Komplexe Fehlersituationen in heutigen Verkehrsflugzeugen: Ist die Leistungsgrenze der Operatoren erreicht / überschritten?

Max Körte

Zusammenfassung

Heutige Verkehrsflugzeuge der dritten Jet-Generation weisen eine deutlich erhöhte Komplexität der einzelnen Systeme sowie ihrer Interdependenzen auf. Zwei Ereignisse, der Unfall Air France AF 447 vom 01.06.2009 sowie der Zwischenfall Quantas QF 32 vom 4.11.2010 mit einer A380, verdeutlichen, dass die Ausgestaltung der Systemarchitektur des zentralen Warn- und Kontrollsystems einer kritischen Betrachtung hinsichtlich der Mensch-Maschine-Interaktion bedarf. Sobald eine Kaskade von Systemfehlern in rascher zeitlicher Abfolge auftritt, sind die Operatoren, hier die Piloten, überfordert.

Es wird diskutiert, inwieweit heutige Warnsysteme im Fall gravierender Systemausfälle ihre Aufgabe erfüllen können. Für künftige komplexe Systemarchitekturen von Verkehrsflugzeugen muss ein Umdenken dahingehend stattfinden, dass die Wechselwirkung ausgefallener oder beeinträchtigter Bordsysteme erfasst, verarbeitet und in einer schnell und eindeutig interpretierbaren Art und Weise den Operatoren an Bord und am Boden zur Verfügung gestellt wird.

Können Techniken der Künstlichen Intelligenz, *Ambient Intelligence*, *Ubiquitous Computing* mittels multimedialer Zustandsdarstellung der Gesamtsituation des Flugzeugs helfen, die zu erwartenden schweren Un- und Zwischenfällen der jetzigen Megaliner zu reduzieren, da – auch wenn diese in absoluten Zahlen sehr gering sein werden – die Aufmerksamkeit der Öffentlichkeit infolge hoher Todesfallzahlen sehr hoch sein wird?

Der Vortrag weist aus Sicht eines Praktikers auf bestehende Schwachpunkte hin und bietet Anregungen für Verbesserungen, ohne eine „*best practice solution*“ nennen zu können.

1 Sicherheit und Statistik

Der zivile Luftverkehr ist von allen Transportmitteln das sicherste! Die IATA (2014) stellt in ihrem neuesten Jahresbericht fest, dass die Sicherheit über den Fünfjahreszeitraum 2009-2013 zugenommen hat. Der entsprechende Wert liegt jetzt bei 0,48 Totalverlusten (*fatal losses*) pro 1 Million Flüge von im Westen gebauten Strahlverkehrsflugzeugen. In absoluten Zahlen ausgedrückt sind im

Schnitt der betrachteten Fünfjahresperiode 86 Flugzeuge als Totalverluste zu beklagen. Positiv formuliert – und damit den hohen Sicherheitsstandard der zivilen Verkehrsluftfahrt verdeutlichend – sind im Jahr 2013 bei insgesamt 36,4 Millionen Flügen mehr als 3 Milliarden Passagiere sicher an ihr Ziel befördert worden.

Betrachtet man die Unfallursachen, ergibt sich als hauptsächliche Unfallursache der Verlust der Kontrolle über das Flugzeug, während dieses in der Luft ist. Über den Fünfjahreszeitraum gerechnet, kamen dadurch 1.546 Menschen ums Leben. Die Ursachen, die zu einem solchen Kontrollverlust im Flug – das ist eine der katalogisierten Ursachen – geführt haben, sind überwiegend akribisch untersucht, analysiert und dokumentiert: mehrmals verlor die Besatzung hoch automatisierter Flugzeuge bei komplexen und zeitlich rasch ablaufenden Systemfehlern die Kontrolle über ihr Flugzeug und stürzte ab.

Hier noch näher hinzuschauen und zu fragen, ob die Besatzung unter den gegebenen Umständen überhaupt eine reelle Chance hatte, ist das Anliegen des Autors.

2 Die Kontrolltätigkeit der Operatoren anhand von Flugzeuggenerationen

Lufttransport-Verkehrsflugzeuge der ersten Jet-Generation verlangten von den Flugbesatzungen ein hohes Maß an analytischer Beurteilung im Fall von Systemfehlern. Durch Beobachtung und Analyse der Warn- und Kontrolleinrichtungen im Cockpit musste sich die Besatzung ihr „Bild“ vom Gesamtzustand des Flugzeugs machen. Diesen Überblick zeitnah und realitätsgerecht zu finden, war zeitaufwendig, Zeit war nicht immer vorhanden. Infolgedessen gab es fehlerbehaftete Analysen aufgrund falscher Rückschlüsse auf den tatsächlichen Zustand des Flugzeugs.

Der Einzug von Warn- und Kontrollrechnern (*Flight Warning and Control Computer)* der zweiten Jet-Generation (Bild 1) brachte erhebliche Verbesserung in zeitnaher und realitätskonformer Weise: Die Systeme teilen ihren jeweiligen Zustand mit und geben selektive, systembezogene Handlungsanweisungen, wie mit den Fehlern bestmöglich umzugehen ist.

Heutige Verkehrsflugzeuge der dritten Jet-Generation weisen eine deutlich erhöhte Komplexität der einzelnen Systeme sowie ihrer Interdependenzen auf. Bei auftretenden Anomalitäten, Teilsystemfehlern und Totalausfällen ganzer Systeme ist die zeitnahe und kohärente Übersicht des Gesamtzustandes des Flugzeugs, insbesondere sein Energiestatus, immer dann erschwert bzw. unmöglich, wenn die Warneinrichtungen nur teilweise korrekt den Zustand wiedergeben; es sind Fälle von Falschanzeigen dokumentiert, die verbunden mit den Handlungsanweisungen nachweislich das Flugzeug in eine noch bedrohlichere Lage gebracht haben oder hätten.

Anhand von zwei Unfällen stellt der Verfasser dar, dass die Ausgestaltung der Systemarchitektur des Zentralen Warn- und Kontroll- Computers (*Electronic Centralized Aircraft Monitor* - ECAM bei Airbus und *Engine Indicating and*

Crew Alerting System - EICAS bei Boeing), der zugrundeliegenden Software bzw. der hierfür erforderlichen elektrischen Versorgung einer kritischen Betrachtung hinsichtlich der Mensch-Maschine-Interaktion bedarf; auch wenn noch so unwahrscheinliche Fehler – bis zu ~ 10^7 – in der Zulassung nachgewiesen werden und damit dargestellt werden, kann ich aus meiner jahrzehntelangen Erfahrung als Flugkapitän, Ausbilder und Prüfer sowohl mit Boeing als auch mit Airbus feststellen, dass immer wieder (zugegeben) seltene Ereignisse eintreten, die als Systemfehler erkannt und zur Anzeige gebracht werden; diese Anzeigen und besonders die Warnmeldungen sind in diesen seltenen, aber dann meist kritischen Fällen mitunter irreführend. Wenn die Besatzung in solchen Fällen den Handlungsanweisungen folgt und die entsprechenden Aktionen „nach Kochbuch, sprich elektronischer Checkliste“ abarbeitet, tut sie der Gesamtsituation des Flugzeugs keinen guten Dienst, ja der Zustand kann sich noch verschlimmern und die Lage kann leicht endgültig außer Kontrolle geraten.

Bild 1: Cockpit A300/A310 (Quelle: Airbus).

3 Exemplarische Unfälle

Am Beispiel des abschließend geklärten Unfalls der AF 447 vom 01.06.2009 (BEA, 2012) wird eindrucksvoll sichtbar, dass gravierende Systemausfälle innerhalb kürzester Zeit unter schwierigen atmosphärischen Bedingungen die Besatzung mit den gegenwärtig zur Verfügung stehenden Warneinrichtungen überforderten und das Flugzeug unkontrollierbar wurde: 25 dokumentierte

Fehlermeldungen innerhalb von ca. 4 Minuten kamen zur Anzeige, auf die die Besatzung zeitnah und in der richtigen Reihenfolge hätte reagieren müssen. War sie dazu in der Lage? Nein. Das Ergebnis ist bekannt. Die Frage muss lauten: Warum konnten die Piloten diese gravierende Störung der Bordsysteme nicht beherrschen?

Der Zwischenfall Quantas QF 32 vom 4.11.2010 macht deutlich, dass gravierende, nahezu zeitgleich auftretende Systemfehler die Besatzung vor erhebliche Probleme stellten, die u.a. nur durch die geballte Analyse- und Entscheidungseffektivität einer 5-köpfigen Besatzung einen Unfall um Haaresbreite verhinderte. Bemerkenswert ist bei diesem Fall, dass Handlungsanweisungen des zentralen Warnsystems irreführend, ja geradezu fälschlich waren; hier zeigte sich in aller Schärfe die irrige Meinung, mit ausreichender Rechenkapazität an Bord sei alles beherrschbar.

Zu AF 447 vom 01.06.2009 RIO-PAR A330-203 (BEA, 2012; BEA, o.J. a; BEA, o.J. b): Die Unfallursachen sind abschließend geklärt. Aufgrund der 25 Warnmeldungen innerhalb eines Zeitraums von 4 Minuten geht die französische Flugunfalluntersuchungsbehörde davon aus, dass die für die Geschwindigkeitsmessung erforderlichen Staurohre einen maßgeblichen Einfluss auf das Unfallgeschehen gehabt haben (Bild 2).

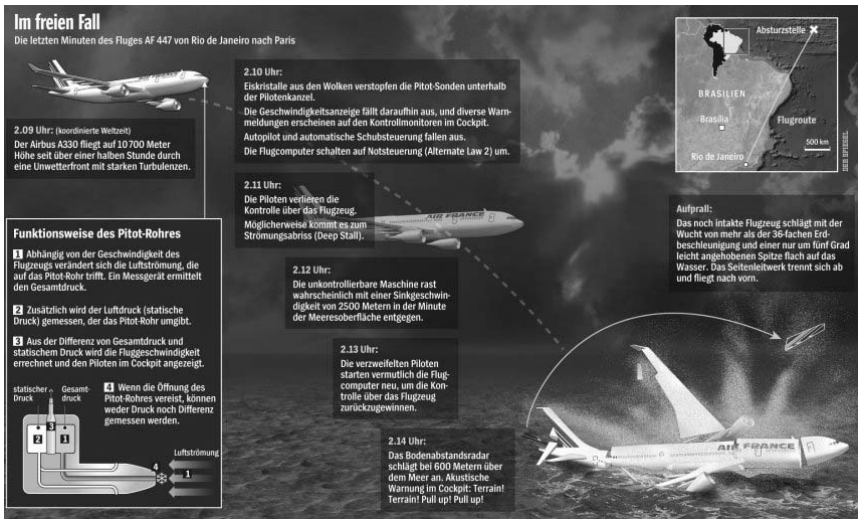

Bild 2: Schematische Darstellung Unfallverlaufs AF 447 (Traufetter, 2010)

Vom Verfasser durchgeführte Tests im Simulator haben leider ergeben, dass Linienbesatzungen ohne Kenntnis dieses hoch anspruchsvollen und sehr dynamischen Szenarios das Flugzeug nur ausnahmsweise unter Kontrolle bringen können. Wenn man bedenkt, dass der Unfall zu einer vom Biorhythmus ungünstig

geprägten Nachtzeit unter schwierigen Umweltbedingungen – Flug in instabilen Wolkenformationen mit hoher Konvektivität und entsprechender Turbulenz – auftrat, waren die Chancen zu überleben gering.

Herkömmliche Anzeige- und Warngeräte, wie das ECAM von Airbus (Bild 3) und das EICAS von Boeing, sind bei Auftreten derart massiver Systemfehler nicht geeignet, der Besatzung Hilfe und Handlungsanleitung für die Fortsetzung eines sicheren Fluges zu bieten. Die Ereignisse und damit die Anzahl der Warnmeldungen mit den diesbezüglich abzuarbeitenden Routinen überschlagen sich förmlich – es fehlt die Kapazität und u.U. auch die physische Fähigkeit der Piloten.

Bild 3: Das Warn- und Kontrollsystem (ECAM) ist Gegenstand dieses Artikels, exemplarisch dargestellt in der A380 (Quelle: Airbus).

Zu QF 32 vom 04.11.2010 SIN-SYD A380 (Robinson, 2010): Der Vorgang ist gut dokumentiert, die Presse berichtete umfangreich; weniger bekannt ist die Tatsache, dass ein katastrophaler Unfall nur um Haaresbreite vermieden wurde. Maßgeblich beigetragen hat der Umstand, dass 5 sehr erfahrene Piloten mittels eines strukturierten Entscheidungsmodells im Team die jeweiligen Entscheidungen getroffen haben; normalerweise besteht die Besatzung aus nur 2 Piloten, die ihren Arbeitsplatz nicht verlassen können, um z.B. eine Sichtkontrolle aus der Passagierkabine über große Mengen austretenden Kraftstoffs aus den Flächentanks vorzunehmen.

Hätte dieser Zwischenfall in einem Total Loss geendet, wäre die damals durchaus kritische Markteinführung der A380 möglicherweise anders gelaufen, wahrscheinlich über einen längeren Zeitraum gestoppt worden.

In Kurzform: Was war passiert?

Bedingt durch die Desintegration eines Triebwerks im Steigflug aus Singapur entstanden an Struktur und Systemen erhebliche Schäden, die die Besatzung vor erhebliche Probleme stellte, das Flugzeug in der Luft zu halten und sicher am Ausgangspunkt zu landen. Die Ursache der Triebwerksexplosion lag in einer geplatzten Ölleitung, die infolge zu geringer Wandstärke einen Ermüdungsriss mit anschließenden Bruch erlitt; das freiwerdende Öl entzündete sich durch die heiße Luft im Bereich des Hoch- und Mitteldrucklagers, worauf sich das Feuer bis zur Scheibe der einstufigen Mitteldruckturbine durchfraß. Die Befestigung auf der Welle versagte und Scheibenstücke durchschlugen aufgrund ihrer hohen Energie die Triebwerksgondel, Teile des Pylon, des Flügels und des Rumpfes.

Die Auswirkung auf Manövrierfähigkeit und Funktion der Systeme war extrem (siehe auch Auszüge aus Robinson, 2010, im Wortlaut):

- Handbetrieb mit eingeschränkter Steuermöglichkeit,
- nur Triebwerk 3 arbeitet normal,
- Triebwerk 2 ist explodiert,
- die Außentriebwerke 1 und 4 sind nur beschränkt regulierbar (*degraded mode*),
- einseitiger Kraftstoffaustritt unter hohem Druck mit bis auf 10 t aufbauender Massendifferenz (*Imbalance*) aus leckgeschlagenen Kraftstofftanks in der linken Flügelfläche,
- Schäden am Hydrauliksystem – das Fahrwerk muss von Hand ausgefahren werden, das normale Bremssystem, das Antiblockiersystem sowie die Schubumkehr funktionierten nicht mehr,
- gravierende Schäden an der Stromversorgung.

Zudem geriet die Schwerpunktlage außerhalb des zertifizierten Bereichs: Die Gesamtmasse lag deutlich höher als die maximal zulässigen Landemasse. Die Vielzahl der Fehler und Systemausfälle konnte der Anflugrechner, mittels dessen Anfluggeschwindigkeit, Klappenstellung, erforderliche Landbahnlänge u.a. Parameter errechnet werden, nicht verarbeiten – ein derartig katastrophales Fehlerszenario war nicht vorgesehen. Ein alternatives Berechnungsverfahren anhand von Tabellen ist an Bord nicht griffbereit verfügbar. Die eigentlichen Probleme entstanden nach der Landung – das Flugzeug kam 140 m (!) vor Bahnende zum Stillstand mit glühend heißen Bremsen (>900 Grad C) bei gleichzeitig ausströmendem Kraftstoff. Dass sich hier keine Katastrophe ereignete, ist ein Wunder.

Die Aussagen des überwachenden Kapitäns sprechen für sich; sie beschreiben mit Deutlichkeit die Schwachstellen des Systems und sind deshalb im Anhang zu Robinson (2010) im Wortlaut wiedergegeben:

1. Die Architektur des Warnsystems (ECAM, Bild 4) bildet exakt alle Fehler ab, wie sie von den Sensoren, unvollständig oder fälschlich, gemeldet werden, d.h. in einem dynamischen Umfeld mit einer großen Anzahl von zeitnah auftretenden Fehlern ist das ECAM überfordert, besonders dann, wenn Beschädigungen an den elektrischen Leitungen (wie in diesem Fall durchschlugen Fremdkörper Leitungen) die Funktion der Sensoren einschränken oder sogar funktionsunfähig machen.
2. Die dazugehörigen elektronischen Checklisten, um mit den einzelnen Fehlern umzugehen, „kennen“ nur die spezifische Handlungsfolge für den jeweiligen Fehler – das jeweilige System „weiß“ nichts vom Zustand der benachbarten Systeme.
3. Hierdurch sind Handlungsaufforderungen vorprogrammiert, die unsinnig bzw. auch nicht ausführbar sind, weil die benachbarten Systeme ebenfalls Defekte aufweisen, die eine reale Ausführung der Anweisungen unmöglich machen.

Tritt wie in diesem Fall eine Lawine von Handlungsanweisungen auf – wobei einige dieser Meldungen anderen widersprachen – dann ist immer noch, aber dann ganz besonders, die geballte Analysefähigkeit der Operatoren gefragt, um zu entscheiden, welche Anweisungen für die augenblickliche Situation wichtig sind bzw. welche Handlungsanweisungen schlichtweg zu ignorieren, da falsch, sind (*contradicting*).

Bild 4: Zentrales Warn-, Anzeige- und Kontrollgerät A380 (ECAM) mit Fehlermeldungen und Handlungsanweisungen

4 Lösungsvorschläge

Der Zwischenfall der Quantas, der um Haaresbreite in einer Katastrophe unvorstellbaren Ausmaßes hätte enden können und vermutlich ein schwerer Rückschlag für das A380 Einführungsscenario gewesen wäre, zeigt anhand der Aussagen der Besatzung anschaulich, dass die kontinuierliche Analyse und Darstellung der Gesamtsituation des Flugzeugs an jedem Punkt der Flugbahn von großem Vorteil wäre.

Bei komplexen, dynamisch ablaufenden Fehlersituationen muss die Besatzung in die Lage versetzt werden, die Gesamtsituation des Flugzeuges schnell und eingängig zu erfassen. Wie könnte das praktisch verwirklicht werden? *Ambient Intelligence* könnte ein Werkzeug sein, um den Zustand der Nachbarsysteme an Bord des Flugzeuges zu jedem Zeitpunkt abzubilden, zu analysieren und darzustellen; darauf abgestimmte Handlungsanweisungen für die Besatzung wären ein großer Vorteil hinsichtlich Sicherheit und Belastungsreduzierung. Es ist geradezu gefährlich, Handlungsanweisungen für ein bestimmtes System zur Anzeige zu bringen, die entweder nicht ausführbar sind bzw. zu keinem Erfolg führen können, da das betroffene Nachbarsystem die entsprechenden Korrektur- und Belebungsmaßnahmen aufgrund seiner eingeschränkten Fähigkeiten nicht zulässt.

> Zitat aus Robinson (2010): *„But there are other salient points – the 'avalanche' of messages from the A380's systems (some contradicting each other) meant that the crew drew on their full resources to decide which were important and which could be disregarded."*

Der Verfasser favorisiert ein Gesamtschaubild (*General Situation Display*) – ähnlich wie in der Raumfähre Spaceshuttle der NASA – das zu jedem Zeitpunkt ein kohärentes Abbild des Gesamtsystemzustands des Flugzeugs darstellt. Es müsste mit heutiger Darstellungstechnik möglich sein, ein leicht aufzunehmendes und zu verarbeitendes Bild der Gesamtsituation des Flugzeugs zu vermitteln (Dubois, 2013). Primäre Anzeige auf dem ECAM sollte sein: *Fly the aircraft manually!* Fast immer ist die automatische Lagesteuerung betroffen. Es macht keinen Sinn, sich mit den diversen Betriebsarten *(submodes)* zu beschäftigen.

Als erster Schritt muss die Analyse der Gesamtsituation vollzogen werden: In welchem technischen Zustand befindet sich mein Flugzeug? Was funktioniert noch? Muss ich mich primär um die Kontrolle der Flugbahn kümmern, weil Autopilot und Schubregelung „ausgestiegen" sind? Wie ist mein Energiestatus? Wieviel „Luft unter dem Kiel" habe ich, wie ist mein aerodynamischer Zustand oder bewege ich mich bereits an meiner flugmechanischen Leistungsgrenze? Funktioniert die Steuerung? In welchen Betriebsarten?

Es genügt eben nicht, in solchen komplexen Fehlersituationen die Besatzung mit einer Lawine von Warnmeldungen mit den dazugehörigen elektronischen Handlungsanweisungen zu überschütten: Der Mensch ist schlichtweg überfordert: Bedenkt man zudem, dass Handlungsanweisungen in einem Mehrpilotencockpit

immer im Team nach klar festgelegter Rollenverteilung (*Crew Coordination Concept*) abgearbeitet werden müssen, wird die Lage nur noch schwieriger: Wie können 46 Warnmeldungen innerhalb 4 Minuten mit den dazugehörigen Handlungsanweisungen unterschiedlicher Dringlichkeit – da überlebensnotwendig – koordiniert im Team abgearbeitet werden? Und jede Handlungsanweisung darf nicht blind befolgt werden, sie muss vielmehr hinterfragt und auf ihre Sinnhaftigkeit bzw. Realitätsabbildung überprüft werden.

Die bei Airbus verfügbare STATUS-Funktion in alphanumerischen Zeichen ist zwar vorhanden, allerdings erst nach Abarbeiten der Handlungsanweisungen und dann auch nur selektiv für die bearbeiteten Systemfehler.

Die automatische Darstellung von Handlungsanweisungen (Checklisten), die zur Fehlerbehebung bzw. Minimierung der diesbezüglichen Auswirkung führen, sind der zweite Schritt. Heutige Warnsysteme erzeugen zu schnell die Handlungsanweisungen für ein individuelles System, das von seinem Nachbarsystem keine Kenntnis hat – fällt zeitnah ein weiteres System gleicher Wichtigkeit aus, wird das letztere priorisiert, ohne dass die ursprünglich generierte Checkliste abgearbeitet werden konnte.

Bild 5: Thales Vision 2020 (Dubois, 2013)

Vorschläge des Verfassers sind offensichtlich erkannt; die Industrie arbeitet daran, wenn auch nur sehr zögerlich (Croft, 2013). Interessanterweise konzentriert man sich vorerst auf die hochtechnischen Business Jets. Die Firma Thales will die neue Darstellungstechnologie nutzen und hinsichtlich Systemdarstellung zu allererst das grobe Bild anbieten, um mit einem Blick die Gesamtfehlersituation zu erfassen; erst mit einem zweiten Schritt – hier manuell über Berührungs-

bildschime (*touch screens*) – und mit nur einer Eingabe wird die nächste Ebene sichtbar (Bild 5). Es wird spannend werden, zu verfolgen, wie bei komplexen Fehlern diese nächste Ebene kohärent und leicht interpretierbar ausgestaltet wird.

5 Wertung

Der Verfasser ist sich bewusst, dass heutige Verkehrsflugzeuge eine bisher unerreichte technische Sicherheit bieten; es ist aber auch Tatsache, dass die Komplexität der Systemarchitektur erheblich zugenommen hat (allein 1200 Softwarepakete sind in der A380 geladen, bisher waren es weniger als 100), d.h. bei schwerwiegenden Systemfehlern, die zeitnah gleichzeitig auftreten, verändert sich der Gesamtstatus ungemein dynamisch – ohne geeignete Hilfsmittel wird die Besatzung, meist nur 2 Piloten, augenblicklich vor große Herausforderungen gestellt, den Überblick zu behalten.

Wäre der Besatzung der AF 447 unmittelbar bewusst geworden, dass nur ein sofortiges, sehr feinfühliges manuelles Kontrollieren der Flugbahn ihres Flugzeugs an seiner aerodynamischen Leistungsgrenze, den drohenden Absturz hätte verhindern können, wäre es möglicherweise anders ausgegangen. Die Handlungsaufforderung des ECAM an erster Stelle: Fly the aircraft manually! hätte die Besatzung wachgerüttelt.

Die unmittelbare Vermittlung des Gesamtenergiestatus wäre nach Überzeugung des Verfassers die richtige Vorgehensweise gewesen – optisch, akustisch, taktil – wie auch immer. Die Anzeige von lawinenartig anrollenden, sich überschlagenden Warnmeldungen kann nicht die Lösung sein. Das Gegenteil ist der Fall: Tests im Simulator mit ausgesuchten, erfahrenen Besatzungen, die über das zu erwartende Szenario nicht vorab informiert waren, zeigen, dass eine derartige Fehlersituation im Glücksfall beherrschbar ist. In der Mehrzahl der Fälle geriet der – auf neusten technischen Entwicklungsstand befindliche – Simulator außer Kontrolle und die Übung musste abgebrochen werden. Mit der heutigen Darstellungstechnik verbunden mit akustischen und alphanumerischen Nachrichten sind in diesen, zugebenermaßen sehr seltenen Fehlerfällen die Piloten im Normalfall nicht in der Lage, die Situation zu meistern, d.h. den Flug sicher weiterzuführen.

Oder müssen wir wieder das „von Hand Fliegen“ in großer Höhe trainieren und uns auf alte Tugenden des Pilotenberufs (*common airmanship*) konzentrieren? Ersteres sollte der Vergangenheit angehören; die Jets der 1. Generation waren deutlich trainingsintensiver hinsichtlich manuellen Fliegens. Letzteres ist bei aller Automation das Gebot der Stunde!

Es ist eben genau die Crux der Technikgläubigkeit, dass angezeigte Warn- und Fehlermeldungen meist – ohne ausreichende Analyse durch die Operatoren – als zutreffend angesehen werden und die damit verbundenen Handlungsanweisungen befolgt, sprich abgearbeitet werden – auch wenn diese ausnahmsweise falsch sind.

Wo gibt es Vergleichbares? Schaltzentralen von Kernkraftwerken, Energieversorgern, Feuerwehrzentralen, Kommandostationen von Schiffen? Auf letzteren

hatte der Verfasser unlängst Gelegenheit, Vergleiche anzustellen. Auf der Brücke eines 5.000 Passagiere-Kreuzfahrtschiffs wurde der Fehlerfall „Feuer an Bord“ dargestellt– eines der gefährlichsten Szenarien. Das imposante *General Situation Display* in Größe einer Schreibtischplatte lokalisiert den Brandherd in der ersten Ebene und die möglichen Ursachen in weiteren Ebenen. Interessant ist, dass nach Aussage des Kapitäns die angegebenen Handlungsanweisungen – analog zu ECAM/EICAS – nicht automatisch oder manuell umgesetzt werden; vielmehr wird im Team die Situation analysiert, mögliche Falschmeldungen ausgeschlossen und erst dann wird eine Entscheidung herbeigeführt, wie zu verfahren ist. Auch wenn dieses Beispiel aus trivialen Gründen „hinkt“ – der Zeitdruck ist nicht vergleichbar mit dem in der Luftfahrt –, ist man sich offensichtlich in der Seefahrt über die Tücken automatisierter Fehlerbehebungsprozesse im Klaren.

Das Gegenargument zum oben formulierten Vorschlag lautet: In den allermeisten Fällen funktioniert das Gesamtsystem Flug mit allen seinen Teilaspekten ja hervorragend, die unglaublich niedrigen Unfallzahlen des Transportmittels Verkehrsluftfahrt belegen dies eindrucksvoll. Also wozu eine Neuentwicklung?

Ja, aber… Die Firma Honeywell arbeitet am Thema Artificial Intelligence (Croft, 2013): Die Hilfestellung, die vernetzte Bordsysteme bei Auftreten von Abnormitäten geben können sollen, wird als Assistierte Beeinflussung (*assisted interaction*) benannt. Im Fehlerfall und besonders in extrem seltenen und untrainierten Fehlersituationen soll das System die Operatoren zu den richtigen Prozeduren leiten, um diese sicher abzuarbeiten: Keinesfalls wird weitere Automation dahingehend vorgesehen, prozedurale Schritte automatisch ablaufen zu lassen. Die Entscheidung des Kapitäns bleibt unangetastet. Der Fall QF 32 könnte somit in der Nachschau des Entwicklungssimulators womöglich wesentlich unspektakulärer ablaufen, so es gelingt, neben hoher Fehlertoleranz die anspruchsvolle Zulassung der Luftfahrtbehörden zu erlangen.

Lohnt der Aufwand einer Neuentwicklung des Warnsystems und seiner Systemdarstellung? Brauchen wir wirklich z.B. ein General Situation Display o.ä., mittels dessen die Gesamtsituation des Unternehmens Flug leicht erfassbar zu jeder Tages- und Nachtzeit, bei Turbulenz und sonstigen widrigen Umweltbedingungen dargestellt und vermittelt werden kann? – Ja!

Wenn es um Sicherheit geht, versagt die herkömmliche Kosten-Nutzen-Analyse. Anhand der Unfallstatistiken sind die diesbezüglichen Unfallhäufigkeiten einigermaßen bekannt, und Unfälle wie die erwähnten sind sehr selten (1-2 Fälle von Desintegration eines Triebwerks pro Jahr, 15 Fälle von vereisten Staurohren innerhalb der letzten 8 Jahre). Sicher kann man eine Neuentwicklung infolge der hohen Kosten und der rigiden Zulassungsbestimmungen (Bauvorschriften) erst in der kommenden Flugzeuggeneration verwirklichen – entwickeln und testen im Labor sollte man aber schon jetzt. Es ist der Mühe wert! Und die Auswirkungen eines Unfalls eines Megaliners wie die A380, B787 oder B747-8 sind ungleich höher als bisher.

Dieser Beitrag soll als Plädoyer für eine intensive Beschäftigung mit seltenen, aber meist gravierenden Fehlerfällen verstanden werden.

Literatur

BEA (o.J. a): Interim Report on the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro – Paris, (2011), http://www.bea.aero/docspa/2009/f-cp090601.en/pdf/f-cp090601.en.pdf

Zum besseren Verständnis nachfolgend ein Auszug hieraus:

BEA (o.J. b): Interim Report No. 2 on the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro – Paris, http://www.bea.aero/docspa/2009/f-cp090601e2.en/pdf/f-cp090601e2.en.pdf

BEA (2012): Final Report on the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro – Paris, July 2012. http://www.bea.aero/docspa/2009/f-cp090601.en/pdf/f-cp090601.en.pdf

Croft, J. (2013): Honeywell Future Flight Deck To Ease Pilot Workload, Aviation Week and Space Technology, Oct 28, 2013.

Dubois, T. (2013): Thales Displays 2020-ready Business Jet Cockpit. AIN online. http://www.ainonline.com/aviation-news/nbaa-convention-news/2013-10-22/thales-displays-2020-ready-business-jet-cockpit

International Air Transport Association (IATA) (2014): IATA Releases 2013 Safety Performance - Encouraging Signs for African Safety. IATA Press Relase, 01.04.2014. http://www.iata.org/pressroom/pr/Pages/2014-04-01-02.aspx

Robinson, T. (2010): EXCLUSIVE - Qantas QF32 flight from the cockpit, Royal Aeronautical Society, 08.12.2010, http://www.aerosociety.com/News/Insight-Blog/1567/EXCLUSIVE-Qantas-QF32-flight-from-the-cockpit

Traufetter, G. (2010): Gehirnschlag im Cockpit, *Der Spiegel*, 8/2010, 22.02.2010.

Zum besseren Verständnis nachfolgend zwei Auszüge, die die Kernaussagen wiedergeben:

Auszug aus BEA (o.J. b)

25 Fehlermeldungen innerhalb von 4 Minuten, auch wenn der geneigte Leser mit den Abkürzungen vermutlich wenig anfangen kann, scheint mir die Wiedergabe in der Zeitachse folgerichtig: Die Lawine der Fehlermeldungen „verschüttet“ das klare denken der Besatzung zu einem vom Biorhythmus äußerst ungünstigen Zeitpunkt. Innerhalb von 37 Sekunden verabschieden sich der Autopilot, die automatische Schubregelung sowie das Steuerungssystem, womit das Flugzeug am oberen Rand seiner Enveloppe bei den vorherrschenden klimatischen Bedingungen nur mit großer Feinfühligkeit und ausreichender Übung auf seiner Flugbahn gehalten werden kann. Die Nachricht, dass die Staurohre vereist und damit deren Daten unbrauchbar geworden sind, findet sich nicht: Die Symptome der Krankheit sind in aller Detailliertheit dargestellt und akustisch zum Gehör gebracht (wenn das Gehirn so viele akustische Warnungen unterschiedlicher Tonhöhe überhaupt verarbeiten kann!)

02:10:10	.1/WRN/WN0906010210 221002006	AUTO FLT AP OFF
02:10:16	.1/WRN/WN0906010210 226201006	AUTO FLT REAC W/S DET FAULT
02:10:23	.1/WRN/WN0906010210 279100506	F/CTL ALTN LAW
02:10:29	.1/WRN/WN0906010210 228300206	FLAG ON CAPT PFD SPD LIMIT
02:10:34	#0210/+2.98-30.59	
02:10:41	.1/WRN/WN0906010210 228301206	FLAG ON F/O PFD SPD LIMIT
02:10:47	.1/WRN/WN0906010210 223002506	AUTO FLT A/THR OFF
02:10:54	.1/WRN/WN0906010210 344300506	NAV TCAS FAULT
02:11:00	.1/WRN/WN0906010210 228300106	FLAG ON CAPT PFD FD
02:11:15	.1/WRN/WN0906010210 228301106	FLAG ON F/O PFD FD
02:11:21	.1/WRN/WN0906010210 272302006	F/CTL RUD TRV LIM FAULT
02:11:27	.1/WRN/WN0906010210 279045506	MAINTENANCE STATUS EFCS 2
02:11:42	.1/WRN/WN0906010210 279045006	MAINTENANCE STATUS EFCS 1
02:11:49	.1/FLR/FR0906010210 34111506	EFCS2 1,EFCS1,AFS PROBE-PITOT 1X2 / 2X3 / 1X3
02:11:55	.1/FLR/FR0906010210 27933406	EFCS1 X2,EFCS2X FCPC2 (2CE2) /WRG:ADIRU1 BUS ADR1-2 TO FCPC2,HARD
02:12:10	.1/WRN/WN0906010211 341200106	FLAG ON CAPT PFD FPV
02:12:16	.1/WRN/WN0906010211 341201106	FLAG ON F/O PFD FPV
02:12:51	.1/WRN/WN0906010212 341040006	NAV ADR DISAGREE
02:13:08	.1/FLR/FR0906010211 34220006	ISIS 1 ISIS(22FN-10FC) SPEED OR MACH FUNCTION,HARD
02:13:14	.1/FLR/FR0906010211 34123406	IR2 1,EFCS1X,IR1,IR3 ADIRU2 (1FP2),HARD
02:13:45	.1/WRN/WN0906010213 279002506	F/CTL PRIM 1 FAULT
02:13:51	.1/WRN/WN0906010213 279004006	F/CTL SEC 1 FAULT
02:14:14	.1/WRN/WN0906010214 341036006	MAINTENANCE STATUS ADR 2
02:14:20	.1/FLR/FR0906010213 22833406	AFS 1 FMGEC1(1CA1),INTERMITTENT
02:14:26	.1/WRN/WN0906010214 213100206	ADVISORY CABIN VERTICAL

Auszug aus Robinson (2010)

Ähnlich wie beim Unfall der AF wird die Besatzung mit einer Lawine von Fehlermeldungen überrollt; damit sich der geneigte Leser ein Bild der Dramatik der Lage an Bord während des Fluges und am Boden machen kann, habe ich die wichtigsten der Aussagen der Besatzung im Wortlaut wiedergegeben und auf Übersetzung und Kommentierung verzichtet. Es gibt wenige Unfälle derartiger Dramatik, die so gut dokumentiert und nachvollziehbar sind: Ein Lehrstück für Operatoren, wie mit hochentwickelter Technik umzugehen ist!

"*We had a number of checklists to deal with and 43 ECAM messages in the first 60 seconds after the explosion and probably another ten after that. So it was nearly a two-hour process to go through those items and action each one (or not action them) depending on what the circumstances were."*

"In the shutdown process the ECAM has an option of 'damaged' or not and of course we chose 'damaged' which then leads you through discharging some fire bottles and shutting the engine down with the fire shut-off switch. We did that but unfortunately we got no confirmation of any fire bottles being discharged. Subsequently that was more wiring damage that didn't give us the

indication. As it turns out, we did have one discharged bottle and one that didn't which was comforting."

"It was getting very confusing with the avalanche of messages we were getting. So the only course of action we have is the discipline of following the ECAM and dealing with each one as we came through with them."

"We were getting messages about imbalance, losing fuel out of one side and not the other. And those messages were some of the ECAM messages that we didn't follow. We were very concerned the damage to the galleries, the forward and aft transfer galleries, whether they were intact, whether we should be transferring fuel. We elected not to."

"We didn't have the ability to dump fuel, the fuel dumping system had failed and we were about 50 tonnes over our maximum landing weight. In the Airbus and the A380 we don't carry performance and landing charts, we have a performance application. Putting in the ten items affecting landing performance on the initial pass, the computation failed. It gave a message saying it was unable to calculate that many failures."

"So we then looked at them in more detail and rejected ones that we considered minor and things that were affecting landing performance on wet runways. It was a beautiful day in Singapore thankfully and not wet so it obviously wasn't going to affect our landing performance. After we'd eliminated about three or four items the computer happily made a calculation and it gave us a touchdown speed of about 165kt and showed us about 130m of surplus runway (it's a 4,000m runway) so basically said we could stop on the runway."

"We shut down in the normal way. As I mentioned earlier we had the APU running but sadly it wouldn't take up any electrical load – so the aircraft went into 'essential power' or battery power, which gives you the use of only one VHF radio. That was dedicated to the fire commander, the fellow in charge on the ground. He advised us we still had an engine running. So they were very reluctant to come near the aircraft with the engine running. He also advised us we had some high-pressure fuel leaks coming out of the left-hand wing and as we had used maximum braking effort to stop the wing gear temperatures had gone over 900degs C, so raw fuel pouring on hot brakes. So our concerns were obviously fires and we 'encouraged' the fire service to come closer, which they did. We made all effort to try and shut down the No1 Engine but unfortunately it continued to run."

"We've lost our satellite phone so the trusty mobile phones came out and called the company in Sydney to relay back to the company in Singapore, to dispatch some stairs and buses to the aircraft. We were 4,000m down the end of the runway and steps don't go very fast so it was nearly an hour before we got the first set of stairs to the aircraft and another hour by the time the last passenger departed the aircraft. So it was nearly two hours on the ground with major fuel leaks and engines running."

„We've got a situation where there is fuel, hot brakes and an engine that we can't shut down. And really the safest place was onboard the aircraft until such time as things changed. So we had the cabin crew with an alert phase the whole time through ready to evacuate, open doors, inflate slides at any moment. As time went by, that danger abated and, thankfully, we were lucky enough to get everybody off very calmly and very methodically through one set of stairs.

Questions were asked 'why did we spend so long in the air'? But we had to spend that time in the air to determine the state of the aircraft and it took that long to do that.

We tried to recreate it in the sim and we can't!

we had, as an example, messages that would say 'aircraft CoG out of limits' and was asking us to move fuel from horizontal stabiliser forward to bring it within limits and the next message would say the 'THS transfer not available'. So one message contradicting another

We didn't blindly follow the ECAMs. We looked at each one individually, analysed it, and either rejected it or actioned it as we thought we should.

Another key point was in 'tricking' the performance calculator to come up with an acceptable landing speed – again a demonstration of superb airmanship so vital in these incidents."

Bild 6: Das Flugzeug kommt am Ende der Landebahn in einem Sumpf von unter hohem Druck austretenden Kerosin mit 900 Grad heißen Bremsen zum Stehen: Wie durch ein Wunder entstand kein Brand!

Autor

Flugkapitän Prof. Dr.-Ing. M. Körte Körte-Aviation Consulting
Tutzing

Kontakt: max.koerte@t-online.de