

hochschule für angewandte wissenschaften
FACHBEREICH FAHRZEUGTECHNIK UND FLUGZEUGBAU **hamburg**
university of applied sciences

Berliner Tor 5
20099 Hamburg

FLUGZEUGBAU

theoretische Arbeit

Zuverlässigkeit und Sicherheit
eines Lasten- und Personenaufzuges
für Großraumflugzeuge

Verfasser: Jörg Hansing

in Zusammenarbeit mit:
Airbus Deutschland GmbH, Hamburg

Abgabedatum: 30.06.2002

Prüfer: Prof. Dr.-Ing. Dieter Scholz, MSME



Kurzreferat

Diese Arbeit handelt von den Grundlagen der Zuverlässigkeitsrechnung, wie sie in zunehmenden Maße nicht nur im Flugzeugbau, sondern in weiten Teilen der Industrie zur Anwendung kommen. Die Gründe für die Zweckmäßigkeit dieser Techniken werden in dieser Arbeit ebenso angesprochen, wie die wichtigsten Begriffe und Definitionen, wobei, um dem Schwerpunkt Flugzeugbau treu zu bleiben, auf Verfahren, die bei der Firma Airbus gebräuchlich sind, besonders eingegangen wird. Zu den Verfahren gehören auch die Einsatzkriterien der Verfahren, um eine der Problemstellung angemessene Auswahl zu treffen. Dafür sind Wertungsmöglichkeiten für potentielle Fehler gegeben.

Im weiteren Verlauf wird auf mathematische Grundgleichungen zur Ermittlung von Kennwerten eingegangen, die zum Nachweis von Forderungen aus dem Lastenheft benötigt werden. Zur weiteren Illustration der Rechnungen und Anwendung der Failure Mode and Effect Analysis basiert diese Arbeit auf einer Konzeptstudie eines Lasten- und Personenaufzuges für Großraumflugzeuge. Die Zuverlässigkeit betreffende Punkte der Anforderungsliste werden in zuverlässigkeitsspezifische Kennwerte übersetzt, die dann für die in der Konzeptstudie beschriebenen Antriebsvarianten nachgewiesen werden. Die benötigten Ausfallraten für generische Komponenten sind der Literatur entnommen. Da in der dem Beispiel zugrundeliegenden Konzeptstudie die zuverlässigkeitsrelevanten Kennwerte unberücksichtigt bleiben, werden Veränderungen am gewählten Konzept vorgeschlagen, um die Anforderungen an die Zuverlässigkeit zu erfüllen.

Zum Schluss wird beispielhaft der Ansatz einer Failure Mode Effect and Criticality Analysis durchgeführt, sowie die wichtigsten Aufgaben einer Zonal Safety Analysis angesprochen, die zu einem wesentlich späteren Zeitpunkt der Konstruktion gebraucht wird, um die fehlerfreie Integration des fertigen Aufzuges in das Gesamtsystem Flugzeug zu gewährleisten.

Zuverlässigkeit und Sicherheit eines Lasten- und Personenaufzuges für Großraumflugzeuge

Theoretische Arbeit nach § 11 (3) Ziffer 6 der Prüfungsordnung.

Hintergrund

Konzeptstudien beschäftigen sich mit einem integrierten Lasten- und Personenaufzug für Großraumflugzeuge wie den Airbus A380. Dabei soll der Aufzug einen Transport vom Vorfeld über den Frachtraum bis zum Haupt- und Oberdeck ermöglichen. Verschiedene Varianten derartiger Aufzüge wurden in einer Diplomarbeit an der HAW Hamburg untersucht. Die in dieser Diplomarbeit favorisierte Variante soll als Basis für die hier durchzuführenden Zuverlässigkeits- und Sicherheitsuntersuchungen dienen.

Aufgabe

- Beschreibung des dieser Arbeit zugrunde liegenden Lasten- und Personenaufzuges.
- Beschreibung ausgewählter Grundlagen der Zuverlässigkeitsrechnung.
- Beschreibung ausgewählter Grundlagen der Nachweisführung im Bereich Zuverlässigkeit und Sicherheit bei der Zulassung ziviler Flugzeuge.
- Erstellen einer *Preliminary Hazard Analysis* detailliert durch:
 - eine *Failure Mode Effect and Criticality Analysis* (FMEAC),
 - eine Zuverlässigkeitsrechnung basierend auf Zuverlässigkeitsblockschaltbildern (*Reliability Block Diagram*, RBD) unter Nutzung von Fehlerraten aus der Literatur,
 - erste Überlegungen zu einer *Zonal Safety Analysis* bezogen auf den Einbauort des Aufzuges.

Die Ergebnisse sollen in einem Bericht dokumentiert werden. Bei der Erstellung des Berichtes sind die entsprechenden DIN-Normen zu beachten.

Inhaltsverzeichnis

0. Aufgabenstellung.....	1
1. Einführung	3
2. Verfahren und Fehlerarten	4
2.1 Verfahren	4
2.2 Fehlerbewertung.....	6
2.3 Schlussfolgerung.....	7
3 Berechnung einfacher Systeme	8
3.1 Grundbegriffe	8
3.2 Darstellungsmethoden.....	9
3.3 Diskretisierungsvoraussetzungen.....	9
3.4 Wahrscheinlichkeiten in der Serienschaltung.....	10
3.5 Zuverlässigkeit der Serienschaltung.....	10
3.6 Wahrscheinlichkeiten in der Parallelschaltung	11
3.7 Zuverlässigkeit der Parallelschaltung.....	11
4 Zuverlässigkeit am Beispiel eines Lasten- und Personenaufzuges für Großraumflugzeuge.....	13
4.1 Anforderungen.....	13
4.2 Varianten.....	14
4.3 Beispielrechnung	<i>Fehler! Textmarke nicht definiert.</i>
4.4 Systembeschreibung und -optimierung.....	<i>Fehler! Textmarke nicht definiert.</i>
5 Ablauf einer FMECA	<i>Fehler! Textmarke nicht definiert.</i>
5.1 Systemdefinition.....	<i>Fehler! Textmarke nicht definiert.</i>
5.2 FMEA-Blätter.....	<i>Fehler! Textmarke nicht definiert.</i>
6. Zonal Safety Analysis.....	<i>Fehler! Textmarke nicht definiert.</i>
7. Zusammenfassung	<i>Fehler! Textmarke nicht definiert.</i>
Literaturverzeichnis	<i>Fehler! Textmarke nicht definiert.</i>
Anhang: FMEA -Datenblätter	A1

1 Einleitung

Die Komplexität und Funktionsvielfalt technischer Systeme ist in den letzten Jahren stark gestiegen. Gleichzeitig stieg auch die Anforderung von Kunden und Betreibern an die Betriebssicherheit und die Zuverlässigkeit eines Systems. Oft steht und fällt der wirtschaftliche Betrieb eines technischen Systems mit der Vorhersagbarkeit seines Ausfallverhaltens. Erst mit vorhersagbarem Ausfallverhalten ist, z.B. im Luftverkehr, eine Zulassung möglich. Auch die effektive Planung der Wartungs- und Instandsetzungsintervalle ist ohne Berechnungen des Zuverlässigkeitsverhaltens nicht möglich.

Diese Arbeit soll dem Leser einen Überblick über die im Flugzeugbau für die Einordnung und Berechnung einfacher Systeme gebräuchlichen Techniken zur Zuverlässigkeitsrechnung geben. Die Schritte auf dem Weg dahin laufen über die Nennung und Definition von Grundbegriffen und die Einordnung und Diskretisierung des Systems zu einer funktionellen Verknüpfung von Komponenten, die es erst ermöglicht, einen Überblick über die Funktion der einzelnen Komponenten sowie ihr Zusammenspiel im System zu gewinnen.

Als Beispielsystem dient hier die Konzeptstudie eines Lastenaufzuges für Großraumflugzeuge, wie er für den Einsatz im Airbus A380 vorgesehen ist. Es handelt sich dabei um einen auf das Flugvorfeld herunter fahrbaren Lift für den Transport von bordeigenen Cateringwagen, sog. Trolleys. Um auch bei steigenden Passagierzahlen die Turnaround-Zeiten, d.h. die Zeit zwischen zwei Flügen, nicht steigen zu lassen, ist es sinnvoll, das Bestücken der Trolleys vor dem Start bzw. Landung durchzuführen und für den Ladevorgang einen separaten Kanal zu schaffen, um Fracht- und Eingangstüren für andere Arbeiten freizuhalten.

Aus dieser Aufgabenbeschreibung ist bereits der Stellenwert des Liftes für die Zuverlässigkeit im Gesamtkonzept des Flugzeuges sichtbar. Seine Funktion betrifft in erster Linie die Zuverlässigkeit des Flugzeuges in Bezug auf Pünktlichkeit und Komfort für Passagiere. Der Einfluss auf sicherheitsrelevante Systeme, d. h. Systeme, welche die Unversehrtheit der Passagiere und der Besatzung gewährleisten sollen, geht wahrscheinlich nicht über ein grundsätzlich vorhandenes Mindestmaß hinaus. Allerdings ist eine Sicherheitsanalyse notwendig, um das Wort „wahrscheinlich“ aus dem vorhergehenden Satz streichen zu können.

2 Verfahren und Fehlerarten

Hier geht es prinzipiell um die Vorstellung der gängigen Analyseverfahren, sowie um die Einordnung von Fehlern. Die Verbindung von auftretenden Fehlerarten und einigen Systemcharakteristiken gibt die Randbedingungen für die Analysetoolauswahl vor, so dass es möglich ist, nach einer ersten Übersicht über das System den weiteren Fortschritt aus den Verfahren selbst zu ziehen.

2.1 Verfahren

Zu Beginn einer jeden Sicherheitsanalyse steht nach [Davidson 1988] die Einstufung des betrachteten Systems, um eine für die Aufgabe geeignete Auswahl an Analysetools zu finden. Zur Auswahl stehen:

- Failure Mode and Effect Analysis

Eine Methode zur systematischen Erfassung und Beurteilung von Fehlern auf jedes Bauteil bezogen, die es ermöglicht, Verbesserungsschwerpunkte und -notwendigkeiten schnell zu erfassen.

- Fehlerbaumanalyse oder Blockschaltbilddiagramm

Dient der Darstellung und Verdeutlichung von Funktionsabläufen in einem System. Geeignet zur Analyse der Fehlerfortpflanzung bei Ausfall einzelner Systemfunktionen.

- Zonal Safety Analysis

Analysiert die Auswirkungen eines Fehlers auf die umgebenden Systeme. Sehr wichtig zur Fehlerbeurteilung, da ein Fehler, der im Hinblick auf sein „Heimatsystem“ nur geringfügige Konsequenzen hat, auf andere Systeme einen schwerwiegenden Einfluss haben kann.

Z. B. sind in den dreißiger Jahren Flugzeugabstürze vorgekommen, weil ein heruntergefallenes Mikrofon die Steuersäule blockiert hat.

Allerdings ist eine ZSA sehr aufwendig durchzuführen, weil es meistens erforderlich ist, eine Mock-up oder ein sehr detailliertes 3D-Computermodell zur Verfügung zu haben, da eine räumliche Beeinflussung aus Zeichnungen fast unmöglich abzuleiten ist.

- Failure Mode and Effect Summary

Eine Zusammenfassung mehrerer FMEA zu einer Gesamtheit. [Davidson 1988] benutzt die FMEA nur auf Komponentenebene und bezeichnet die übergeordnete Analyse des Gesamtsystems (Flugzeug oder Bauteil) als FMES.

- Failure Mode and Effect Criticality Analysis

[Airbus 1990] erweitert die FMEA noch um einen weiteren Schritt, die Analyse der Fehlergefährlichkeit (Criticality Analysis, CA). Hier wird die Schwere des Fehlers ausdrücklich quantitativ bestimmt. Bei der Bewertung wird für jede Fehlerart eines Teiles eine Kennzahl nach der Formel

$$C_m = b * a * I_p * t$$

bestimmt.

Als Parameter gehen in die Rechnung ein:

- C_m Die Fehlerkennzahl
- α Wahrscheinlichkeit des Missionsabbruchs
- β Auftretensrate dieser Fehlerart
- λ_p Ausfallrate des Teils
- t Dauer der betrachteten Missionsphase

Da einige der Tools gerade in der quantitativen Analyse sehr aufwendig sind, wird eine Entscheidung getroffen, ob eine qualitative, und damit weniger aufwendige, Analyse ausreicht. Als Einstufungskriterien dabei sind nach [AC 251309]:

- erwartete Schadenskategorie
Alle Systeme, die möglicherweise Folgeschäden der Kategorie Major oder schlimmer aufweisen, müssen einer Sicherheitsanalyse unterzogen werden.
- Fehlerkombinationen
Auch wenn ein Fehler für sich genommen nur geringfügige Konsequenzen hat, kann es doch sein, dass er Bestandteil einer Verkettung von geringfügigen Fehlern ist, die insgesamt genommen schwerwiegende Auswirkungen hat. Besteht der Verdacht, dass dies der Fall ist, muss eine Sicherheitsanalyse gemacht werden.
- Systemkomplexität
Nicht so sehr entscheidend für die Frage ob eine Sicherheitsanalyse gemacht werden muss, sondern eher, welches Analysetool gewählt wird. Beispiele für gebräuchliche Tools sind z.B. FMEA, zonal gegliederte Analyse, Blockschaltbilder, Fehlerbaumanalyse. Als eine Richtlinie gilt auch, dass ein System als komplex anzusehen ist, wenn es Mikroprozessoren beinhaltet.
- Eher als Hilfe in der Vorgehensweise ist die Einstufung der Systemähnlichkeit und der Konventionalität des Systems, wobei die beiden Begriffe auf eine Vergleichbarkeit des Systems mit bereits vorhandenen und sich im Einsatz befindlichen abzielen.

Die oben genannten Einstufungskriterien sind maßgebend für die Auswahl der Analyseverfahren. Für komplexe Systeme sind quantitative Analysetools wie die FMECA notwendig, der im allgemeinen eine Diskretisierung des Systems durch Blockschaltbilder vorangeht. Für einfache Systeme, deren Fehlerschwere in der Kategorie Minor bleibt, muss überhaupt keine Sicherheitsanalyse gemacht werden, an allen anderen Systemen werden qualitative Untersuchungen mit Hilfe einer FMEA und Fehlerbaumanalyse durchgeführt.

2.2 Fehlerbewertung

Fehlerkategorie

- Minor
Geringfügige Fehler haben keinen Einfluss auf die Sicherheit des Flugzeuges und haben auch keinen nennenswerten Anstieg der Arbeitsbelastung der Crew zur Folge. Als Beispiel hierfür ist eine ausgefallene Leselampe im Passagierraum zu nennen.
- Major
Größere Fehler zeichnen sich durch die Reduktion der Sicherheitsmargen im Flugbetrieb oder die vermehrte Arbeitsbelastung der Crew aus, die in dem Fall deutlich weniger Kapazität für die Bewältigung ungünstiger Arbeitsumstände hat. Auch leichte Verletzungen oder deutliche Unbequemlichkeiten sind in dieser Fehlerkategorie möglich.
- Hazardous
Schwerwiegende Fehler bedeuten eine steigende Arbeitsbelastung der Crew bis zu einem Maß, dass ihnen die Bewältigung schwieriger Arbeitsumstände nicht mehr möglich ist. Als zweite Möglichkeit kommt in Betracht, dass die Sicherheitsmargen des Flugzeuges im Bereich des Fehlers nahezu oder vollständig ausgeschöpft werden. Des Weiteren sind ernsthafte Verletzungen bei wenigen Insassen möglich.
- Catastrophic
Katastrophale Fehler verhindern eine kontrollierte Fortsetzung des Fluges oder eine Landung. Es sind fast mit Sicherheit Tote zu beklagen.

Auftretenswahrscheinlichkeit

Ein weiteres Maß für die Fehlerbewertung ist ihre erlaubte Auftretenshäufigkeit [AC1251309].

- Wahrscheinliche Fehler haben eine Auftretenshäufigkeit von mehr als $1 \cdot 10^{-5}$
- Unwahrscheinliche Fehler treten mit einer Wahrscheinlichkeit zwischen $1 \cdot 10^{-5}$ und $1 \cdot 10^{-7}$ auf.
- Sehr unwahrscheinliche Fehler treten mit einer Wahrscheinlichkeit zwischen $1 \cdot 10^{-7}$ und $1 \cdot 10^{-9}$ auf.
- Extrem unwahrscheinliche Fehler treten mit einer Wahrscheinlichkeit von weniger als $1 \cdot 10^{-9}$ auf.

Als Verknüpfung zwischen Auftretenswahrscheinlichkeit und Fehlerauswirkung gilt relativ einfach, je höher die Auftretenswahrscheinlichkeit, desto geringer dürfen die Fehlerauswirkungen sein. Katastrophale Fehler dürfen nur mit einer Wahrscheinlichkeit von $<1 \cdot 10^{-9}$ auftreten.

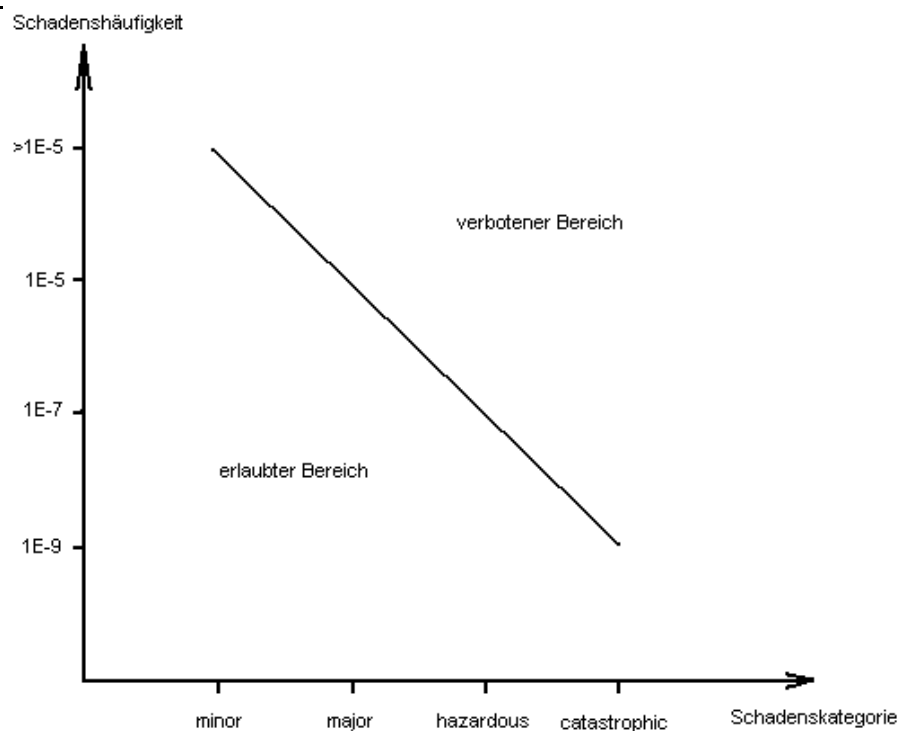


Bild 2.1: Zusammenhang zwischen Schadensart und -häufigkeit [AC 251309]

2.3 Schlussfolgerung

Eine Hilfestellung für den Umgang mit den oben genannten Kriterien bietet [Airbus 1990]. Danach gilt es zu entscheiden, ob eine qualitative Sicherheitsanalyse ausreicht, oder ob quantitative Daten erforderlich sind.

- qualitative Analyse
 - Für ein System mit geringer Komplexität oder hoher Komplexität aber Fehlerkonsequenzen, die schlimmstenfalls in die Kategorie „Major“ fallen, reicht eine qualitative Sicherheitsanalyse aus. Diese umfasst
 - eine Evaluation des Designs
 - eine Evaluation der Installation ins Flugzeug
 - Fehlerbaumanalyse oder Blockdiagramm
 - Failure Mode and Effect Analysis
- quantitative Sicherheitsanalyse
 - Für alle Systeme, die komplex oder nicht konventionell sind, oder die Fehler mit schwerwiegenden oder katastrophalen Konsequenzen zur Folge haben können, ist eine detaillierte Analyse mit Hilfe der o.g. Tools zu machen, die hier allerdings mit Zahlenwerten für die Ausfallwahrscheinlichkeit zu versehen und auszurechnen sind.

3 Berechnung einfacher Systeme

Das folgende Kapitel behandelt die Berechnung zuverlässigkeitsrelevanter Kennwerte, deren Nachweis für Forderungen aus dem Lastenheft oder den Zulassungsvorschriften notwendig sind. Der Nachweis erfolgt über die rechnerische Kombination der Ausfallwahrscheinlichkeiten der einzelnen Systemkomponenten zu einem Gesamtwert. Solche Kennwerte sind z.B.

- Ausfallwahrscheinlichkeit
- Betriebszeit zwischen zwei Ausfällen (Mean Time To Failure)

Letztere wird auch zur Aufstellung eines Wartungsplanes benötigt, da sich auf diese Weise Wartungsintervalle für die einzelnen Komponenten eines Systems bestimmen und koordinieren lassen.

Zur quantitativen Bestimmung der Systemzuverlässigkeit einfacher Systeme dienen die Grundlagen der Wahrscheinlichkeitsrechnung. Komplexe Systeme mit einem Aufbau, der sich nicht durch einfachen seriellen oder parallelen Aufbau darstellen lässt, erfordern komplexere Rechnungen. Beispiele für einen komplexen Systemaufbau sind:

- **partielle Redundanz**
n Komponenten sind parallel geschaltet, zur uneingeschränkten Systemfunktion sind r Komponenten erforderlich ($r < n$).
- **Stand-by Redundanz**
n Komponenten sind vorhanden. Aber nur die r Komponenten, die zur Funktion des System nötig sind, sind in Betrieb ($r < n$). Fällt eine der Komponenten aus, wird eine Ersatzkomponente zugeschaltet.

Eine weitere Einschränkung betrifft die Einsatzart der betrachteten Systeme. Das bisher Gesagte und die im folgenden dargestellten Rechnungen beziehen sich auf Systeme, die auf Anforderung funktionieren und deren Ausfall offenkundig ist. Eine weitere Klasse betrifft Systeme, bei denen ein Teil der Betriebszeit aus einer Bereitschaftsfunktion besteht. Ein Beispiel sind Notsysteme.

Im weiteren werden die Grundberechnungen für aktive, einfache parallele und serielle Systeme vorgestellt

3.1 Grundbegriffe

Wahrscheinlichkeit

Wahrscheinlichkeit ist eine dimensionslose Zahl, die in einem statistischen Experiment die Eintretenshäufigkeit eines Ereignisses angibt. Wenn z.B. bei 120 Würfelwürfen der Würfel 20 mal sechs Augen anzeigt, ist die Wahrscheinlichkeit, bei einem Wurf mit diesem Würfel eine Sechs zu würfeln, gleich 20%. Dabei bedeutet eine Wahrscheinlichkeit von 100% bzw. 1 das sichere Eintreten eines Ereignisses, wohingegen 0(%) das sichere nicht Eintreten des Ereignisses bedeutet.

Zuverlässigkeit

Um die Zuverlässigkeit eines System zu ermitteln, muss nun die Zeit eingebracht werden. Danach ergibt sich die Zuverlässigkeit eines Systems als die Wahrscheinlichkeit, dass ein System über eine Zeitperiode funktionsfähig bleibt.

Verfügbarkeit

Die Verfügbarkeit gibt den prozentualen Anteil an einem Zeitraum an, den ein System funktionsfähig war. Dabei ist es unwichtig, ob und wie oft das System repariert werden musste.

3.2 Darstellungsmethoden

Die Berechnung eines Kennwertes für ein Gesamtsystem setzt die Kenntnis des Systemaufbaus sowie der Ausfallwahrscheinlichkeiten der einzelne Komponenten voraus.

Die Unterteilung des Systems in Komponenten und deren Verknüpfung lässt sich mit folgenden Methoden darstellen:

Blockschaltbilder

Blockschaltbilder dienen der Darstellung der funktionalen Verknüpfung der Komponenten eines Systems. Die Verbindungen zwischen den einzelnen Komponenten symbolisieren dabei den Material- oder Kraftfluss durch das System. Sie müssen dabei nichts mit den physischen Verbindungen der Elemente zu tun haben, sondern zeigen einfach nur die Funktionsweise des Systems.

logisches Zuverlässigkeitsdiagramm

Hier sind nicht die Komponenten des Systems direkt dargestellt, sondern die logischen Verknüpfung ihrer Zustände. Grundsätzlich werden die Systemfunktionen durch UND bzw. ODER -Verknüpfungen miteinander verschaltet, um Serien- oder Parallelschaltungen zu symbolisieren. Hierbei handelt es sich um eine sehr einfache Form der Fehlerbaumanalyse.

3.3 Diskretisierungsvoraussetzungen

Um Berechnungen an Systemen mit mehreren verknüpften Komponenten vornehmen zu können, müssen einige Voraussetzungen erfüllt sein.

- Die Ausfälle der einzelnen Komponenten müssen unabhängig voneinander sein.
- Jede Funktion des Systems muss auf eine Komponente übertragbar sein
- Jede Komponente bzw. Funktion muss mit einer separaten Ausfallwahrscheinlichkeit versehen werden können.

3.4 Wahrscheinlichkeiten in der Serienschaltung

Zwei Komponenten, die für die Funktionsfähigkeit eines Systems erforderlich sind, sind in Serie geschaltet. Damit ist die Wahrscheinlichkeit, dass das System funktioniert, P_{ges} , gleich dem Produkt der beiden Einzelwahrscheinlichkeiten P_1 und P_2 für die Funktionsfähigkeit der Einzelkomponenten:

$$P_{ges} = P_1 * P_2$$

Daraus ergibt sich im Umkehrschluss die Wahrscheinlichkeit, dass ein System nicht funktioniert mit:

$$F_{ges} = 1 - P_{ges}$$

bzw.

$$F_{ges} = F_1 * F_2 - F_1 * F_2$$

Angewandt auf ein System mit mehreren in Serie geschalteten Komponenten ergibt das folgende Wahrscheinlichkeiten:

$$P_{ges} = \prod_{j=1}^n P_j$$

bzw.

$$P_{ges} = 1 - \prod_{j=1}^n (1 - P_j)$$

Für die Verfügbarkeit eines solchen Systems gilt folgende Beziehung:

$$A_{ges} = \prod_{j=1}^n A_j$$

sowie für die Nichtverfügbarkeit

$$\begin{aligned} U_{ges} &= 1 - A_{ges} \\ &= 1 - \prod_{j=1}^n (1 - A_j) \end{aligned}$$

Wenn die Nichtverfügbarkeiten sehr klein sind, $U_n \ll 1$, dann kann man die Gleichung vereinfachen zu:

$$U_{ges} = \sum_{j=1}^n U_j$$

3.5 Zuverlässigkeit der Serienschaltung

Bei Komponenten mit konstanten Ausfallraten λ_i gilt für die Wahrscheinlichkeit der Funktionsfähigkeit der Komponente zum Zeitpunkt t :

$$R_i(t) = e^{-\lambda_i * t}$$

eingesetzt in Gleichung (2.4) wird daraus im Endeffekt

$$R_i(t) = e^{-(\sum \lambda_i) t}$$

Hieraus wird ersichtlich, dass die Ausfallrate des Gesamtsystems gleich der Summe der Ausfallraten der Komponenten ist:

$$I_s = \sum_{j=1}^n I_j$$

Die Wahrscheinlichkeit einer Fehlfunktion ab dem Zeitpunkt t ist analog zu Gleichung (2.2):

$$F_s(t) = 1 - R_s(t)$$

Die durchschnittliche Systemlebensdauer (MTTF) beträgt

$$MTTF = 1 / \sum_{j=1}^n I_j$$

3.6 Wahrscheinlichkeiten in der Parallelschaltung

Ein System umfasst n Komponenten die im Betrieb gleichzeitig benutzt werden. Auch wenn bis auf eine der Komponenten Alle ausfallen, funktioniert das System ohne Einschränkungen weiter, d.h., die Komponenten sind parallel geschaltet. Man spricht auch von vollständiger Redundanz. Für die Berechnung redundanter Systeme ergibt sich eine Umkehrung der Gleichungen der Reihenschaltung. Die Wahrscheinlichkeit, dass das System ausfällt, ist folglich

$$F_{ges} = F_1 * F_2$$

Daraus folgt die Wahrscheinlichkeit der Funktionsfähigkeit mit

$$\begin{aligned} P_{ges} &= 1 - F_{ges} \\ &= P_1 + P_2 - P_1 P_2 \end{aligned}$$

Für n -fach redundante Systeme gilt

$$P_{ges} = 1 - \prod_{j=1}^n (1 - P_j) \quad \text{mit} \quad F_{ges} = \prod_{j=1}^n F_j$$

Die Verfügbarkeit eines Systems ergibt sich aus dem Zusammenhang

$$U_{ges} = \prod_{j=1}^n U_j$$

daraus folgt

$$A_{ges} = 1 - \prod_{j=1}^n (1 - A_j) \quad \text{mit} \quad U_j = 1 - A_j$$

3.7 Zuverlässigkeit der Parallelschaltung

Zuverlässigkeit bei parallelen Systemen bedeutet die Wahrscheinlichkeit, dass zum Zeitpunkt t noch mindestens eine der redundanten Komponenten intakt ist. Wenn man nun den einzelnen Komponenten j eine Ausfallrate λ_j zuordnet, ist die Wahrscheinlichkeit eines Systemausfalls vor dem Zeitpunkt t

$$F_{ges}(t) = \prod_{j=1}^n F_j(t)$$

$$= \prod_{j=1}^n (1 - e^{-\lambda_j t})$$

Wenn man die Wahrscheinlichkeit eines Systemausfall in einer bestimmten Missionszeit errechnen will, die um Größenordnungen kleiner ist als die durchschnittliche Lebenszeit der Komponenten, d.h. $t \ll 1/\lambda$, dann gilt vereinfachend:

$$e^{-\lambda t} = 1 - \lambda t$$

und folglich

$$F_{ges}(t) = t^n \prod_{j=1}^n \lambda_j$$

Die Systemzuverlässigkeit lautet allgemein

$$R_{ges}(t) = 1 - F_{ges}(t)$$

Die Durchschnittszeit bis zum Auftreten de Fehlers (MTTF, Mean Time To Failure) eines Systems mit zwei Komponenten ist danach

$$MTTF = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} + \frac{1}{\lambda_1 + \lambda_2}$$

4 Zuverlässigkeit am Beispiel eines Lasten- und Personenaufzuges für Großraumflugzeuge

In der nachfolgenden Betrachtung sollen die oben dargelegten Grundlagen auf eine in einer Diplomarbeit [Airbus 2001] vorgestellten Entwurfsstudie angewendet werden.

Die Entwurfsstudie beinhaltet eine Ausscheidung unterschiedlicher Antriebsvarianten. Die Bewertung der dort betrachteten Varianten wird hier um den Aspekt der Zuverlässigkeit erweitert. Dazu ist es zuerst notwendig, die gestellten Anforderungen in zuverlässigkeitsrelevante Kennwerte zu übersetzen (Kapitel 4.1).

In Kapitel 4.2 werden die funktionellen Elemente des Antriebes jeder Alternative in Blockschaltbildern dargestellt, um Klarheit über die Verknüpfungen der einzelnen Komponenten zu erhalten.

Jeder Komponente wird in Kapitel 4.3 eine generische Ausfallrate aus der Literatur [AC251309] zugeordnet. Aufgrund der oben dargestellten Grundlagenberechnungen wird dann überprüft, ob die Antriebsvariante die unten aufgelisteten Anforderungen erfüllt.

4.1 Anforderungen

- Die Ausfallwahrscheinlichkeit des Aufzugsystems soll kleiner als $10^{-5}/h$ sein. Daraus ergibt sich die Festlegung des Liftes auf ein einfaches System, dessen Ausfall keine Auswirkungen der Kategorie Hazardous oder schlimmer hat.
- Als Lebenszeit des Aufzuges werden 100.000 Flugstunden angenommen. Das entspricht ungefähr 1.600.000 kompletten Umläufen. Die Laufzeit ergibt sich aus dem Kehrwert der Ausfallwahrscheinlichkeit.
- Bevor ein nicht bekannter Fehler behoben wird, dürfen maximal 750 Flugstunden vergehen. Daraus lässt sich die maximale Ausfallwahrscheinlichkeit für den letzten Pfad (s. folgende Seite) durch das System ableiten:

$$F_{ges} = \frac{1}{750h} = 1,334 * 10^{-3} \frac{1}{h}$$

- Bevor ein bekannter Fehler am Aufzug behoben wird, sollen maximal 240 Flugstunden vergehen dürfen.
- Alle Liftkomponenten sollen so ausgelegt werden, dass keine präventiven Checks außerhalb der Standard-Checks vorgenommen werden müssen. Das Intervall ist auf 490 Stunden festgelegt, da jeder Fehler 490 h nach seinem Auftreten entdeckt werden muss.

Als nächster Schritt erfolgt die Darstellung der einzelnen Varianten als Blockschaltbild, um daraus die Verschaltung der einzelnen Komponenten zu ermitteln.

4.2 Varianten

Die einzelnen Komponenten werden als rechteckige Blöcke dargestellt, die entsprechend ihrer funktionellen Abfolge im System mit Linien verbunden sind. Diese Verbindungen bezeichnen sog. Pfade durch die Systemarchitektur. Am Beginn jedes Pfades steht eine Anfangskomponente, z.B. die Steuereinheit bei der Variante A des hydraulischen Antriebes. Redundant auftretende Komponenten bedeuten eine Verzweigung des Pfades, während seriell geschaltete Komponenten einfach einen Pfad fortsetzen. Der Pfad endet an der Komponente, die sichtbar die Gesamtfunktion des (Unter)systems für den Benutzer darstellt. Fällt eine Komponente entlang eines Pfades aus, ist der Pfad bis zur nächsten Kreuzung mit einem intakten Pfad unterbrochen. Das System ist solange funktionsfähig, wie man einen Pfad, den letzten funktionierenden Systempfad, ununterbrochen von der Start- bis zur Endkomponente verfolgen kann.

Die Prinzipskizzen stammen aus [Airbus 2001]

1. Antrieb mit Gewindespindel

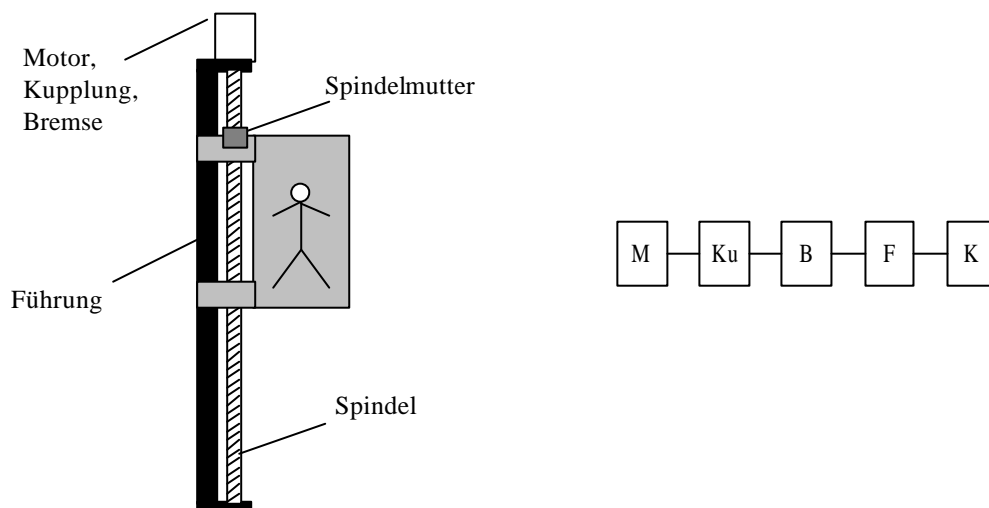


Bild 4.1 System mit einer Gewindespindel angetrieben.

M: Motor, F: Führung, K: Kabine, Ku: Kupplung, B: Bremse

Die Spindelmutter ist an der Aufzugskabine befestigt und wird von der Spindel bewegt. Die Spindel dient sowohl dem Antrieb als auch der Führung der Kabine. Das Drehmoment wird durch einen Motor zur Verfügung gestellt, der über eine Kupplung von der Spindel getrennt werden kann. Zur Arretierung der Kabine dient eine Bremse.

2. Antrieb mit Hydraulikzylindern

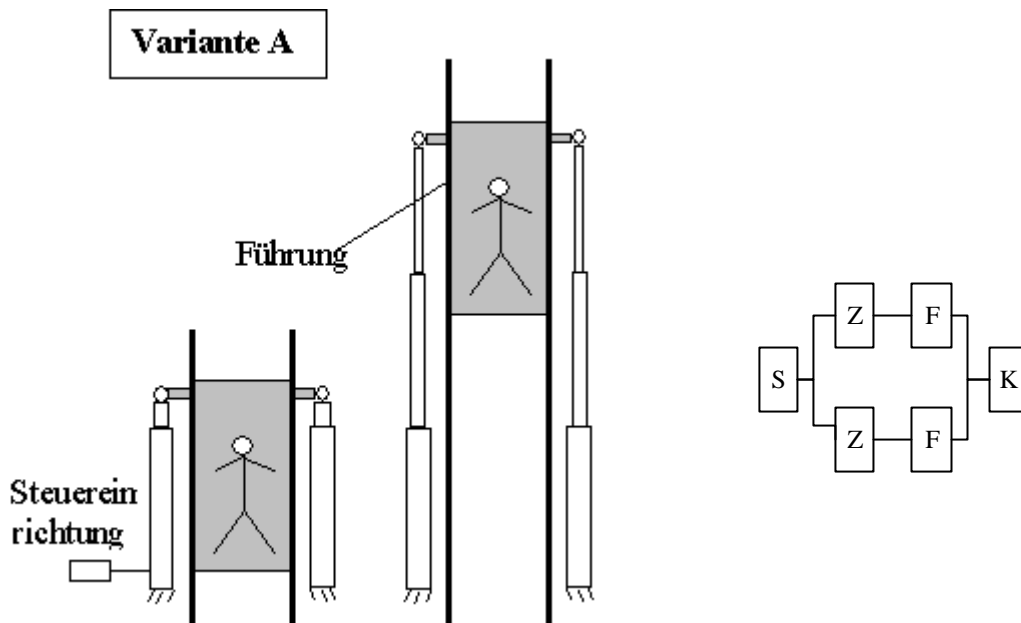


Bild 4.2 Antrieb mit redundanten Hydraulikzylindern
S: Steuerung, Z: Zylinder, F: Führung, K: Kabine

Zwei Hydraulikzylinder schieben die Aufzugskabine in einem Führungsrahmen auf- und abwärts. Bei entsprechender Lagerung der Kabine kann das System den Ausfall eines Zylinders kompensieren.

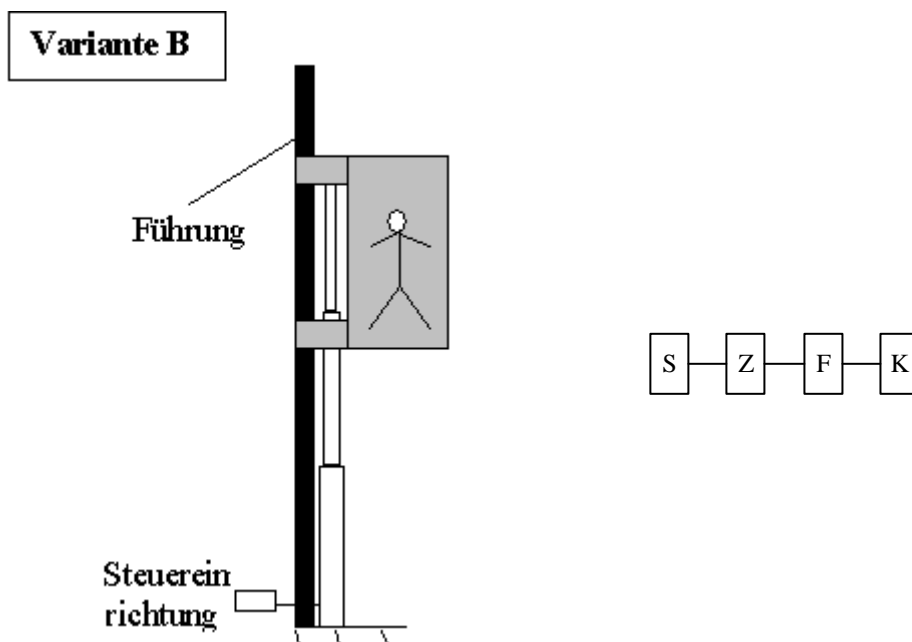


Bild 4.3 Antrieb mit einem Hydraulikzylinder
S: Steuerung, Z: Zylinder, F: Führung, K: Kabine

Der Unterschied zu Variante A ist der zentrale Antriebszylinder mit Führung, so dass dieses System ohne Redundanz ausgelegt ist.

3. Magnetischer Linearantrieb

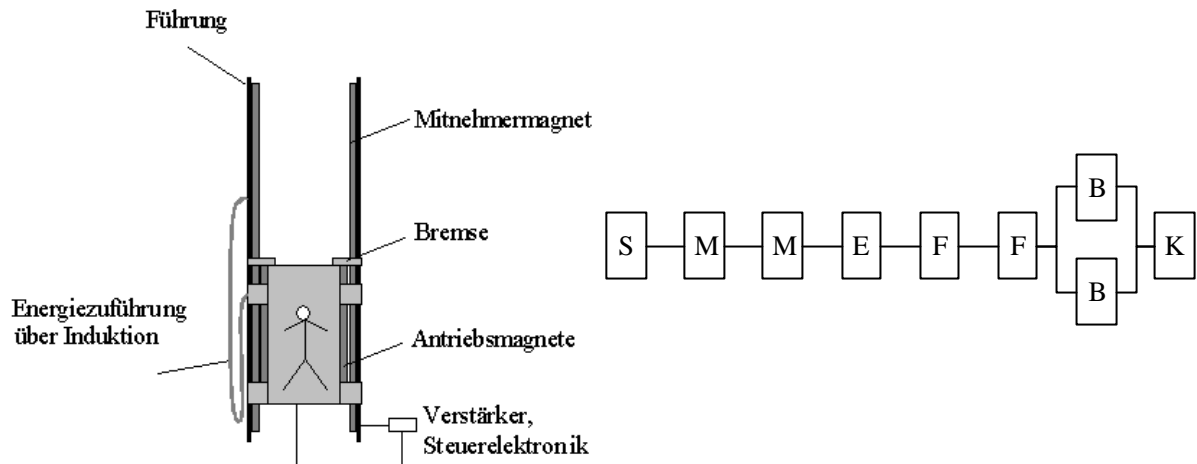


Bild 4.4 Antrieb mit magnetischer Levitation (MagLev)

S: Steuerung, M: Linearmotor, E: Energieversorgung, F: Führung, B: Bremse, mobil, K: Kabine

An einem Führungsrahmen sind die Führungsmagnete befestigt. Die Kabine wird durch die Magnetkräfte der an der Kabine befestigten Antriebsmagnete bewegt. Für die Frage der Redundanz kommen zwei Möglichkeiten in Frage: Nur wenn die Magneten so stark ausgeführt werden, dass einer die Kabine allein bewegen kann, könnte man das System mit einer Redundanz im Antrieb versehen. Da der Gewichtszuwachs durch die Magnete und die Stromversorgung bei Verdopplung der Leistung wesentlich höher ist als bei der Hydraulik, wird das System als nicht redundant angesehen.

4. Riemengetriebene Treibscheibe ohne Gegengewicht

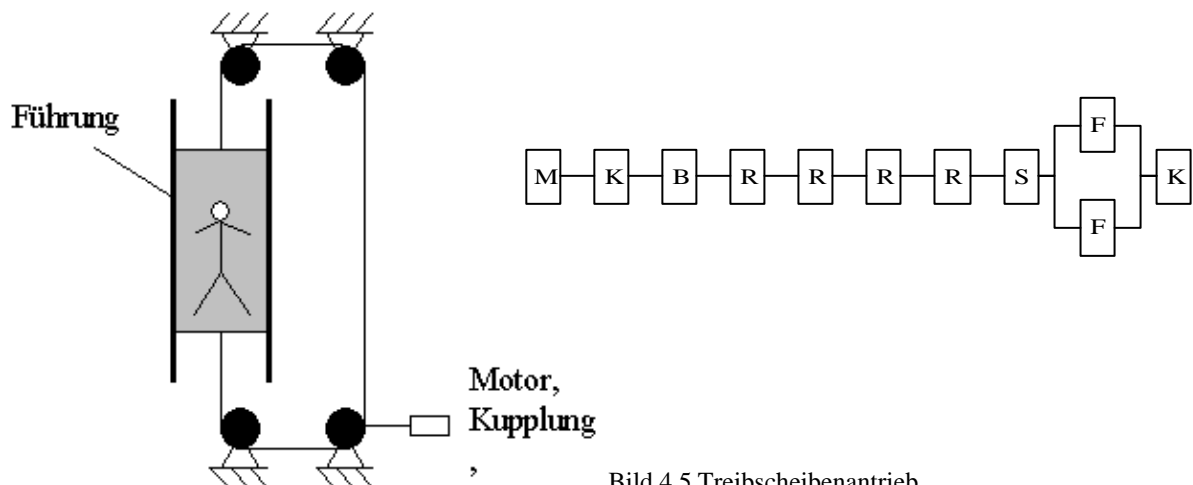


Bild 4.5 Treibscheibenantrieb

M: Motor, K: Kupplung, B: Bremse, R: Rolle, S: Seil, F: Führung, K: Kabine

Ein umlaufender Riemen, an dem die Aufzugskabine befestigt ist, bewegt sich über vier Rollen, von denen eine von einem Motor angetrieben wird. Die Rolle ist gebremst und kann durch eine Kupplung vom Motor getrennt werden. Die Kabine wird durch zwei Schienen seitlich geführt. Soweit der Aufbau nach [Airbus 2001]. Um diesen Aufbau zu ermöglichen ist es nötig, das Seil nach safe-life-Kriterien auszulegen, so dass seine Ausfallwahrscheinlichkeit $10^{-7} > F > 10^{-9}$ beträgt, da die Auswirkungen eines Seilrisses in die Kategorie Hazardous fallen.

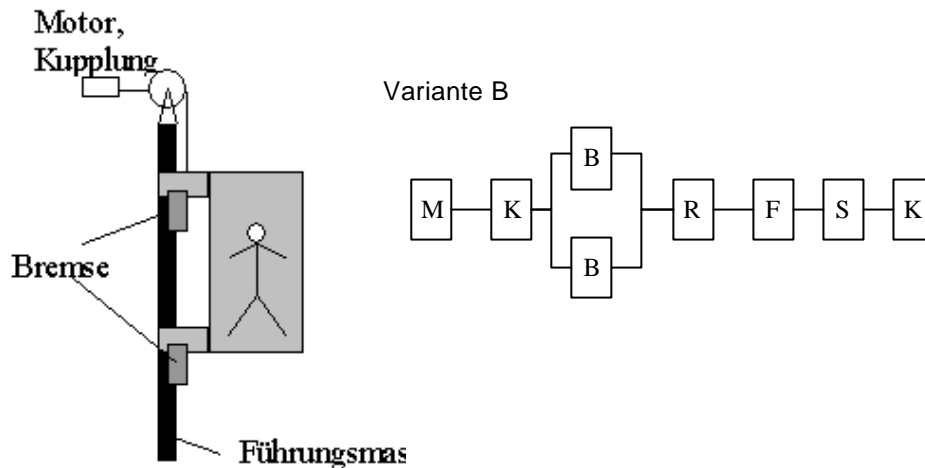


Bild 4.6 Treibscheibenantrieb mit redundanter Bremsenausführung

M: Motor, K: Kupplung, B: Bremse, R: Rolle, S: Seil, F: Führung, K: Kabine

Funktioniert nach demselben Prinzip wie Variante A, nur dass nur noch eine Rolle am Mast befestigt ist. Die Bremsen sind nun redundant ausgeführt und arretieren die Kabine direkt an der Führungsschiene.

5. Zahnstangenführung mit Zahnantrieb

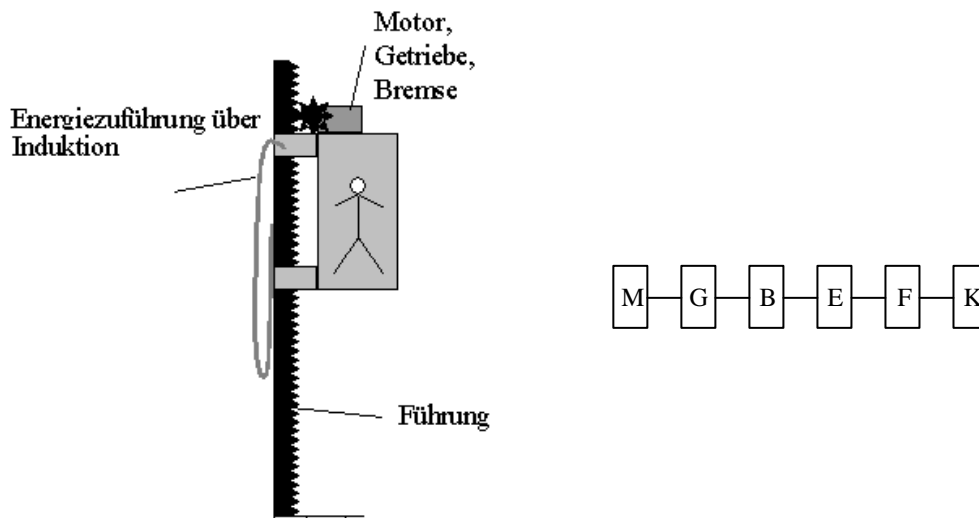


Bild 4.7 Zahnstangenführung

M: Motor, G: Getriebe, B: Bremse, E: Energieversorgung, F: Führung

Die Antriebseinheit mit Motor Getriebe und Bremse ist an der Kabine angebracht. Die Kabinenbewegung wird über ein Zahnrad und eine Zahnstange realisiert. Auch hier ist eine safe-life-Auslegung notwendig, da das Zahnrad die einzig arretierbare Verbindung zur Zahnstange darstellt.

6. Zahnriemenantrieb

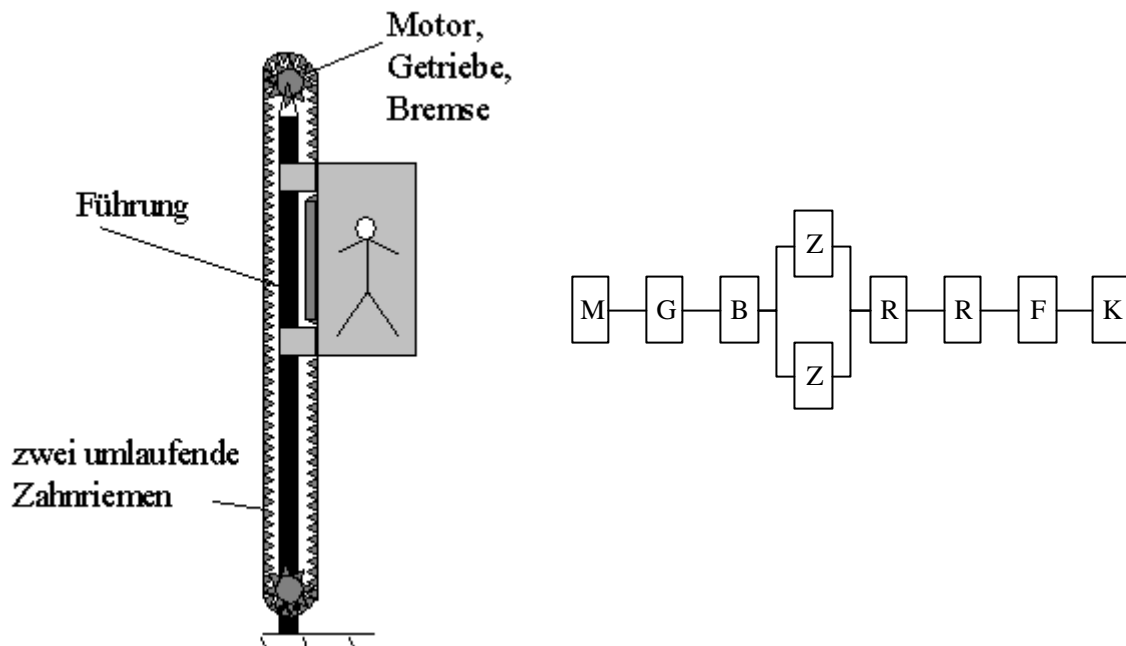


Bild 4.8 Zahnriemenantrieb

M: Motor, G: Getriebe, B: Bremse, Z: Zahnriemen, R: Rolle, F: Führung

Die Antriebseinheit bewegt eine Laufrolle, über die beide Riemen rollen, an denen die Kabine aufgehängt ist. Die ganze Konstruktion ist an einem Mast in den Rumpf eingebaut. Das Riemenpaar sichert die fail-safe-Auslegung der Kabinenbefestigung, während die Laufrolle durch die Bremse blockiert werden kann.

4.3 Beispielrechnung

In diesem Abschnitt sollen die Anforderungen an die Zuverlässigkeit für die einzelnen Ausführungsvarianten des Liftes überprüft werden.

Wie sich aus den Formeln ersehen lässt, ist für die Annahme eines zeitunabhängigen Ausfallverhaltens, d.h. einer exponentialverteilten Zuverlässigkeitsfunktion mit konstanter Ausfallrate, die Bestimmung dieser Ausfallrate von zentraler Bedeutung. Dazu ist man meistens auf umfangreiche Versuchsreihen angewiesen, in denen in Laufzeitversuchen das Ausfallverhalten solcher Teile untersucht wird. [RADC 1985] fasst die Ergebnisse einzelner

Studien zusammen und gibt eine Auflistung der Ausfallraten ausgewählter nichtelektronischer Bauteile wieder.

Für die Anwendung auf die Liftvarianten werden folgende Komponenten (mit Umweltbedingungen) benötigt:

- Motor, fest (M_f) $\lambda_m = 1,34 \cdot 10^{-6}$
- Motor, mobil (M_m) $\lambda_{mm} = 2,76 \cdot 10^{-5}$
- Kupplung, fest (K_f) $\lambda_k = 1,3 \cdot 10^{-6}$
- Bremse, fest (B_f) $\lambda_b = 1,6 \cdot 10^{-6}$
- Bremse, mobil (B_m) $\lambda_{bm} = 2,1 \cdot 10^{-4}$
- Getriebe, fest (G_f) $\lambda_g = 5 \cdot 10^{-6}$
- Getriebe, mobil (G_m) $\lambda_{gm} = 1,9 \cdot 10^{-5}$
- Getriebe, schaltbar (G_s) $\lambda_{gs} = 1,8 \cdot 10^{-5}$
- Führung (F) $\lambda_f = 1 \cdot 10^{-9}$
- Hydraulikzylinder (H) $\lambda_z = 3,59 \cdot 10^{-5}$
- Linearmotor (LM) $\lambda_{lm} = 1,11 \cdot 10^{-5}$
- Steuereinrichtung (ST) $\lambda_{st} = 2,7 \cdot 10^{-6}$
- Rollen (R) $\lambda_r = 3,0 \cdot 10^{-6}$
- Riemen (Ri) $\lambda_{ri} = 1,7 \cdot 10^{-5}$
- Antriebsseil (S) $\lambda_s = 1 \cdot 10^{-7}$
- Energieversorgung, induktiv (E) $\lambda_e = 9,5 \cdot 10^{-6}$
- Energieversorgung, Kabel (E) $\lambda_k = 5,5 \cdot 10^{-6}$

[RADC 1985] unterscheidet mehrere Umweltbedingungen für seine Bauteile, z.B. fest eingebaut oder beweglich, Einbau in Transport- oder Kampfflugzeuge, Verwendung am Boden oder auf Schiffen. Sofern die Daten verfügbar sind, wird hier mit der Kategorie AUT (Airborne, unmanned, Transport) gearbeitet. Ansonsten gilt die Kategorie GF (Ground fixed) für alle Teile, die an der Führung angebracht sind, oder GM (ground mobile) für alle Teile, die mit der Kabine bewegt werden. Einige Bauteile sind nicht aufgeführt und müssen durch andere ersetzt werden. Z.B. sind die Transportrollen nicht enthalten, aber da der Ausfall einer Rolle fast immer durch Lagerschaden verursacht wird, werden die Werte für ein Kugellager benutzt.

Der Linearmotor ist nicht in der Liste enthalten, es werden die Werte eines festen Elektromotors mit hoher Leistung verwendet. Anstelle der Steuereinheit kommen die Werte des elektronischen Reglers zum Einsatz.

Die Beispielrechnung wird anhand der Variante Hydraulikzylinder A durchgeführt.

Gesucht wird:

-
- Die MTTF des Gesamtsystems: T_s
 - Die MTTF des letzten Systempfades T_f
 - Die Ausfallwahrscheinlichkeit F

Zuerst ist die Ausfallwahrscheinlichkeit der einzelnen Komponenten zu ermitteln.

$$F(t = 1h) = 1 - e^{-t}$$

$$F_{\text{Zylinder}} = 3,59 \cdot 10^{-5} \text{ 1/h}$$

$$F_{\text{Führung}} = 1 \cdot 10^{-9} \text{ 1/h}$$

Damit beträgt die Ausfallwahrscheinlichkeit der beiden Zylinder zusammen:

$$F_{Z_g}(t = 1h) = t^2 \prod_{j=1}^2 I_Z$$

$$F_{Z_g} = 1,29 \cdot 10^{-9} \text{ 1/h}$$

Die Ausfallwahrscheinlichkeit der beiden Führungen beträgt

$$F_{F_g} = 1 \cdot 10^{-18} \text{ 1/h}$$

Die Ausfallwahrscheinlichkeit der Steuereinrichtung beträgt

$$F_S = 2,7 \cdot 10^{-6} \text{ 1/h}$$

Damit ist die Ausfallwahrscheinlichkeit des Gesamtsystems

$$F_{\text{ges}} = F_Z \cdot F_F \cdot F_S$$

$$F_{\text{ges}} = 1 - (1 - F_{Z_g})(1 - F_{F_g})(1 - F_S)$$

$$F_{\text{ges}} = 2,7 \cdot 10^{-6} \text{ 1/h}$$

Damit beträgt die MTTF des Gesamtsystems

$$MTTF_{\text{Sys}} = 1 / \sum_{j=1}^3 I_3$$

$$MTTF_{\text{Sys}} = 370370 \text{ h}$$



Die Ausfallwahrscheinlichkeit eines Pfades beträgt

$$F_P = 1 - (1 - F_S)(1 - F_Z)(1 - F_F)$$

$$F_P = 3,86 \cdot 10^{-5}$$

Die MTTF eines Systempfades, bestehend aus der Steuereinheit, einem Zylinder und einer Führung beträgt:

$$MTTF_{Pfad} = 1 / (\lambda_S + \lambda_Z + \lambda_F)$$

$$MTTF_{Pfad} = 25906h$$

Die Ergebnisse für alle Varianten sind hier in tabellarischer Form dargestellt. Orange Farbung bedeutet, die Variante muss modifiziert werden, um die Anforderungen zu erfüllen.

	Ausfallwahrscheinlichkeit [1/h]		MTTF [h]	
	System	Pfad	System	Pfad
Antrieb mit Gewindespindel	4,26E-6	4,26E-6	235849	235849
Antrieb mit Hydraulikzylinder Variante A	2,7E-6	3,86E-5	370370	25096
Antrieb mit Hydraulikzylinder Variante B	3,86E-5	3,86E-5	25096	25096
Maglev	3,44E-5	2,44E-4	29031	4092
Triebsscheibe mit Riemen Variante A	1,63E-5	1,63E-5	61196	61196
Triebsscheibe mit Riemen Variante B	5,74E-6	7,34E-6	184843	142653
Zahnriemen	1,40E-05	3,10E-05	71729	32320
Zahnstange	2,62E-4	2,62E-4	3815	3815

Da die in der Konzeptstudie getroffene Auswahl nicht von diesen Überlegungen beeinflusst und im weiteren noch erheblich modifiziert wurde, wird diese Rechnung auch im Kapitel 4.4 für die gewählte Variante gemacht.

4.4 Systembeschreibung und -optimierung

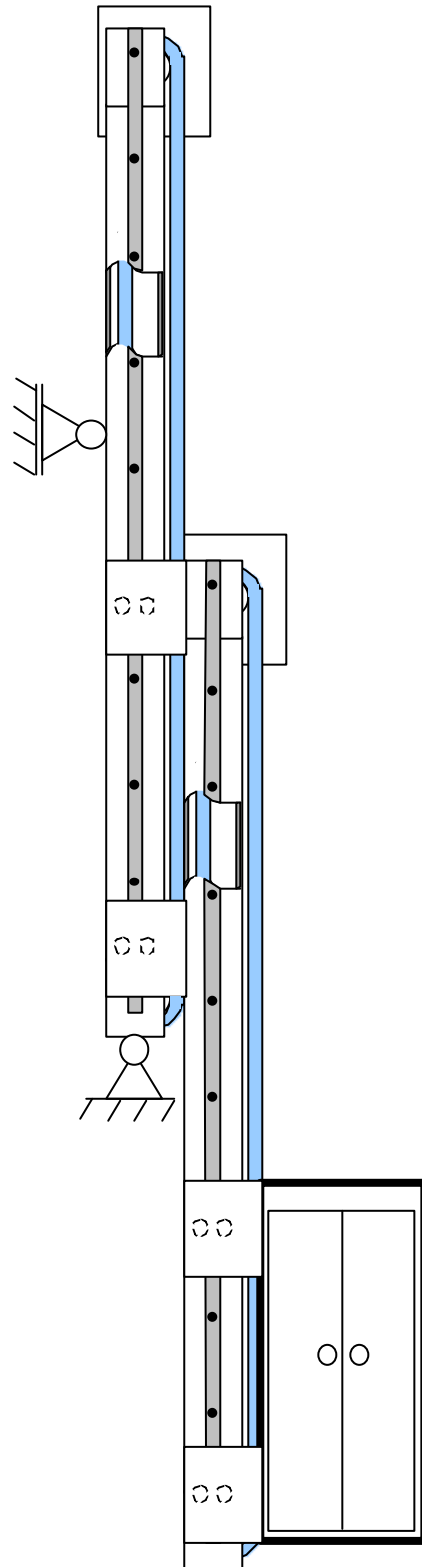


Bild 4.9: Prinzip der Liftvariante mit Zahnriemen [Airbus 2001]

Die in [Airbus 2001] gewählte Variante, Antrieb mit Zahnriemen (Variante 6), besteht aus einem Einzelmast in Teleskopausführung, an dem die Kabine (K) mit einem Zahnriemenantrieb bewegt wird. Der Ausfahrmechanismus für den Teleskopteil des Mastes wird ebenfalls über einen Zahnriemenantrieb realisiert. Der Teleskopteil bringt die Kabine durch einen Rumpfdurchbruch in der unteren Rumpfschale auf das Flugvorfeld herunter. Er ist an zwei Zahnriemen (R) aufgehängt, die am festen Teil des Mastes (F) über zwei Rollen (W) umlaufen und durch die fest installierte Antriebseinheit 1, bestehend aus einem Motor (M), einem Getriebe (G) und einer elektrisch angesteuerten Lamellenbremse (B), angetrieben werden. Die zweite Antriebseinheit ist an den Teleskopteil des Mastes angebracht und bewegt die Kabine. Daraus ergibt sich folgende Funktionsstruktur für den Betrieb am Boden:

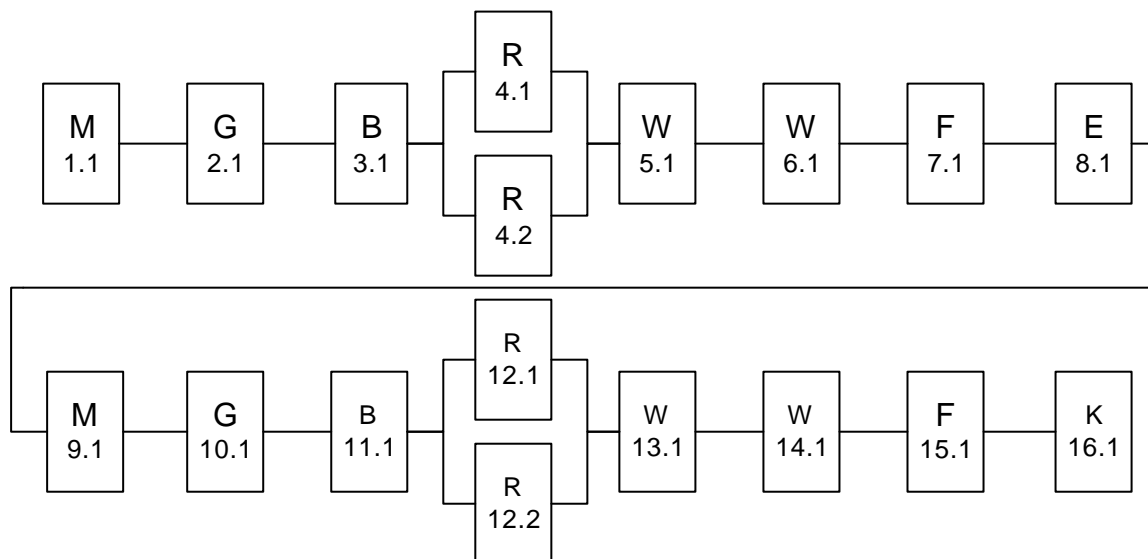


Bild 4.9: Funktionsstruktur für den Bodenbetrieb

Der Aufbau ist im Vergleich zur oben besprochenen Variante aus dem Antriebsentwurf um den Teleskopteil und ein Kabel zur Energieübertragung erweitert. Für die Komponenten am festen Mastteil sind die Ausfallraten für feste Komponentengewählt, während am Teleskopteil des Mastes mobile Komponenten zu Anwendung kommen.

Für diese Systemkonfiguration ergaben sich folgende Werte:

- Ausfallwahrscheinlichkeit des Gesamtsystems $F = 2,86 \cdot 10^{-4} \text{ 1/h}$

$$\text{MTTF} = 3497 \text{ h}$$

Mit diesen Werten verfehlt der Aufzug die Mindestanforderungen erheblich. Dies ist hauptsächlich auf fehlende Redundanz zurückzuführen, da alle für die Zuverlässigkeit

erforderlichen Komponenten einfach vorhanden sind. Die redundante Ausführung der Riemen ist fast wirkungslos, da ihre Ausfallwahrscheinlichkeit 3 Zehnerpotenzen geringer ist, als die der kritischen Komponenten, die sich in der mobilen Antriebseinheit befinden.

Erschwerend kommt hinzu, dass die von [Airbus 2001] vorgeschlagene Ausführung der Bremse, die in Ruhestellung die zu bremsende Komponente (entweder Mast oder Kabine) arretiert, zwar einen erheblichen Beitrag zur Betriebssicherheit des Liftes beisteuert, weil die Gefahr eines Absturzes der Kabine oder des Teleskopteils des Mastes vermindert wird, aber keine Auswirkungen auf die Zuverlässigkeit hat, weil eine ausgefallene Bremse alle nachfolgenden, beweglichen Komponenten blockiert.

Eine weit höhere Zuverlässigkeit bei annähernd gleicher Komponentenzahl verspricht der Lift mit folgender Funktionsstruktur

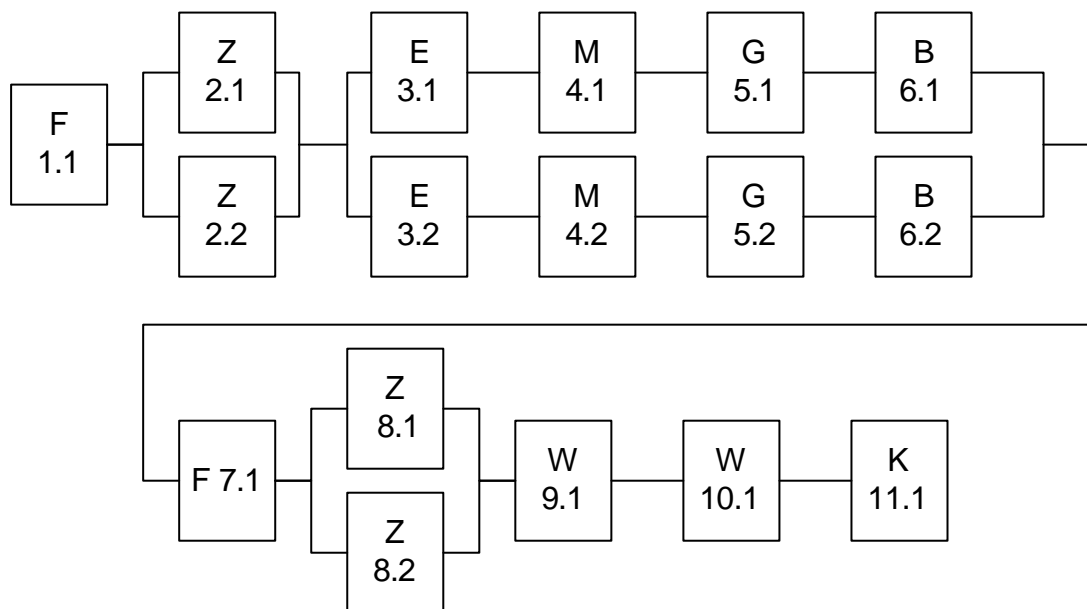


Bild 4.10: Durch Redundanz verbesserte Funktionsstruktur

Die damit erreichten Werte sind:

- Ausfallwahrscheinlichkeit des Gesamtsystems $F = 6,01 \cdot 10^{-6} \text{ 1/h}$
- MTTF des Gesamtsystems $\text{MTTF} = 166389 \text{ h}$

Die Verbesserungen wurden durch zwei Maßnahmen erreicht, deren *konstruktive Umsetzung noch zu prüfen ist*. Zu einen **müssen beide Antriebseinheiten in der Lage sein, sowohl den Teleskopteil des Mastes als auch die Kabine zu bewegen**. Dazu müssen beide

Antriebseinheiten mobiler Natur sein und am Teleskopteil des Mastes angebracht werden. Dadurch wird eine zweite Energieversorgung notwendig. Auch an die Getriebe werden hohe Anforderungen gestellt:

- Sie müssen in der Lage sein, die Antriebsleistung von den Riemen des Mastes auf die der Kabine zu schalten und umgekehrt.
- Die nicht angetriebene Einheit muss arretiert sein.
- Das redundante Getriebe muss das Ausgefallene aus dem Antriebsstrang entfernen können und seine Rolle übernehmen.

Zum anderen sind damit die Führungsrollen für die Zahnriemen am starren Mastteil überflüssig, weil zwei starre Riemen, an denen sich der Motor und damit der Teleskopteil des Mastes bewegen, ihren Zweck genauso erfüllen.

5 Ablauf einer FMECA

Die Failure Mode Effect and Criticality Analysis (FMECA) ist ein Instrument der Qualitätssicherung bei der Konstruktion eines Produktes und der Erstellung des Produktionsprozesses von Seiten des Teileherstellers und auf der Seite des Kunden eine Möglichkeit zur Beurteilung der Produktqualität. Die FMEA ist eine standardisierte und systematische Vorgehensweise zur Analyse und Verbesserung von Schwachstellen und Fehlern in der Konstruktion und Produktion von einzelnen Bauteilen bis hin zu komplexen Systemen. Sie ist dabei keine eigenständiger Bestandteil des Herstellungsprozesses, sondern ein „nebenbei“ ausgeführter Arbeitsschritt, der während der gesamten Lebensdauer eines Teiles, von den ersten Kontruktionsschritten bis hin zur Auslieferung an den Kunden und den praktischen Einsatz, immer wieder aktualisiert wird und dessen Ergebnisse möglichst bald in Änderungen des Produktes oder des Produktionsprozesses einfließen müssen, um eine effektive Prozessoptimierung zu erreichen.

In der Literatur [Ruta 1999, Franke 1987] wird zwischen drei FMEA-Einsatzgebieten unterschieden:

- Konstruktions - FMEA
Findet in der Konstruktionsphase des Bauteils oder Gesamtsystems Anwendung.
- Prozess - FMEA
Befasst sich mehr mit dem Produktionsprozess des Bauteiles als dem Bauteil selbst.
- Produkt - FMEA
Eine Zusammenfassung der beiden erstgenannten FMEA. Hier wird verstärkt auf die Sicht des Kunden geachtet, der in diesem Prozess auch mit einbezogen wird.

Nach [MIL-SPEC 1980] besteht eine FMEA aus acht Schritten:

- Systemdefinition
Erfolgte im Kapitel 4.4 sowie in Kapitel 5.1
- Block-Diagramm erstellen
Erfolgte im Kapitel 4.4
- Fehlermöglichkeiten analysieren
- Worst-Case-Szenario erstellen
- Fehlervermeidungsprozeduren entwickeln
- Designänderungen prüfen
- Auswirkung der Änderungen analysieren
- Dokumentation

5.1 Systemdefinition

Die Beispielanalyse soll hier für die modifizierte Variante 6 durchgeführt werden, deren Zuverlässigkeitskennwerte in Kapitel 4 nachgewiesen wurden.

Als Systemgrenze werden die unmittelbar zum Lift selbst gehörenden Komponenten gewählt, um die Komplexität in Grenzen zu halten. Zum Lift selbst gehörend heißt, alle Komponenten, die ohne den Lift nicht ins Flugzeug installiert würden. Damit gehört der Verschluss der Rumpfdurchführung zum System.

Eine weitere Systemgrenze betrifft die Energieversorgung. Hier wird als Schnittstelle der Anschluss der Bordenergie an die mobile Stromversorgung der mastmontierten Antriebseinheiten gewählt.

Eine weitere Festlegung betrifft die Art der geplanten Analyse:

- Systemanalyse
- Funktionsanalyse

Die Systemanalyse, auch Hardware-Analyse genannt, zerlegt das System in seine einzelnen Komponenten und analysiert die Fehlermöglichkeiten jeder Komponente und die Auswirkung auf andere Bauteile. Dies ist ein Ansatz, um einfach aufgebaute Systeme mit Funktionen, die einer Komponente klar zuzuordnen sind, zu analysieren.

Da der Lift in seinen grundsätzlichen Komponenten bereits bekannt ist, wird sich auch die Analyse auf die Komponentenebene beziehen. Damit ergeben sich folgende Komponente als Analysebestandteile:

- Liftkabine
- 2 Antriebseinheiten
 - Motor
 - Getriebe
 - Bremse
 - Antriebsriemen
- 2 Führungsschienen
- Energieversorgung
- Rumpfdurchführung

5.2 FMEA-Blätter

In den FMEA Blättern sind die Arbeitsschritte

1. Fehlermöglichkeiten analysieren

Das bedeutet, eine Auflistung aller möglichen Fehler, die zum Ausfall einer Komponente führen können, wird erstellt. Dabei werden die möglichen Fehler in Formblättern aufgelistet und nach bestimmten Kriterien geordnet:

- Jeder Fehler erhält eine eigene Identifikationsnummer.
- Das Bauteil, in dem der Fehler auftritt, wird benannt, um seine Nomenklatur innerhalb der Systembeschreibung aufzuführen.
- Die betroffene Funktion der Komponente wird aufgeführt, sowie ihre Verbindung zu den benachbarten Komponenten.

-
- Manche Fehler können nicht in jeder Phase des Fluges, sondern nur in bestimmten Situationen auftreten. Z.B. ist eine Bremsblockade nur möglich, wenn die Bremse eigentlich gelöst sein sollte.
 - Die Art des auftretenden Schadens.
 - Unter Schadensauswirkungen, lokal, nächster Level und final, versteht man die Auswirkung des Schadens an der Komponente auf das Gesamtsystem in unterschiedlichen Fortschrittsgraden. Angefangen von den direkt angrenzenden Komponenten bis hin zur höchst denkbaren Stufe des Ausfalls.
 - Die Schwere des Fehlers wird nach Kapitel 2.2 aufgeführt.
2. Worst-Case-Szenario erstellen
 3. Fehlervermeidungsprozeduren entwickeln
 4. Designänderungen prüfen

zusammengefasst. Die Blätter sind im Anhang zu finden. Der Punkt Designänderungen prüfen wird als eigenes FMEA-Blatt durchgeführt, sofern die Fehlervermeidung ein neues Bauteil erfordert, z.B. die Bewegungsdämpfung des Mastes.

Criticality Analysis

Die CA dient jetzt der Einordnung der in der FMEA gefundenen Fehlermöglichkeiten nach ihrer Gefährlichkeit. Die Einstufung erfolgt durch die oben bereits erläuterten Kriterien Auftretenswahrscheinlichkeit und Schwere des zu erwartenden Schadens. [Airbus 1990] führt die Einteilung mit Hilfe folgender Kennwerte durch:

- Failure Effect Probability α Gibt die Wahrscheinlichkeit an, mit der ein Fehler das vorhergesagte Schadensniveau erreicht. Dieser Wert wird für jedes Schadensniveau bestimmt.
- Failure Mode Ratio β . Die Wahrscheinlichkeit, dass ein bestimmter Fehlermodus bei einem Bauteil auftritt. Dadurch wird berücksichtigt, dass ein Bauteil auf mehr als eine Weise ausfallen kann. Die beiden bislang genannten Werte können nur abgeschätzt werden, da keine genauen Daten verfügbar sind.
- Ausfallrate λ
- Operationszeit t

Daraus errechnet sich die sog. Failure Mode Criticality nach der Formel

$$C_m = \alpha \beta \lambda t$$

Durch Aufsummieren aller für ein Bauteil vorhanden C_m -Werte erhält man die Item Criticality C_i , welche die Zuverlässigkeitsrelevanz des Bauteiles darstellt.

Die Einstufung der in der FMEA betrachteten Fehlerfälle hat folgende Ergebnisse gebracht:

ID	Severity	Data Source	Failure			Operating Time [h]	C _m	C _i
			Effect Probability	Mode Ratio	Rate			
1.1	C	[8]	0,1	1	1,00E-09	1,E+05	0,00001	0,0001
3.1	ma	[8]	0,1	1	5,50E-06	1,E+05	0,055	0,055
4.1	ma	[8]	1	0,7	2,76E-05	1,E+05	1,932	2,5116
4.2	ma	[8]	0,1	0,1	2,76E-05	1,E+05	0,0276	
4.3	ma	[8]	1	0,2	2,76E-05	1,E+05	0,552	
5.1	ma	[8]	1	0,2	1,90E-05	1,E+05	0,38	1,9
5.2	ma	[8]	1	0,4	1,90E-05	1,E+05	0,76	
5.3	ma	[8]	1	0,4	1,90E-05	1,E+05	0,76	
6.1	ma	[8]	1	0,8	2,10E-04	1,E+05	16,8	17,22
6.2	C	[8]	0,1	0,1	2,10E-04	1,E+05	0,21	
6.3	H	[8]	0,1	0,1	2,10E-04	1,E+05	0,21	
8.1	mi	[8]	1	0,3	1,70E-05	1,E+05	0,51	1,7
8.2	mi	[8]	1	0,1	1,70E-05	1,E+05	0,17	
8.3	mi	[8]	1	0,6	1,70E-05	1,E+05	1,02	
9.1	ma	[8]	0,1	1	3,00E-06	1,E+05	0,03	0,03

Je höher der C_i-Wert hierbei ist, desto kritischer ist der Fehler, weil er entweder sehr häufig auftritt und/oder gravierende Konsequenzen hat. In der hier vorliegenden Analyse sind zwei Bauteile besonders kritisch, der Motor 4 (C_i = 2.5) sowie die Bremse (C_i = 17.22). Wenn man die Zuverlässigkeit des Liftes erhöhen will, ist es am effektivsten, diese beiden dringlichsten Fehlerquellen zu beseitigen, um einerseits die Häufigkeit der Fehler zu senken, durch redundante Ausführung der Bremse wird die ausgesprochen schlechte Ausfallrate der Bremse verbessert, andererseits mögliche schwerwiegende Folgen eines Liftausfalles abgemildert. Allerdings ist die redundante Ausführung der Liftbremse und des Motors bereits in der verbesserten Konfiguration des Liftes aus Kapitel 4.4 enthalten.

Analyse der Änderungen

Umfasst eine zweite FMEA, die nun auf sich geänderte oder neu hinzugekommene Komponenten bezieht. Für diese Bauteile müssen die gleichen Verfahren angewandt werden, wie für das System in seiner Ursprungskonfiguration benutzt wurden. Dieses Verfahren ist z.T. bereits in Kapitel 4.4 durchgeführt, zumindest was Änderungen im System angeht. Auf eine erneute FMEA wird im weiteren verzichtet, da die Art der Komponenten sich nicht geändert hat.

Dokumentation

Da es sich hier nur um ein Beispiel handelt, entfällt dieser Punkt.

6 Zonal Safety Analysis

Nach [Davidson 1988] resultiert die Notwendigkeit einer ZSA aus der Forderung, dass „the installation of Systems which do not perform any airworthiness-related functions should be accomplished in a manner which ensures their independence of function and physical separation from airworthiness-related components.“

Zu diesem Zweck muss für jede Zone des Flugzeuges eine eigene ZSA erstellt werden, die im besonderen auf Kriterien eingeht, wie

- Gegenseitige Beeinflussung von Systemen
- Einfluss von Wartungsfehlern auf umliegende Systeme
- Berücksichtigung von Beschädigungen von außen
- Beachtung der Installationskriterien

Folgende Vorgehensweise ist für die Durchführung der ZSA empfohlen:

- Einteilung des Flugzeuges in Zonen

Für den Lift bedeutet das, dass für jede Zone, durch die der Lift führt, eine eigene ZSA zu erstellen ist.

Wenn man die möglichen Einbaupositionen des Liftes in der A380 auf die A340 überträgt, erhält man folgende betroffenen Zonen:

Lift 1, 2: Zone 140, 250

Lift 3: Zone 160, 260

- Im zweiten Schritt geht es um die Aufteilung der Zuständigkeiten zur Überprüfung der Installationsbestimmungen der einzelnen Systeme, die in einen generellen und einen speziellen Teil aufgeschlüsselt sind.

Der generelle Teil beschäftigt sich mit den Anschlüssen der einzelnen Systeme untereinander und mit der Struktur. Dabei soll sichergestellt werden, dass durch Schläuche, Rohre, Kabel, Drähte und ähnliches keine Probleme entstehen.

Fehlerquellen sind hierbei:

- Vertauschte Anschlüsse
- Kraftübertragung und mechanische Belastung, z.B. durch Festhalten
- Freigängigkeit bei bewegten Systemen
- Deutliche Trennung von Primär- und Backupsystem

Des Weiteren ist die wartungsgerechte Installation zu beachten, um zu gewährleisten, dass Komponenten auch nach Austausch die o.g. Kriterien erfüllen.

Die Einzelteile in einer Zone, sowie die Zugangspanel, Nachfüllstutzen u. ä. müssen korrekt gekennzeichnet und gut zugänglich sein, um Verwechslungsfehler zu vermeiden.

Der letzte wichtige Punkt in dieser Betrachtung ist der Aspekt der Drainage im weitesten Sinne. Es ist von äußerster Wichtigkeit, dass alle Objekte, die bei der Erstmontage oder Wartung/Instandsetzung ausgelaufen, verlorengegangen oder sonstwie aus dem Zusammenhang des Systems entfernt oder unberechtigt eingebracht wurden, zuverlässig an leicht einsichtigen Punkten gesammelt werden oder aus der Zone herausgeleitet werden. Das gilt sowohl für Betriebsstoffe in fester oder flüssiger Form als auch für gebrochene oder heruntergefallene Bolzen, vergessene Werkzeuge, Putzmittel oder ausgelaufene Transportgüter.

Um ein Beispiel anzuführen, es kommt darauf an, zu verhindern, dass Cola aus zwei ausgelaufenen Cola-Dosen, die mit dem Lift auf das Oberdeck gefahren wurden, aus der Kabine herausläuft und sich in einem Winkel zwischen Außenhaut, Spant und Stringer sammelt, um dort Korrosion hervorzurufen.

Der spezielle Teil der Installationsanweisungen ist nun die Anwendung des Obengenannten en detail auf die Zone.

- Hydraulische Systeme sind möglichst weit unten im Flugzeug anzuordnen, um zu vermeiden, dass auslaufendes Hydrauliköl die Klimaanlage kontaminiert oder elektrische Systeme beschädigt.
- Um Schäden durch strukturelle Verformungen zu vermeiden, müssen Sicherheitsabstände zwischen Leitungen und Struktur bzw. zwischen Leitung und Leitung gewährleistet sein. Dabei müssen die Anschlüsse und Abstandhalter in der Lage sein, die Beschleunigungskräfte aufzunehmen, die gerade bei schweren Leitungen auftreten können.
- Elektrische Systeme müssen vor Kurzschlüssen und Bedienpersonal vor elektrischen Entladungen geschützt werden.
- Auf korrekte Sicherung für Schrauben und andere Verbindungselemente ist zu achten.
- ...

Aus dieser Aufstellung ist zu entnehmen, mit welchem Detaillierungsgrad eine solche ZSA auszuführen ist, und wie wichtig es ist, ein möglichst originalgetreues Modell oder einen Prototypen vor Augen zu haben.

7 Zusammenfassung

Diese Arbeit beschäftigt sich mit dem Zuverlässigkeitsaspekt einer Entwurfsarbeit. Dabei wurde nach einer Einführung in die Grundbegriffe und Methoden der Zuverlässigkeitsrechnung eine bestehende Konzeptstudie um zuverlässigkeitsrelevante Methoden erweitert.

Dazu gehört die Umsetzung der bestehenden Anforderungen in Kennwerte. Der Nachweis dieser Kennwerte ist im Rahmen dieser Konzeptstudie noch mit einfachen Formeln möglich, die zuvor vorgestellt wurden. Trotzdem ergaben sich auch hierbei Diskrepanzen zwischen den Anforderungen an den Entwurf und seinen Möglichkeiten, was eine Modifikation der Entwurfsvariante erforderlich machte.

Hierbei zeigt sich noch eine Schwierigkeit der reinen Zuverlässigkeitsbetrachtung ohne Verzahnung mit den für die konstruktive Seite zuständigen Abteilungen, da die Umsetzung der Verbesserungen nicht ohne weiteres möglich sein muss.

Die Failure Mode Effect and Criticality Analysis, deren Datenblätter sich im Anhang befinden, bietet dem Leser einen Einblick in das Verfahren, ohne Anspruch auf Vollständigkeit zu erheben, da eine FMECA über den kompletten Lebenszyklus eines Produktes fortgeführt werden muss.

Gleichwohl haben sich aus der zugehörigen Criticality Analysis Ansatzpunkte für eine Konzeptverbesserung ergeben, die auch in die Optimierung des Entwurfes eingeflossen sind.

Die zum Schluss erwähnte Zonal Safety Analysis ist ein Tool, das viel später im Entwurfsprozess zum Einsatz kommt, so dass hier noch keine Erkenntnisse gewonnen werden konnten, da sich die bisher zu beachtenden Grundregeln eher als allgemeine Konstruktionsregeln zu verstehen sind und kein zentraler Bestandteil einer ZSA sind.

Literaturverzeichnis

- Davidson 1988** DAVIDSON, John: The reliability of mechanical systems: Mechanical Engineering Publications Limited, 1988
- Airbus 1990** WOHLFAHRT, J.: justification of reliability and safety: Deutsche Airbus, Ref: GQ 22-111/90, September 1990
- AC 251309** Federal Aviation Administration: System Design And Analysis: Advisory Circular, 21.6.1988
- Airbus 2001** SZAMEIT, Jan: Konzeptstudie eines integrierten Lasten- und Personenaufzuges für Großraumflugzeuge: Hochschule für angewandte Wissenschaften, 2001
- RADC 1985** Hughes Aircraft Co. RADC: Nonelectric Reliability Notebook Revision B: NTIS, Oct 1985
- Franke 1987** FRANKE, Wolf D.: FMEA: Verlag moderne Industrie, 1987
- Ruta 1999** RUTA, Andreas: Fehlermöglichkeits und Einflussanalyse FMEA für die Produktionslogistik: Fortschritt-Berichte VDI Nr.518, 1999
- MIL-SPEC 1980** MIL-STD-1629A: Proceres for performing a Failure Mode, Effects and Criticality Analysis: U.S Military Spcifications, 24.11.1980

Fehlermöglichkeits- und -einflussanalyse auf Bauteilebene

System Trolley Lift
 Level 1, 7 Führung
 Referenzezeichnung
 Mission

Datum 03.03.02
 Seite 1 von 6
 Übersetzt von
 Genehmigt von

Nr.	Bauteil	Funktion	Fehlerart	Missionsphase	Schadensart	Schadensauswirkungen			Fehlerkategorie	Ausgleichsvorkehrungen	worst case
						lokal	nächster Level	final			
1	1.1	Führung des Liftes	Deformation	Beladung Flug	Liftausfall	starke Beanspruchung der Führung	Belastung der Rumpfstruktur	Schäden am Rumpf	catastrophic	Lagerung anpassen (Bestandteil des Pre-Design)	Zelle zerstört

Fehlermöglichkeits- und -einflussanalyse auf Bauteilebene

System Trolley Lift
 Level 3 Energieleitung
 Referenzezeichnung
 Mission

Datum 03.03.02
 Seite 1 von 6
 Übersetzt von
 Genehmigt von

Nr.	Bauteil	Funktion	Fehlerart	Missionsphase	Schadensart	Schadensauswirkungen			Fehlerkategorie	Ausgleichsvorkehrungen	worst case
						lokal	nächster Level	final			
1	3.x	Energie bereitstellen	Bruch	Beladung Flug	Antriebsausfall	keine Energie	Motor liefert kein Drehmoment	Mast 2 / Kabine fährt nicht	major	zweite Energieversorgung	Liftausfall

Fehlermöglichkeits- und -einflussanalyse auf Bauteilebene

System
Level
Referenzzeichnung
Mission

Trolley Lift
4 Motor

Datum
Seite
Übersetzt von
Genehmigt von

03.03.02
2 von 6

Nr.	Bauteil	Funktion	Fehlerart	Missionsphase	Schadensart	Schadensauswirkungen			Fehlerkategorie	Ausgleichsvorkehrungen	worst case
						lokal	nächster Level	final			
1	4.x	Drehmomenterzeugung	kein Motoranfahren	Beladung Flug	Antriebsausfall	kein Drehmoment	Mast 2 / Kabine fährt nicht	Liftausfall	major	2. Motor	Liftausfall
2	4.x	Drehmomenterzeugung	unkontrolliertes Motoranfahren	Beladung Flug	Strukturschaden	Mast 2 / Kabine fährt	keine Bremsung	Strukturschaden	hazardous	Energieversorgung in Ruhestellung trennen	Strukturschaden
3	4.x	Drehmomenterzeugung	Blockade	Beladung Flug	Antriebsausfall	kein Drehmoment	Mast 2 / Kabine fährt nicht	Liftausfall	major	2. Motor 1. Motor auskuppeln	Liftausfall

Fehlermöglichkeits- und -einflussanalyse auf Bauteilebene

System
Level
Referenzzeichnung
Mission

Trolley Lift
5 Getriebe

Datum
Seite
Übersetzt von
Genehmigt von

03.03.02

3 von 6

Nr.	Bauteil	Funktion	Fehlerart	Missions- phase	Schadens- art	Schadensauswirkungen			Fehler- kategorie	Ausgleichs- vorkehrungen	worst case
						lokal	nächster Level	final			
1	5.x	Drehmoment übersetzung	Blockade	Beladung Flug	Antriebs- ausfall	kein Drehmoment	Mast 2 / Kabine fährt nicht	Liftausfall	major	2. Getriebe	Liftausfall
2	5.x	Drehmoment übersetzung	Fehlfunktion	Beladung	Antriebs- ausfall	kein Drehmoment	Mast 2 / Kabine fährt nicht	Liftausfall	major	2. Getriebe	Liftausfall
3	5.x	Drehmoment übersetzung	Fehlfunktion	Flug	Antriebs- ausfall	kein Drehmoment	Mast 2 / Kabine fährt nicht	Liftausfall	major	2. Getriebe	Liftausfall

Fehlermöglichkeits- und -einflussanalyse auf Bauteilebene

System
Level
Referenzzeichnung
Mission

Trolley Lift
6 Bremse

Datum
Seite
Übersetzt von
Genehmigt von

03.03.02
4 von 6

Nr.	Bauteil	Funktion	Fehlerart	Missions- phase	Schadens- art	Schadensauswirkungen			Fehler- kategorie	Ausgleichs- vorkehrungen	worst case
						lokal	nächster Level	final			
1	6.x	Arretierung Mast 2 / Kabine	Blockade	Beladung Flug	Antriebs- ausfall	kein Drehmoment	Mast 2 / Kabine fährt nicht	Liftausfall	major	2. Antriebs- einheit	Liftausfall
2	6.x	Arretierung Mast 2 / Kabine	Fehlfunktion	Flug	Struktur- schaden	kein Abbremsen	Struktur- schaden Rumpftür	Struktur- schaden	catastrophic	2. Antriebs- einheit	Zelle zerstört
3	6.x	Arretierung Mast 2 / Kabine	Fehlfunktion	Beladung	Antriebs- ausfall	kein Abbremsen	Mast 2 / Kabine beschädigt	Liftausfall Personen- schaden	hazardous	2. Antriebs- einheit	Liftausfall

Fehlermöglichkeits- und -einflussanalyse auf Bauteilebene

System
Level
Referenzezeichnung
Mission

Trolley Lift
7 Riemen

Datum
Seite
Übersetzt von
Genehmigt von

03.03.02
5 von 6

Nr.	Bauteil	Funktion	Fehlerart	Missionsphase	Schadensart	Schadensauswirkungen			Fehlerkategorie	Ausgleichsvorkehrungen	worst case
						lokal	nächster Level	final			
1	2.x, 8.x	Kraftübertragung Mast Kabine	Riss	Beladung Flug	Wartungskosten	Kippmoment Mast 2 Kabine	starke Beanspruchung Führung	vorgezogene Inspektion	minor	2. Antriebseinheit	Liftausfall
2	2.x, 8.x	Kraftübertragung Mast Kabine	Riss	Flug	Wartungskosten	Kippmoment Mast 2 Kabine	starke Beanspruchung Führung	vorgezogene Inspektion	minor	Herausfallen des Riemens vermeiden	Liftausfall
3	2.x, 8.x	Kraftübertragung Mast Kabine	Überdehnung	Beladung	Wartungskosten	kein Abbremsen	starke Beanspruchung Führung	vorgezogene Inspektion	minor	Riemenstraffer	Liftausfall

Fehlermöglichkeits- und -einflussanalyse auf Bauteilebene

System
Level
Referenzezeichnung
Mission

Trolley Lift
9, 10 Umlenkrollen

Datum
Seite
Übersetzt von
Genehmigt von

03.03.02
5 von 6

Nr.	Bauteil	Funktion	Fehlerart	Missionsphase	Schadensart	Schadensauswirkungen			Fehlerkategorie	Ausgleichsvorkehrungen	worst case
						lokal	nächster Level	final			
1	9.1, 10.1	Riemenführung	Lagerschaden	Beladung Flug	Motormehrbelastung	verstärkte Reibung	starke Beanspruchung Motor	Überhitzung	major	Betriebsdauer begrenzen	Liftausfall

Fehlermöglichkeits- und -einflussanalyse auf Bauteilebene

System Trolley Lift
 Level Rumpfdurchbruch
 Referenzzeichnung
 Mission

Datum 03.03.02
 Seite 6 von 6
 Übersetzt von
 Genehmigt von

Nr.	Bauteil	Funktion	Fehlerart	Missions- phase	Schadens- art	Schadensauswirkungen			Fehler- kategorie	Ausgleichs- vorkehrungen	worst case
						lokal	nächster Level	final			
1		Durchfahrt durch den Rumpf	kein Öffnen	Beladung	Liftausfall	Rumpf verschlossen		Liftausfall	major		Liftausfall
2		Durchfahrt durch den Rumpf	kein Schliessen	Beladung	Startver- zögerung	Tür schließt nicht	Rumpfdurch- gang offen	Startver- zögerung	major	manuelle Verriegelung	Startver- zögerung