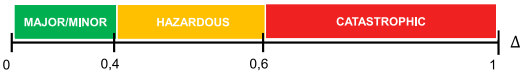

BILD 3: Kritikalität des Fehlerfalls in Abhängigkeit von Δ

Je größer das Wendemoment bei dem Fehlerfall, desto größer ist die resultierende Kursabweichung. Je größer der Verlust der Steuerautorität, desto langsamer kann der Kursfehler korrigiert werden. Deshalb ist der Fehlerfall als kritisch anzunehmen, wenn der Verlust der Steuerautorität am größten oder katastrophal (roter Bereich) oder das Wendemoment maximal ist.

3.4 Richtlinien zur Bewertung der Kritikalität im Landeanflug

Für die Bewertung der Kritikalität im Landeanflug wird die Zulassungsrichtlinie EASA CS-25.671 herangezogen [1]. Eine Ausfallbedingung während eines Flugs darf keine katastrophale Folgen haben, die eine sichere Landung durch den Piloten oder im unbemannten Fall durch den Regler verhindern würde. Die Bewertungskriterien für die Klassifizierung der Fehlerfälle bei der Landung werden aus den Zulassungsrichtlinien für den Allwetterbetrieb AMC CS-AWO [2] entnommen.

Die AMC AWO.A.ALS.106 fordert, dass in 10^{-6} der Testfälle der Aufsetzpunkt frühestens 200 ft bis spätestens 2700 ft nach der Landebahnschwelle liegen muss.

Ein seitliches Aufsetzen mit dem äußeren Fahrwerk um mehr als 21 m (70 ft) von der Mittellinie der Landebahn entfernt muss unter der Annahme einer 45 m (150 ft) breiten Landebahn vermieden werden. Angenommen wird, dass das Hauptfahrwerk zum Schwerpunkt einen Hebelarm von $y_{\text{gear}} = 5$ m hat, sodass für die laterale Ablage des Schwerpunkts (in Symmetrieebene) als Grenzwert 21 m - 5 m = 16 m (53 ft) geprüft werden muss. (siehe BILD 4). Für die Formulierung der Kriterien sei x_{dist} der Abstand zwischen der Landebahnschwelle und des Aufsetzpunktes sowie y_{dist} der seitliche Abstand zwischen Fahrwerk und der Landebahnmittellinie.

- Ist der Aufsetzpunkt longitudinal früher als $x_{\min}$ (200 ft) oder später als $x_{\max}$ (2700 ft) oder setzt das äußere Fahrwerk lateral mit einer betragsmäßig größeren Abweichung als $y_{\max}$ (53 ft) auf, so wird die Landung und somit der Testfall als unsicher eingestuft (das Flugzeug landet außerhalb der Landebahn).
- Ansonsten ist der Testfall als sicher einzustufen.

TCP : Threshold Crossing Point

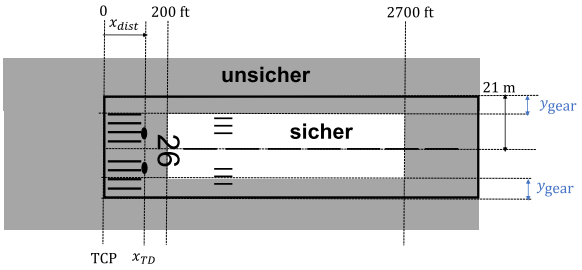

BILD 4: Darstellung der zulässigen Grenzen für den Aufsetzpunkt x_{TD} auf der Landebahn.

4 BEISPIELSZENARIO

4.1 Definition des Fehlermodes

Laut EASA CS-25.671 (c) muss nach einem Fehler das Flugsteuerungssystem fähig sein, den Flug sicher fortsetzen und landen zu können. In den dazugehörenden Acceptable Means of Compliance (AMC) wird verlangt, dass folgende Fehlermodi berücksichtigt werden müssen [1].

- *Actuator Jam*: Blockade der Stellfläche in neutraler oder einer kommandierten Position.
- *Loss of Control of Surface*: Ein Fehler, bei der die Stellfläche nicht auf Befehle reagiert. Die Fehlerquellen können beispielsweise eine mechanische Unterbrechung, eine Unterbrechung des Steuerkabels oder ein Verlust von Steuerbefehlen aufgrund von Aktuatorelektronikfehlern sein.
- *Oscillatory Failure*: Ein Fehler, der zur übermäßigen Schwingung der Stellflächen führt. Die Fehlerquellen können beispielsweise eine Destabilisierung des Regelkreises oder ein oszillierendes Verhalten des Sensorsignals bzw. der Aktuatorelektronik sein. Der Fehlermode ist abhängig von der Periodendauer der Schwingung, ihrer Frequenz und Amplitude.
- *Restricted Control*: Eine Störung, die dazu führt, dass die erreichbare Stellfläche begrenzt ist. Zu den Fehlerquellen gehören Störungen durch externe Objekte, Fehlfunktionen eines Wegbegrenzers (*travel limiters*) und Fehlfunktionen von Schutzfunktionen (*envelope protection*).
- *Runaway or Hardover*: Ein Fehler, der zum unkommandierten Weglaufen der Stellfläche mit maximaler Stellrate bis zum mechanischen Limit führt. Fehlerquellen sind u.a. blockierte Servoventile, Computer- oder Aktuatorelektronik-Fehlfunktionen.
- *Stiff or Binding Controls*: Eine Fehlfunktion, die zu einem erheblichen Anstieg der Steuerkräfte führt. Zu den Fehlerquellen gehören Ausfälle von Steuerkraftsimulatoren, korrodierte Lager, verklemmte Riemenscheiben und Schäden, die eine hohe Reibung verursachen.

In diesem Beitrag wird nur der Fehlerfall *Loss of Control of Surface* untersucht. Betrachtet werden CAN-Bus-Kanalausfälle, die zum Ausfall von Stellflächen führen. Der Fehlerfall tritt beim Start des Landeanflugs auf. Die Stellflächen verfahren im Fehlerfall in die Neutralposition.

4.2 Voridentifizierung kritischer Fehlerfälle

Die signifikanten Fehlerfälle werden mit dem Verlust der Roll-Steuerautorität Δ (Gleichung 14) und dem Wendemoment $\hat{N}_F$ bestimmt. TAB 7 zeigt den Verlust der Steuerautorität und das Wendemoment, das bei vollen Wölbklappen- bzw. Bremsklappenkommandos für die CAN-Bus-Kanalausfälle aus TAB 1 entsteht.

TAB 7: Verlust der Steuerautorität Δ und Wendemoment $\hat{N}_F$ der CAN-Bus-Kanalausfälle

	Ra	Rb	Ba	Bb	Bc
Δ	**0,2182**	0,1613	0,0855	0,0632	0,0912
$\hat{N}_F$	0,0057	-0,0057	-0,0957	0,0957	**0,3196**

Nach BILD 3 sind alle CAN-Bus-Kanalausfälle der Kritikalität *major/minor* zuzuordnen. Da die Einstufung nach BILD 3 noch nicht bestätigt wurde, wird für die CAN-Bus-Fehlerfälle Ra und Bc mit der Flugsimulation überprüft, ob sie zu einer unsicheren Landung führen würden.

4.3 Flugsimulation

Simuliert wird ein beispielhafter Anflug ohne Wind. Das Flugzeug befindet sich vor dem Einnehmen des Gleitstrahls in einem stationären Horizontalflug in einer Höhe von 400 m über MSL bei einer Fluggeschwindigkeit von 21.3 m/s (EAS) mit einer Masse von 2700 kg. Die hinterste Schwerpunktlage wird untersucht. Die Masse ist konstant und ändert sich während der Simulation nicht.

BILD 5 zeigt die Ergebnisse der nichtlinearen Simulation für den letzten Teil der automatischen Landung aus einer Höhe von 20 ft über Boden bis zum Aufsetzen. Das Flugzeug befindet sich in der Phase des Haltens der Sinkrate, wofür die Hinterkantenklappen η_F für die Regelung der Sinkrate ausgefahren werden.

Dargestellt sind im oberen Plot die Höhe über dem Boden, im mittleren Plot die laterale Abweichung zur Landebahnmittellinie und im unteren Plot die Distanz bis zur Landebahnschwelle.

Die Distanz bis zur Landebahnschwelle ist stets positiv. Ab dem Zeitpunkt, wo die Distanz x_{dist} zunimmt, hat das Flugzeug die Landebahnschwelle passiert. Zusätzlich sind im Plot die Grenzen für eine unsichere Landung (grauer Bereich) für den lateralen Abstand zur Landebahnmittellinie und für den Abstand bis zur Landebahnschwelle dargestellt. Die senkrechten Linien stellen den Zeitpunkt des Aufsetzens ($H_{\mathrm{gnd}} = 0$ ft) bei dem jeweiligen CAN-Bus-Fehlerfall dar.

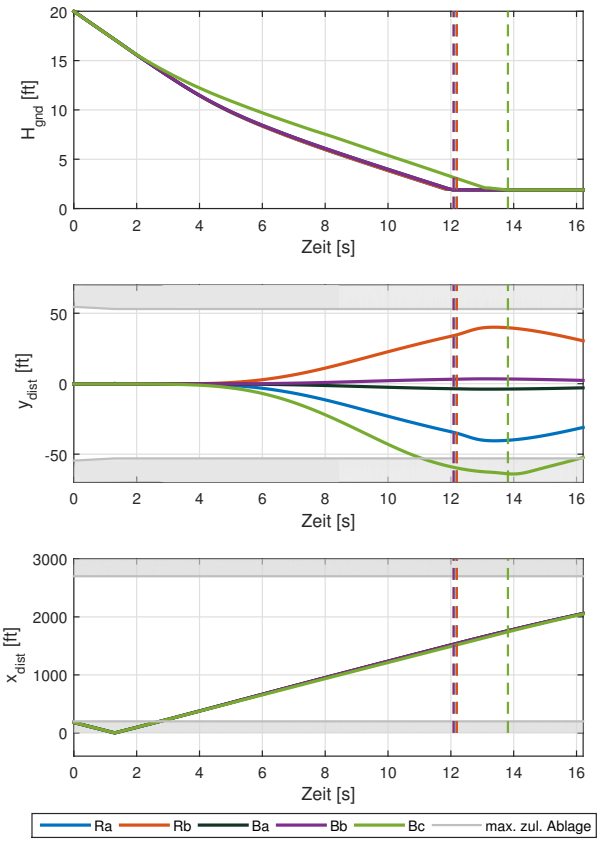

BILD 5: Landesimulation der CAN-Bus-Fehlerfälle

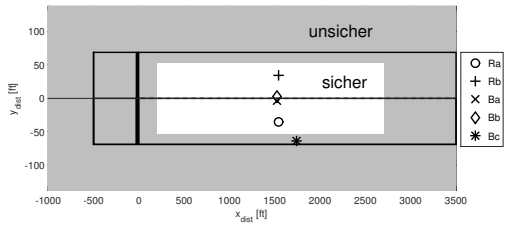

BILD 6: Aufsetzpunkte der automatischen Landung bei CAN-Bus-Kanalausfällen

BILD 6 zeigt die Landebahn mit den fünf Aufsetzpunkten bei den jeweiligen CAN-Bus-Fehlerfällen sowie die Grenzen, die in der CS-AWO definiert sind (siehe Abschnitt 3.4). Werden Grenzen der CS-AWO überschritten, dann ist die Landung unsicher, ansonsten sicher. Von den beiden als kritisch identifizierten CAN-Bus-Fehlerfällen Ra und Bc überschreitet der CAN-Bus-Fehlerfall Bc die Grenze zu einer unsicheren Landung.

Bei dem CAN-Bus-Fehlerfall Bc verfahren die Stellflächen 1L und 5L in die Neutralposition und beim CAN-Bus-Ausfall Ra die Stellflächen 2L und 6L. Beim Abflachen des Gleitwinkels unter 100 ft fahren die Klappen aus und eine asymmetrische Auftriebsverteilung entsteht, welche zu einer zunehmenden seitlichen Ablage zur Landebahnmittellinie führt.

Das Flugzeug setzt beim CAN-Bus-Ausfall Bc 59 ft seitlich der Landebahnmittellinie und somit außerhalb der Landebahn auf (seitliche Ablage größer 53 ft). Somit zeigt die Simulation der automatischen Landung, dass der Ausfall des CAN-Bus-Kanals Bc zu einer unsicheren Landung führt und ein signifikanter Fehlerfall ist. Der Ausfall des CAN-Bus-Kanals Bc führt zum Verlust der Stellfläche 1L, die den größten Anteil an der Bremsklappenwirkung hat. Der kritische Wert für $\hat{N}_\xi$ sollte auf 0,3 gesetzt werden und nicht wie im BILD 3 auf 0,4.

Im Höhenprofil ist im ersten Plot in BILD 5 zu sehen, dass bei dem Ausfall des CAN-Bus-Kanals Bc (grüne Kurve) ein geringeres Abflachen der Flugbahn erfolgt, welches zu einem späteren Aufsetzen auf der Landebahn führt (siehe BILD 6) und deshalb ein stärkeres Abdriften zur Folge hat.

Beim zweiten als kritisch identifizierten CAN-Bus-Fehlerfall Ra landet das Flugzeug zwar innerhalb der geforderten Landezone, befindet sich aber in der Nähe der seitlichen Ablagegrenze. Zusätzliche geringe Störungen wie Seitenwind können bewirken, dass die seitliche Ablagegrenze überschritten wird.

4.4 Monte-Carlo-Simulation

Die Monte-Carlo-Simulationen (MCS) werden zur Analyse von Flugreglern für die automatische Landung und für die Zulassungsnachweise eingesetzt. MCS ist ein stochastisches Verfahren und dient dazu, eine große Anzahl von Zufallsexperimenten für statistische Analysen durchzuführen. Die Umgebungsbedingungen P_i sind über eine Verteilungsfunktion F vorgegeben. Für jeden Parametern werden 2000 Stichproben generiert, simuliert und skalare Kriterienwerte K_j berechnet.

Die Auswirkung von stochastisch ändernden Parameter können mit einer geringen Anzahl von Simulationen abgeschätzt werden. MCS wird bei der Untersuchung der automatischen Landung für variierender Umgebungsbedingungen wie Wind, Turbulenz, Temperatur, Flugplatzhöhe und Landebahnsteigung im nominalen und fehlerhaften Fall angewendet. Die CS-AWO [2] definiert mittlere Risiken (*average risk*) bei denen alle Parameter probabilistisch variiert werden und Grenzrisiken (*limit risk*), bei denen einzelne Parameter auf ihre Extremwerte fixiert werden.

4.5 Grenzfallsimulation

Für die CAN-Bus-Ausfälle ist ein relevanter Parameter der Seitenwind, weil dieser die seitliche Ablage zur Landebahnmittellinie beim Aufsetzen beeinflussen kann. Für das HALE-Flugzeug wird der maximal zulässige Seitenwind in 10 m Höhe auf den Wert $v_W = 3\ \mathrm{m/s}$ fixiert.

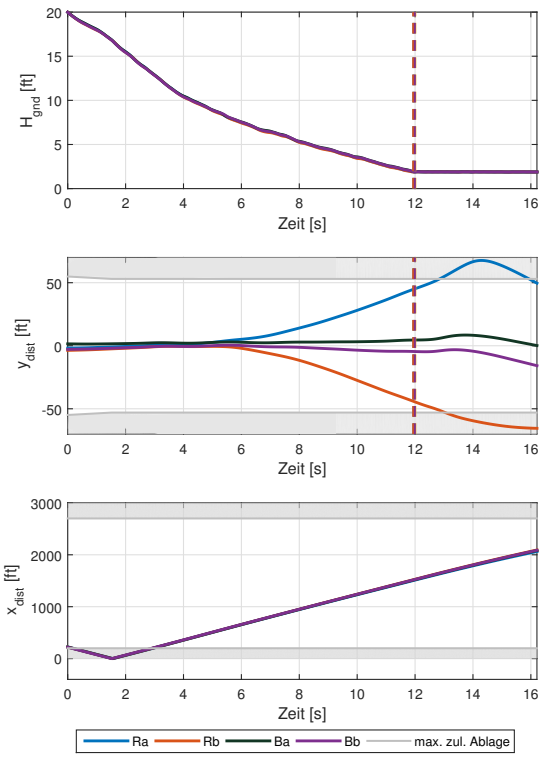

BILD 7: Landesimulation der CAN-Bus-Fehlerfälle (Eingabeparameter AR aus TAB 8)

Die Grenzfälle mit den entsprechenden Zustände sind in TAB 8 aufgelistet.

TAB 8: Abgeleitete Eingabegrößen mit maximaler seitlicher Ablage aus der *average risk* (AR) und *limit risk* (LR) Analyse für den fehlerfreien Fall

Parameter	AR	LR
$u_{W,10}$ $[\mathrm{m/s}]$	-0.6	-2
$v_{W,10}$ $[\mathrm{m/s}]$	3	-3
x_{CG} $[\mathrm{m}]$	-6.79	-6.65
h_{Rwy} $[\mathrm{m}]$	1636.16	2769.94
T $[\mathrm{K}]$	-2.86	-5.26
γ_{Rwy} $[^\circ]$	0.38	0.32
y_{dist} $[\mathrm{m}]$	-6.63	6.18

Die Simulation der CAN-Bus-Fehlerfälle Ra, Rb, Ba, Bb mit den Eingabeparametern (AR) aus TAB 8 ist in BILD 7 dargestellt.

In BILD 5 zeigte sich bereits bei den CAN-Bus-Fehlerfällen Ra und Rb eine sehr hohe seitliche Ablage. Das Flugzeug befand sich aber während des Aufsetzens sowie beim Abrollvorgang innerhalb der Landezone. Mit den Eingabeparametern des *average risk* Grenzfalls zeigt sich bei der Simulation der CAN-Bus-Fehlerfälle in BILD 7 eine noch höhere seitliche Ablage für die CAN-Bus-Ausfälle Ra und Rb. Zwar befindet sich das Flugzeug beim Aufsetzen innerhalb der Landezone, jedoch driftet das Flugzeug durch den starken Seitenwind ab und verlässt die Landebahn. Folglich führen die CAN-Bus-Fehlerfälle Ra und Rb zu einer unsicheren Landung.

Ein ähnliches Verhalten zeigt auch die Simulation mit den Eingabeparametern (LR) aus TAB 8 in BILD 8. Auch hier weisen die CAN-Bus-Fehlerfälle Ra und Rb nach dem Aufsetzen eine zunehmende seitliche Ablage und driften von der Landebahn ab.

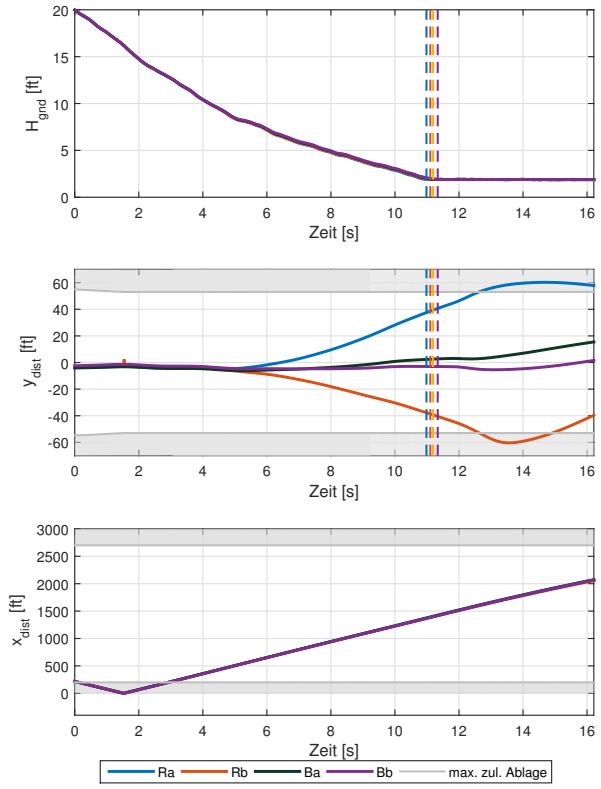

BILD 8: Landesimulation der CAN-Bus-Fehlerfälle (Eingabeparameter LR aus TAB 8)

Aus der Monte-Carlo-Simulation resultieren zwei weitere CAN-Bus-Kanalausfälle, welche bei der automatischen Landung zu einer unsicheren Landung führen. Je mehr Stellflächen von einem CAN-Bus-Kanal angesprochen werden, desto kritischer ist der Fehlerfall. Den CAN-Bus-Kanälen Ba und Bb wird nur eine Stellfläche zugewiesen (siehe TAB 1), während alle anderen CAN-Bus-Kanäle zwei Stellflächen zugewiesen sind. Ihr Ausfall ist deshalb weniger kritisch.

4.6 Reduktion von Doppelfehlerfällen

Gegeben seien die Variablen $\{Ra, Rb, Ba, Bb, Bc\}$ im Testraum T_1, die die CAN-Bus-Kanäle der Systemarchitektur darstellen.

(15) $$\{Ra, Rb, Ba, Bb, Bc\} \in T_1$$

Jeder dieser Variablen $\{Ra, Rb, Ba, Bb, Bc\}$ im Testraum T_1 sind Kombinationen der Stellflächen $\{1L...6R\}$ zugeordnet. Die Variablen $\{1L...6R\}$ definieren Testraum T_2 und entsprechen den Stellflächen, die von den CAN-Bus-Kanälen $\{Ra, Rb, Ba, Bb, Bc\}$ angesprochen werden (siehe TAB 9).

TAB 9: Testraum T_1, analog zu TAB 1

Ra	2L, 6L
Rb	2R, 6R
Ba	3L
Bb	3R
Bc	1L, 5L

Im ersten Schritt werden doppelte und symmetrische Testfälle aus dem Testraum T_1 eliminiert (siehe TAB 10).

TAB 10: Eliminierter Testraum T_1

	Ra	Rb	Ba	Bb	Bc
Ra	-	-	-	-	-
Rb	Ra, Rb	-	-	-	-
Ba	Ra, Ba	Rb, Ba	-	-	-
Bb	Ra, Bb	Rb, Bb	Ba, Bb	-	-
Bc	Ra, Bc	Rb, Bc	Ba, Bc	Bb, Bc	-

Die Integration von Testraum T_2 in Testraum T_1 und die erneute Reduktion der symmetrischen und doppelten Testfälle ergibt den Testraum T_3 (siehe TAB 11).

TAB 11: Testraum T_3

	Ra	Rb	Ba	Bb	Bc
Ra	-	-	-	-	-
Rb	~~2L 6L 2R 6R~~	-	-	-	-
Ba	2L 6L 3L	~~2R 6R 3L~~	-	-	-
Bb	2L 6L 3R	~~2R 6R 3R~~	~~3L 3R~~	-	-
Bc	2L 6L 1L 5L	2R 6R 1L 5L	3L 1L 5L	3R 1L 5L	-

Allein durch Eliminieren von symmetrischen und doppelten Fehlerfällen bleiben von 25 Kombinationen nur 6 übrig.

Die Zulassungsrichtlinie EASA CS-25.1309 [1] definiert, dass ein einfacher Fehlerfall nicht zu einem katastrophalen Flugzustand führen. Die CAN-Bus-Fehlerfälle Ra, Rb, Bc, die seitlich der Landebahn aufsetzen oder abrollen und somit unsicher sind, können als katastrophal angenommen werden. Diese müssen bei der Untersuchung von Mehrfachfehlern nicht mehr betrachtet werden und können eliminiert werden. Dies entspricht in TAB 11 die Zeilen und Spalten $1, 2, 5$.

4.7 Lessons Learned

Es wurde gezeigt, dass mit einfachen flugmechanischen Berechnungen die Worst-Case-Szenarien bei ausfallenden Stellflächen identifiziert werden können. Beispielhaft zeigte die Simulation, dass ohne Windstörungen nur einer der identifizierten Fehlerfälle tatsächlich katastrophale Auswirkungen hat. Mit der MCS konnten zwei weitere katastrophale Fehlerfälle bei Seitenwind identifiziert werden. Das Resultat ist, dass zunächst die Einzelfehlerfälle, welche zu einer unsicheren Landung führen würden durch Änderung der Systemarchitektur oder des Flugreglers gelöst werden müssen, bevor Doppelfehler untersucht werden. Dieser Beitrag zeigt wie die Untersuchung von Fehlerfällen im frühen Entwicklungsstadium effektiv gestaltet werden kann. Die Flugzeugsystementwicklung ist ein iterativer Prozess. Aus den Fehlerfallanalysen werden Anforderungen abgeleitet, die in der weiteren Entwicklung beachtet werden müssen.

5 ZUSAMMENFASSUNG UND AUSBLICK

Der Beitrag demonstriert, wie aus einer komplexen Flugsteuerungssystemarchitektur zu untersuchende Fehlerfälle reduziert und beispielhaft signifikante CAN-Bus-Kanalausfälle identifiziert werden können. Ein erstes Identifizieren der signifikanten Fehler erfolgte durch vereinfachte analytische flugmechanische Berechnungen.

Mit der Methode konnten schnell Fehler in der Kommunikation zwischen Flugsteuerungsrechner und Stellflächenaktuatorik mittels Worst-Case-Szenarien vorhergesagt werden. In diesem Beitrag wurden kritische CAN-Bus-Kanäle identifiziert, die keine sichere Landung und Abrollen nach der Landung ermöglichen. Es wurde vereinfacht angenommen, dass der Fehlerfall bereits zu Beginn des Landeanflugs aktiv ist. In künftigen Untersuchungen sollte darüber hinaus der Aktivierungszeitpunkt des Fehlers mit betrachtet werden.

Die nichtlineare Simulation der automatischen Landungen bestätigte die richtig ausgewählten Worst-Case-Fehlerfälle. Mit den aus MCS gewonnenen Eingabeparametern wurden weitere Fehlerfälle identifiziert, die zwar eine Landung innerhalb der Landezone ermöglichen, jedoch beim Abrollen von der Landebahn abdriften. Mit der EASA CS-25.671 Anforderung, dass ein einfacher Fehlerfall keine katastrophale Auswirkung besitzen darf, müssen Fehlerfälle mit katastrophaler Auswirkung bei der Untersuchung von Mehrfachfehler nicht betrachtet werden. Es stellte sich heraus, dass infolge der Reduktion der mehrfachen, symmetrischen und zu unsicheren Landung führenden Fehlerfällen keine Mehrfachfehler untersucht werden müssen.

Die nichtlineare Simulation in Kombination mit MCS erwies sich als ein effizientes Werkzeug, die Fehlerfälle bereits im frühen Entwicklungsprozess systematisch zu bewerten. Insbesondere bei der automatischen Landung und bei unbemannten Flugzeugen ohne Pilot ist mit der MCS die Reproduzierbarkeit der Tests und der Ergebnisse gewährleistet. Die für die Flugsimulation verwendeten Modelle müssen mit realen Flugversuchsdaten validiert werden.

Wichtig ist zu erwähnen, dass die in diesem Beitrag demonstrierte Methode ein Werkzeug ist. Sie soll erfahrene Piloten und Entwicklungsingenieure bei der Einstufung von Fehlerfällen unterstützen, sie aber nicht komplett ersetzen. Die Wissensbasis von Testpiloten oder Testingenieuren ist ein integraler Bestandteil bei der Untersuchung und Bewertung von Fehlerfällen.

6 DANKSAGUNG

Diese Arbeit entstand zunächst im Kooperationsvorhaben „FCL-Methods „ mit der Leichtwerk AG. Das diesem Bericht anschließend zugrunde liegende Vorhaben „Innovative Bausteine für sicherheitskritische Flugsteuerungssysteme für unbemannte Arbeitsflugzeuge, die in der Stratosphäre fliegen (IBAS) „ wurde mit Mitteln des Landes Niedersachsen unter dem Förderkennzeichen ZW1-80158888 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

LITERATUR

[1] European Aviation Safety Agency (EASA). Certification Specification For Large Aeroplanes CS-25 Amendment 25. Brüssel, 24 June 2020.

[2] European Aviation Safety Agency (EASA). Certification Specifications for All Weather Operations (CS-AWO): Issue 2. Brüssel, 31 January 2022.

[3] Ibrahim Karakaya and Robert Luckner. *Automatisierte Untersuchung und Bewertung von Fehlerfällen in elektronischen Flugsteuerungen mittels Flugsimulation*. Deutsche Gesellschaft für Luft- und Raumfahrt-Lilienthal-Oberth e.V., 2020.

[4] Ibrahim Karakaya and Robert Luckner. *Automatisiertes Testen von Mehrfachfehlern in der Aktuatorik hinsichtlich ihrer Auswirkungen auf flugmechanische Eigenschaften*. Deutsche Gesellschaft für Luft- und Raumfahrt-Lilienthal-Oberth e.V., 2020.