AUTOMATISIERTES TESTEN VON MEHRFACHFEHLERN IN DER AKTUATORIK HINSICHTLICH IHRER AUSWIRKUNGEN AUF FLUGMECHANISCHE EIGENSCHAFTEN

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

Zusammenfassung

Im Flugzeugbau wird bereits in der frühen Konzeptphase mit der Entwicklung sicherheitskritischer, komplexer und hochintegrierter Systeme begonnen. Die geplanten Flugzeugfunktionen werden in der Hauptentwicklungsphase mit erheblichem Aufwand entsprechend SAE ARP 4754A sowie SAE ARP 4761 im Detail zu einer Systemarchitektur ausgearbeitet. Für die Entwicklung der Flugregelungsfunktionen und für die Nachweisführung sind zur Bewertung der Flugeigenschaften im Rahmen der Zulassung Tests durch die Luftfahrtbehörden gefordert. Die umfangreichen Tests sind kosten- und zeitintensiv. Dieser Beitrag betrachtet ein effizientes, automatisiertes und strukturiertes Testen der Fehlerfälle. Dazu gehört auch das Untersuchen von Mehrfachfehlern, d.h. dem Ausfall mehrerer Komponenten. Heutige Systemarchitekturen verwenden redundante Rechner und Stellflächen für die Flugsteuerung. Daraus ergibt sich eine erhebliche Testmenge, die abgebildet und untersucht werden muss. In diesem Beitrag werden Schwierigkeiten bei der quantitativen Untersuchung von Einfach- und Mehrfachfehler entsprechend Zulassungsspezifikation CS AMC 25.1309 adressiert. Die Untersuchung der Mehrfachfehler in der Aktuatorik erfolgt mit der Flugsimulation eines hochfliegenden Flugzeugs mit langer Flugdauer.

Nomenklatur

Abkürzungen

CS	Certification Specification
CAT	Catastrophic
CAS	Calibrated Airspeed
EASA	European Aviation Safety Agency
FHA	Functional Hazard Analyse
HALE	High Altitude Long Endurance
PASA	Preliminary Aircraft Safety Assessment
TAS	True Air Speed
UAV	Unmanned Aerial Vehicle

Formelzeichen (groß)

$\underline{\underline{A}}$	Systemmatrix
$\underline{\underline{B}}$	Stellmatrix
$\underline{\underline{C}}$	Ausgangsmatrix
$\underline{\underline{D}}$	Durchgangsmatrix
H_{bar}	barometrische Höhe
V	Fluggeschwindigkeit

Formelzeichen (klein)

m	Masse
p	Rollrate
r	Gierrate
s	Halbspannweite
$\underline{u}$	Stellgrößenvektor
$\underline{x}$	Zustandsvektor
$\underline{\dot{x}}$	Ableitung des Zustandsvektors

Griechische Symbole (groß)

Φ	Hängewinkel
Φ_1	Hängewinkel nach dem ersten Fehlerfall
Φ_2	Hängewinkel nach dem zweiten Fehlerfall
$\hat{\Phi}_1$	Kritikalität des Hängewinkels nach dem ersten Fehlerfall
$\hat{\Phi}_2$	Kritikalität des Hängewinkels nach dem zweiten Fehlerfall

Griechische Symbole (klein)

β	Schiebewinkel
β_1	Schiebewinkel nach dem ersten Fehlerfall
β_2	Schiebewinkel nach dem zweiten Fehlerfal
$\hat{\beta}_1$	Kritikalität des Schiebewinkels nach dem ersten Fehlerfall
$\hat{\beta}_2$	Kritikalität des Schiebewinkels nach dem zweiten Fehlerfall
$\dot{\delta}_{\max}$	maximale Stellrate
ξ	Querruderstellung
ζ	Seitenruderstellung

Notiz: Im Beitrag ist der Fehlermode ein dynamischer Ausfall (z.B. Weglaufen einer Stellfläche). Ein Fehlerfall entspricht einer Ausfallbedingung mit einem Fehlermode.

doi:10.25967/530227

1 EINLEITUNG

Die Entwicklung von sicherheitskritischen, komplexen und hochintegrierten Flugzeugsystemen muss frühzeitig begonnen werden. Sie ist aufwendig und schwierig, weil die Funktionen und ihre Kritikalität in der Entwurfsphase zunächst nur grob bekannt sind. Das gilt beispielsweise für die Funktionen mit denen Höhenruder-, Querruder- oder Seitenruderausschläge kommandiert werden sollen.

Für die Systementwicklung werden Richtlinien entsprechend SAE ARP 4754A und SAE ARP 4761 verwendet. Die Zulassungsvorschriften der Luftfahrtbehörde EASA CS 23.2510 bzw. CS 25.1309 (Equipment, systems, and installations) fordern eine Untersuchung von Fehlerfällen bei allen Flugzuständen. Das beinhaltet viele zeitintensive Test und erfordert sehr aufwändige manuelle Arbeit. Hierzu gehört auch das Untersuchen von Mehrfachfehlern (Ausfall von mehreren Komponenten) und ihre Auswirkung auf die Flugmechanik.

Große Flugzeughersteller haben die dafür erforderlichen Ressourcen, doch für kleine und mittlere Luftfahrtunternehmen stellt die Entwicklung von sicherheitskritischen, komplexen Flugzeugfunktionen vor allem in der Flugsteuerung und in der Avionik eine große Herausforderung dar. Bei dieser Aufgabe kann die Flugsimulation als Hilfsmittel verwendet werden, um automatisiert, systematisch und effizient kritische Fehlerfälle ausfindig zu machen, zu bewerten und daraus Anforderungen and die Systemarchitektur abzuleiten (siehe BILD 1).

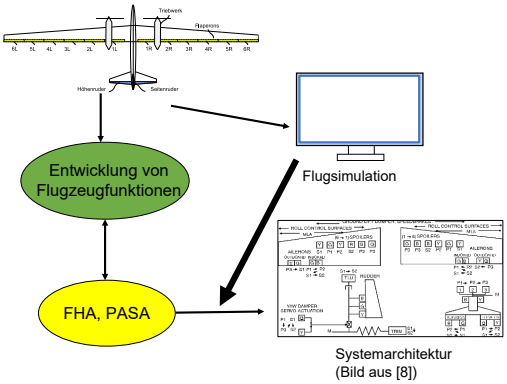

BILD 1: Flugsimulation zum Ableiten von Anforderugnen an die Systemarchitektur. Systemarchitektur aus [1]

Ziel dieses Beitrags ist das Untersuchen von Einfach- und Mehrfachfehler entsprechend CS AMC 25.1309 11.d.4(1) mittels Flugsimulation. Dazu wird eine Methode für die automatisierte, strukturierte Analyse von Mehrfachfehlern demonstriert.

Hierfür wird die aus dem nichtlinearen Modell linearisierte lineare Flugsimulation eines hoch fliegenden Flugzeugs mit langer Flugdauer (HALE) verwendet.

2 FEHLERKLASSIFIZIERUNG

Eine Ausfallbedingung (*failure condition*) ist eine Bedingung, die sich entweder auf das Flugzeug, auf die Arbeitsbelastung des Piloten oder auf die Gesundheit der Insassen oder auf alle, auswirkt. Sie kann durch einen oder mehrere Ausfälle (*failures*) oder Fehler (*errors*) enstehen. Zu ihrer Bewertung tragen die Flugphase und relevante widrige Betriebs- oder Umweltbedingungen oder externe Ereignisse bei. [2]. Die Ausfallbedingungen werden entsprechend ihrer Schwere nach CS 25.1309 klassifiziert. Sie lauten frei und gekürzt übersetzt wie folgt:

***No Safety Effect*:** Ausfallbedingungen, die keinen Einfluss auf die Sicherheit haben.

***Minor*:** Ausfallzustand, der die Sicherheit des Flugzeugs nicht signifikant reduziert und Handlungen der Besatzung erfordert, die klar im Rahhmen ihrer Fähigkeiten liegen, aber beispielsweise zu einer leichten Verringerung der Sicherheitsmargen, einer leichten Erhöhung der Arbeitsbelastung der Besatzung und einigen physischen Unannehmlichkeiten für die Insassen führt.

***Major*:** Erhebliche Reduktion der Sicherheitsmargen und der funktionalen Fähigkeiten des Flugzeugs, erheblich erhöhte Arbeitsbelastung oder Bedingungen, die die Effizienz der Besatzung beeinträchtigen, physischer Stress für Passagier einschließlich möglicher Verletzungen.

***Hazardous*:** Große Reduktion der Sicherheitsmargen und der funktionalen Fähigkeiten des Flugzeugs, hohe physische Belastung der Besatzung oder exzessive Arbeitsbelastung, so dass nicht sicher ist, dass sie die Flugmission akkurat und vollständig durchführen kann, sowie ernsthafte oder tödliche Verletzungen einer relativ kleinen Anzahl von Passagieren resultieren.

***Catastrophic*:** Ausfallbedingungen, die einen weiteren sicheren Flug und eine sichere Landung verhindern.

Die Art der Fehlerfallanalyse wird in CS AMC 25.1309 11.d.(4) adressiert. Das Signalflussdiagramm in BILD 2 zeigt die Vorgehensweise zur Auswahl der richtigen Untersuchungsmethode.

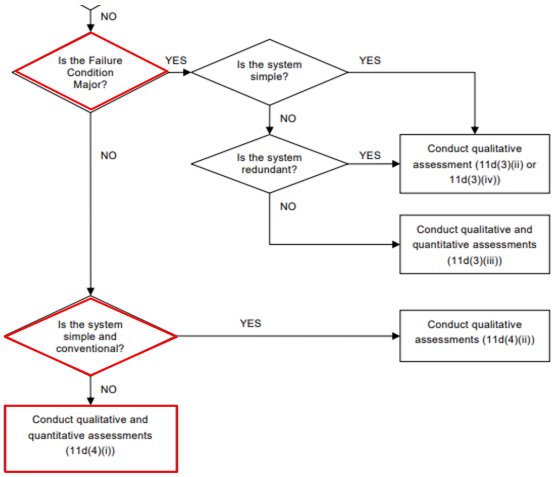

BILD 2: Signalflussdiagramm zur Vorgehensweise bei der Untersuchung und Bewertung von schwerwiegenden Fehlerfällen, Ausschnitt aus [2]

Dieser Beitrag befasst sich mit dem elektronisch steuerungssystem, das weder einfach noch kon aufgebaut ist. Er konzentriert sich auf die Unte von Fehlerfällen mit Folgen, die gefährlich (*ha* und katastrophal (*catastrophic*) sind. In diesen F nach CS AMC 25.1309 qualitative und quantitati suchung durchzuführen. Dieser Beitrag demons quantitative Untersuchungen.

Für die quantiative Untersuchung von Aktua muss der Flugzustand mit folgenden Parameterr werden:

1. Flugphase,
2. Konfiguration,
3. Masse,
4. Schwerpunkt,
5. Staudruck, Luftdichte,
6. Wind.

Außerdem sind kritische Fehlerfälle zu ermitteln. Fälle mit den Konsequenzen *hazardous* und *catastrophic* sind gesondert und detailliert zu untersuchen. Hierfür wird die Methode der Auswahl eines Worst-Case-Szenarios ausgewählt, welche in Abschnitt 3.5 beschrieben wird.

3 UNTERSUCHUNGSMETHODE

3.1 Definition der Fehlerfälle

Insgesamt können folgende Fehlermodi untersucht werden:

- *Actuator Jam*: Blockade der Stellfläche in neutraler Position oder in einer kommandierten Stellflächenposition.
- *Transient Runaway*: Transientes Weglaufen der Stellfläche,
- *Unlimited Runaway*: Unbegrenztes Weglaufen der Stellfläche mit maximaler Stellrate bis zum mechanischen Limit,
- *Surface Float*: Auswehen des Ruders,
- *Surface Oscillation*: Oszillieren des Ruders.

Untersucht wird der Fehlerfall *Unlimited Runaway* (auch *Hardover* genannt). Es ist ein zeitabhängiger dynamischer Fehlerfall, der ein unbegrenztes Weglaufen der Stellfläche mit maximaler Stellrate bis zum Maximalausschlag beschreibt.

BILD 3 zeigt den zeitlichen Verlauf einer weglaufenden Stellfläche. Der Fehler beginnt ab dem Zeitpunkt t_0 in der Ruderstellung d_0. Die Ruderstellung d_0 ist ein kommandierter Wert, welcher sich aus dem momentanen Flugzustand ergibt. Der Ruderausschlag d_1 ist entweder die mechanische Grenze für die Ruderfläche (beim unbegrenzten Auswandern der Stellfläche) oder ein bestimmter Wert (limitiertes Auswandern). Das limitierte Weglaufen der Stellfläche ergibt sich, wenn der Fehler erkannt wird und die Stellfläche in der momentanen Position eingefroren und anschließend in eine neutrale Position gefahren wird.

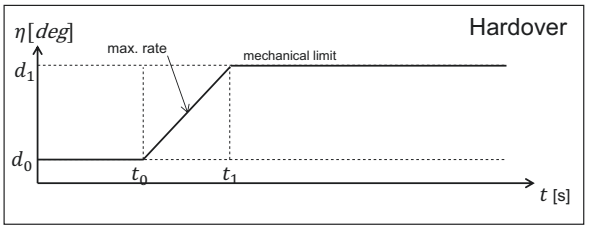

BILD 3: *Hardover, unbegrenztes Weglaufen der Stellfläche*

Es wird angenommen, dass das unbegrenzte Wegwandern der Stellfläche der kritischste Fehlermode ist.

Die Anzahl der zu untersuchenden Fälle hängt von der Anzahl der Stellflächen und der Anzahl der zu untersuchenden Fehler ab. Bei 12 Stellflächen folgen beispielsweise bei Betrachtung von Doppelfehlern insgesamt

(1) $(12 \cdot 2) - 12 = 132$ Fehlerfälle .

Symmetrische Fehlerfälle können intelligent eliminiert werden, wenn das Flugzeug symmetrisch ist. Dadurch reduzieren sich die zu untersuchenden Fälle um 50%. Da auch meist das Vorzeichen des Ruderausschlags beim Weglaufen relevant ist, folgen 132 zu untersuchende Fehlerfälle.

3.2 Flugbereich und Konfiguration

Die Flugzustände im zu untersuchenden Flugbereich in BILD 4 sind über ein Gridding-Verfahren definiert. Sie liegen an den als kritisch anzusehenden Flugbereichsgrenzen (minimale Höhe und Geschwindigkeit, maximale Höhe und Geschwindigkeit) sowie im mittleren Staudruckbereich.

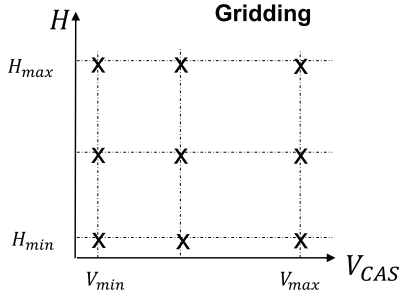

BILD 4: Untersuchender Flugbereich

Untersucht wird die hinterste Schwerpunktlage. Die Masse ist konstant und ändert sich nicht während der Simulation.

3.3 Systemarchitektur des untersuchenden Flugzeugs

Das HALE-Flugzeug ist zur Rollsteuerung mit jeweils sechs Flaperons auf der linken- und rechten Flügelhälfte ausgestattet. Sie werden mit einem elektrischen Aktuator angesteuert. Die Flaperons werden zum Rollen um die Längsachse, das Seitenruder wird zum Gieren um die Hochachse und das Höhenruder zum Nicken um die Nickachse verwendet. Für die Steuerung um die Rollachse ist das Flugzeug mit 12 Stellflächen überaktuiert. BILD 5 zeigt die Draufsicht des HALE-Flugzeugs. Dieser Beitrag konzentriert sich auf Fehler in der Rollsteuerung. Das Seitenruder und Höhenruder werden deshalb hier nicht betrachtet.

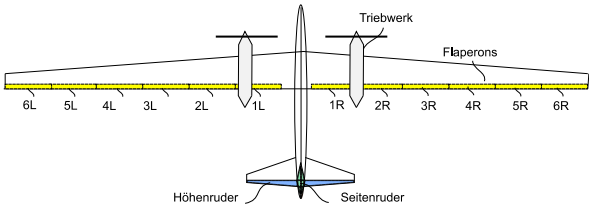

BILD 5: Draufsicht auf ein exemplarisches HALE-Flugzeugs

Die Umwandlung zwischen dem Querruderkommando ξ und den Einzelklappen ξ_{iL}, ξ_{iR} geschieht im Verhältnis 1/3. Bei maximalem Querruderkommando von $\pm$ 10 Grad schlagen die Einzelklappen auf $\pm$ 30 Grad aus. Dieses Mischungsverhältnis ist Resultat aus aerodynamischen Analysen.

3.4 Modell der Flugmechanik

Die Flugdynamik wird üblicherweise durch eine nichtlineares Modell simuliert. Hier wird vereinfachend ein lineares Zustandsraum-Modell der Seitenbewegung verwendet.

$$\dot{\underline{x}} = \underline{\underline{A}} \cdot \underline{x} + \underline{\underline{B}} \cdot \underline{u} \quad . \tag{2}$$

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 Stellgrößen dar.

Die Zustandsgrößen $\underline{x}_i$ sind die Gierrate r, der Schiebewinkel β, die Rollrate p und der Hängewinkel Φ.

$$\underline{x} = [r, \beta, p, \Phi]^{\mathrm{T}} \quad . \tag{3}$$

Die Stellgrößen $\underline{u}_i$ beinhalten die Einzel-Querruderklappen ξ_{iL}, ξ_{iR} und das Seitenruder ζ

$$\underline{u} = [\xi_{iL}, \xi_{iR}, \zeta]^{\mathrm{T}}_{i=1\ldots6} \tag{4}$$

Die den Einzelklappen zugeordnete Stellmatrix $\underline{\underline{B}}$ wird durch das bekannte Übersetzungsverhältnis zwischen Querruderkommando und Einzelklappenausschlag zu einer nur vom gesamten Querruderkommando ξ abhängigen Stellmatrix umgewandelt

$$\underline{\underline{\bar{B}}} = 3 \cdot \begin{bmatrix} B_{r,\xi_{1L}} + B_{r,\xi_{2L}} + \cdots + B_{r,\xi_{6R}} \\ B_{\beta,\xi_{1L}} + B_{\beta,\xi_{2L}} + \cdots + B_{\beta,\xi_{6R}} \\ B_{p,\xi_{1L}} + B_{p,\xi_{2L}} + \cdots + B_{p,\xi_{6R}} \\ B_{\Phi,\xi_{1L}} + B_{\Phi,\xi_{2L}} + \cdots + B_{\Phi,\xi_{6R}} \end{bmatrix} \quad . \tag{5}$$

Das Pilotenmodell kommandiert einen Querruderausschlag ξ mit

$$u = \xi = f(x) + g(\mathrm{Fehler}) \; . \tag{6}$$

Der Regler $f(x)$ ist in [4] erläutert. Zusätzlich kann die Fehlererkennung ein Kommando zur Fehlerkompensation $g(\mathrm{Fehler})$ kommandieren.

3.5 Methode: Auswahl eines Worst-Case-Szenarios

Bei der Analyse der Fehlerfälle ist ein Worst-Case-Szenario auszuwählen. Der kritische Fehlerfall ist der Ausfall der Stellfläche, die das größte Rollmoment erzeugt. Es wird angenommen, dass die äußerste Stellfläche ξ_6 aufgrund des Hebelarms das größte Rollmoment erzeugt. Folgender Ablauf wird ausgeführt:

1. **Erster Fehlerfall:** Unlimited Runaway der äußeren Stellfläche (bspw. ξ_6),
2. **Pilotenreaktion:** Drei Sekunden später (Reaktionszeit für Reiseflug aus [3]) wird der Pilot (hier ein Basisregler der Seitenbewegung entsprechend [4]) aktiv,
3. **Fehlererkennenung:** Zusätzlich zur Pilotenreaktion als Option: nach drei Sekunden Fehlererkennung und zur Fehlerkompensation gleicher Ausschlag auf der Gegenseite (zusätzlich zum Gegensteuern aller Stellflächen durch den Piloten oder durch den Regler). Typischerweise sind die Fehlererkennungszeiten in der Größenordnung 40 ms bis 100 ms. Die drei Sekunden Reaktionszeit des Automatismus sind hier zur Illustration gewählt, um die stationäre Wirkung der Kompensation besser zeigen zu können,
4. **Zweiter Fehlerfall:** Unlimited Runaway der gegenüberliegenden äußeren Stellfläche (die zur Kompensation genutzt wurde) mit entgegengesetztem Vorzeichen.

Das HALE-Flugzeug könnte beispielsweise optional pilotiert sein also sowohl vom Piloten als auch vom Regler geflogen werden können. Hier wird zur Illustration der manuelle Flug simuliert mit drei Sekunden Reaktionszeit des Piloten, bei dem ein erster - noch nicht optimierter - Basisregler der Seitenbewegung nach [4] als Pilotenmodell verwendet wird. Das Weglaufen der Stellfläche in dem Zeitraum t_0 bis t_1 entspricht einem integrierenden Verhalten mit maximaler Stellrate $\dot{\delta}_{\max}$ (siehe Gleichung 7).

$$\delta(t) = \int_{t_0}^{t_1} \dot{\delta}_{\max} \, \mathrm{dt} \; . \tag{7}$$

Der gesamte Ablauf des Doppelfehlers ist in BILD 6 dargestellt.

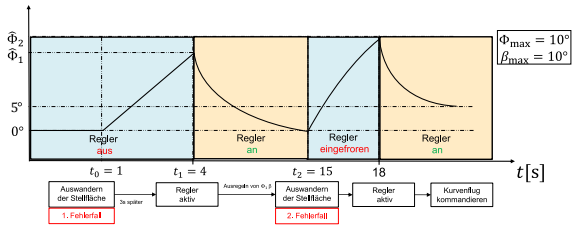

BILD 6: Testablauf für den Doppelfehler

Bei dem ersten Fehler wandert die erste Stellfläche ξ_i eine Sekunde nach Simulationsstart bis zum mechanischen Limit aus. Nach drei Sekunden wird das Pilotenmodell aktiv und der Hängewinkel und Schiebewinkel durch das Weglaufen der Stellfläche werden abgebaut. Um die Rollrate durch die ausgewanderte Stellfläche auszugleichen, wird die gegenüberliegende Stellfläche (bspw. Flaperon 6L $\rightarrow$ Flaperon 6R) in die gleiche Richtung ausgelenkt.
Nachdem ein stationärer Zustand erreicht wird, wird der zweite Fehlerfall aktiv und die zweite gegenüberliegende

Stellfläche ξ_j wandert aus. Der Regler wird hierbei nicht ausgeschaltet, sondern eingefroren. Drei Sekunden nach dem zweiten Fehlerfall wird der Regler wieder eingeschaltet. Es wird anschließend ein Hängewinkelkommando von fünf Grad vorgegeben. Das soll zeigen, ob nach einem Doppelfehler noch ein Kurvenflug fliegbar ist.

3.6 Bewertung der Fehlerfälle

Beim Weglaufen der Stellflächen gilt, dass die im operationellen Betrieb maximal zulässigen Hängewinkel $\Phi_{\max}$ und Schiebewinkel $\beta_{\max}$ nicht überschritten werden sollen. Die Grenzen leiten sich Flugleistungs- und Steuerbarkeitsanforderungen ab. Für das HALE-Flugzeug werden sie wie folgt gewählt:

(8) $$\Phi_{\max} = 10^\circ$$

(9) $$\beta_{\max} = 10^\circ \quad .$$

Die angenommenen maximal zulässigen Hängewinkel und Schiebewinkel müssen im weiteren Verlauf der Entwicklung durch Flugsimulationen bestätigt werden, weil diese flugzeugspezifisch sind.

Die Bewertung des ersten Fehlerfalls erfolgt analog zu [6] mit normierten Parametern. Für den Schiebewinkel und Hängewinkel sind die normierten Parameter

(10) $$\hat{\Phi}_1 = \frac{\Phi(t_0 + 3\ \mathrm{s})}{\Phi_{\max}}$$

(11) $$\hat{\beta}_1 = \frac{\beta(t_0 + 3\ \mathrm{s})}{\beta_{\max}} \quad .$$

Die Bewertung des zweiten Fehlerfalls erfolgt drei Sekunden nach dem Zeitpunkt t_2, ab dem das Flugzeug zurück auf den Ausgangsflugzustand zurück geregelt wurde. Es ergeben sich für den zweiten Fehlerfall folgende normierte Hängewinkel und Schiebewinkel

(12) $$\hat{\Phi}_2 = \frac{\Phi(t_2 + 3\ \mathrm{s})}{\Phi_{\max}}$$

(13) $$\hat{\beta}_2 = \frac{\beta(t_2 + 3\ \mathrm{s})}{\beta_{\max}} \quad .$$

Normierte Parameter haben bei der Bewertung den Vorteil, dass sie einheitenlos sind. Ist der normierte Parameter größer eins, so werden die Grenzen des Hängewinkels oder Schiebewinkels überschritten. Dieser Fehlerfall wird für Höhen über 1000 ft nach AC23-17C [3] *hazardous* klassifiziert. Für Höhen unter 1000 ft wäre der Fehlerfall *catastrophic*. Für HALE-Flugzeuge wird hier eine niedrigere Flughöhe (500 ft) als Grenzwert vorgeschlagen, da zum einen die Grenzen $\Phi_{\max}$ und $\beta_{\max}$ niedriger angestellt sind und die Fluggeschwindigkeit sehr gering ist. Es resultieren folgende Bewertungskriterien:

Höhe	catastrophic	hazardous	major/minor
$\geq$ 500 ft	$\hat{\Phi}_{1/2} \geq 2$	$\hat{\Phi}_{1/2} \geq 1$	$\hat{\Phi}_{1/2} < 1$
	$\hat{\beta}_{1/2} \geq 2$	$\hat{\beta}_{1/2} \geq 1$	$\hat{\beta}_{1/2} < 1$
< 500 ft	$\hat{\Phi}_{1/2} \geq 1$	$\hat{\Phi}_{1/2} < 1$	–
	$\hat{\beta}_{1/2} \geq 1$	$\hat{\beta}_{1/2} < 1$	

Zudem definiert die Spezifikation [2], dass kein einzelner Fehlerfall *catastrophic* sein darf. Ist der erste Fehlerfall *catastrophic*, so braucht der zweite Fehlerfall nicht untersucht werden, aber das Design muss geändert werden.

4 ERGEBNIS

Im Folgenden werden die Fehlerfälle des Worst-Case-Szenarios diskutiert. Die Zeitschriebe enthalten im

1. Plot : Seitenruder und Querruderausschlag,

2. Plot : Einzelklappenausschläge,

3. Plot : Hängewinkel mit Kritkalitätsgrenzen,

4. Plot : Schiebewinkel mit Kritikalitätsgrenzen.

Es wird eine Stellratenbegrenzung von 200 °/s angenommen. BILD 7 zeigt den Fehlerfall der Stellfläche 6L und 6R , bei der der Pilot nicht durch eine sofortige Fehlererkennung und Kompensation des Rollmoments durch Ausschlagen der gegenüberliegenden Stellfläche unterstützt wird.

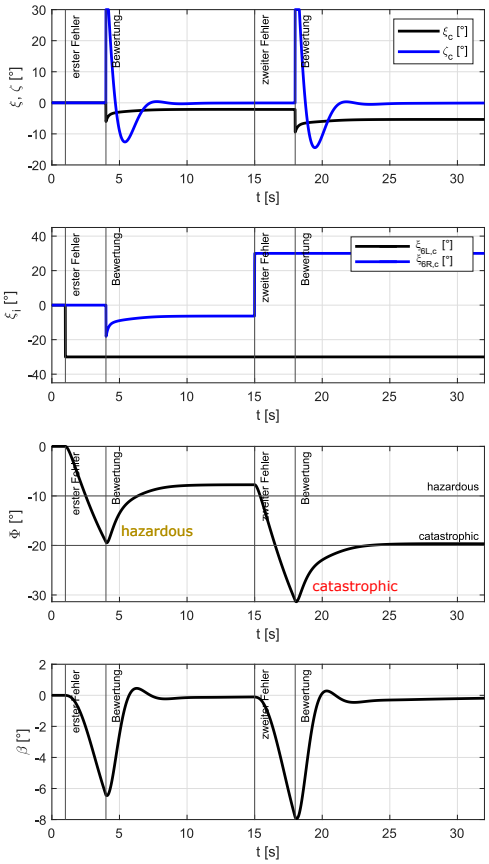

BILD 7: Ausfall der Stellflächen 6L und 6R, H = 18000 m, V_{CAS} = 30 m/s, keine automatische Fehlererkennung

Nach einer Sekunde tritt der erste Fehler auf und die Stellfläche ξ_{6L} wandert in negative Richtung bis zum mechanischen Limit (-30°) aus. Das Flugzeug rollt bis auf fast 20°, überschreitet damit die *hazardous*-Grenze und erreicht sogar fast die *catastrophic*-Grenze. Dabei entstehen Schiebewinkel von über 6°. Drei Sekunden nach dem ersten

Fehler wird der Regler, der den Piloten simuliert, aktiv und baut den Hängewinkel und den Schiebewinkel wieder ab. Es stellt sich heraus, dass der manuelle Flug Schwierigkeiten macht, wenn der Piloten nach der Reaktionszeit entsprechend AC 23-17 C von drei Sekunden [3] nicht von einer automatischen Fehlererkennung unterstützt wird. Nach dem ersten Fehlerfall existiert durch die asymmetrische Rollmomentenverteilung zwischen der linken und rechten Flügelhälfte ein stationärer Hängewinkelfehler. Der Regler ist nicht robust genug, diesen Hängewinkel vollständig abzubauen. Es bleibt ein Restfehler beim Hängewinkel von ca. 8°.
Der erste Fehlerfall wird als *hazardous* eingestuft, weil der maximale Hängewinkel von 10 Grad überschritten wird. Drei Sekunden nach dem zweiten Fehler ist der Hängewinkel mit $\Phi \approx 32^\circ$ mehr als doppelt so groß wie der maximal definierte Hängewinkel ($\Phi_{\max} = 10^\circ$). Aus diesem Grund wird zweite Fehlerfall als *catastrophic* eingestuft.

BILD 8 zeigt den Fehlerfall der Stellfläche 6L und 6R, bei dem der Pilot nach dem ersten Fehlerfall durch eine sofortige Fehlererkennung und Kompensation des Rollmoments durch Ausschlagen der gegenüberliegenden Stellfläche unterstützt wird und bei dem zweiten Fehlerfall nicht.

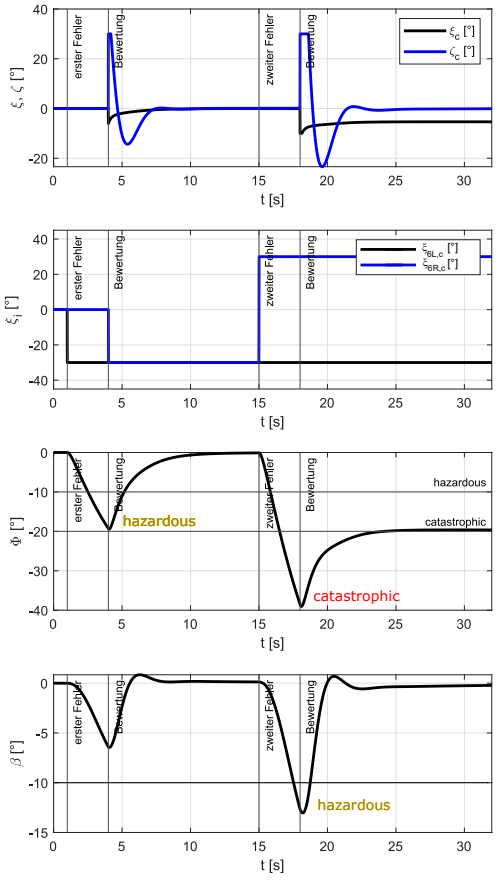

BILD 8: Ausfall der Stellflächen 6L und 6R, H = 18000 m, V_{CAS} = 30 m/s, mit automatischer Fehlererkennung

Das Rollmoment infolge des ersten Fehlers wird durch die sofortige Kompensation durch das Pilotenmodell fast vollständig kompensiert, sodass das Pilotenmodell den Hängewinkel abbauen kann und kein stationärer Fehler übrig bleibt.

Der erste Fehlerfall wird als *hazardous* eingestuft. Bei dem zweiten Fehlerfall, bei dem keine sofortige Fehlererkennung und Kompensation mehr aktiv ist, wird der Fehlerfall als *catastrophic* eingestuft.

Mögliche aus diesem Fehlerfall ableitbare Anforderung oder Variationsmöglichkeiten sind eine

- kürzere Zeit für die automatische Fehlererkennung und -kompensation,
- Optimierung des Reglers hinsichtlich Robustheit,
- Reduktion der Fluggeschwindigkeit und damit der Ruderwirksamkeit der Querruder nach dem ersten Fehlerfall.

Es wurde angenommen, dass die äußerste Stellfläche der Worst-Case-Fall ist. Um dies zu verifizieren gilt es, auch die gleichen Fehlerfälle für die äußeren Stellflächen 5L und 5R zu untersuchen. Für das gleiche Szenario wie bei BILD 8 sind die Zeitverläufe für die Stellflächenausfälle 5L und 5R in BILD 9 dargestellt.

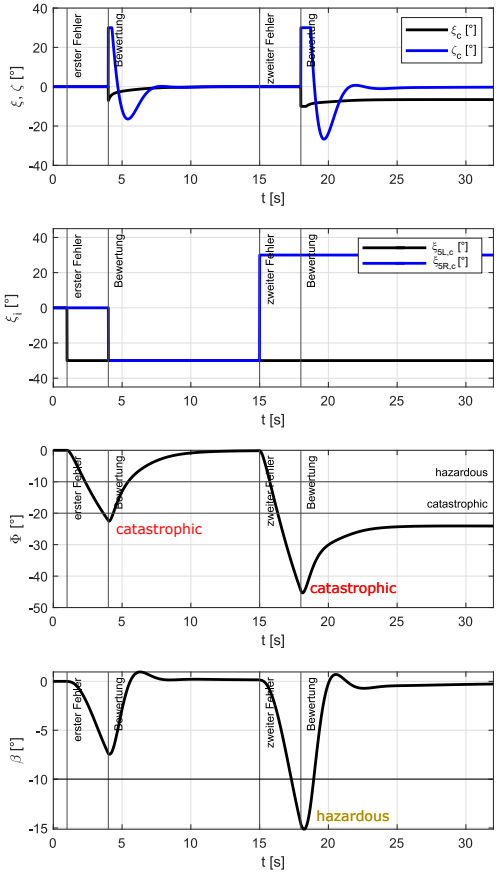

BILD 9: Ausfall der Stellflächen 5L und 5R, H = 18000 m, V_{CAS} = 30 m/s, mit automatischer Fehlererkennung

Die Zeitverläufe zeigen, dass die Ausfälle der Stellflächen 5L und 5R kritischer als bei den äußeren Stellflächen sind. Bereits 1,5 s nach dem ersten Fehler überschreitet der Hängewinkel die *hazardous*-Grenze und 2,7 s später liegt über der *catastrophic*-Grenze. Deshalb ist der erste Fehlerfall bereits *catastrophic*. Der zweite Fehler braucht hiermit

nicht untersucht werden. Das Ergebnis ist plausibel, weil der Rollmomentenbeiwert der Stellfläche 5 größer als der der Stellfläche 6 ist. Auf eine Untersuchung der Stellflächen 1-4 wird verzichtet, da die Auswirkungen von Fehlern durch Analyse der aerodynamischen Beiwerte als weniger kritisch abgeschätzt werden kann. Die elliptische Auftriebsverteilung über dem Flügel ist die Ursache dafür, dass die Rollmomente an den Stellflächen 5L und 5R am größten sind.

Das unbegrenzte Weglaufen einer Stellfläche führt zum Verlust von Steuerautorität. Insbesondere bei Verlust einer äußeren Stellfläche ist die Rollleistung begrenzt und das Fliegen von Kurven wird schwieriger. Aus diesem Grund gilt es zu untersuchen, ob nach einem Einfachfehler und anschließender automatischer Gegenreaktion durch Ausschlagen der gegenüberliegenden Stellfläche bei geringer Höhe und Fluggeschwindigkeit (kritischster Fall) ein Kurvenflug möglich ist - wie der beispielsweise beim Landeanflug notwendig sein kann. Die Ergebnisse der Simulation hierfür sind in BILD 10 dargestellt. Simuliert werden die Einfachfehler 5L sowie 6L. Die Fehler (Ausfall der Stellfläche 5L bzw. Ausfall der Stellfläche 6L) sind im zweiten Plot schwarz dargestellt. Der blaue Graph beschreibt die Gegenreaktion der Stellfläche 6R bzw. 5R nach drei Sekunden Reaktionszeit. Im ersten, dritten und vierten Plot stellt die durchgezogene Linie den ersten Fehlerfall (5L und 5R) und die gestrichelte Linie den zweiten Fehlerfall (6L und 6R) dar. Der Ausfall der Stellflächen 5L und 5R führt zu einem minimal größeren Hängewinkel. Es wird auch ein größerer Querruderausschlag für die Kompensation benötigt. Grund ist das größere Rollmoment der Stellflächen 5L und 5R, das es durch den Ausfall zu kompensieren gilt.

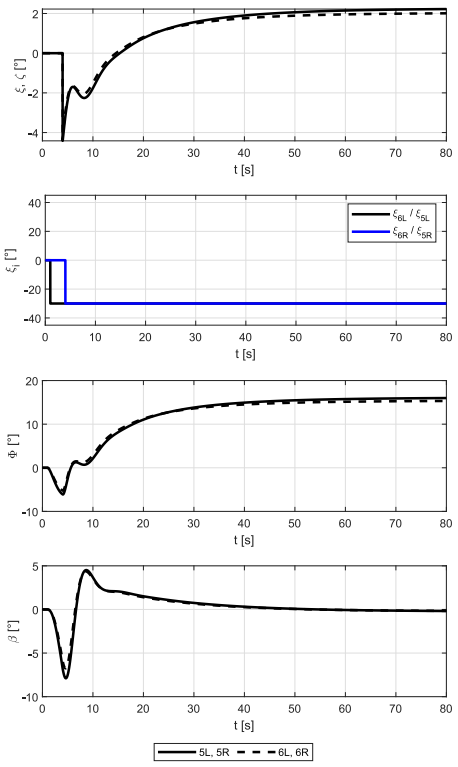

BILD 10: Kurvenflug nach einem Doppelfehler, 100 m Höhe, 12 m/s kalibrierte Fluggeschwindigkeit

Die Zeitverläufe zeigen, dass trotz Verlust von Steuerautorität ein Landeanflug durchgeführt werden kann. Der Schiebewinkel kann trotz des Fehlers minimiert werden.

5 LESSONS LEARNED

Die Ergebnisse zeigen, dass Erfahrung bei der Definition der kritischen Szenarien zur Untersuchung von Fehlerfällen notwendig ist. Vor allem, wenn das Flugzeugverhalten anfangs noch nicht ausreichend bekannt ist, ist es schwierig, kritische Fehlerfälle ausfindig zumachen. Dies gilt beispielsweise für neuartige HALE-Flugzeuge, deren flugmechanische Eigenschaften wenig bekannt sind und für die Zulassungsrichtlinien noch mit den Luftfahrtbehörden vereinbart werden müssen. Hier kann die Flugsimulation helfen.

Um die mühsam gesammelten Erfahren abzusichern, ist ein Ziel, eine Wissensbasis aufzustellen, welche für die automatisierte Fehlerfallgenerierung genutzt werden kann. Für das Aufstellen der Wissensbasis bedarf es ein einheitliches Format zur Definition der Fehlerfälle. Die Wissensbasis kann sich zunächst an den Zulassungrichtlinien für konventionelle Flugzeuge (bspw. CS 25) orientieren, bis gleichwertige Vorschriften für unbemannte HALE-Flugzeuge existieren.

Das Format sollte geeignet sein, die zeitliche Abfolge der Fehlersequenz darzustellen. Zur Definition der komplexen, kritischen Szenarien erscheint der Ansatz der objektorientierten Programmierung (OOP) geeignet zu sein. ist eine Methodik der Softwareentwicklung, die in der Beziehungen zwischen Daten und Algorithmen in Form von Objekten dargestellt werden. Es ermöglicht effektiv die modulare Zerlegung eines komplexen Systems in einzelne Teile. [7]

Für jeden Fehlerfall kann die Flugzeugkonfiguration wie beispielsweise die Flugzeugmasse, Schwerpunktlage, Klappenstellung in einem Unterobjekt definiert werden. Eine mögliche Baumstruktur für die Definition eines Fehlerfalls ist in BILD 11 dargestellt.

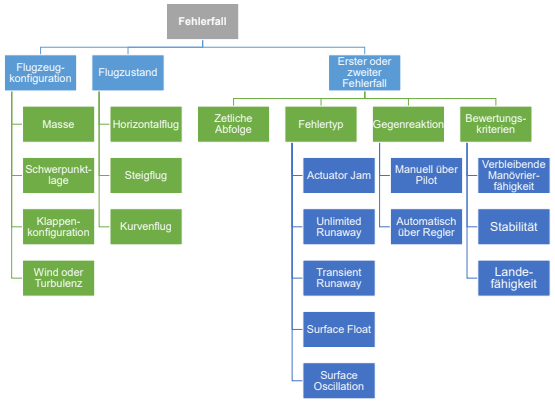

BILD 11: Baumstruktur zur Definition der Fehlerfälle

Analog dazu kann der Flugzustand, in dem ein Fehlerfall auftritt, definiert sein. Das können ein Horizontalflug, Steigflug oder ein Kurvenflug sein. Für den ersten und zweiten Fehlerfall ist die zeitliche Reihenfolge relevant. Da -

außer bei der *Common Cause Analyse* - Mehrfachfehler nicht gleichzeitig auftreten, wird immer abgewartet bis sich nach einem Fehler wieder ein definierter Flugzustand eingestellt hat. Alternativ könnte die Simulation natürlich auch mit dem vorliegen des ersten Fehlers neu gestartet werden. Aus einer Liste von Fehlertypen kann für den ersten Fehlerfall und für den zweiten Fehlerfall ein Fehlertyp ausgewählt werden. Bei Untersuchung von Doppelfehlern bedarf es einer Gegenreaktion durch den Piloten oder vom Regler. Die Untersuchung von Doppelfehlern in einem Zeitschritt ist wichtig bei der *Common Mode Analyse*, welche aber erst in einem späteren Schritt betrachtet werden soll. Jedem Fehlerfall müssen ein oder eventuell sogar mehrere Bewertungskriterien zugeordnet werden, die analog wie die Fehlertypen aus einer Liste von Bewertungskriterien ausgewählt werden kann. Hierfür können bereits existierende Kriterien aus der CS 25 oder eigene, beim flugmechanischen Entwurf verwendete Kriterien verwendet werden. Beispiele sind die verbleibende Manövrierfähigkeit, die Stabilität oder die Landefähigkeit in Bodennähe.

6 ZUSAMMENFASSUNG UND AUSBLICK

Der Beitrag demonstriert beispielhaft, wie Mehrfachfehler in der Aktuatorik untersucht und bewertet werden können. Hierfür wurde, wie in der EASA CS AMC 25.1309 gefordert, eine quantitative Untersuchung durchgeführt. Es hat sich gezeigt, dass die Definition der der kritischen Szenarien zur quantitativen Untersuchung von Doppelfehlern einige Erfahrung und Kenntnisse der Flugmechanik erfordert.

Für die automatisierte Testfallgenerierung ist es deshalb sinnvoll eine Wissensbasis in einem vorgegebendem Format zu erstellen, welche für die automatisierte Fehlerfallgeneration angewendet wird. In die Wissensbasis kann das Know-How von erfahrenen Entwicklungsingenieuren eingehen und sie sollte Erkenntnisse sammeln, die im Laufe eines Projektes gewonnen werden. Zum Erstellen der Wissensbasis ist ein Format zur Definition der Fehlerfälle, der Szenarien und der Bewertungskriterien notwendig, mit dem ein Fehlerfall einheitlich, flexibel und effizient definiert und hinsichtlich seiner Kritikalität bewertet werden.

Die Anzahl der zu untersuchenden Fehlerfälle kann beispielsweise durch Nutzung von Symmetrieeigenschaften oder mit einer Methode zu Auswahl der kritischsten Fehlerfälle durch Suche nach Worst-Case-Szenarien intelligent reduziert werden. Das ist vor allem bei heutigen Flugzeugen mit sehr komplexen Systemarchitekturen, die sehr viele Tests erfordern, sinnvoll.

In einem ersten Schritt werden mit der Untersuchung der Einfachfehler alle katastrophalen Fehlerfälle identifiziert. Da diese in der Flugsteuerung nicht zulässig sind, müssen Lösungen gefunden werden, die die Konsequenz des Fehlers mindestens auf *hazardous* reduzieren. Erst dann hat es Sinn, Doppelfehler zu untersuchen.

Die Flugsimulation kann verwendet werden, um die kritischen Fehler zu identifizieren. Dies kann beispielsweise über ein Worst-Case-Search nach [8], [5] geschehen, der die kritischen Flugzustände ausfindig macht.

Um die Menge an Ergebnisse besser und kompakter sichtbar zu machen, ist ein automatischer Reportgenerator sinnvoll.

7 DANKSAGUNG

Dieses Vorhaben wurde in dem Projekt FCL-HALE am Fachgebiet Flugmechanik, Flugregelung und Aeroelastizität an der Technischen Universität Berlin durch den Drittmittelgeber Leichtwerk AG finanziert.

LITERATUR

[1] D. Briére, C. Favre, and P. Traverse. A family of fault-tolerant systems: electrical flight controls, from airbus a320/330/340 to future military transport aircraft. volume 19, pages 75 – 82, 1995, doi: 10.1016/0141-9331(95)98982-P.

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

[3] Federal Aviation Administration (FAA). AC 23-17C: Systems and Equipment Guide for Certification of Part 23 Airplanes and Airships. Washington D.C., 2011.

[4] Yassin Gazmawe and Robert Luckner. *Präsentation: Auslegung eines Basisreglers der Seitenbewegung für ein hochfliegendes unbemanntes Flugzeug hoher Streckung*. Deutsche Gesellschaft für Luft- und Raumfahrt-Lilienthal-Oberth e.V., 2020.

[5] Hans-Dieter Joos and Harald Pfife. Robust flight control system design verification and validation by multi-objective worst-case search. In *AIAA Guidance, Navigation, and Control Conference*, Reston, Virigina, 2012, doi: 10.2514/6.2012-4998. American Institute of Aeronautics and Astronautics.

[6] 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.

[7] Ulrich Stein. *Objektorientierte Programmierung mit MATLAB - Klassen, Vererbung, Polymorphie*. Carl Hanser Verlag, München, 2015.

[8] Andreas Varga, Anders Hansson, and Guilhem Puyou. Optimization based clearance of flight control laws: A civil aircraft application. volume 416 of *Lecture notes in control and information sciences*, Berlin, 2012, doi: 10.1007/978-3-642-22627-4.