Sonderdruck aus M. Grandt & S. Schmerwitz (Hrsg.) (2014), Der Mensch zwischen Automatisierung, Kompetenz und Verantwortung (DGLR-Bericht 2014-01). Bonn: Deutsche Gesellschaft für Luft- und Raumfahrt – Lilienthal-Oberth e.V.; ISBN 978-3-932182-81-2

Quantitative Berechnung der Auftrittswahrscheinlichkeit menschlicher Fehlhandlungen und ihre Verwendung in der Sicherheitsanalyse komplexer Mensch-Maschine-Systeme

Laura Polster & Henning Butz

Zusammenfassung

Komplexe Systeme müssen neben weitreichenden funktionalen oft auch hohen Sicherheitsanforderungen genügen. Das rein technische Betriebsrisiko kann heute, dank gut durchdachter Systemarchitekturen und ausgereifter Prozessstandards, nahezu beliebig weit reduziert werden. Dieser Determinismus geht leider verloren, sobald Menschen in die Betriebsabläufe komplexer Systeme involviert sind. Selbst aufwändig trainierte und geschulte Operateure, die strikte Prozeduren einhalten, verursachen 70-80% aller fatalen Systemunfälle. Sie sind damit drei- bis viermal tödlicher als das System, das sie bedienen. Bei untrainierten Operateuren kann dieser Faktor noch erheblich höhere Werte annehmen. Das 80:20-Verhältnis steht seit 30 Jahren wie in Stein gemeißelt. Es ändert sich auch nicht, wenn durch die technische Evolution das absolute Betriebsrisiko technischer Systeme und Anlagen immer weiter reduziert wird.

Die Zementierung der Verhältnisse ist ein Phänomen, dem seit Jahren auf unterschiedliche Weise versucht wird beizukommen: durch besseres Training, andere Prozeduren, „kooperative“ Automation, adaptive Mensch-Maschine-Schnittstellen, „menschlichere“ Semantiken usw. – leider bisher erfolglos. Die Systeme bleiben offenbar an vielen Stellen unvereinbar mit dem menschlichen Leistungsvermögen.

Wir sind der Auffassung, dass die Dominanz menschlicher Fehlerursachen unter anderem auf die unterschiedlichen Methoden der Sicherheitsanalysen bei den „technischen“ gegenüber den „menschlichen“ Anteilen eines Mensch-Maschine-Systems (MMS) zurückzuführen ist: während die Sicherheitsanalyse der „technischen“ Seite quantitative Verfahren verwendet, erfolgt die Analyse der „menschlich“ bedingten Sicherheitsrisiken weitgehend empirisch mit qualitativen Bewertungsmethoden.

Nach dem Grundsatz: nur was man messen kann, kann man auch beherrschen, schlagen wir in diesem Beitrag eine Methode zur quantitativen Behandlung menschlicher Faktoren im Kontext mit der Analyse technischer Risiken von MMS vor. Das Verfahren basiert auf dem Konzept nebenläufiger Markov-Prozesse. Es

liefert konkrete Werte für die Auftrittswahrscheinlichkeit von spezifischen menschlichen Fehlhandlungen. Gleichzeitig entstehen Modelle, die das menschliche Handeln im Umfeld von möglichen Fehler-korrigierenden oder auch Fehler-induzierenden Ereignissen dynamisch beschreiben.

Das Verfahren soll dazu beitragen, die Ursachen für den 80%-Anteil operativer Fehler an fatalen Systemunfällen besser zu verstehen, um so die Quote in der Zukunft auf ein vertretbares Maß zu reduzieren.

Ein wichtiger Beitrag wird auch für die Analyse und Prognose von Fehlhandlungen untrainierter Operateure in komplexen Situationen erwartet. Diese Problematik ist weitgehend unerforscht, wird aber zunehmend relevant durch den rasanten Anstieg des Automatisierungsgrades in Kraftfahrzeugen.

Der Beitrag basiert auf den Ergebnissen einer Masterarbeit, die Ende April 2014 an der University of the West of England, UWE in Bristol, UK, abgeschlossen wurde. Gegenwärtig laufen Bestrebungen, das Verfahren in bestehende Sicherheitsanalysewerkzeuge zu integrieren.

1 Einleitung

Die Führung sicherheitskritischer Systeme erfolgt heute zumeist vollautomatisch. Systeme, die umfangreiche Funktionalität mit hoher Kritikalität verbinden, werden dabei schnell komplex. Die Methoden, um das technische Versagensrisiko kritischer, komplexer Systeme auf ein prognostizierbares Minimum zu begrenzen, sind weit fortgeschritten und nachweislich verlässlich. Sicherheitsarchitekturen verwenden generell dissimilare Redundanz sowie „*Command / Monitoring (COM-MON)*“-Signalstrukturen zur Herstellung der notwendigen Systemintegrität und -verfügbarkeit(Storey, 1996). Zur Auslegung des konkreten Designs bzw. zur Ermittlung der erzielbaren Sicherheitsreserve werden kombinatorische und probabilistische Fehleranalytiken verwendet, bspw. Fehlerbäume oder die Fehlzustandsart- und -auswirkungsanalyse („*failue mode and effects analysis*“, FMEA)-Logik (DIN EN 60812; Boudali, 2007). Auf der Basis quantitativer Ausfallwahrscheinlichkeiten können so Ereigniswerte für das Auftreten kritischer Systemfehler und Funktionsausfälle sehr verlässlich vorausberechnet werden. Auf umgekehrtem Weg kann die Systemarchitektur entsprechend dem Erwartungswert eines konkret spezifizierten minimalen Systemrisikos entworfen werden.

Langjährige Statistiken zeigen, dass die spezifizierten Sicherheitsziele kritischer technischer Anlagen – bspw. konkretisiert in der Anzahl unkontrollierter Ausfälle pro Betriebsstunde – zuverlässig eingehalten werden. Das ändert sich, sobald Menschen in den Betriebsablauf komplexer, sicherheitskritischer Systeme eingreifen. Ausnahmslos steigt dann die Anzahl der „System“-Fehler signifikant an, wenn die „System“-Grenzen der MMS-Kontur um den Operateur erweitert gedacht werden (Clarke et al., 2010).

Die menschliche Beteiligung an der Systemführung ist oft unerlässlich. Sie ist insbesondere immer dann notwendig, wenn Systeme in einem ambivalenten

Umfeld betrieben werden, das die Automatik nicht eindeutig zu interpretieren vermag. Ein weiteres häufiges Motiv für Mensch-Maschine-Interaktion ist die Kompensation von Funktionsdegradationen des Systems im Fehlerfall (Stichwort „Rückfallebene Mensch“). Die menschliche Bandbreite möglicher (kreativer) Reaktionen auf Fehlerzustände ist sehr flexibel und breit. Sie ist damit oft deutlich kostengünstiger als die Alternative unzähliger, individueller technischer Kompensationsmaßnahmen. Leider vergrößert das aktive Eingreifen eines Menschen in komplexe Prozesse das Betriebsrisiko erheblich(Melnik, 2008).

Die Auswertung von Unfallstatistiken aus verschiedenen Anwendungsbereichen zeigen übereinstimmend, dass der Anteil menschlicher Fehler, die zu einem fatalen Funktionsversagen führen, drei- bis viermal so hoch ist wie der durch technische Fehler bedingte Unfallanteil. Diese Verhältnis ist seit Jahrzehnten konstant, obwohl in diesem Zeitraum bedeutende Fortschritte in der Verbesserung der absoluten Systemsicherheit um mehr als eine Größenordnung erzielt werden konnten: der Mensch bleibt drei- bis viermal tödlicher als das System, das er bedient.

Dabei betrifft diese Feststellung generell nur Situationen, wo geschulte Operateure – oft mittels trainierter Prozeduren – die Systembedienung vornehmen. Das Versagenspotential untrainierter Operateure in komplexen Prozessen ist noch weitgehend unerforscht. Deshalb kann nur vermutet werden, dass die zuvor genannte 80:20-Relation der Unfallrisiken sich wesentlich zu Ungunsten des menschlichen Anteils verschlechtern wird, wenn Menschen ohne Prozedurtraining mit komplexer Automatik umgehen müssen. Die Frage wird tendenziell zunehmend relevant, da private Kraftfahrzeuge zukünftig mit deutlich mehr, komplexeren und zudem verkoppelten Assistenzfunktionen ausgestattet werden sollen, ohne dass die Fahrer mit deren Bedienung vertraut gemacht, geschweigen denn trainiert werden können.

Der inakzeptabel hohe und scheinbar invariable Anteil menschlicher Fehler an der Gesamtbilanz fataler Systemunfälle korrespondiert mit den unterschiedlichen Herangehensweisen bei der Analyse und beim Entwurf technischer sowie prozeduraler Maßnahmen zur Realisierung spezifizierter Sicherheitsziele. Während auf der physikalischen Seite des Systems die eingangs beschriebenen quantitativen Verfahren (Zuverlässigkeit Block Diagramme - ZBD, Fehlerbaumanalysen - FTA oder Fehler Merkmal Effekt Analysen - FMEA) zur objektiven Berechnung und zum Nachweis der geforderten Systemsicherheit verwendet werden, kommen auf der menschlichen Seite im Wesentlichen nur qualitative Methoden (NASA-Task Load Index, SAGAT - Situation Awareness Global Assessment Technique) zur Anwendung. Bei diesen gestaltet es sich naturgemäß schwierig, sie in die Betrachtungen der quantitativen Analysen (z.B. Fehlerbäume) einzubeziehen. Ebenso wenig werden die oft vielseitigen Wechselbeziehungen zwischen dem/den Menschen und dem/den Automaten in ihren

Fehlerinduktions- und -korrekturpotentialen in angemessener Weise dynamisch erfasst, wie sie in einer komplexen Betriebssituation gegeben sind.

Im Folgenden wird eine Methode beschrieben, die es ermöglicht, menschliche Fehlerfaktoren probabilistisch zu quantifizieren sowie diese über Prozessmodelle mit der Proballistik von weiteren Fehler-induzierenden, bzw. Fehler-korrigierenden Effekten und Ereignissen in einem komplexen Betriebsumfeld zu korrelieren. Dadurch verändern sich die korrespondierenden Ereigniswahrscheinlichkeiten dynamisch in Abhängigkeit von den vorgesehenen technischen oder prozeduralen Maßnahmen. Zudem wird der Prozess der Fehlerentwicklung (oder -kompensation) sichtbar und ggf. auf stationäre Wahrscheinlichkeitswerte konvergiert. Die Ergebnisse sind geeignet, um in gängigen, quantitativen Analyseverfahren der Sicherheitstechnik – wie bspw. FTA, FMEA, ZBD etc. – weiterverwendet zu werden. So kann der Effekt von operativen Fehlhandlungen auf sicherheitskritische oder gar fatale „*Top Events*“ analytisch nachvollzogen und quantifiziert werden, sowohl im Kontext mit weiteren parallelen oder sequenziellen Bedienfehlern als auch im Kontext mit technischen Systemfehlern oder Korrekturmaßnahmen.

Der Ansatz verwendet nebenläufige Markov-Prozessmodelle, die eine gegebene Betriebssituation beschreiben, in der sowohl Menschen mit Menschen oder mit Automaten über Prozesse, als auch Automaten mit Menschen über ihre Benutzungsschnittstellen miteinander korrespondieren (Boudali, 2007). So entsteht ein Bild über die Wirksamkeit der technischen oder prozeduralen Maßnahmen, die zur Reduktion der Eintrittswahrscheinlichkeit fehlerhafter Handlungen vorgesehen sind. Zur Ermittlung der Häufigkeit von fatalen Funktionsausfällen, die durch Kombinationen von mehreren menschlichen oder menschlichen und technischen Fehlern entstehen, können die aus dem Markov-Modell berechneten Wahrscheinlichkeitswerte in Fehlerbäumen oder FMEA Analysen weiter verwendet werden.

Im Folgenden wird die skizzierte Methode ausführlich beschrieben und an zwei Beispielen in ihrer Wirkungsweise demonstriert.

2 Markov-Modelle und Fehlerbaumanalysen

Das in dem vorliegenden Beitrag vorgestellte Verfahren verfolgt zwei Ziele:

1. Die Ermittlung und Zuordnung konkreter, verlässlicher Ereigniswahrscheinlichkeiten zu möglichen menschlichen Fehlhandlungen in komplexen Mensch-Maschine-Betriebssituationen.
2. Die Weiterverwendung der ermittelten Ereigniswahrscheinlichkeiten im Rahmen von Fehlerbaumanalysen. Dort werden die Fehlerereignisse mit den Auftrittswahrscheinlichkeiten korrespondierender Systemfehler oder weiterer menschlicher Fehlhandlungen korreliert. So kann der Beitrag menschlicher Fehler zum Auftreten unzulässiger (sicherheitskritischer) Betriebssituationen (Top Events, TE) quantitativ erfasst werden.

Die beiden verwendeten Methoden ergänzen sich in idealer Weise:

- Der Fehlerbaum vermittelt eine statische Sicht auf ein Fehlerszenario, das in dieser Konstellation notwendig ist, um das Top Event mit einer Wahrscheinlichkeit auszulösen, die sich kombinatorisch aus den Einzelwahrscheinlichkeiten der Basis-Fehlerereignisse herleitet.
- Der Markov-Prozess vermittelt eine dynamische Sicht auf die Übergänge zwischen Fehlerereignissen oder zu Fehler-korrigierenden Zuständen sowie ein Bild der sich verändernden Auftrittswahrscheinlichkeiten im Zusammenspiel mit anderen Fehler- oder Korrekturoptionen, die ggf. auf stationäre Werte konvergieren.

Damit kann auf der Ebene der Markov-Modelle zunächst eine Optimierung der Betriebsabläufe des betrachteten MMS vorgenommen werden. Dies kann durch Veränderung von Zustandstransitionen, Einführung weiterer korrigierender Zustandselemente oder durch Verbesserung der Korrekturoptionen einzelner Elemente (Zustände im Markov-Modell) erfolgen. Die Optimierung endet, wenn das geforderte Minimum der relevanten Fehlerzustände erreicht ist oder wenn keine weitere Minimierung mehr möglich oder sinnvoll ist (z.B. aus Kostengründen). Mit den minimierten Werten kann im Fehlerbaum der Einfluss der betrachteten Fehler in Kombination mit anderen Fehlern auf ein relevantes Top Event analysiert werden.

Markov-Modelle eignen sich zur Analyse stochastisch-diskreter Ereignissysteme(Lunze, 2012). Deshalb müssen bei der Anwendung auf MMS-Betriebssituationen die auftretenden Fehlhandlungen, bzw. entsprechende Korrekturmaßnahmen jeweils als diskrete Zustände interpretiert werden. Dies ist keine Einschränkung der Allgemeinheit. Sollte sich eine Handlung dynamisch über mehrere Schritte entwickeln, könnten diese im Markov-Modell durch einzelne Zustände repräsentiert und über angemessene Transitionswahrscheinlichkeiten miteinander verkettet werden. Die für unsere Zwecke geeigneten Markov-Ketten besitzen die folgenden Eigenschaften(Lunze, 2012):

- Der Zustandsraum umfasst nur eine endliche Anzahl von Zuständen;
- Die bedingte Wahrscheinlichkeit des Folgezustands eines Systems ist nur eine Funktion des vorangehenden Systemzustands (die Markov Kette hat kein Gedächtnis);
- Die Transitionswahrscheinlichkeit von einem Zustand zum nächsten ist zeitunabhängig konstant;
- Jedem Systemzustand wird zu Beginn eine Eintrittswahrscheinlichkeit zugeordnet;
- Die Summe der Eintrittswahrscheinlichkeiten aller Anfangszustände ist 1, d.h., das System muss sich in einem Zustand befinden.

- Die Summe aller Transitionswahrscheinlichkeiten von einem Zustand zu anderen oder in sich selbst zurück ist 1 (ein Zustand muss in einen anderen übergehen oder in sich selbst zurückführen).

Zur Veranschaulichung der Funktionsweise des Modells einer Markov-Kette, betrachten wir nachfolgend ein einfaches Beispiel in Anlehnung an eine Cockpit Situation:

Beispiel: „Unzulässige Prozedur“

Das Markov-Modell besitzt drei Zustände:

1. Den Fehlerzustand „improper procedure“ (IP) = e_1,
2. die Prozedur „cross crew correction“ (CCC) = e_2 sowie
3. den sicheren Zustand “safe state recovery” (SSR) = e_3.

Zwischen allen Zuständen bestehen potentiell Transitionsmöglichkeiten sowie auch Transitionen zurück in den Ausgangszustand selbst. Ob und mit welcher Wahrscheinlichkeit sie real auftreten, muss bei der Modellbildung berücksichtigt werden. Sie sind u.a. ein Maß für die Güte der Korrekturmechanismen im Prozess. Ein hohes Korrekturpotential bedeutet: geringe Transition in Fehlerzustände hinein und hohe Transition aus Fehlerzuständen hinaus. So existiert wahrscheinlich ein Übergang von (IP) zu (CCC), was nichts anderes bedeutet, als dass eine falsche Prozedur (IP) von der Cockpit Crew wahrgenommen wird und den (CCC)-Prozess auslöst, der die Situation ggf. in den sicheren Zustand (SSR) überführt. D.h., auch zwischen (CCC) und (SSR) existiert eine Transition mit hoher Wahrscheinlichkeit. Weiterhin könnte die falsche Prozedur (IP) ggf. auch nicht wahrgenommen werden. Dann verharrt sie auch im nächsten Schritt im gleichen Zustand, d.h. (IP) führt in sich selbst zurück. Andererseits kann eine Cockpit-Prozedur nicht nur korrigieren, sondern möglicherweise auch eine falsche Prozedur provozieren. Damit wird es auch eine Transition von (CCC) zu (IP) geben. Deren Wahrscheinlichkeit sollte deutlich geringer sein als die der Transition von (IP) zu (CCC). Anderenfalls wäre das ein Indiz für eine äußerst bedenkliche *Cross Crew Coordination*. Die fehlerhafte Prozedur (IP) kann sich natürlich auch unmittelbar in den sicheren Zustand (SSR) begeben, falls dem Piloten sein Fehler selbst auffällt (möglicherweise angeregt durch eine Warnanzeige, die dann im Markov-Modell als zusätzlicher Zustand mit entsprechenden Transitionswahrscheinlichkeiten berücksichtigt werden sollte). Damit existiert auch eine Transition von (IP) zu (SSR). Vielleicht auch in die umgekehrte Richtung, denn es ist nicht ausgeschlossen, dass aus einem sicheren Zustand heraus eine falsche Prozedur ausgeführt wird, bspw. aufgrund eines Aufmerksamkeitsdefizits. Ganz sicher gibt es einen Übergang von (SSR) zu (CCC), denn Prozeduren werden dauernd ausgeführt, auch wenn alles stabil läuft. Mit einer hohen Wahrscheinlichkeit wird auch der Zustand (SSR) in sich selbst zurückführen. (CCC) soll keine Rekursion aufweisen. Die hier beschriebene Situation ist in Bild 1 dargestellt.

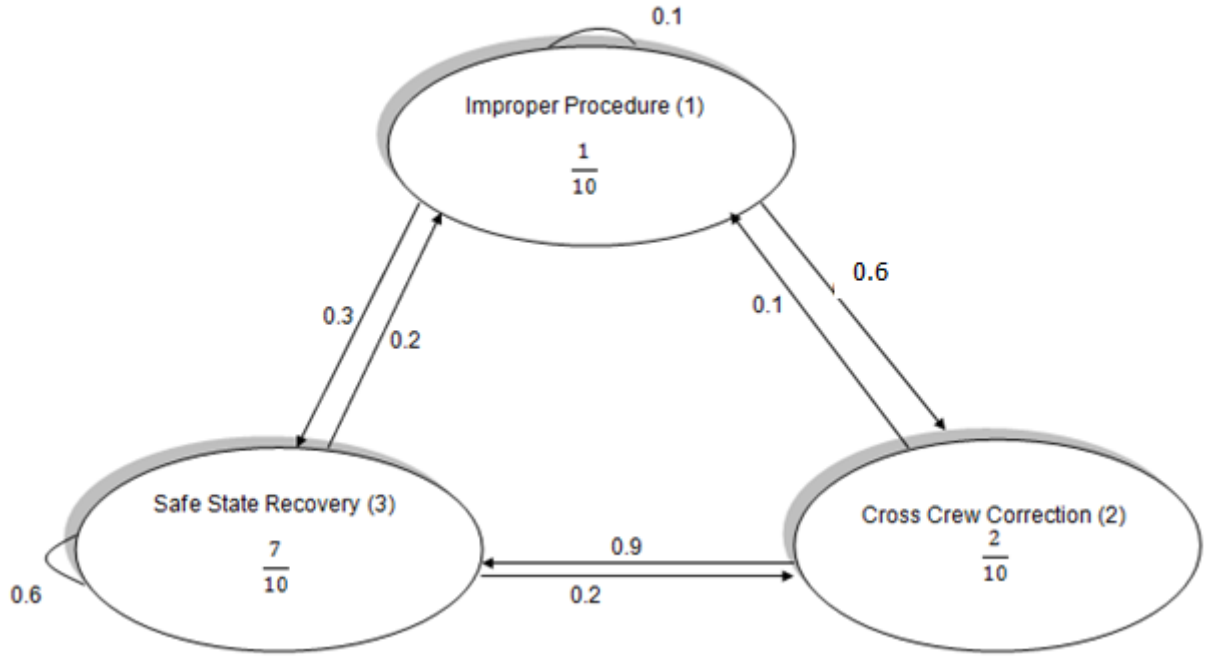

Bild 1: Markov-Modell mit drei Zuständen, deren Eintritts- und möglichen Transitionswahrscheinlichkeiten

Das Markov Modell samt der Vorgänge, die darin ablaufen, kann mithilfe der Vektor- und Matrizenrechnung mathematisch formalisiert werden. Der Vorgang umfasst acht Schritte(Siegel, 2003):

1. Bestimmung des Zustandsraumes: Der Zustandsraum {M} beschreibt die Zustände, die das System einnehmen kann. Die Systemzustände werden als Komponenten eines Zeilenvektors dargestellt. Der Wert der einzelnen Vektorkomponente ist die Eintrittswahrscheinlichkeit der einzelnen Systemzustände.

$$\{M\} = (e_1, e_2, e_3) = \underline{e} \tag{1}$$

Wobei e_1, e_2, e_3 im oben gewählten Beispiel die Zustände (IP), (CCC) und (SSR) repräsentieren. Die Zustände sind zeitdiskret. Das bedeutet, dass das System zu einem gegebenen Zeitpunkt nur einen Zustand einnehmen kann. Die Elemente des Zeilenvektors $\underline{e}$ können nur Werte zwischen null und eins annehmen.

$$e_i = [0 \ldots 1] \tag{1a}$$

Außerdem ist die Summe der Zeilenvektorelemente eins.

$$\sum_{i=1}^{m} e_i = 1 \tag{1b}$$

2. Bestimmung der Übergangs- oder Transitionswahrscheinlichkeiten: der Wert definiert die Wahrscheinlichkeit p_{ij}, mit der ein Zustand e_i zum Zeitpunkt $t = n\text{-}1$ in den Zustand e_j zum Zeitpunkt $t = n$ übergeht.

$$p_{ij} = \Pr\{(e_i \rightarrow e_j) \setminus (t{=}n\text{-}1 \rightarrow t{=}n)\} \tag{2}$$

Die Übergangswahrscheinlichkeiten können nur Werte zwischen null und eins annehmen.

$$p_{ij} = [0 \ldots 1] \tag{3}$$

Die Summe der Übergangswahrscheinlichkeiten von einem gegebenen Zustand in die m übrigen Zustände des Zustandsraums oder in sich selbst zurück ist immer eins.

$$\sum_{j=1}^{m} p_{ij} = 1 \tag{4}$$

3. Im dritten Schritt wird das Kreisdiagramm erstellt, das den Markov-Prozess beschreibt. Das Kreisdiagramm enthält die möglichen Zustände des Systems, alle möglichen Transitionen zwischen den Zuständen sowie die Anfangswerte der Zustandswahrscheinlichkeiten und die Transitionswahrscheinlichkeiten. Die spezifischen Parameter können experimentell oder aus Incident-Statistiken (z.B. *Line Operation Safety Audit*, LOSA) ermittelt werden. Das Kreisdiagramm für unser Beispiel zeigt Bild 1.
4. Im vierten Schritt wird die Transitionsmatrix $\underline{P}$ aufgestellt. $\underline{P}$ enthält alle Übergangswahrscheinlichkeiten p_{ij} zwischen den Zuständen ($e_i \rightarrow e_j$), $i = 1, \ldots, m$; $j = 1, \ldots, m$ des Systems, wobei die einzelnen Komponenten die Bedingung (3) und die Zeilensummen von $\underline{P}$ jeweils der Bedingung (4) genügen müssen. In unserem Beispiel ergibt sich die folgende Transitionsmatrix:

$$\mathrm{P} = \begin{pmatrix} 1/10 & 6/10 & 3/10 \\ 1/10 & 0 & 9/10 \\ 2/10 & 2/10 & 6/10 \end{pmatrix} \tag{5}$$

Die Multiplikation des Zeilenvektors $\underline{e}\,(t_{n-1})$ der Zustandswahrscheinlichkeiten aus Gleichung (1) zum Zeitpunkt t_{n-1} von rechts mit der Transitionsmatrix $\underline{P}$ liefert die veränderten Auftrittswahrscheinlichkeiten der Systemzustände nach einem Transitionsvorgang zum Zeitpunkt t_n.

$$\underline{e}\,(t_n) = \underline{e}\,(t_{n-1}) \times \underline{P} \tag{6}$$

Die weitere Multiplikation des resultierenden Zustandsvektors, $\underline{e}\,(t_n)$ von rechts mit der Transitionsmatrix $\underline{P}$, liefert die Zustandswahrscheinlichkeiten des nächst folgenden Zeitintervalls t_{n+1} usw.

$$\underline{e}\,(t_{n+1}) = \underline{e}\,(t_n) \times \underline{P} \tag{7}$$

Mit Gleichung (6) kann (7) auch als

$$\underline{e}\,(t_{n+1}) = \underline{e}\,(t_{n-1}) \times \underline{P} \times \underline{P} = \underline{e}\,(t_{n-1}) \times \underline{P}^2 \tag{8}$$

geschrieben werden. Durch Verallgemeinerung der Rekursion aus Gleichung (8) folgt unmittelbar für die Zustandswahrscheinlichkeiten zum Zeitpunkt t_k in Relation zu den Anfangswahrscheinlichkeiten zum Zeitpunkt t_0 (d.h. n=1):

$$\underline{e}\,(t_k) = \underline{e}\,(t_{1-1}) \times \underline{P} \times \underline{P} \times \underline{P} \times \underline{P} \ldots . \times \underline{P} = \underline{e}\,(t_0) \times \underline{P}^k \tag{9}$$

Damit beschränkt sich die Iteration des Markov-Modells auf die Bestimmung der Anfangsverteilung $\underline{e}_0$ aller Auftrittswahrscheinlichkeiten von Systemzuständen im Zustandsraum $\{M\}$ sowie auf die Kalkulation der Potenzen der Transitionsmatrix.

5. Bestimmung der Anfangsverteilung der Zustandswahrscheinlichkeiten. Die Werte werden im Zustandsvektor

$$\underline{e}_0 = (e_1, e_2, e_3, \ldots e_i, , e_j, \ldots, e_m) \tag{10}$$

zusammengefasst. In unserem Beispiel sei die Anfangsverteilung durch die folgenden Wahrscheinlichkeitswerte beschrieben:

$$\underline{e}_0 = (1/10, 2/10, 7/10) \tag{11}$$

6. Im sechsten Schritt wird simuliert, wie die Zustandswahrscheinlichkeiten

$$\underline{e}_i = (e_1, e_2, e_3, \ldots e_i, , e_j, \ldots, e_m) = \underline{e}(t_i) \tag{12}$$

in Anwesenheit potentieller Fehler-induzierender und Fehler-korrigierender Systemzustände iterativ variieren. Es ist leicht nachzuvollziehen, dass sich die Auftrittswahrscheinlichkeit der Systemzustände über die sequenziellen Schritte eines Markov-Prozesses verändern werden, da sie mit jeder Iteration der Markov-Kette von verschiedenen Zuständen angeregt werden bzw. sich in diverse Zustände der Kette auflösen können.

Nach einer endlichen Zahl von Iterationen konvergieren die hier betrachteten Markov-Modelle asymptotisch auf stationäre Transitionswahrscheinlichkeiten. In diesem Fall nehmen die Elemente einer Matrixspalte identische Werte an. Mathematisch übersetzt bedeutet dieser Sachverhalt, dass sich die Spalten der n-ten und $(n+1)$-ten Potenz der Transitionsmatrix nicht mehr unterscheiden. Der vorletzte Schritt besteht demnach darin, die stationäre Potenz der Transitionsmatrix zu bestimmen.

7. Ermittlung der stationären Transitionsmatrix, d.h. der Grenzmatrix. Dies kann rekursiv über eine Differenzbildung mit anschließender Auswertung einer Grenzwertungleichung der Art

$$\underline{\Delta} = \underline{P}^n - \underline{P}^{n-1} < \underline{\varepsilon} \tag{13}$$

erfolgen. In unserem Beispiel konvergiert die Transitionsmatrix nach fünf Iterationsschritten auf die stationäre Grenzmatrix. Sie hat dann das folgende Aussehen:

$$\underline{P}^5 = \begin{pmatrix} 0.162 & 0.221 & 0.617 \\ 0.162 & 0.221 & 0.617 \\ 0.162 & 0.221 & 0.617 \end{pmatrix} \tag{14}$$

8. Der achte und letzte Schritt dient zur Berechnung der stationären Verteilung der Zustandswahrscheinlichkeiten im Zustandsraum $\{M\}$. Nach den zuvor angestellten Überlegungen ergibt sich die stationäre Verteilung der Ereigniswahrscheinlichkeiten des Markov-Systems zu

$$\underline{e}_{stat} = \underline{e}_0 \text{ x } \underline{P}^n = \underline{e}_0 \text{ x } \underline{P}_{stat}. \quad (15)$$

Im konkreten Fall des gewählten Beispiels erhalten wir somit das folgende Ergebnis:

$$\underline{e}_5 = \underline{e}_0 \text{ x } \underline{P}^5$$

$$= (0.1; 0.2; 0.7) \text{ x } \begin{pmatrix} 0.162 & 0.221 & 0.617 \\ 0.162 & 0.221 & 0.617 \\ 0.162 & 0.221 & 0.617 \end{pmatrix}$$

$$= (0.0162+0.0324+0.1134;\ 0.0221+0.0442+0.1547$$
$$+0.0617+0.1234+0.4319)$$

$$= (0.162; 0.221; 0.617) = \underline{e}_{stat}. \quad (16)$$

Die stationäre Grenzverteilung der Ereigniswahrscheinlichkeiten der einzelnen Systemzustände e_{stat}, die man auch „Fixvektor“ nennt, ist identisch mit den Werten der Spaltenelemente der Grenzmatrix P_{stat}. Dieses Ergebnis gilt generell, da die Summe der Ereignisvektorelemente immer 1 ist. Damit kann das Spaltenelement der Transitionsmatrix als Faktor vor die Summe der Ereignisvektorelemente gezogen werden, was einer Multiplikation mit eins entspricht.

So folgt unmittelbar aus den voranstehenden Überlegungen, dass die stationären Auftrittswahrscheinlichkeiten der Markov-Ereignisse völlig unabhängig von den Werten der Anfangswahrscheinlichkeiten sind und nur von den Transitionswahrscheinlichkeiten zwischen den Ereignissen abhängen. Prozesse mit dieser Eigenschaft nennt man ergodisch. Formal ist diese Eigenschaft immer dann gegeben, wenn in einer der Potenzen der Transitionsmatrix eine Spalte auftritt, in der kein Element den Wert Null annimmt (Spaltenkriterium). Dann konvergieren die Potenzen der Transitionsmatrix asymptotisch auf die Grenzmatrix. Der Fixvektor der Grenzmatrix repräsentiert die stationären Erwartungswerte der möglichen Systemereignisse, wie sie über lange Zeiträume (Zeitmittel) oder viele ähnliche Situationen (Scharmittel) durchschnittlich auftreten werden. Für die Anwendung bedeutet diese Tatsache, dass das Ziel erhöhter MMS-Fehlertoleranz im Wesentlichen über den Entwurf verbesserter Transitionsbedingungen zwischen Fehlerzuständen und Korrekturzuständen erreicht werden kann.

3 Fallbeispiele

Im Folgenden soll anhand zweier Fallbeispiele gezeigt werden, wie Mensch-Maschine-Situationen mittels Markov-Modellen dargestellt und hinsichtlich des Auftretens kritischer Ereignisse analysiert werden können. Als erste Fallstudie wählen wir wieder eine Cockpit-Betriebssituation, bspw. den Landeanflug eines Verkehrsflugzeugs mit zwei Piloten. Wir nehmen an, dass wie üblich einer der Piloten den Landeanflug ausführt, während der andere Kontrollfunktionen ausübt. Daneben bekommt die Crew Anweisungen von der Flugverkehrsführung sowie diverse Meldungen (optisch, haptisch, akustisch) von den im Cockpit installierten Anzeige- und Bediengeräten. Der Einfachheit halber gehen wir davon aus, dass

die relevanten Prozeduren sich auf die Aktionen „*cross crew correction* (CCC)“, „*check list execution* (CLE)“ sowie „*auto pilot mode selection* (APMS)“ beschränken. Dazu kommen die Anweisungen der „*air traffic control* (ATC)“. Bei den Geräten wollen wir Warnungen, „*master caution annunciation* (MCA)“ sowie Protektionen, „*risk area protection* (RAP)“, als Beispiele für die Korrekturebene zwischen den Menschen und den Systemen einbeziehen. Als mögliche Fehlerzustände werden die „*improper procedure* (IP)“, „*wrong AP mode selection* (WMS)“ sowie das „*improper maneuver* (IM)“ im Modell berücksichtigt. Der Sichere Zustand ist mit „*safe state recovery* (SSR)“ im Modell repräsentiert und könnte bspw. die konkreten Manöver „*Go-Around* (Durchstarten)“ oder „*regain stable approach*“ beinhalten.

Damit umfasst unser Modell zehn Ereignisse, die als mögliche Systemzustände auftreten können: (IP), (WMS), (IM), (CCC), (CLE), (APMS), (ATC), (MCA), (RAP) und (SSR). Zwischen den Ereignissen bestehen ggf. bilaterale Beziehungen, die den Übergang von einem Ereignis in ein anderes oder in sich selbst zurück symbolisieren.

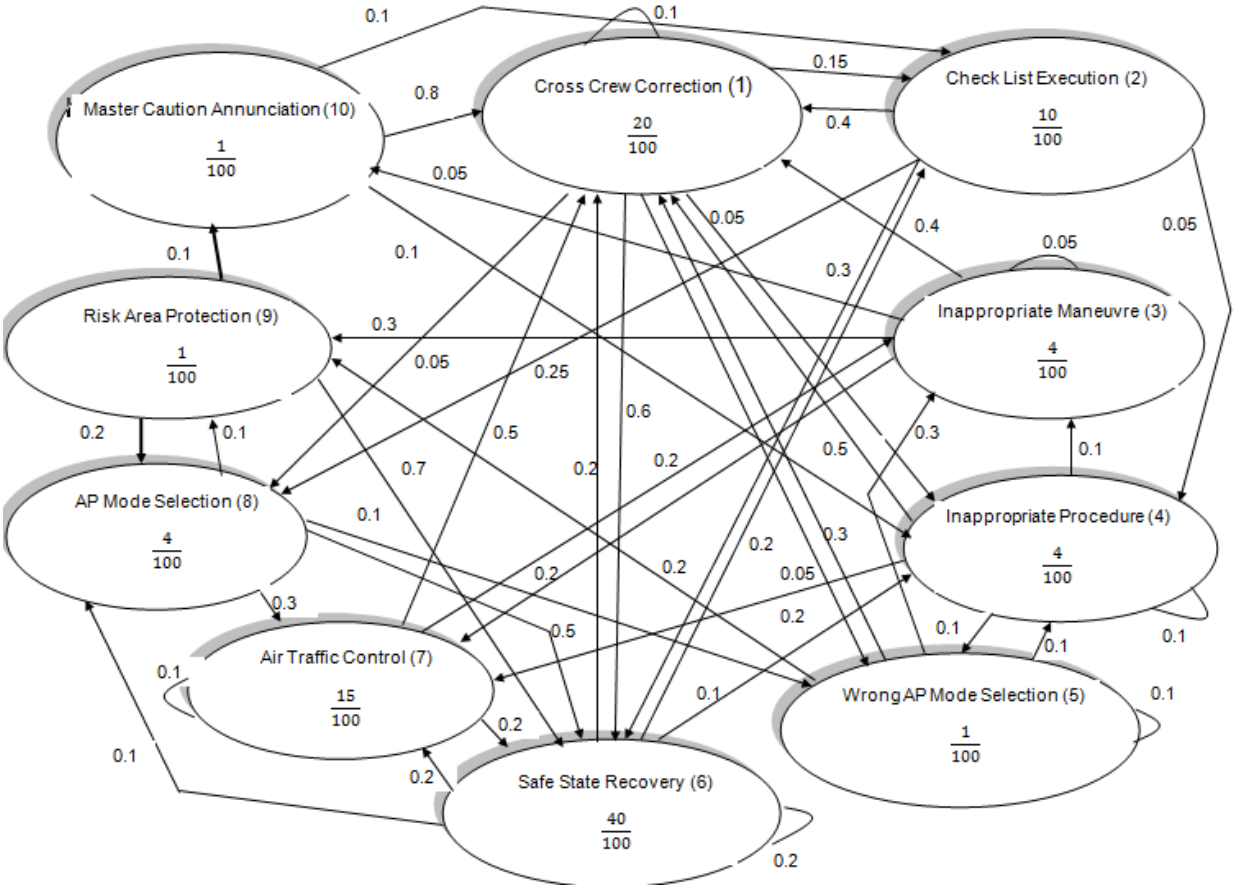

Bild 2: Markov-Modell der Cockpit-Situation „Landeanflug“, Verkehrsflugzeug.

Die Übergänge finden mit individuellen Wahrscheinlichkeiten statt, die von den Eigenschaften der beteiligten Ereignisse abhängen (bspw. die Qualität einer *risk protection*-Funktion oder einer ATC-Anweisung). Die Struktur des gewählten Markov-Modells ist in Bild 2 dargestellt.

Um zu verstehen, wie das Markov-Modell funktioniert, betrachten wir in Bild 2 die drei unteren Zustände auf der rechten Seite. Sie beschreiben die möglichen Fehlhandlungen, die in unserem Landeanflug-Beispiel auftreten sollen: *Wrong AP Mode Selection* (WMS), *Improper Procedure* (IP) sowie *Improper Maneuvre* (IM). Die Anfangswerte für die Ereigniswahrscheinlichkeiten sind in die Zustandsellipsen eingetragen. Sie können bspw. aus den Statistiken von *Flight-Incident-Report*-Repositorien (z.B. LOSA) entnommen bzw. aus beobachteten Simulatorversuchen berechnet werden. Wir verwenden hier LOSA-Daten. Die Linien zwischen den Ereignissen repräsentieren die Übergangswahrscheinlichkeiten von einem Zustand in den nächsten. So wird bspw. angenommen, dass durch die Selektion eines falschen AP Modes mit einer Wahrscheinlichkeit von 10% (Wert 0.1) bzw. in 10% der Fälle eine inkorrekte Prozedur folgt. Mit der gleichen Wahrscheinlichkeit wird ein falscher AP Mode im Rahmen einer falschen Prozedur erwartet. Mit einer wesentlich höheren Wahrscheinlichkeit von 30% wird sich dagegen ein unangemessenes Manöver direkt aus einer falschen AP-Einstellung ergeben, wohingegen eine falsche Prozedur wieder nur in 10% der Fälle zu einem unangemessenen Manöver führt. Falsche Prozeduren können aber auch aus Routineereignissen, wie bspw. *Check List Execution* (CLE), hervorgehen. Dies wird in Bild 2 oben rechts mit einer Wahrscheinlichkeit von 5% unterstellt.

Die eingenommenen Fehlerzustände können auch mit einer gewissen Wahrscheinlichkeit unbemerkt bleiben. Dann führt die Transition in den eigenen Zustand zurück (bspw. zu 10% bei IP). In der Mehrzahl der Fälle werden sie durch Warnungen und Prozeduren korrigiert und verlassen. Dies ist in Bild 2 auf der linken Seite zu sehen: die falsche AP Mode-Einstellung wird bspw. in 20% der Fälle durch AP-eigene Protektionsfunktionen (RAP) entdeckt und entweder automatisch in einen korrekten Mode (zu 20% Übergang in APMS) geschaltet oder in einen sicheren Zustand (70% zu SSR) überführt. Alternativ lösen die Schutzfunktionen einen Alarm aus (zu 10% Übergang nach MCA). Ausgelöst durch die akustische Warnung (MCA) werden zu 80% *Cross Crew Corrections* (CCC) oder zu 10% Checklisten (CLE) durchlaufen. In 10% der Fälle kann ein Alarm (MCA) allerdings auch missverstanden werden und eine unangemessene Prozedur (IP) auslösen. Die alarmierte Crew (CCC) sollte mit einer Wahrscheinlichkeit von 60% unmittelbar den sicheren Flugzustand (SSR) wiedererlangen. In 5% der Fälle resultiert aus (CCC) ein neues AP Setting (APMS), welches dann mit einer Wahrscheinlichkeit von 50% den sicheren Zustand (SSR) wiederherstellt. Vergleichbare Übergänge bestehen zwischen der Checklist-Prozedur (CLE) und der *AP Mode Selection* (APMS) (25%) sowie in direkter Verbindung zum sicheren Flugzustand (SSR) (30%).

Die beschriebenen Übergangswahrscheinlichkeiten werden in der Transitionsmatrix $\underline{P}_0$ zusammengefasst (Tab. 1).

Tab. 1: Transitionsmatrix $\underline{P}_0$ des Betriebsszenarios „Landeanflug“ Verkehrsflugzeug

CCC	CLE	IM	IP	WMS	SSR	ATC	APS	RAP	MCA
0,1	0,15	0	0,05	0,05	0,6	0	0,05	0	0
0,4	0	0	0,05	0	0,3	0	0,25	0	0
0,4	0	0,05	0	0	0	0,2	0	0,3	0,05
0,5	0	0,1	0,1	0,1	0	0,2	0	0	0
0,3	0	0,3	0,1	0,1	0	0	0	0,2	0
0,2	0,2	0	0,1	0	0,2	0,2	0,1	0	0
0,5	0	0,2	0	0	0,2	0,1	0	0	0
0	0	0	0	0,1	0,5	0,3	0	0,1	0
0	0	0	0	0	0,7	0	0,2	0	0,1
0,8	0,1	0	0,1	0	0	0	0	0	0

Die Anfangswerte der Ereigniswahrscheinlichkeiten bilden den Ereignisvektor $\underline{e}_0$ (Tab. 2). Sie basieren auf den Angaben der LOSA-Statistik.

Tab. 2: Anfangswertvektor $\underline{e}_0$ der Ereigniswahrscheinlichkeiten

CCC	CLE	IM	IP	WMS	SSR	ATC	APS	RAP	MCA
0,2	0,1	0,04	0,04	0,01	0,4	0,15	0,04	0,01	0,01

Das formalisierte Markov-Modell beschreibt eine Situation, in der unzulässige Manöver und Prozeduren oder falsche AP-Einstellungen durch wirkungsvolle Schutzfunktionen (RAP) erkannt, angezeigt (MCA) und schließlich mittels abgestimmter Prozeduren (CCC) / (CLE) korrigiert werden (SSR). Durch fortlaufende Multiplikation des Ereignisvektors mit Potenzen der Transitionsmatrix wird das Zusammenspiel der Cockpitereignisse simuliert. Die Ereigniswahrscheinlichkeiten verändern sich dabei solange, bis sie schließlich in der stationären Grenzmatrix $\underline{P}_S$ (Tab. 3) zum Fixvektor $\underline{e}_S$ (Tab. 4) konvergieren.

Tab. 3: Stationäre Transitionsmatrix $\underline{P}_S$ des Betriebsszenarios „Landeanflug“ Verkehrsflugzeug

CCC	CLE	IM	IP	WMS	SSR	ATC	APS	RAP	MCA
0,212	0,107	0,039	0,062	0,023	0,372	0,119	0,041	0,020	0,004
0,212	0,107	0,039	0,062	0,023	0,372	0,119	0,041	0,020	0,004
0,212	0,107	0,039	0,062	0,023	0,372	0,119	0,041	0,020	0,004
0,212	0,107	0,039	0,062	0,023	0,372	0,119	0,041	0,020	0,004
0,212	0,107	0,039	0,062	0,023	0,372	0,119	0,041	0,020	0,004
0,212	0,107	0,039	0,062	0,023	0,372	0,119	0,041	0,020	0,004
0,212	0,107	0,039	0,062	0,023	0,372	0,119	0,041	0,020	0,004
0,212	0,107	0,039	0,062	0,023	0,372	0,119	0,041	0,020	0,004
0,212	0,107	0,039	0,062	0,023	0,372	0,119	0,041	0,020	0,004
0,212	0,107	0,039	0,062	0,023	0,372	0,119	0,041	0,020	0,004

Tab. 4: Fixvektor $\underline{e}_S$ der stationären Ereigniswahrscheinlichkeiten

CCC	CLE	IM	IP	WMS	SSR	ATC	APS	RAP	MCA
0,212	0,107	0,039	0,062	0,023	0,372	0,119	0,041	0,020	0,004

Die stationäre Lösung beschreibt den Zustand einer Cockpit-Situation, in der alle möglichen Wege zwischen allen möglichen Ereignissen vielfach durchlaufen wurden. Das Ergebnis repräsentiert die mittleren Erwartungswerte der einzelnen Cockpitereignisse. Wie anhand von Gleichung (16) gezeigt wurde, sind die Grenzwahrscheinlichkeiten ergodischer Ereignisse unabhängig von deren Anfangszustand und identisch mit den Werten der Spaltenelemente der Grenzmatrix, mithin des Fixvektors. Das Ergebnis zeigt, dass die statistischen Angaben – bspw. aus der LOSA-Datenbank – für das Auftreten von Routine- / Korrekturprozeduren (CCC) und (CLE) sowie auch für fehlerhafte Manöver (IM) und Prozeduren (IP) durch das Modell recht genau bestätigt werden. Demgegenüber treten *Mode Selection Fehler* (WMS) doppelt so häufig auf als zu Beginn der Simulation geschätzt. Sie werden allerdings auch doppelt so oft durch Protektionen erkannt und kompensiert als eingangs angenommen. Ergänzende Korrekturinstanzen, bspw. das (ATC) sowie Warnungen (MCA), melden sich auch deutlich seltener als angenommen. Das Modell zeigt eine zufriedenstellende Übereinstimmung mit den statistisch ermittelten Werten der Realität. Darüber hinaus liefert es berechnete Werte, die man für die analysierte Betriebssituation „Landeanflug“ bisher nur schätzen konnte. Außerdem zeigt es, dass der sichere Flugzustand nur zu 37% der Zeit eingenommen wird. Dies Ergebnis überrascht zunächst. Bei näherer Betrachtung des Modells und der Simulationsergebnisse

wird aber schnell klar, dass das berechnete Resultat der Realität entspricht. Abgesehen von den rund 10%, zu denen sich das MMS per se in unzulässigen Manövern und Prozeduren befindet, sind auch die Ereignisse (CCC) sowie (CLE) nicht unbedingt sichere Zustände. Denn entweder wurden sie durch einen Fehler ausgelöst, der während ihrer Dauer weiterhin besteht oder sie nehmen die Crew mental in Anspruch, so dass zumindest eine gewisse Ablenkungsgefahr besteht (z.B. Head Down beim (CLE)), die oft mit einem sicheren Flugzustand nicht vereinbar ist. Gleiches gilt auch für die Ereignisse *AP Mode Selection* (APMS), (ATC) und Warnung (MCA): neben der Absorption von Aufmerksamkeit lösen sie auch oft transiente Ereignisse aus (Manöver, Systemumschaltungen etc.), die das Gefahrenpotential erhöhen. Das Markov-Modell enthüllt solche Mechanismen und verweist damit auf die Notwendigkeit zur Analyse von Maßnahmen, die das Verweilen in Ablenkungszuständen minimieren.

Um zu verstehen, wie mit Hilfe von Markov-Modellen Veränderungen in einem MMS dargestellt und analysiert werden können, betrachten wir den Fall, dass die „menschlichen“ Korrektur- und Überwachungsaktivitäten (CCC und ATC) entfallen. Sie werden ersetzt durch intensivere Protektionsfunktionen und Warnungen der Systeme (hier des AP) sowie durch vermehrte Nutzung der Checklisten (CLE). Allerdings können diese Ereignisse damit umgekehrt eher wieder zu Fehlerzuständen führen („*Mode Confusion*“, bspw. (WMS) oder (IP)), da sie a) häufiger auftreten und b) nicht mehr durch redundante Prozeduren (CCC) und (ATC) moderiert werden. Das Szenario entspricht der Situation eines General Aviation (GA) Fliegers im „single pilot“-Anflug auf ein Flugfeld ohne Flugsicherungskontrolle. Der Graph des Markov-Modells dieser Anordnung zeigt Bild 3.

Die Übergangswahrscheinlichkeiten zwischen den einzelnen Ereignissen der simulierten Situation sind weitgehend identisch mit den Werten des zuvor beschriebenen Referenzbeispiels. Dort, wo Übergänge zu den entfernten Betriebsereignissen (CCC) und (ATC) bestanden, wurden sie sinnvoll auf andere Systemzustände „umgeleitet“. So wird bspw. im ersten Beispiel eine falsche Prozedur (IP) mit einer Wahrscheinlichkeit von 50% durch das (CCC) und zu 20% durch (ATC) entdeckt und korrigiert. In Beispiel 2 entfallen diese Instanzen. Stattdessen wird der Fehler nun zu 20% durch Protektionen und zu 10% im Rahmen von Checklist-Kontrollen korrigiert. Zu 40% wird aber davon ausgegangen, dass die falsche Prozedur schließlich zu einem inkorrekten Manöver führt. Auch die Anfangswerte der Ereigniswahrscheinlichkeiten wurden in Anlehnung an das erste Beispiel gewählt, da Orientierungswerte aus offiziellen Statistiken wie LOSA für GA nicht bekannt waren. Auch hier wurden wieder die Auftrittswahrscheinlichkeiten der entfallenen Ereignisse (CCC) und (ATC) im Weiteren auf die verbliebenen Korrekturinstanzen (CLE) und (RAP) verteilt.

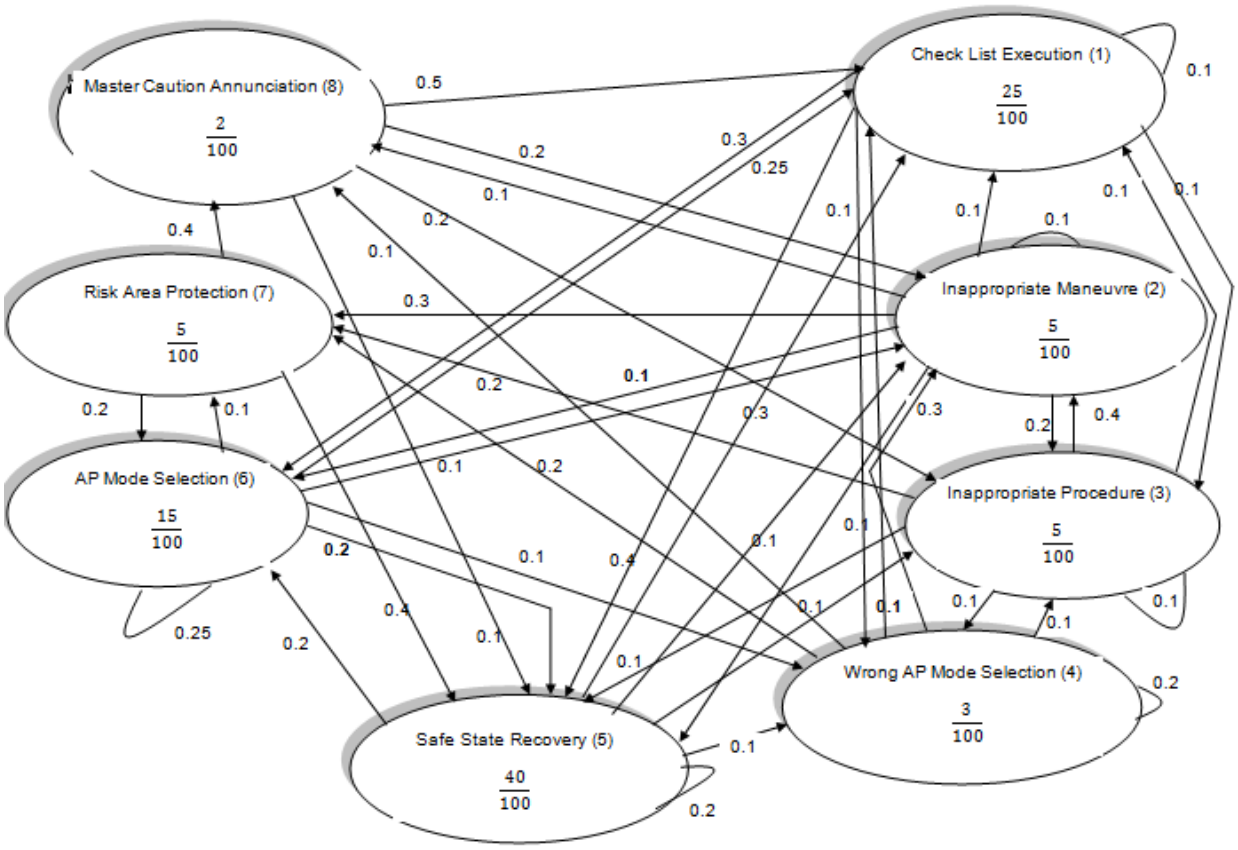

Bild 3: Markov-Modell der Cockpit Situation „Landeanflug“, General Aviation

Durch mathematische Formalisierung des Modells erhält man die folgende Transitionsmatrix $\underline{P}_0$ (Tab. 5):

Tab. 5: Transitionsmatrix $\underline{P}_0$ des Betriebsszenarios „Landeanflug“ General Aviation

CLE	IM	IP	WMS	SSR	APS	RAP	MCA
0,1	0	0,1	0,1	0,4	0,3	0	0
0,1	0,1	0,2	0	0,1	0,1	0,3	0,1
0,1	0,4	0,1	0,1	0,1	0	0,2	0
0,1	0,3	0,1	0,2	0	0	0,2	0,1
0,3	0,1	0,1	0,1	0,2	0,2	0	0
0,25	0,1	0	0,1	0,2	0,25	0,1	0
0	0	0	0	0,4	0,2	0	0,4
0,5	0,2	0,2	0	0,1	0	0	0

und den dazugehörenden Ereignisvektor $\underline{e}_0$ (Tab. 6):

Tab. 6: Anfangswertvektor $\underline{e}_0$ der Ereigniswahrscheinlichkeiten

CLE	IM	IP	WMS	SSR	APS	RAP	MCA
0,25	0,05	0,05	0,03	0,4	0,15	0,05	0,02

Die Simulation des zweiten Modells führt zu der in Tabelle 7 angegebenen Grenzmatrix $\underline{P}_S$.

Tab. 7: Stationäre Transitionsmatrix $\underline{P}_S$ des Betriebsszenarios „Landeanflug“ General Aviation

CLE	IM	IP	WMS	SSR	APS	RAP	MCA
0,181	0,123	0,092	0,081	0,210	0,168	0,088	0,056
0,181	0,123	0,092	0,081	0,210	0,168	0,088	0,056
0,181	0,123	0,092	0,081	0,210	0,168	0,088	0,056
0,181	0,123	0,092	0,081	0,210	0,168	0,088	0,056
0,181	0,123	0,092	0,081	0,210	0,168	0,088	0,056
0,181	0,123	0,092	0,081	0,210	0,168	0,088	0,056
0,181	0,123	0,092	0,081	0,210	0,168	0,088	0,056
0,181	0,123	0,092	0,081	0,210	0,168	0,088	0,056

mit dem daraus abgeleiteten Fixvektor $\underline{e}_S$ (Tab. 8):

Tab. 8: Fixvektor $\underline{e}_S$ der stationären Ereigniswahrscheinlichkeiten General Aviation

CLE	IM	IP	WMS	SSR	APS	RAP	MCA
0,181	0,123	0,092	0,081	0,210	0,168	0,088	0,056

Das Ergebnis zeigt, dass die Checkliste deutlich seltener (ca. 30%) konsultiert wird als vermutet. Ebenso wenig werden die angenommenen Ereigniswahrscheinlichkeiten der Fehlerzustände sowie des sicheren Zustands bestätigt. Während die kritischen Ereignisse (IP), (IM) und (WMS) z.T. mehr als doppelt so oft auftreten wie angenommen, befindet sich das System mit einer um fast 50% geringeren Wahrscheinlichkeit im sicheren Zustand (SSR) als ursprünglich unterstellt. Dieses Ergebnis korrespondiert durchaus mit den Erfahrungen und Erwartungen, dass der „single pilot“-Approach eines GA-Fliegers dem Sicherheitsstandard eines Anflugs mit vollständiger Cockpit Crew unter ATC-Kontrolle unterlegen ist.

4 Schlussfolgerung

Die vorliegende Schrift beschreibt einen neuen Ansatz zur quantitativen Berechnung von Auftrittswahrscheinlichkeiten menschlicher Fehlerereignisse in komplexen Mensch-Maschine-Systemen (MMS). Die Methode verwendet dazu das Verfahren der nebenläufigen Markov-Prozesse. Das Markov-Modell interpretiert Situationen des MMS als eine Folge von Ereignissen, die mit berechneten, gemessenen oder aus bekannten Statistiken ermittelten Wahrscheinlichkeiten ineinander übergehen. Da die Prozesse ergodisch sind, führen sie zu stationären Ergebnissen. Sie repräsentieren das Verhalten des Systems entweder über sehr lange Zeiträume oder aber über sehr viele gleichartige Situationen des Mensch-Maschine-Systems (Zeitmittel = Scharmittel). Das bedeutet, das System hatte Gelegenheit, alle möglichen Übergänge zwischen den Zuständen seiner Ereignisse mit ausreichender Häufigkeit zu durchlaufen. Die ermittelten Ereigniswahrscheinlichkeiten können deshalb als signifikant interpretiert werden. Der Wert der Markov-Prozesse besteht darüber hinaus darin, dass mit verschiedenen Modellanordnungen und -parametrierungen experimentiert werden kann. Dies eröffnet die Möglichkeit, Verbesserungsmaßnahmen – dargestellt durch veränderte Parameter der Transitionswahrscheinlichkeiten – in ihrer Wirkung auf das Auftreten von Fehlerereignissen zu untersuchen. Damit lassen sich auch Einsichten in die Empfindlichkeit des Systems gegenüber Fehler-auslösenden oder -kompensierenden Ereignissen gewinnen. Da das Verfahren noch neu ist, bedarf es sicherlich noch einer Reihe repräsentativer Pilotanwendungen, um Erfahrungen zu sammeln, wie die Parameter der Modelle in Korrelation zu technischen und prozeduralen Vorkehrungen zu skalieren sind.

Literatur

Boudali, H., Crouzen, P., & Stoelinga, M. (2007). *Dynamic Fault Tree analysis using Input/Output Interactive Markov Chains.* Abgerufen am 29. November 2013 von http://wwwhome.cs.utwente.nl/~marielle/papers/BCS07.pdf

Clarke, L. A., Osterweil, L. J., & Avrunin, G. S. (2010). *Supporting Human-Intensive Systems, UMassAmherst.* Abgerufen am 04. December 2013 von http://www.umass.edu/eei/EEI%20Website%20Articles/Supporting%20Human-Intensive%20Systems.pdf

Lunze, J. (2012). *Ereignisdiskrete Systeme - Modellierung und Analyse dynamischer Systeme mit Automaten, Markovketten und Petrinetzen.* München: Oldenburg.

Melnik, R. V. (2008). *Coupling control and human factors in mathematical models of complex systems, ScienceDirect.* Abgerufen am 01. December 2013 von www.elsevier.com/locate/engappai

Siegel, C. (13. March 2003). *Facharbeit Mathematik: Markow-Ketten.* Abgerufen am 15. September 2013 von http://www.xmarks.com/site/www.siegel-christian.de/seiten/facharbeit/markow.html

Storey, N. (1996). *Safety-Critical Computer Systems* (1 ed.). Edinburg: Prentice Hall.

.

Autoren

L. Polster, MEng BSc	University of the West of England – UWE Bristol
Dipl.-Ing. H. Butz	Advanced System Engineering Solutions – ASES Jork

Kontakt: lpolster@gmx.de
henningbutz@web.de