

# Automatisierung im Cockpit – Responsibility and Authority Gedanken über die Automatisierungen in modernen Verkehrsflugzeugen

**Frank Müller-Nalbach, Flugkapitän i.R.**  
**(Vereinigung Cockpit e.V., Arbeitsgruppe Konstruktion und Flugbetrieb)**

## Zusammenfassung

Das Cockpit Design heutiger Verkehrsflugzeuge stellt eine kontinuierliche Evolution bisheriger Entwürfe dar. Mit jeder neuen Generation wurde der Automatisierungsgrad erhöht. Aber der Cockpit Design-Ansatz mit seinen Verfahren wurde nicht konsequent angeglichen und überarbeitet. Die prozentuale Abnahme der Hull Losses ist zum Stillstand gekommen, was für die Zukunft mehr Unfälle bedeutet. Daher ist eine Neuorientierung des Flugzeug-, System- Cockpit Designs notwendig. Gemäß ICAO Annex 2; 2.3.1. muss der verantwortliche Flugzeugführer zu jeder Zeit die volle Autorität über das Flugzeug haben können. Kann er diese Verantwortung in aktuellen Designs tatsächlich wahrnehmen? Und falls nicht, was sind die Konsequenzen daraus? Ein Weg könnte ein „Design for Responsibility“ sein (Herczeg, 2014): Es ist eine Denkweise, die die Frage der Verantwortung für den Einsatz sicherheitskritischer Mensch-Maschine-Systeme zu einem Designmerkmal erhebt. Als Beispiel für eine solche Technologie wird hier ein erweitertes ECAM mit Trendanalyse und einer „What-If“-Preview Funktion gezeigt, wie es an der TU Darmstadt im Rahmen einer unveröffentlichten Diplom-Arbeit angedacht worden ist.

## 1. WIRD DAS EXISTIERENDE HEUTIGE AIRCRAFT UND COCKPIT DESIGN MIT SEINEM LAYOUT UND SEINEN VERFAHREN DEN ANFORDERUNGEN DER ZUKUNFT GERECHT?

### ICAO Annex 2, 2.3.1

"The pilot-in-command of an aircraft shall, whether manipulating the controls or not, be responsible for the operation of the aircraft in accordance with the rules of the air, ..."

"...except that the pilot-in-command may depart from these rules in circumstances that render such departure absolutely necessary in the interests of safety."

Die UNO mit ihrem Ableger für den zivilen Flugverkehr, der ICAO, hat zur Verantwortung für die Sicherheit eine klare Meinung<sup>1)</sup>. Sie besagt dass der PIC die letztendliche Verantwortung trägt und das er alles Notwendige tun muss, um die Sicherheit gewährleisten zu können. Alle Anderen müssen ihn dabei unterstützen. Die Frage ist, ob er das heute wirklich kann?

Die zentrale Forderung der „Human Centered Automation“ ist:

### **“HE WHO HAS THE FINAL RESPONSIBILITY MUST HAVE THE FINAL AUTHORITY”**

Hat der Commander tatsächlich die Eingriffsmöglichkeiten? Kann er seine Verantwortung ausüben, und was bedeutet es, wenn er es nicht kann?

## 2. BRAUCHEN WIR: „THE PILOT ORIENTED AIRCRAFT“?

### „The Pilot oriented Aircraft“

Captain Dan Maurino [Flight Safety and Human Factors ICAO]

14<sup>th</sup> Human Factors Symposium  
DUBLIN, October 2, 3 & 4, 2001

When We Look at Daily Practice

**Greatest threats to safety:  
unfamiliar, unanticipated events**

 VEREINIGUNG  
COCKPIT

Automatisierung im Cockpit | Responsibility and Authority | Cpt. Frank Müller-Nalbach

Bild 1

Im Hintergrund ein A380 der Qantas. Der Incident in Singapur ist hier sicherlich bekannt. Warum waren die Folgen des `uncontained engine failures` so gravierend?<sup>6)</sup> Weil sich das Triebwerk bei seinem Versagen nicht an die Zulassungsvorschriften gehalten hat! Flugzeugkonstrukteure bauen für solche Vorfälle extra sogenannte „Dry Bays“ ein, wo keine wichtigen Leitungen verlaufen. Diese werden nach den Zulassungsbedingungen des Triebwerks angelegt, die festlegen, wo die Teile bei einem solchen Fehler hinfliegen sollen. Hier haben sie es nicht getan und damit erhebliche Schäden angerichtet, die so nicht eingeplant und berechnet waren. Die Abarbeitung dieser Fehler im ECAM System dauerte eine Stunde. Erst dann war klar, was noch in Ordnung war und funktionierte, und was kaputt war. Es zeigte sich auch hier, dass tatsächlich auftretende Fehler, auf Grund der Komplexität und der gegenseitigen Abhängigkeit der einzelnen Systeme, sich selten an die

Fehlerbäume der Berechnungen der Ingenieure halten. Es entstehen oft unvorhersehbare Kombinationen von einzelnen und partiellen Fehlern, die schwer zu beurteilen und teilweise unlogisch sind<sup>2</sup>). Erfahrungen aus den Simulator-Fehler Ereignissen helfen kaum. Derartige Fehlerkombinationen sind im SIM kaum zu programmieren. Das was hilft ist das Erlernen einer generellen Fehlerstrategie. Aber ist es bei solch großen Fehlern für die Crew nicht wichtiger zu wissen was noch funktioniert? (Welche Hydraulik/Elektrik? Steuerflächen? Vorflügel? Landeklappen? Fahrwerk? Bremsen? etc.). Es kann sonst Verwirrung herrschen im Cockpit, was dann zu Fehlern führt. Man übersieht etwas, schaltet das falsche Triebwerk ab, man folgt der falschen Geschwindigkeitsanzeige und macht dann damit alles noch schlimmer.

Bild 3  
Ich möchte auf die Generationskurven 3 und 4 hinweisen, die faktisch parallel zur Zeitachse verlaufen. Nach den deutlichen Erfolgen der Verbesserung der Flugsicherheit von der 1. zur 2. und eingeschränkt auch noch zur 3. Generation ist der weitere Erfolg marginal. Es ist keine signifikante Abnahme der Hull Losses über die Zeit mehr festzustellen. Das bedeutet aber, dass bei weiter zunehmendem Verkehr (wie prognostiziert) die absoluten Unfallzahlen steigen werden. Ist das für Alle akzeptabel? Sicher fallen die Zahlen jetzt noch leicht. Es gibt immer noch Flugzeuge der älteren Generationen, die nicht so sicher wie die der 3. und 4. Generation sind, diese werden aber immer weniger.

„The Pilot oriented Aircraft“

Captain Dan Maurino [Flight Safety and Human Factors ICAO]

What is the safety concern(s) in aviation for which the integration of HF knowledge is a solution?

**The mis-management of adverse events resulting from unanticipated interactions between organizations, people & technology**

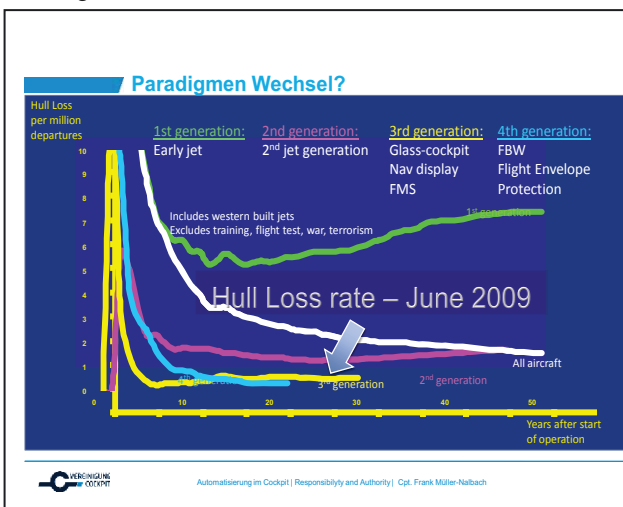
Automatisierung im Cockpit | Responsibility and Authority | Cpt. Frank Müller-Nalbach

Bild 2

- Es passt dann Alles nicht mehr zusammen:
- Die Anzeigen mit der dahinterliegenden Technik.
  - Die alten Verfahren mit dem neuen Umfeld.
  - Das Flugtraining von damals mit den neuen Aufgaben.
  - Das Cockpit design mit den neuen Umständen, Aufgaben, Prozeduren und Prioritäten.

3. PARADIGMEN WECHSEL?

Halten wir uns einmal die Zahlen, Kurven und Statistiken vor Augen.



4. WIE KÖNNTE SO ETWAS AUSSEHEN?

**Das Design der Systeme, der Verfahren und des Cockpits muss die Wahrnehmung dieser Verantwortung ermöglichen und unterstützen!**

Hierzu lief mir folgender Vortrag über den Weg, der das Problem der Verantwortung und der Zugriffsmöglichkeit gut darstellt:

Design for Responsibility:

„Die Rolle des Operateurs zwischen Automation und Verantwortung“

Prof. Dr. Michael Herczeg [Universität Lübeck]  
56. FA-Sitzung Anthropotechnik der DGLR (14.-15.10.2014 Ottobrunn)

Der Mensch zwischen Automatisierung, Kompetenz und Verantwortung“

Ohne den ganzen Vortrag hier wiederholen zu wollen, möchte ich die originäre Zusammenfassung zitieren:

- Design for Responsibility ist eine Denkweise, die die Frage der Verantwortung für den Einsatz sicherheitskritischer Mensch-Maschine-Systeme zu einem Designmerkmal erhebt. Verantwortung kann nicht einfach verteilt werden, sie muss aus einem geeigneten Systemdesign ableitbar sein.
- Die Realisierung von teilautomatisierten Mensch-Maschine-Systemen orientiert sich an menschlichen Fähigkeiten und Denkweisen und bezieht deren Grenzen mit ein.
- Der Mensch delegiert an die Maschine, behält aber dabei die Kontrolle über das Gesamtgeschehen und ist aufgrund der Automatisierungsmodelle in der Lage, das Verhalten und die Begrenzung der Automation zu überwachen und zu verstehen.

- *Beim Versagen von Automation bleibt dem menschlichen Operateur genügend Zeit, um sich im Rahmen seiner natürlichen und erlernten Fähigkeiten ein Bild von der Lage zu machen und bedarfsweise einzugreifen.*
- *Die Maschine wird zu einem Hilfsmittel zur Abstraktion, um Verantwortung für komplexe Systeme und Automationen überhaupt tragen zu können und nicht zur Ursache für deren Verlust.*
- *Die Konsequenz können niedrigere Automatisierungsgrade sein, die zwar den Verlust von Komfort, nicht aber den Verlust von Kontrolle oder Kompetenz bedeuten.*

**Erst wenn eine Automation nachweislich besser als die menschlichen Fähigkeiten ist, ist die Verlagerung der Verantwortung von Operateuren auf eine Maschine im Sinne einer Gesamtrisikobetrachtung vorstellbar und sinnvoll.<sup>3)</sup>**

Das ist in seiner Gesamtheit ein bedenkenswürdiger Ansatz. Für den täglichen Gebrauch würde ich es auch temporär gelten lassen, getreu dem Leitsatz: „Never except an inferior performance of an automated system!“, d.h. wenn z.B. der AP nach einem Engine failure die Geschwindigkeit von  $V_2$  nicht einhält, dann den AP auszuschalten, das Flugzeug manuell auf den richtigen Flugweg steuern und dann den AP wieder einzuschalten.

Die Flugzeugsysteme sollten in der Art und Weise, wie sie mit der Crew kommunizieren, sich so weit wie möglich an „menschlichem Verhalten“ orientieren, wie ein „CREW MEMBER“ agieren und die Verfahren müssen dementsprechend integriert werden.

#### Wie könnte so etwas aussehen

**Recommendation 6 - Flight Deck System Design:**  
 ...For new systems, manufacturers should design flight deck systems such that the underlying system should be more understandable from the flight crew's perspective by including human-centered design processes.<sup>5)</sup>

FAA 130908 Studie vom 5.Sep.2013: „Operational use of flight path management systems“

Ihre Anzeigen müssen die notwendige Genauigkeit und Tiefe besitzen, um sie in den Grenzen der heutigen Technik darzustellen, ihre Richtigkeit überprüfen zu können und somit das Flugzeug unter allen Bedingungen innerhalb der notwendigen Grenzen bedienen und steuern zu können.



Automatisierung im Cockpit | Responsibility and Authority | Cpt. Frank Müller-Nalbach

Bild 4

Ich darf nicht die Übersicht verlieren. Ich muss wissen, wo ich mich innerhalb der Systeme befinde, nur dann kann ich Situationsgerecht reagieren, entscheiden und handeln. Das Design sollte die Stärken des Menschen unterstützen! Man muss sich unter diesen Gesichtspunkten die Fragen stellen:

- Sind die ECAM/EICAS Verfahren, bzw. die Checklisten eigentlich Technik/Fehler orientiert

oder Crew/operationell orientiert? Sind sie flexibel und situationsbedingt anpassbar?

- Was ist mit Trendanalysen? Muss bis zu einem vorgegebenen Grenzwert gewartet werden um dann überraschend zu warnen?
- Was ist wichtiger im Notfall, zu wissen was ausgefallen ist, oder zu wissen was noch funktioniert?

#### „Fly the Aircraft!“

ist die primäre Aufgabe, nicht Systemanalyse. (Die findet statt, wenn der Flugzustand stabilisiert ist und man Zeit dafür hat)

Beispiel: Qantas QF32, A380, VH-OQA at Singapore.04.11.2010

Betrachten wir doch die Verfahren einmal genauer unter diesen Gesichtspunkten:

Die ECAM/EICAS Listen, ihre Darstellung und Orientierung. Für wen sind sie designed worden, was stand dabei im Vordergrund? Die Technik oder die Operation? Gibt es nur ein „Schema F“, oder kann ich sie situationsbedingt anpassen?

Um ein einfaches Beispiel zu nehmen um was es geht: Für einen Startabbruch gibt es eine Checkliste, die je nach Flugzeug länger oder kürzer sein kann, die: „Rejected Take-Off Checklist“. Danach wird nach dem Stillstand des Flugzeuges und dem erforderlichen Abhandeln des Fehlers, der zum Startabbruch geführt hat, das Flugzeug „heruntergefahren“ und für die mögliche Evakuierung vorbereitet.

Tritt allerdings ein so schwerwiegender Fehler auf, das eine sofortige Evakuierung klar erkennbar notwendig ist, gibt es die - teilweise - `inoffizielle` Kurzform: „Stopp! Aus! Raus!“, bedeutet: Parkbremse setzen (Flugzeug darf nicht mehr rollen), alle Triebwerke ausschalten, Evakuierung einleiten. So wird, bei Konzentration auf das Wichtigste, wertvolle Zeit zur Rettung der Passagiere und Crew gewonnen.

Die Frage ist, besteht solch eine Möglichkeit auch bei den elektronischen Listen?

Kann ich wählen, welche Anzeige ich in diesem Moment haben möchte? Ist es bei schweren Fehlern wirklich wichtig zu wissen, ob auch noch der Battery Charger 2 ausgefallen ist, oder wäre es wichtiger zu wissen, was denn noch funktioniert?

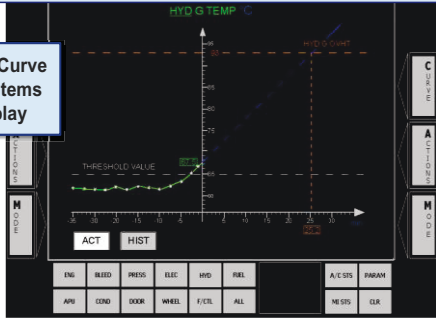
Die primäre Aufgabe ist IMMER das Flugzeug zu fliegen, sonst ist der Rest auch hinfällig!

Als Beispiel möchte ich eine – leider wegen Krankheit nicht eingereichte, nicht gehaltene und nicht veröffentlichte – Diplomarbeit aus dem Jahr 2001 der TU-Darmstadt nehmen (TUD enhanced pilot assistance)<sup>5)</sup>:

Wie könnte so etwas aussehen

Beispiel: ERWEITERTES ECAM MIT TRENDANALYSE; PREVIEW; EXECUTE FUNKTIONEN

Trend Curve in Systems Display



Nicht veröffentlichte Diplomarbeit TU-Darmstadt: ENHANCED PILOT ASSISTANCE FOR ERROR MANAGEMENT



Automatisierung im Cockpit | Responsibility and Authority | Cpt. Frank Müller-Nabach

Bild 5

Warum Trendanalyse? Hat früher der Flugingenieur gemacht. Er hatte alle System Anzeigen permanent im Blick und hat frühzeitig gemerkt, wenn z.B. die Hydrauliktemperatur anstieg. Er konnte sehen: schnell oder langsam, gab es noch andere Hinweise auf Fehler (z.B. Vibrationen). Die nächste Frage nach ANSCHAUEN der entsprechenden Checkliste: „Brauchen wir das System jetzt, oder ist es z.B. für den Anflug und/oder die Landung wichtig?“

Ich könnte also das System jetzt abschalten und für die wichtige Flugphase retten.

Dann könnte ich ganz normal meinen Zielflughafen anfliegen und müsste nicht zum Ausweichflughafen ausweichen (Bremsfähigkeit bei nasser kurzer Bahn, Turbulenzen im Anflug, etc.), bzw. ich müsste nicht Probleme beim Anflug oder Verlassen der Landebahn bei ATC anmelden und den Verkehr am HUB beeinträchtigen

Das ist mit den heutigen Systemen so nicht möglich. Ich sehe sie nicht permanent, sie warnen beim Erreichen des Threshold Wertes ohne eine Historie/Prädiktion (Zeitverlauf) und ich muss das System nach ECAM/EICAS abschalten, mit allen Konsequenzen.

Warning/System Display:

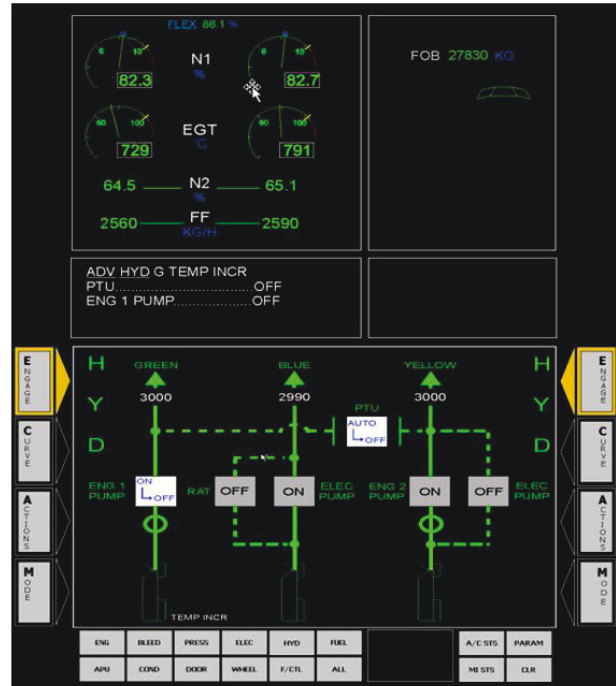


Bild 6

Hier im Warning/System Display kann ich sehen, was geschaltet werden muss, ich kann „virtuell“ vorschalten und mir anschauen was die Konsequenzen sind. Habe ich es als Crew verstanden und bin einverstanden, dann kann ich es mit EXECUTE schalten lassen. Und zwar ohne dann nachts bei Turbulenz am Overhead Panel-monitored-zu schalten.

Mission Status Page:



Bild 7

Hier werden die operationellen Konsequenzen angezeigt und was ich deswegen überprüfen muss. Diese können auch per Data Link ATC mitgeteilt werden.

## Aircraft Status Page:



Bild 8

Und hier ist der technische Zustand des Flugzeuges, mit abrufbarer Hintergrund Information

## 5. EIN AUSBLICK

Automatische Eingriffe sind keinesfalls unerwünscht. Sie sind zur Optimierung der Flugdurchführung heutzutage unverzichtbar. Sie sollen aber durch die Crew erkennbar, nachvollziehbar, begrenzt und übersteuerbar sein, im Fall des Falles; mit logischen, situationsgerechten Verfahren! Nur auf diese Weise kann man dem PIC die erforderliche, kompetente Zugriffsmöglichkeit ermöglichen.

- Der Zugriffsrahmen sollte durch die Crew beeinflussbar sein (z.B. die Begrenzung für Auto-Slat/Flap Systeme innerhalb einer vorgewählten Range durch die Crew, [z.B. wegen starker Turbulenz oder starker Vereisung]).
- Sie sollten klar erkennbar und nachvollziehbar sein (eben wie die Handlungen eines Crew Members).
- Gleiche Eingaben über die Flight Control Interfaces (Sidestick, Controlwheel & Yoke, etc.) sollen gleichwertige Reaktionen des Flugzeuges bewirken, egal in welcher Mode/welchem Control Law sich das EFCS (Electronic Flight Control System) gerade befindet.
  - z.B. nicht doppelte Rollrate im Direct Law im Vergleich zum Normal Law
  - z.B. kein automatisches Einfahren der Spoiler für die Yaw Kompensation beim Übergang von der Flight- zum Ground-Mode (A320 Hamburg Incident) (*Der Wind hört ja nach dem Aufsetzen nicht schlagartig auf!*)

- Manche, durchaus gut gemeinte, Features können den Arbeitsaufwand erhöhen und besonders unter Stress zum Verlust der Situational Awareness beitragen. „Ist das jetzt normal, soll das so sein, oder ist es Teil des Fehlers?“ „Was passiert hier eigentlich? Habe ich richtig gehandelt?“

Ich möchte hier auf keinen Fall missverstanden werden, zurück zur B707 oder noch früher ist keine Option und kontraproduktiv!

Aber...: **Es ist eindeutig festzustellen:**

Ein Paradigmen Wechsel im Design der Flugzeuge und deren Cockpits ist notwendig um die Flugsicherheit und die Effizienz der Operation weiter zu erhöhen!

**Ein optimal auf einander abgestimmtes  
Gesamtsystem  
AIRCRAFT ↔ CREW  
ist für die Zukunft unabdingbar!**

Nicht auf der einen Seite das Flugzeug und auf der anderen die Besatzung, sondern beide zusammen sind das System!

---

QUELENNACHWEIS:

- 1) ICAO Annex 2.2.3.1.
- 2) Captain Dan Maurino [Flight Safety and Human Factors ICAO]14th Human Factors Symposium, DUBLIN, October 2, 3 & 4, 2001
- 3) Prof. Dr. Michael Herczeg [Universität Lübeck] Design for Responsibility:  
„Die Rolle des Operateurs zwischen Automation und Verantwortung“ (56. FA-Sitzung Anthropotechnik der DGLR:“ Der Mensch zwischen Automatisierung, Kompetenz und Verantwortung“ 14.15.10.2014 Ottobrunn)
- 4) Oliver Albert (Alexandra von Eckartsberg Patrick Wipplinger): “enhanced pilot assistance for error management” (Nicht veröffentlichte Diplomarbeit TU-Darmstadt)
- 5) FAA\_130908 Studie vom 5.Sep.2013: `Operational use of flight path management systems`
- 6) Richard Woodward, IFALPA EVP technical standards:QANTAS A380 uncontained engine failure IFALPA aircraft design and operation (ADO) committee meeting sanur beach, bali, indonesia, 1.-3.12.2010
1. AP: Auto Pilot (Automatische Flugsteuerung)
2. ATC: Air Traffic Control
3. DGLR: Deutsche Gesellschaft für Luft und Raumfahrt e.V.
4. ECAM: Electronic Centralized Aircraft Monitoring
5. EFCS: Electronic flight control system
6. EICAS: Engine Indication and Crew Alert System
7. EVP: Executive Vice President
8. ICAO: International Civil Aviation Organization
9. IFALPA: International Federation of Airline Pilot Associations
10. FAA: Federal Aviation Agency
11. PIC: Pilot in Command, verantwortlicher Flugzeugführer
12. SIM: Simulator
13. V<sub>2</sub>: Berechnete „sichere Startgeschwindigkeit“, Grundlage für die Flugwegberechnung für die Hindernisfreiheit beim Start

ABKÜRZUNGEN: