27. April 2010, GDV, Berlin

Risikobeurteilung

Materialien zu einem Referat

Alfred Mörx

diam-consult
Ingenieurbüro für Physik
Pretschgasse 21/2/10
A-1110 Wien/Österreich

Tel.: +43-(0)1-769-67-50-12
Fax.: +43-(0)1-769-67-50-20
Email: management@diamcons.com
www.diamcons.com

Inhaltsübersicht

1 Sicherheit, Risiko und Restrisiko technischer Systeme

1.1 Der Begriff „Sicherheit“

Der Begriff der Sicherheit, als unverzichtbarer Basisbegriff für alle Überlegungen zur Sicherheitstechnik, ist heute als "Freiheit von unvertretbaren Schadensrisken" weitestgehend anerkannt.

Dies bedeutet, dass Sicherheit eine Freiheit ist, die jedes unvertretbare Schadensrisiko ausschließt und es erlaubt, eine Situation eindeutig als "Sicher" oder "Gefährlich" zu klassifizieren. Ziel der Planung, Ausführung und Betrieb von Maschinen und Anlagen ist es, Sicherheit zu erreichen und Gefahren auszuschließen.

Alle in dem Themenkreis geführten Diskussionen um die eindeutige Abgrenzung von "Sicherheit" und "Gefahr" sind der Fachwelt seit vielen Jahren bekannt, sodass ich hier nur auf die Kernaussagen eingehen möchte.

Die Abgrenzung von Gefahr und Sicherheit ist durch die Einführung des Begriffs "Höchstes vertretbares Risiko" getroffen; die Zusammenhänge sind in Bild 1-1dargestellt.

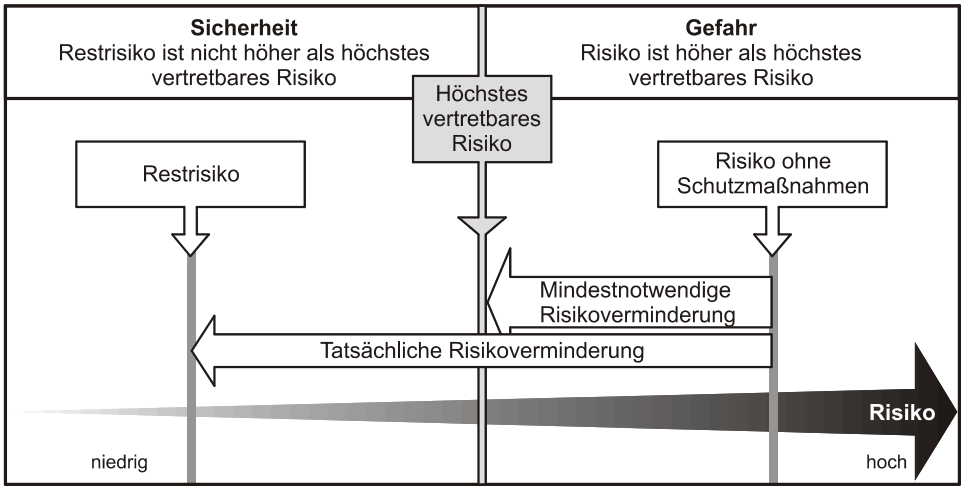


Bild 1-1 Sicherheit und Gefahr, Risiko, höchstes vertretbares Risiko und Restrisiko

1.2 Sicherheitsphilosophie

In der Praxis muss nun durch geeignete Maßnahmen sichergestellt werden, dass das Risiko, das nach Anwendung von Maßnahmen verbleibt, möglichst gering, in keinem Fall jedoch größer als das höchste vertretbare Risiko ist.

Der Begriff des höchsten vertretbaren Risikos darf jedoch keinesfalls mit dem Begriff des Restrisikos verwechselt werden, da es ja das Bestreben jedes mit sicherheitsrelevanten Aufgaben beschäftigten Technikers sein muss, das auch bei Anwendung von technischen Maßnahmen niemals vollständig auszuschließende Restrisiko möglichst weit unter die vertretbare Grenze zu drücken.

Das in den einzelnen Ländern der Welt von Maschinen und Anlagen zu fordernden (und vom Anwender erwartete) maximale Restrisiko ist erfahrungsgemäß sehr unterschiedlich.

Darüber hinaus ist auch das höchste vertretbare Risiko nicht für alle Maschinen und Anlagen identisch, sondern von den besonderen Umständen der Nutzung abhängig. (So ist. z. B. das höchste vertretbare Risiko in landwirtschaftlichen und gartenbaulichen Anwesen u.U. unterschiedlich von jenem in Büros oder Wohngebäuden.)

Auch das *Komfortbedürfnis der Maschinen- und Anlagennutzer*, das sich indirekt durch die Art der in der Anlage zum Einsatz kommenden Maschinen und Betriebsmittel ausdrückt, wirkt sich auf das vom Anwender (unausgesprochen) von der Maschine oder Anlage erwartete Restrisiko aus.

Überlegungen zum höchsten vertretbaren Risiko werden, insbesondere in gewerblich und/oder industriell genutzten Maschinen und Anlagen, zunehmend vor dem Hintergrund der *Schadensfolgekosten* geführt werden.

Schadensfolgekosten können dabei als Kosten definiert werden, die unter anderem infolge unzureichender Zuverlässigkeit der Energieversorgung (z. B. durch Fehlauslösungen von Schutzeinrichtungen bei Gewittern) beim Ausfall einer Maschine, eines Anlagenteils oder eines Betriebsmittels entstehen.

Ohne Anspruch auf Vollständigkeit zu erheben, sind die wesentlichen Komponenten der möglichen Schadensfolgekosten in Bild 1-2 zusammengestellt.

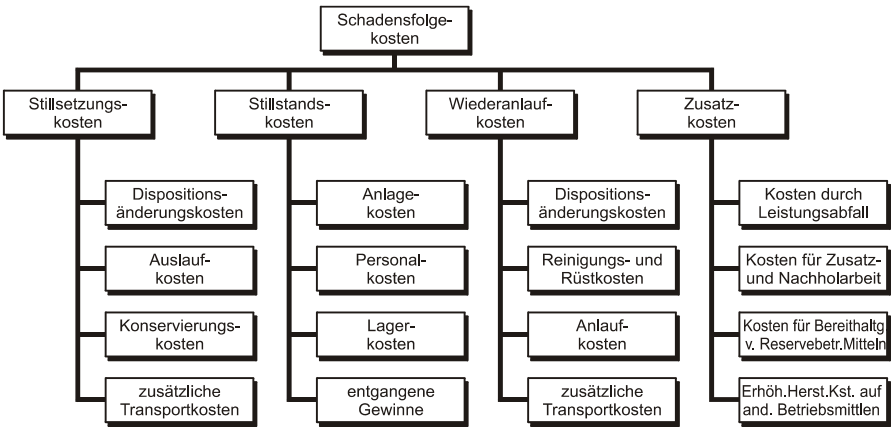


Bild 1-2 Schadensfolgekosten und mögliche Komponenten

2 Risikobegriff in den Grundlagen für technische Normen

risk	combination of the probability of occurrence of *harm* and the severity of that *harm*
harm	physical injury or damage to the health of people, or damage to property or the environment
safety	freedom from unacceptable *risk* *Safety* is achieved by reducing risk to a tolerable level (defined as: tolerable risk)
tolerable risk	risk which is accepted in a given context based on the current values of society Tolerable risk is achieved by the iterative process of risk assessment (risk analysis and risk evaluation) and risk reduction. Tolerable risk is determined by the search for an optimal balance between the ideal of absolute safety and the demands to be met by a product, process or service, and factors such as benefit to the user, suitability for purpose, cost effectiveness, and conventions of the society concerned. It follows that there is a need to review continually the tolerable level, in particular when developments, both in technology and in knowledge, can lead to economically feasible improvements *to attain the minimum risk compatible* with the use of a product, process or service.
residual risk	*risk* remaining after *protective measures* have been taken
protective measure	means used to reduce risk

Source: ISO/IEC Guide 51: Safety aspects – Guidelines for their inclusion in standards; Second Edition 1999

3 Sicherheit und Risiko

Bis zum Ende der 1970er Jahre gab es für jede Maschine oder Anlage spezifische Sicherheitsmaßnahmen, die zur Erhöhung der Sicherheit empfohlen oder vorgeschrieben waren. Dabei gab es kaum einen Zusammenhang zwischen der verwendeten Technik, dem tatsächlichen Risiko und der möglichen Gefährdung.

Erst zu Beginn der Achtziger Jahre etablierte sich international eine etwas einheitlichere Sichtweise. Anhand des zu erwartenden Risikos einer Maschine oder Anlage erstellte man genaue technische oder organisatorische Forderungen, die eine Reduzierung der Gefahr auf gemeinsam festgelegten methodischen Grundlagen bewirkten.

Das Risiko (R) ergibt sich dabei durch eine Wahrscheinlichkeitsaussage, die das zu erwartende Schadensausmaß (S) und die zu erwartende Eintrittswahrscheinlichkeit[1] (E) eines Schadens berücksichtigt.

In vielen Fällen wird ein einfacher multiplikativer Ansatz gewählt, wie zum Beispiel:

$$R = S \cdot H$$

3.1 Riskoelemente

Unter Riskoelementen versteht man im weitersten Sinn jene Faktoren, die das Risiko beeinflussen; diese werden nach einer von Fachleuten (teilweise auch normativ) festgelegten Verknüpfungsvorschrift verbunden und zu einer Risikoaussage zusammengeführt.

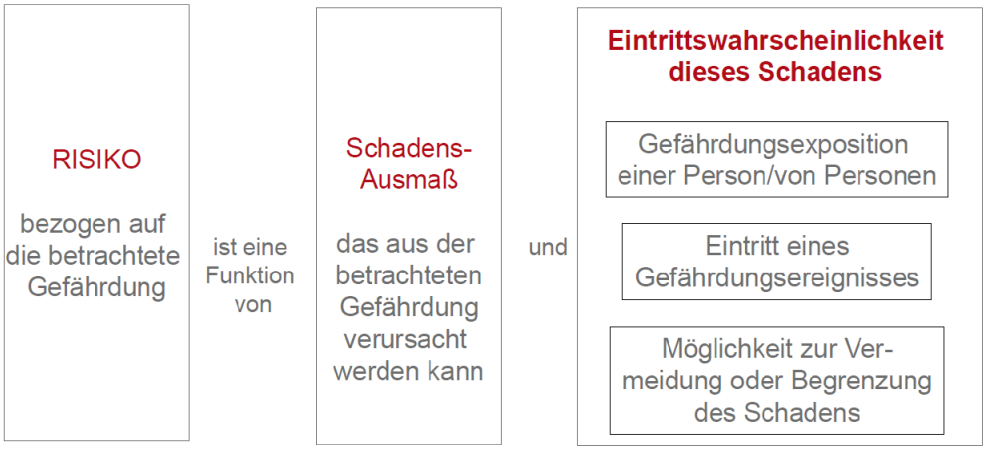
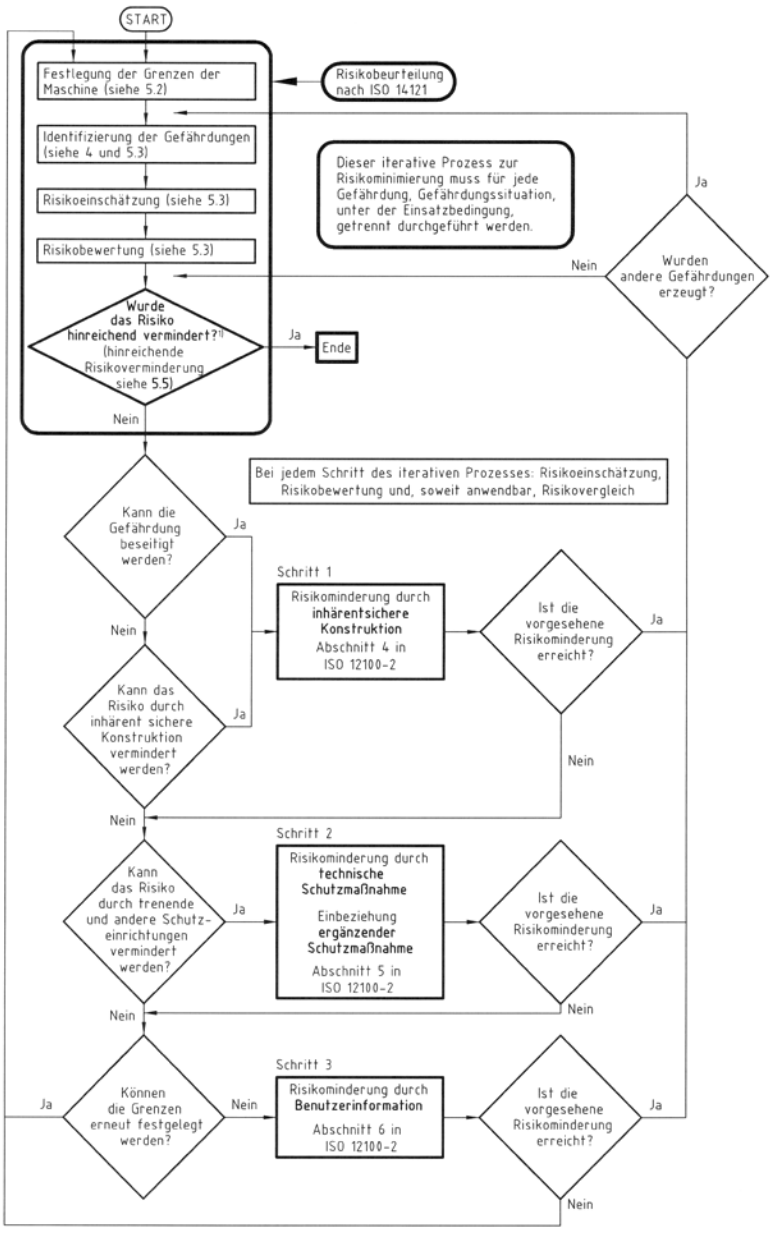


Bild 3-1 Risikoelemente gemäß EN ISO 14121 im Fachbereich „Maschinensicherheit“

[1] Die Eintrittswahrscheinlichkeit kann aus der (relativen) Häufigkeit abgeschätzt werden.

4 Risikoanalyse

Für die systematische Untersuchung von Gefährdungen wurde eine Reihe von Verfahren entwickelt. Für jedes Verfahren gibt es ein spezielles Anwendungsgebiet. Deshalb kann es notwendig werden, sie für die Anwendung auf die jeweilige Aufgabenstellung zu adaptieren. Diese Anpassung bzw. die geeignete Kombination von Verfahren ist Bestandteil einer qualifizierten System- und Risikoanalyse. Technische Risikoanalysen im Bereich der Sicherheit werden oft als iterative Prozesse angesetzt.



1) Beim erstmaligen Stellen der Frage wird sie mit dem Ergebnis der Ausgangsrisikobewertung beantwortet.

Bild 4-1 Schematische Darstellung des 3-stufigen iterativen Prozesses zur Risikominderung; entnommen EN ISO 12100-1:2003

4.1 Grundtypen der Risikoanalyse

Es gibt zwei Grundtypen der Risikoanalyse; sie werden als deduktive bzw. induktive Verfahren bezeichnet.

Bei *deduktiven* Verfahren wird ein Schlussereignis angenommen und die Ereignisse gesucht, die dieses Schlussereignis hervorrufen könnten.

Bei *induktiven* Verfahren wird der Ausfall eines Maschinenelementes angenommen. Die anschließende Analyse stellt die Ereignisse fest, die dieser Ausfall hervorrufen könnte.

Nachstehend sind einige Verfahren beispielhaft angegeben und kurz charakterisiert.

4.2 Vorläufige Untersuchung von Gefährdungen

PHA[2] ist ein induktives Verfahren mit dem Ziel, für ein festgelegtes System und/oder Untersystem und/oder Maschinenelement in allen seinen Lebensphasen die Gefährdungen, Gefährdungssituationen und Gefährdungsereignisse festzustellen, die zu einem Unfall führen könnten.

Das Verfahren stellt die Unfallmöglichkeiten fest und schätzt qualitativ den Grad einer möglichen Verletzung oder eines möglichen gesundheitlichen Schadens ab. Vorschläge von Schutzmaßnahmen und das Ergebnis ihrer Anwendung werden dann angegeben.

PHA sollte in den Phasen der Konstruktion, des Aufbaus und der Prüfung aktualisiert werden, um neu auftretende Gefährdungen zu entdecken und wo nötig Korrekturen anzubringen.

Die erzielten Ergebnisse können in unterschiedlicher Weise dargestellt werden (z. B. Tabelle, Fehlerbaum).

4.3 "Was-Wenn"-Verfahren

Das "Was-Wenn"-Verfahren ist ein induktives Verfahren.

Für relativ einfache Anwendungen werden Konstruktion und Betrieb der Maschine untersucht. Bei jedem Schritt werden "was-wenn"-Fragen gestellt und beantwortet, um die Wirkung des Ausfalls von Maschinenelementen oder von Verfahrensfehlern hinsichtlich der durch die Maschine hervorgerufenen Gefährdungen bewerten zu können.

Für komplexere Anwendungen kann das "was-wenn"-Verfahren am besten mithilfe einer "Checkliste" und entsprechender Arbeitsteilung durchgeführt werden, um bestimmte Aspekte des Prozesses denjenigen Personen zuzuordnen, die zur Bewertung der jeweiligen Aspekte die größte Erfahrung und Übung haben. Bedienerverhalten und Berufskenntnisse werden begutachtet. Die Eignung der Ausrüstung und der Konstruktion der Maschine, ihre Steuerung und ihre Schutzeinrichtungen werden begutachtet. Es werden die Einflüsse durch die verarbeiteten Werkstoffe untersucht und die Bedienungs- und Instandhaltungsaufzeichnungen geprüft. Im

[2] PHA ... preliminary hazard analysis

Allgemeinen geht die Checklisten-Bewertung der Maschine den unten beschriebenen, mehr verfeinerten Verfahren voran.

4.4 Fehlzustandsart- und -auswirkungsanalyse

FMEA[3] ist ein induktives Verfahren mit dem hauptsächlichen Zweck, die Häufigkeit und die Folgen des Ausfalles von Maschinenelementen zu ermitteln. Wo Verfahrensfehler oder Bedienungsfehler von wesentlicher Bedeutung sind, können andere Verfahren geeigneter sein.

FMEA kann zeitaufwendiger sein als die Fehlerbaumanalyse, weil für jedes Element jede Art des Ausfalls betrachtet wird. Einige Ausfälle haben eine sehr geringe Eintrittswahrscheinlichkeit. Wenn diese Ausfälle nicht im Detail analysiert werden, sollte dies in der Dokumentation aufgezeichnet sein.

4.5 DELPHI-Methode

Ein großer Expertenkreis wird in mehreren Schritten befragt, wobei das Ergebnis des vorhergehenden Schrittes zusammen mit zusätzlichen Informationen allen Teilnehmern übermittelt wird.

Im dritten oder vierten Schritt konzentriert sich die anonyme Befragung auf diejenigen Gesichtspunkte, zu denen bisher keine Übereinstimmung erzielt wurde.

Im Grundsatz ist die Delphimethode ein Voraussageverfahren, das auch zur Entwicklung von neuen Ideen verwendet wird. Dieses Verfahren ist besonders effektiv, weil ausschließlich Fachleute beteiligt werden.

Risikograph

Eine der prinzipiellen Methoden, unabhängig vom Maschinentyp, eine geeignete Maßnahme zur Einhaltung der Sicherheit zu finden, besteht darin, das Risiko mittels des Risikographen[4] zu beurteilen.

[3] Ausfalleffektanalyse; Failure Mode and Effects Analysis; FMEA

[4] eine detaillierte Darstellung der Methode findet sich in EN 954-1 bzw. aktuell in EN ISO 13849

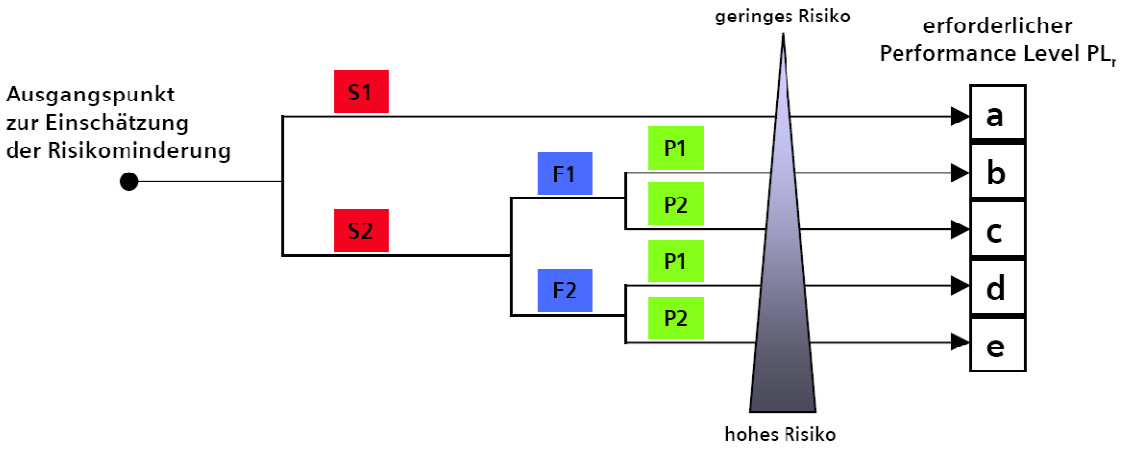


Bild 4-2 Ermittlung des erforderlichen Performance Levels (P_r) mittels Risikograph

Risikoparameter

S **Schwere der Verletzung**

S1	leichte (üblicherweise reversible) Verletzung
S2	schwere (üblicherweise irreversible) Verletzung, einschließlich Tod

F **Häufigkeit und/oder Aufenthaltsdauer (der Gefährdungsaussetzung)**

F1	selten bis öfter und/oder Zeit der Gefährdungsaussetzung ist kurz
F2	häufig bis dauernd und/oder Gefährdungsaussetzung ist lang

P **Möglichkeit zur Vermeidung der Gefährdung oder Begrenzung des Schadens**

P1	möglich unter bestimmten Bedingungen
P2	kaum möglich

5 Zusammenhang PL, PFH

Das Performance Level ist eine Maßzahl, die die durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde beschreibt.

Performance Level (PL)	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (*PFH*) in h^{-1}
a	$\geq 10^{-5}$ bis $< 10^{-4}$
b	$\geq 3 \cdot 10^{-6}$ bis $< 10^{-5}$
c	$\geq 10^{-6}$ bis $< 3 \cdot 10^{-6}$
d	$\geq 10^{-7}$ bis $< 10^{-6}$
e	$\geq 10^{-8}$ bis $< 10^{-7}$

PL … Performance Level

PFH … Probability of a dangerous failure per hour

6 Sicherheitsanforderungsstufe (SIL)

Sicherheits-Integritätslevel (SIL)

6.1 Definition

Die *Sicherheitsanforderungsstufe* ist ein Begriff aus dem Gebiet der Funktionalen Sicherheit und wird in der internationalen Normung gemäß *IEC 61508/IEC61511* auch als *Sicherheits-Integritätslevel (SIL)* bezeichnet.

Er dient der Beurteilung elektrischer/elektronischer/programmierbar elektronischer (E/E/PE)-Systeme in Bezug auf die Zuverlässigkeit von Sicherheitsfunktionen.

Aus der angestrebten Anforderungsstufe ergeben sich die sicherheitsgerichteten Konstruktionsprinzipien, die eingehalten werden müssen, damit das Risiko einer Fehlfunktion minimiert werden kann.

Unter den Sicherheitsanforderungsstufen versteht man gemäß IEC 61508:

Vier diskrete Stufen zur Spezifizierung der Anforderung für die Sicherheitsintegrität von Sicherheitsfunktionen, die dem E/E/PE-sicherheitsbezogenen System zugeordnet werden, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt.

6.2 Sicherheitskreis

Sicherheitsfunktionen dienen in der Industrie dem Schutz der Gesundheit der dort Beschäftigten, der Umwelt und von Gütern.

Diese Sicherheitsfunktionen werden durch einen Sicherheitskreis, der aus verschiedenen Betriebsmitteln, wie z. B. Sensoren, Steuerungselementen und Aktoren bestehen kann, realisiert.

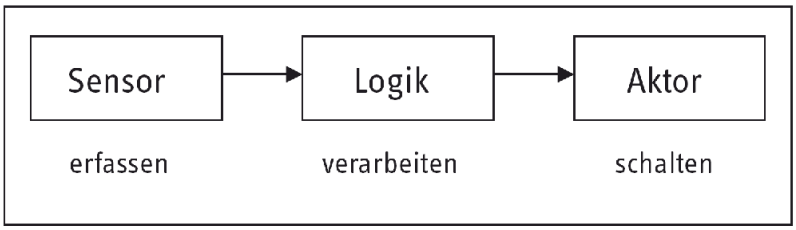


Bild 6-1 Sicherheitsfunktionen und Sicherheitskreis

Die Sicherheitsanforderungsstufe stellt ein Maß für die Zuverlässigkeit des Systems in Abhängigkeit von der Gefährdung dar. Prozesse mit einer geringeren Gefährdung werden durch einen Sicherheitskreis mit geringerem Level aufgebaut als Prozesse mit höherer Gefährdung, bei denen z. B. Menschen getötet werden können.

Beispiele für Sicherheitsfunktionen:

- Notausschaltungen,
- Abschalten überhitzter Geräte
- Überwachung gefährlicher Bewegungen.

Die Betreiber von Anlagen mit sicherheitsrelevanten Funktionen legen im Rahmen einer Gefährdungsbeurteilung den Sicherheits-Integritätslevel für die jeweilige Sicherheitsfunktion fest. Entsprechend dieser Festlegung werden die dafür geeigneten Geräte ausgewählt und zu einem System zusammengeführt.

Die Gerätehersteller beurteilen innerhalb eines Assessments ihre Geräte entsprechend den Normen.

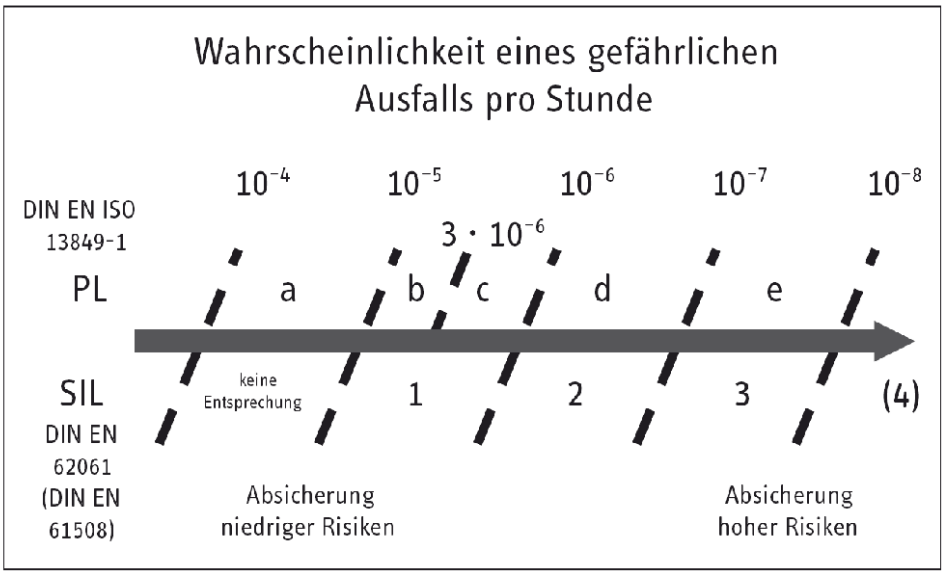


Bild 6-2 Wahrscheinlichkeiten, Zusammenhang SI-Level und P-Level

Bis zum Level 2 kann dies der Hersteller in eigener Verantwortung vornehmen; ab Level 3 wird dies durch einen unabhängigen Dritten durchgeführt, der nach erfolgreicher Zertifizierung ein entsprechendes Zertifikat ausstellt.

Für die Festlegung der Stufe der Sicherheitsintegrität ist zum einen eine Betrachtung des Ausfallverhaltens der betrachteten Baugruppe notwendig. Weiterhin wird in dem Assessment genau beurteilt, ob redundante Strukturen vorliegen, wie das Verhältnis zwischen sicheren Fehlern und unsicheren Fehlern ist und ob die Sicherheitsfunktion kontinuierlich oder auf Anforderung zu betrachten ist. Aus diesen Angaben werden dann die Ausfallraten bestimmt. Diese Kennwerte dienen einer Beurteilung des Sicherheitsintegritäts-Levels entsprechend den Vorgaben der Norm.

Die Betrachtung der Kennzahlen ist aber für die Einstufung der Geräte nicht hinreichend.

Es ist noch eine Betrachtung des Lebensdauerprozesses des Gerätes notwendig. Hierbei werden z. B. die sicherheitsgerichtete Konstruktion und ähnliche Bereiche betrachtet. Das Normenwerk gibt hier spezielle Maßnahmen für die einzelnen Stufen der funktionalen Sicherheit an.

Eine besondere Bedeutung hat dieser Bestandteil bei der Betrachtung von Betriebsmitteln mit komplexen Baugruppen, dies sind z. B. Mikroprozessoren, die über ein internes Programm verfügen. Hier werden in den Normen besondere Maßnahmen dargelegt, um auch auf Programmierfehler reagieren zu können.

Ein besonderes Problem stellen hier z. B. Fehler dar, die nicht durch eigene Entwicklungstätigkeiten entstehen, sondern schon in Softwarewerkzeugen wie Compilern und ähnlichem enthalten sind. Erst die Betrachtung aller Punkte lässt eine Einschätzung zu, ob sich das Betriebsmittel in einem Sicherheitskreis der entsprechenden Sicherheitsanforderungsstufe einsetzen lässt.

Eine Klassifizierung der einzelnen Baugruppen entsprechend dem Sicherheits-Integritätslevel ist nicht sinnvoll, da sich die Normenforderungen auf die Sicherheitskreise beziehen. Dies bedeutet, dass die

Festlegung der Stufe erst für die bekannte Zusammenschaltung der verschiedenen Betriebsmittel wie Sensoren, Aktoren, Steuerungselemente etc. getroffen werden kann.

7 Charakteristische Lebensdauer und Stress-Niveaus

Methoden zur Bestimmung des Produktrisikos aus Ausfallwahrscheinlichkeiten unter definierten Belastungs-Bedingungen („Stress-Levels“)

7.1 Charakteristische Lebensdauer

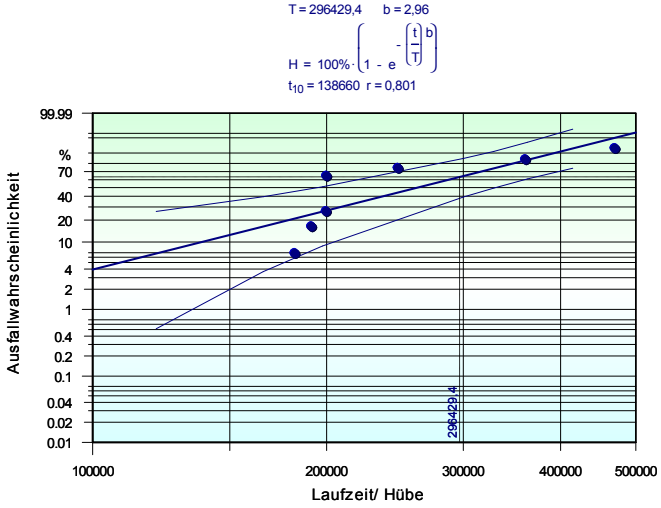


Bild 7-1 Bestimmung der Charakteristischen Lebensdauer durch Auswertung von Lebensdauerversuchen unter definierten Belastungs-Bedingungen; Charakteristische Lebensdauer(T) : Zahl der Ereignisse (z. B. mechanische Hübe) bei der 63,2 % der Einheiten ausgefallen sind.

7.2 Charakteristische Lebensdauer unter „Use-Stress“

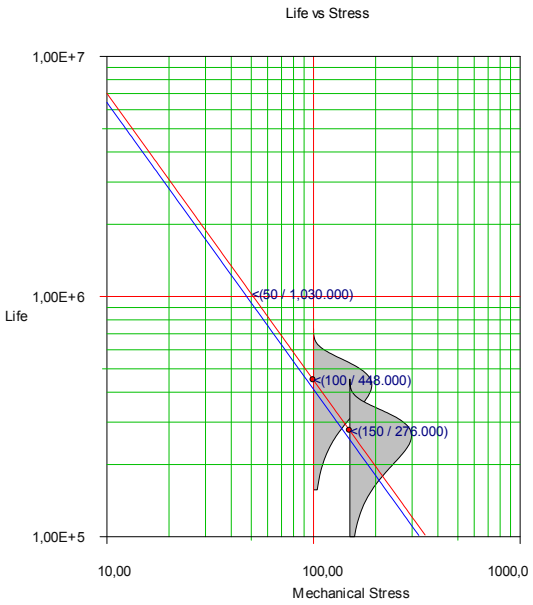


Bild 7-2 Lebensdauer-Stress-Diagramm eines mechanischen Systems; Ermittlung der charakteristischen Lebensdauer für den „Use Stress“ aus „Stress-Test-Verteilungen“

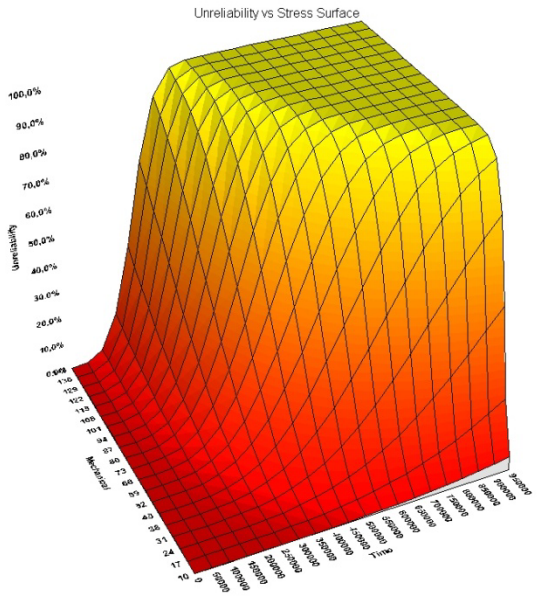


Bild 7-3 Dreidimensionale Darstellung: Zuverlässigkeit, Stress, Zeit (Zahl der Ereignisse)

8 Zur Person

Eur. Phys. Dipl.-Ing. Alfred Mörx

ÖVE, IEEE, Mitglied der New Yorker Akademie der Wissenschaften (NYAS),
eingetragen in das Register der Europäischen Physiker ; Mulhouse Cedex, France
Inhaber von diam-consult, Ingenieurbüro für Physik (www.diamcons.com) in Wien

Vorsitzender des Technischen Komitees *Elektrische Niederspannungsanlagen* im Österreichischen Verband für Elektrotechnik (OVE) sowie Mitarbeiter in zahlreichen nationalen, europäischen (CLC) und internationalen (IEC) technischen Komitees.