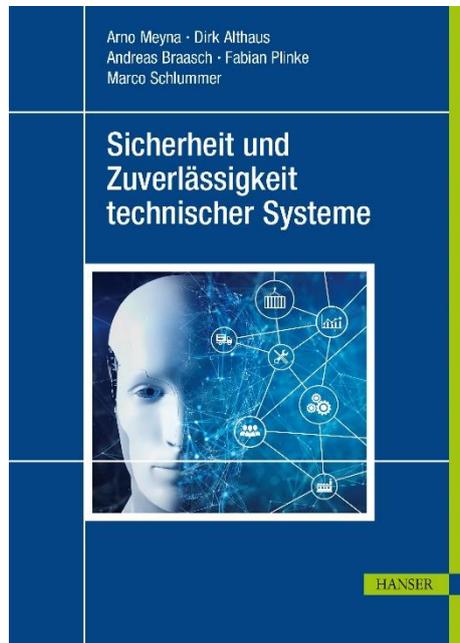


# HANSER



## Leseprobe

zu

## Sicherheit und Zuverlässigkeit technischer Systeme

von Arno Meyna, Dirk Althaus, Andreas Braasch,  
Fabian Plinke und Marco Schlummer

Print-ISBN: 978-3-446-46003-4

E-Book-ISBN: 978-3-446-46808-5

Weitere Informationen und Bestellungen unter

<https://www.hanser-kundencenter.de/fachbuch/artikel/9783446460034>

sowie im Buchhandel

© Carl Hanser Verlag, München

# Inhalt

<b>Vorwort</b> .....	<b>XVII</b>
<b>Das Institut für Qualitäts- und Zuverlässigkeitsmanagement (IQZ)</b> .....	<b>XIX</b>
<b>Teil I: Essenzielle Anforderungen an die Sicherheits- und Zuverlässigkeitstechnik</b> .....	<b>1</b>
<b>1 Herausforderungen für Staat, Gesellschaft und Unternehmen</b> .....	<b>3</b>
1.1 Fragmente der Explikation der Sicherheits- und Zuverlässigkeitstechnik .....	3
1.2 Aktuelle Herausforderungen .....	11
<b>2 Zuverlässigkeit bei Haftungs- und Gewährleistungsfragen</b> ...	<b>17</b>
2.1 Haftungsgrundlage .....	17
2.1.1 Außervertragliche Haftung .....	18
2.1.2 Vertragliche Haftung .....	19
2.1.3 Stand der Technik .....	20
2.1.4 Gewährleistungsmanagement zwischen Unternehmen .....	21
2.2 Schadteilanalyse Feld und No-Trouble-Found-Prozess .....	23
<b>3 Normative Anforderungen in der Sicherheits- und Zuverlässigkeitstechnik</b> .....	<b>26</b>
3.1 Einleitung zu normativen Anforderungen im rechtlichen Kontext ....	26
3.2 Überblick über die Begrifflichkeiten: Safety, Security und Reliability ..	31

<b>Teil II: Zuverlässigkeit im Produktentstehungsprozess</b> .....	<b>37</b>
<b>4 Zuverlässigkeit im Produktentwicklungsprozess</b> .....	<b>39</b>
4.1 Zuverlässigkeitsprozess .....	39
4.2 Bereiche, Rollen und Verantwortlichkeiten .....	46
4.3 Wirtschaftlichkeitsaspekte und Zuverlässigkeitsziele .....	48
4.4 Reifegrad, Musterstände und Freigabeprozesse in der Automobilindustrie .....	51
<b>5 Funktionale Sicherheit im Produktentwicklungsprozess</b> .....	<b>55</b>
5.1 Der sicherheitstechnische Prozess .....	55
5.1.1 Allgemeine Einführung in die Funktionale Sicherheit .....	55
5.1.2 Die Sicherheitsgrundnorm IEC 61508 .....	58
5.1.3 Der sicherheitstechnische Prozess in der zivilen Luftfahrtindustrie .....	62
5.1.4 Funktionale Sicherheit für Straßenfahrzeuge .....	74
5.2 Unterstützende und begleitende Prozesse als Grundvoraussetzung für die Funktionale Sicherheit .....	91
<b>6 Datenquellen und -management</b> .....	<b>100</b>
6.1 Rohdatenerfassung und -management .....	101
6.2 Nutzungsdaten .....	101
6.3 Felddaten .....	102
6.4 Datenschutz am Beispiel Automotive .....	105
<b>7 Nutzungs- und belastungsabhängige Produktentwicklung</b> ...	<b>108</b>
7.1 User Experience, Marktanalysen und Use Cases .....	110
7.2 Kundencluster und -profilerstellung .....	112
7.3 Design for Reliability, nutzungs- und belastungsabhängige Zuverlässigkeit .....	113
<b>Teil III: Grundlagen der Zuverlässigkeits- und Sicherheitsanalyse</b> ..	<b>115</b>
<b>8 Mathematische Grundlagen aus der Wahrscheinlichkeitsrechnung</b> .....	<b>117</b>
8.1 Mengenalgebra .....	117
8.1.1 Grundbegriffe und Definitionen .....	117

8.1.2	Mengenoperationen .....	118
8.2	Grundbegriffe der Wahrscheinlichkeitsrechnung .....	120
8.2.1	Wahrscheinlichkeitsbegriff .....	120
8.2.2	Axiomsystem von Kolmogorov .....	121
8.2.3	Die bedingte Wahrscheinlichkeit .....	124
8.2.4	Unabhängige Ereignisse .....	126
8.2.5	Regel von der totalen Wahrscheinlichkeit .....	126
8.2.6	Satz von Bayes .....	127
8.3	Zufallsgrößen und ihre Wahrscheinlichkeitsverteilung .....	129
8.3.1	Grundbegriffe .....	129
8.3.2	Erwartungswert und Momente einer Verteilungsfunktion ....	133
8.3.3	Quantil, Median und Modalwert .....	138
<b>9</b>	<b>Zuverlässigkeits- und Sicherheitskenngrößen .....</b>	<b>141</b>
9.1	Zuverlässigkeitskenngrößen nicht reparierbarer Systeme .....	141
9.2	Empirische Zuverlässigkeitskenngrößen und weitere Zuverlässigkeitsmerkmale .....	150
9.3	Zuverlässigkeitskenngrößen reparierbarer Systeme, Instandhaltung ..	153
9.4	Sicherheitskenngrößen .....	156
<b>10</b>	<b>Wichtige Verteilungsfunktionen .....</b>	<b>160</b>
10.1	Wichtige Lebensdauerverteilungen und ihre Zuverlässigkeits- kenngrößen .....	160
10.1.1	Exponentialverteilung .....	160
10.1.2	Weibull-Verteilung .....	164
10.1.3	Die spezielle Erlang-Verteilung .....	172
10.1.4	Die Normalverteilung .....	176
10.1.5	Die logarithmische Normalverteilung .....	179
10.1.6	Asymptotische Extremwertverteilung .....	184
10.2	Wichtige diskrete Verteilungsfunktionen .....	190
10.2.1	Binomialverteilung .....	190
10.2.2	Poisson-Verteilung .....	193
10.2.3	Hypergeometrische Verteilung .....	195

<b>11</b>	<b>Ausfallratenmodelle</b> .....	<b>201</b>
11.1	Zeitliches Verhalten der Ausfallrate .....	201
11.2	Ausfallratenangaben .....	202
11.3	Ausfallratendatenhandbücher .....	204
11.4	Ausfallratenmodelle .....	207
11.5	Zeitliche Schwankungen der Ausfallrate .....	214
 <b>Teil IV: Methoden der Zuverlässigkeits- und Sicherheitsanalyse</b> ...		<b>217</b>
<b>12</b>	<b>Einführung in die Methoden der Zuverlässigkeits- und Sicherheitstechnik</b> .....	<b>219</b>
12.1	Allgemeine Einführung .....	219
12.2	Methodenvergleich .....	223
<b>13</b>	<b>Zuverlässigkeitsanalyse einfacher Systemstrukturen</b> .....	<b>229</b>
13.1	Grafische Darstellung von Systemkonfigurationen .....	230
13.1.1	Zuverlässigkeits-Blockschaltbild .....	230
13.1.2	Fehler- oder Funktionsbäume: Darstellung mithilfe logischer Symbole der Booleschen Algebra .....	230
13.1.3	Zustandsdiagramme (Zustandsübergangsgraphen) .....	231
13.2	Logisches Seriensystem .....	232
13.3	Logisches Parallelsystem .....	233
13.4	Parallel-Seriensystem .....	237
13.5	Brückenkonfiguration .....	239
13.6	Berücksichtigung mehrerer Ausfallarten .....	242
13.6.1	Logisches Seriensystem bei zwei Ausfallarten .....	244
13.6.2	Logisches Parallelsystem bei zwei Ausfallarten .....	245
13.6.3	Logisches Parallel-Seriensystem bei zwei Ausfallarten .....	247
13.6.4	Beliebige Konfigurationen .....	250
<b>14</b>	<b>Zuverlässigkeitserhöhung in Planung und Praxis</b> .....	<b>252</b>
14.1	Allgemeine Maßnahmen zur Zuverlässigkeitserhöhung .....	252
14.2	Begriff und Definition der Redundanz .....	255
14.3	Redundanzarten, Grundprinzipien .....	256
14.4	Aktive Redundanz .....	257

14.5	mvn-System	258
14.6	nvn-System	262
14.7	Standby-System – passive Redundanz	265
<b>15</b>	<b>Systembetrachtung</b>	<b>269</b>
15.1	Begriffliche Exemplifikationen	269
15.2	Technisches System	270
15.3	Elektrik/Elektronik/Software-Systemarchitekturen	272
15.4	Ausfallverhalten von Elektrik/Elektronik/Software-Konfigurationen	273
<b>16</b>	<b>Boolesche Modellbildung</b>	<b>275</b>
16.1	Begriffe und Regeln der Booleschen Algebra	275
16.1.1	Die Boolesche Funktion	275
16.1.2	Grundverknüpfungen	277
16.1.3	Axiome der Booleschen Algebra	280
16.1.4	Karnaugh-Veitch-Diagramm	282
16.1.5	Kanonische Darstellung von Booleschen Funktionen	284
16.1.6	Shannonsche Zerlegung	290
16.1.7	Die Boolesche Funktion mit reellen Variablen	292
16.2	Die Systemfunktion	294
16.3	Einführung von Wahrscheinlichkeiten	297
16.4	Fehlerbaumanalyse	299
16.4.1	Einführung	299
16.4.2	Darstellung monotoner Strukturen durch Minimalpfade und Minimal Schnitte	302
16.4.3	Quantitative Fehlerbaumauswertung	306
16.5	Importanzkenngrößen	315
16.5.1	Strukturelle Importanz	315
16.5.2	Marginale Importanz	318
16.5.3	Fraktionale Importanz	320
16.5.4	Barlow-Proschan-Importanz	321
16.6	Bestimmung der mittleren Häufigkeit von Systemausfällen sowie der mittleren Ausfall- und Betriebsdauer	324
16.7	Induktive Zuverlässigkeits- und Sicherheitsanalyse	327

<b>17</b>	<b>Zuverlässigkeitsbewertung mithilfe der Fuzzy-Logik</b>	<b>330</b>
17.1	Grundlagen der Fuzzy-Logik	331
17.1.1	Verknüpfung unscharfer Mengen	334
17.1.2	Fuzzy-Relation	336
17.1.3	Erweiterungsprinzip	340
17.2	Prinzipieller Ablauf einer Fuzzy-Anwendung	341
17.2.1	Fuzzifizierung	342
17.2.2	Fuzzy-Inferenz	342
17.2.3	Defuzzifizierung	343
17.3	Anwendung der Fuzzy-Logik bei der FMEA	348
17.3.1	Eingangsgrößen	348
17.3.2	Fuzzifizierung	351
17.3.3	Verarbeitungsregeln	354
17.3.4	Berechnung der Zugehörigkeitsgrade	355
17.3.5	Defuzzifizierung	357
17.4	Fuzzy-Fehlerbaumanalyse	357
17.4.1	Das Fuzzy-Modell	358
17.4.2	Praktisches Anwendungsbeispiel	362
<b>18</b>	<b>Einführung in die stochastischen Prozesse</b>	<b>366</b>
18.1	Beurteilungskriterien stochastischer Prozesse	368
18.1.1	Definitionsspezifische Beurteilungskriterien	369
18.1.1.1	Markov-Bedingungen	369
18.1.1.2	Regenerationspunkte des Prozesses	369
18.1.2	Anwendungsspezifische Beurteilungskriterien	370
18.1.2.1	Akzeptanz von stochastischen Abhängigkeiten zwischen den Elementen des Prozesses	370
18.1.2.2	Anwendbare Verteilungsfunktionen der Zufallszeiten	370
18.1.3	Klassifizierung stochastischer Prozesse anhand der Beurteilungskriterien	371
18.2	Analysemöglichkeiten eines Parallelsystems mit zwei identischen Einheiten	373

<b>19</b>	<b>Markovsche Modellbildung</b> .....	<b>380</b>
19.1	Der Markovsche Prozess mit diskretem Parameterbereich und endlich vielen Zuständen (Markov-Kette) .....	380
19.1.1	Zustandsgleichung .....	380
19.1.2	Zustandsklassen .....	383
19.1.3	Die absorbierende homogene Markov-Kette .....	385
19.1.4	Ergodensatz für Markovsche Ketten .....	389
19.2	Der Markovsche Prozess mit kontinuierlichem Parameterraum und diskretem Zustandsraum .....	392
19.2.1	Zustandsgleichungen .....	392
19.2.2	Laplace-Transformation der Zustandsgleichung .....	398
19.3	Der Semi-Markov-Prozess .....	405
19.3.1	Einführung .....	405
19.3.2	Definition und Grundbegriffe .....	405
19.3.3	Der absorbierende Semi-Markov-Prozess .....	412
19.3.4	Der ergodische Semi-Markov-Prozess .....	416
<b>20</b>	<b>Monte-Carlo-Simulation</b> .....	<b>421</b>
20.1	Einführung .....	421
20.2	Grundlagen der Monte-Carlo-Simulation .....	423
20.3	Generierung von Zufallszahlen .....	425
20.4	Methoden zur Generierung beliebig verteilter Funktionen .....	429
20.5	Direkte Monte-Carlo-Simulation .....	432
20.5.1	Generierung eines Zustandsübergangs .....	432
20.5.2	Last-Event-Schätzer .....	434
20.5.3	Free-Flight-Schätzer .....	434
20.6	Anwendungsbeispiel .....	437
<b>21</b>	<b>Zuverlässigkeitsbewertung mithilfe der Graphentheorie</b> .....	<b>444</b>
21.1	Gerichteter Graph .....	445
21.1.1	Einige Grundbegriffe .....	445
21.1.2	Lineare Flussgraphen .....	447
21.1.3	Auswertung der linearen Flussgraphen mithilfe der Mason-Formel .....	450

21.2	Anwendung der linearen Flussgraphen auf diskrete Markov-Prozesse	453
21.2.1	Inhomogene Prozessdarstellung	453
21.2.2	Homogene Prozessdarstellung	454
21.2.3	Asymptotisches Verhalten	457
21.2.4	Erwartungswert und Eintrittswahrscheinlichkeit	457
21.3	Anwendung der linearen Flussgraphen auf stetige Markov-Prozesse	458
<b>22</b>	<b>Neuronale Netze</b>	<b>466</b>
22.1	Grundlagen	467
22.1.1	Das biologische Paradigma	467
22.1.2	Aufbau und Arbeitsweise eines künstlichen Neurons	468
22.1.3	Aufbau eines neuronalen Netzes	472
22.1.4	Arbeitsweise neuronaler Netze	473
22.2	Anwendung in der technischen Zuverlässigkeit	477
22.2.1	Neuronale Schätzung der Parameter einer Verteilungsfunktion	477
22.2.2	Neuronale Zuverlässigkeitsprognose	481
<b>Teil V: Zuverlässigkeitsprüfung und -bewertung</b>		<b>487</b>
<b>23</b>	<b>Stichprobenverteilung</b>	<b>489</b>
23.1	Stichprobenverteilung des Mittelwertes	489
23.2	Stichprobenverteilung der Varianz	493
23.3	Stichprobenverteilung der Mittelwerte bei unbekannter Varianz	494
23.4	Stichprobenverteilung für die Differenz und Summe zweier arithmetischer Mittelwerte	495
23.5	Stichprobenverteilung des Quotienten zweier Varianzen	497
<b>24</b>	<b>Grenzwertsätze und Gesetze der großen Zahlen</b>	<b>498</b>
24.1	Grenzwertsätze und Approximationen	498
24.1.1	Approximation der Binomialverteilung durch die Poisson-Verteilung	498
24.1.2	Approximation der hypergeometrischen Verteilung durch eine Binomialverteilung	498
24.1.3	Approximation der Poisson-Verteilung durch eine Normalverteilung	499

24.1.4	Approximation der Binomialverteilung durch die Normalverteilung .....	499
24.1.5	Approximation der hypergeometrischen Verteilung durch die Normalverteilung .....	500
24.1.6	Zentraler Grenzwertsatz .....	501
24.2	Gesetz der großen Zahlen .....	502
24.2.1	Tschebyscheffsche Ungleichung .....	502
24.2.2	Satz von Bernoulli .....	504
<b>25</b>	<b>Statistische Schätzung von Parametern .....</b>	<b>505</b>
25.1	Eigenschaften von Schätzfunktionen .....	505
25.2	Vertrauensintervalle .....	507
25.3	Konfidenzintervall für den Erwartungswert und die Varianz bei normalverteilter Grundgesamtheit und Bestimmung des Stichprobenumfangs .....	508
25.3.1	Konfidenzintervall für den Erwartungswert .....	508
25.3.2	Konfidenzintervall für die Varianz .....	512
25.3.3	Bestimmung des Stichprobenumfangs .....	513
25.4	Die Maximum-Likelihood-Methode (M-L-M) .....	517
25.4.1	Maximum-Likelihood-Schätzer für die Parameter der Binomial- und Poisson-Verteilung .....	520
25.4.2	Maximum-Likelihood-Schätzer für den Parameter einer Exponentialverteilung .....	521
25.4.3	Maximum-Likelihood-Schätzer für die Parameter der Normal- und Lognormalverteilung .....	521
25.4.4	Maximum-Likelihood-Schätzer für die Parameter der Weibull-Verteilung .....	521
25.5	Maximum-Likelihood-Methode bei zensierter und gestutzter Stichprobe .....	524
25.6	Die Momentenmethode .....	532
25.6.1	Momentenschätzer für den Parameter einer Exponentialverteilung .....	534
25.6.2	Momentenschätzer für die Parameter einer Lognormalverteilung .....	536
25.6.3	Momentenschätzer für die Parameter einer Weibull-Verteilung .....	536
25.7	Lineare Regression und die Methode der kleinsten Quadrate .....	536

<b>26</b>	<b>Bestimmung des Verteilungstyps</b>	<b>539</b>
26.1	Wahrscheinlichkeitsnetz der Weibull-Verteilung	539
26.1.1	Konstruktion des Wahrscheinlichkeitsnetzes	539
26.1.2	Gebrauchsanweisung für das Wahrscheinlichkeitsnetz der Weibull-Verteilung nach Stange und Gumbel (DGQ-Lebensdauernetz)	540
26.2	Tests zur Überprüfung des Verteilungstyps – Anpassungstests	547
26.2.1	Der Chi-Quadrat-Anpassungstest	547
26.2.2	Der Kolmogorov-Smirnov-Test (K-S-T)	552
26.3	Vergleich der beiden Anpassungstests	559
<b>27</b>	<b>Test- und Prüfplanung – Testverfahren</b>	<b>560</b>
27.1	Statistische Verfahren	564
27.1.1	Der Binomialprüfplan als attributiver Abnahmeprüfplan	564
27.1.2	Sequenzialprüfung	566
27.1.3	Success Run	569
27.1.4	Sudden-Death	574
27.1.5	Vorwissen und Test	581
27.1.6	End-of-Life-Test	581
27.2	Beschleunigte Lebensdauertests	583
27.2.1	Das Arrhenius-Modell	583
27.2.2	Das Eyring-Modell und dessen Modifikation	584
27.2.3	Das Peck-Modell	585
27.2.4	Dauerschwingversuch nach Wöhler	586
27.2.5	Hochbeschleunigte Testmethoden	590
<b>28</b>	<b>Felddatenanalyse</b>	<b>593</b>
28.1	Allgemeine Einführung	593
28.2	Schichtliniendiagramme und Beanstandungsverläufe	596
28.3	Zuverlässigkeitsprognosen für mechatronische Systeme in Kraftfahrzeugen bei nicht vollständigen Daten	604
28.3.1	Zuverlässigkeitsprognosen für Systeme im Kraftfahrzeug während der Nutzungsphase	604
28.3.2	Zuverlässigkeitsprognosen für zeitnahe Garantiedaten	610

<b>Literaturverzeichnis</b> .....	<b>616</b>
<b>Anhang A</b> .....	<b>631</b>
<b>Anhang B</b> .....	<b>649</b>
<b>Anhang C</b> .....	<b>655</b>
<b>Anhang D</b> .....	<b>657</b>
<b>Anhang E</b> .....	<b>660</b>
<b>Index</b> .....	<b>665</b>

Der Verlag und die Autoren haben sich mit der Problematik einer gendergerechten Sprache intensiv beschäftigt. Um eine optimale Lesbarkeit und Verständlichkeit sicherzustellen, wird in diesem Werk auf Gendersternchen und sonstige Varianten verzichtet; diese Entscheidung basiert auf der Empfehlung des Rates für deutsche Rechtschreibung. Grundsätzlich respektieren der Verlag und die Autoren alle Menschen unabhängig von ihrem Geschlecht, ihrer Sexualität, ihrer Hautfarbe, ihrer Herkunft und ihrer nationalen Zugehörigkeit.

# Vorwort

Sicherheit und Zuverlässigkeit zählen zu den wichtigsten Anforderungen, die heute an ein technisches System gestellt werden. Das vorliegende Werk zu dieser vielseitigen Thematik wurde durch ein Autorenteam des Instituts für Qualitäts- und Zuverlässigkeitsmanagement GmbH (IQZ) erstellt, das seit vielen Jahren auf dem Gebiet der Sicherheit und Zuverlässigkeit tätig ist und daher über ein breit gefächertes und fundiertes Spezialwissen verfügt.

Das Werk basiert einerseits auf Vorlesungs- und Seminarunterlagen sowie Abschlussarbeiten einschließlich Dissertationen, wobei Teilbereiche davon auch im Lehrbuch von Meyna/ Pauli (siehe Lit.) enthalten sind, das ebenfalls im Carl Hanser Verlag publiziert wurde, und andererseits auf Erkenntnissen der vielfältigen industriellen Projekte und dem damit verbundenen Erfahrungsschatz der Autoren.

Die Implementierung, die Erstellung der Bilder, Tabellen etc. sowie die umfangreiche Korrespondenz mit den Autoren und dem Verlag erfolgte durch Frau Xenia Rein, die mit Verve und vielen Anregungen am Gelingen des Werks einen erheblichen Anteil hatte. Dafür möchten sich die Autoren ganz herzlich bei Frau Rein bedanken.

Dem Lektor des Carl Hanser Verlags, Herrn Dipl.-Ing. Volker Herzberg, möchten die Autoren für seine vielen Anregungen und, insbesondere aufgrund der Covid-19-Pandemie, für das entgegengebrachte Verständnis und Vertrauen ihren Dank aussprechen.

Möge das Werk dazu dienen, die dargelegten Erkenntnisse der hochinteressanten Fachdisziplin *Zuverlässigkeits- und Sicherheitstechnik* in Forschung und Lehre sowie insbesondere in der Praxis zu nutzen, weiterzuentwickeln und damit zur Verbesserung der Qualität technischer Produkte einen Beitrag zu leisten.

Wuppertal/Hamburg im Dezember 2022

*Arno Meyna*

*Dirk Althaus*

*Andreas Braasch*

*Fabian Plinke*

*Marco Schlummer*

# Das Institut für Qualitäts- und Zuverlässigkeits- management (IQZ)

Alle Autoren dieses Buches sind Geschäftsführer bzw. leitende Mitarbeiter des Instituts für Qualitäts- und Zuverlässigkeitsmanagement GmbH (IQZ).



Ihr Qualitäts-Zulieferer.

Institut für Qualitäts- und Zuverlässigkeitsmanagement GmbH

[www.iqz-wuppertal.de](http://www.iqz-wuppertal.de)

Das IQZ wurde als innovatives Beratungsunternehmen aus der Bergischen Universität Wuppertal heraus gegründet und hat seine Geschäftstätigkeit im Juni 2012 aufgenommen. Das IQZ bietet seinen Kunden wissenschaftsnahe, lösungsorientierte und ganzheitliche Beratungsdienstleistungen, welche den Stand von Wissenschaft und Technik widerspiegeln, unter anderem in folgenden Bereichen:

Data Science

Funktionale  
Sicherheit

Maschinen-Sicherheit

Warranty  
Management

Zuverlässigkeits-  
Management

Risikomanagement

Qualitätsmanagement

Durch die enge Kooperation mit der Bergischen Universität Wuppertal und der Hochschule Ruhr West kann das IQZ nicht nur auf innovative Methoden nach Stand von Wissenschaft und Technik zurückgreifen, sondern deckt, durch jahrelange Projekterfahrung im Kontext namhafter Unternehmen, auch mehrere Jahrzehnte Facherfahrung im Sicherheits- und Zuverlässigkeitsmanagement ab. Daher können selbst komplexe Beratungs- und Forschungs-

aufträge durch das IQZ erbracht werden, immer mit dem Fokus, maßgeschneiderte Konzepte für die Kunden zu entwickeln und diese Konzepte pragmatisch in die Praxis umzusetzen.

Neben den Forschungs- und Entwicklungsprojekten im Rahmen des Produktentstehungs- und Produktbeobachtungsprozesses von der Planung, Entwicklung, Produktion, Nutzung bis zur Entsorgung in vielen industriellen Bereichen ist das IQZ seit vielen Jahren auch im Haftungs- und Versicherungsbereich mit Tätigkeiten betraut. Dies beinhaltet z. B. die Haftungsabwehr und Verhandlungsunterstützung im Regressfall oder Gutachtertätigkeiten für Versicherungskonzerne. Namhafte, weltweit agierende Versicherer sowie führende Anwaltskanzleien im Bereich Produkthaftung gehören hier zu unseren langjährigen Partnern. Das Kundenspektrum des IQZ reicht vom Kleinstunternehmen, kleinen und mittleren Unternehmen (KMU) bis zum DAX-30-Unternehmen z. B. in der Automobil- und Luftfahrtindustrie.

### **Kontakt**

Institut für Qualitäts- und Zuverlässigkeitsmanagement GmbH

Heinz-Fangman-Str. 4

42287 Wuppertal

Tel.: +49(0)202/515 616 90

Fax: +49(0)202/515 616 89

Mail: [info@iqz-wuppertal.de](mailto:info@iqz-wuppertal.de)

# Teil I:

## Essenzielle Anforderungen an die Sicherheits- und Zuverlässigkeitstechnik

*„Der Mangel an Gewissheit ist die wichtigste Quelle unseres Wissens.“*

*Carlo Rovelli (\* 1956)*



# 1

## Herausforderungen für Staat, Gesellschaft und Unternehmen

### ■ 1.1 Fragmente der Explikation der Sicherheits- und Zuverlässigkeitstechnik

#### Ein kurzer kulturhistorischer Rückblick

Sicherheits- und Zuverlässigkeitstechnik als interdisziplinäres Wissenschaftsgebiet ist eng mit der Entwicklung der Naturwissenschaft und Technik, aber auch mit der Gesellschaft und dem einzelnen Menschen selbst verbunden.

Der moderne Mensch (*Homo sapiens*, lat. „der weise, kluge Mensch“) wird gegenwärtig auf ein Alter von ca. 233 000 Jahren datiert, bezogen auf Knochen und Schädelfragmente des „Kibish Oma I“ in Ägypten (neue Erkenntnisse von Celine Vidal et al., publiziert in der englischsprachigen renommierten Fachzeitschrift „nature“), und breitete sich vom afrikanischen Kontinent ausgehend nach Europa aus. Nachgewiesen sind der *Homo sapiens* und der Neandertaler in Vorderasien vor etwa 40 000 Jahren und in Mitteleuropa vor ca. 10 000 Jahren. Die Begleitfunde, wie Pfeilspitzen, Faustkeile, Steinbeile etc., zeigen die enge Verbundenheit des modernen Menschen mit der Technik. Demnach war der Mensch bei seinem Erscheinen auf der Erde sogleich Techniker. Technik ist also menschliche Uranlage (sinngemäß nach Spengler).

Oswald Spengler schreibt weiter (siehe Lit.):

*„Um das Wesen des Technischen zu verstehen, darf man nicht von der Maschinenteknik ausgehen, am wenigsten von dem verführerischen Gedanken, daß die Herstellung von Maschinen und Werkzeugen der Zweck der Technik sei.“*

Mit der Entwicklung der menschlichen Sprache und der Hochkulturen in Ägypten und Mesopotamien entstand eine neue Qualität der Naturwissenschaft, Technik und Gesellschaft. Es entstanden technische Glanzleistungen, die heute noch bewundert werden, wie z. B. die Pyramiden von Gizeh oder die Megalithbauten in Spanien, deren Errichtung nur durch die systematische Nutzung der damaligen Naturwissenschaft und Technik, verbunden mit einem großen Einsatz von Mensch, Tier und Organisation, ermöglicht wurde.

Im Gegensatz zur „*Techné*“ als Inbegriff allen Könnens, das auf Wissen begründet ist, z. B. Malen und Musizieren als persönliche Fertigkeit, ist die Technik durch Ziele, z. B. Totenkult, und Zwecke, z. B. Bau einer Pyramide, charakterisiert. Nach Dessauer (siehe Lit.) sind technische Objekte durch Raumformen (räumliche Gebilde, ein Gerät, eine Maschine) und Zeit-

formen (eine Methode, ein Verfahren) gekennzeichnet, die aufgrund ihrer Finalität über den technischen Bereich hinausweisen können.

*„Technik kann also mit Recht ein Real-Sein und Real-Werden aus Ideen genannt werden, ein dauerndes Hinüberschreiten von Zweckformen aus der Immanenz in die Erfahrungswelt, die hierdurch im Zeitverlauf bereichert wird“ (Dessauer).*

Nach Bringmann ist Technik mehr als eine Maschine, ein Produktionsprozess; Technik ist selbst Wissenschaft. Donald Bringmann schreibt hierzu im Werk von Dessauer mit dem Titel „Streit um Technik“ (siehe Lit.):

*„Wer in der Technik nur eine angewandte Wissenschaft sieht, lässt das Wesentliche unbetrachtet, das in den technischen Erfindungen und Konstruktionen steckt: jene irrationale seelische Triebkraft, die sich in allen noch so zweckrationalen technischen Gebilden zugleich verbirgt und kundgibt.“*

Betrachtet man nun die Entwicklung der Sicherheits- und Zuverlässigkeitstechnik als wissenschaftliche Teildisziplin der Technik, so war und ist diese zunächst final mit der technologischen Entwicklung selbst verbunden. Die frühen Menschen kannten den Nutzen ihrer Waffen und Gerätschaften, aber auch die Gefahren, die mit einer unsachgemäßen Benutzung verbunden waren. Durch die Weiterentwicklung der Technik gelang es den Menschen jedoch, den vielfältigen Urfahren der Natur und Tierwelt entgegenzutreten und ihre Lebensgrundlage zu sichern.

Nachgewiesen ist auch, dass es zur Zeit der ersten Hochkulturen bereits ein – wie wir heute sagen würden – sicherheitstechnisches Recht gab. Bekannt ist in diesem Zusammenhang der Codex, der unter der Herrschaft des Hammurapi (auch Hammurabi), 6. König der ersten Dynastie (1792 bis 1750 v. Chr.), im altbabylonischen Reich (Babylon wurde 1894/1830 v. Chr. vom semitischen Stamm der Amoriter unter Sumu-abum gegründet) entstand, als älteste bekannte Gesetzessammlung – mit 270 Rechtsgrundsätzen für das tägliche Leben – der Welt, aufgezeichnet auf einer ca. 2,25 m hohen Stele, die 1902 bei Ausgrabungen in Susa gefunden wurde und sich heute im Louvre in Paris befindet (Wikipedia).

Für den Sicherheitstechniker interessant ist in diesem Zusammenhang der Codex der Haftung, welcher in den §§ 228 bis 233 (DIN Mitteilungen, 10/78) beschrieben ist:

- *„Wenn ein Baumeister ein Haus für einen Mann baut und es für ihn vollendet, so soll dieser ihm als Lohn zwei Sekel Silber geben für je ein Sar Haus: (Anm.: 1 Sekel = 360 Weizenkörner = 9,1 Gramm, 1 Sar = 14,88 m<sup>2</sup>).“*
- *„Wenn ein Baumeister ein Haus baut für einen Mann und macht seine Konstruktion nicht stark, so dass es einstürzt und verursacht Tod des Bauherrn: dieser Baumeister soll getötet werden.“*
- *„Wenn der Einsturz den Tod eines Sohnes des Bauherrn verursacht, so sollen sie einen Sohn des Baumeisters töten.“*
- *„Kommt ein Knecht des Bauherrn dabei um, so gebe der Baumeister einen Knecht von gleichem Wert.“*
- *„Wird beim Einsturz Eigentum zerstört, so stelle der Baumeister wieder her, was immer zerstört wurde; weil er das Haus nicht fest genug baute, baut er es auf eigene Kosten wieder auf.“*
- *„Wenn ein Baumeister ein Haus baut und macht die Konstruktion nicht stark genug, so dass eine Wand einstürzt, dann soll er sie auf eigene Kosten verstärkt wieder aufbauen.“*

Weiter findet sich in der Bibel der Juden (600 bis 200 v. Chr.) (5. Buch Moses, 22/8):

*„Wenn du ein neues Haus baust, sollst Du um die Dachterrasse eine Brüstung ziehen. Du sollst nicht dafür, dass jemand herunterfällt, Blutschuld auf Dein Haus laden.“*

Der vorangehend aufgeführte Codex der Haftung zeigt, dass der Baumeister eines Hauses bereits vor 4000 Jahren die Sicherheit implementierte, d.h. nach heutigem Verständnis „in ein Produkt/einen Produktionsprozess hineinentwickelte“. Neben den Gefahren durch die Technik war der Mensch seit jeher einer Vielzahl natürlicher Gefahren einschließlich gesellschaftsbedingten und politischen Gefahren – wie die vielen Kriege und die damit verbundenen schrecklichen Auswirkungen zeigen – ausgesetzt. Nach Heidegger<sup>1</sup> ist die menschliche Existenz ein „*Sein zum Tode*“. Unbestritten ist jedoch, dass die stetig fortschreitende technische Zivilisation umfassende ökonomische, medizinische und soziale Vorteile mit sich brachte, ein „menschwürdiges Leben“ ermöglichte und zu einer erheblichen Verlängerung des menschlichen Lebens führte. Diese Kohärenz von Mensch und Technik als Grundpfeiler von Lebensqualität, Freiheit und Entfaltung wurde mit der Entwicklung großtechnischer Systeme und deren möglichen negativen Auswirkungen für Mensch und Umwelt, die sich aufgrund neuer naturwissenschaftlicher und technischer Erkenntnisse feststellen ließen, zu Beginn des 20. Jahrhunderts zur Inkohärenz und ist heute Gegenstand kontroverser Diskussionen über das „Für und Wider der Technik“.

Ratzinger schrieb hierzu (siehe Lit.):

*„Wenn es zutrifft, daß der innere Ausgangspunkt der Technik in der Erringung von Freiheit durch Gewähren von Sicherheit lag, so muß es von da aus auch die innere Forderung jeder technischen Entwicklung und ihr eigenes Leitmaß sein, sie so zu gestalten, daß daraus nicht größere Unsicherheit und in der Steigerung von Abhängigkeiten größere Unfreiheit entsteht. Sie wird dabei erkennen müssen, daß nicht (wie es anfangs aussah) technisches Tun als solches schon befreiendes und damit sittliches Tun ist, daß aber technisches Tun von sittlichen Maximen geleitet sein muß, um seinem eigenen Ursprung zu genügen, der in einer sittlichen Idee lag.“*

Die systematische Analyse von Gefahrenpotenzialen gleich welcher Art, denen der Mensch in seinem Dasein ausgesetzt ist, deren Risiken er bewusst oder unbewusst eingeht, und die Entwicklung von entsprechenden Schutz- und Verhaltensmaßnahmen zu deren Bewältigung sind seit jeher Aufgabe der entsprechenden wissenschaftlichen Fachdisziplinen der Naturwissenschaft, Ingenieurwissenschaft, Mathematik, Geistes- und Gesellschaftswissenschaft, Medizin und Psychologie sowie deren Spezialisierungen, da nur in diesen das entsprechende Fachwissen vorhanden ist.

Allerdings zeigte es sich, dass die methodische und inhaltliche Fokussierung auf eine oder mehrere Fachdisziplinen der Bedeutung der Sicherheit für den einzelnen Menschen, aber auch die Gesellschaft mit ihrem ethischen, humanen, wirtschaftlichen und politischen Grundverständnis nicht gerecht wird. Hierzu schrieben Peters und Meyna im Vorwort (siehe Lit.):

*„Die Sicherheitstechnik ist eine interdisziplinäre Wissenschaft, deren Schwerpunkt traditionell die Ingenieurwissenschaften bilden. Aber auch die Human- und Sozialwissenschaften, Recht, Ökonomie, Management, Personen- und Objektschutz, Rettungswesen, Umweltschutz, Datenschutz u. a., leisten heute einen nicht unerheblichen Beitrag zur Reduzierung und Bewertung des Risikos und der sicheren Nutzung eines Mensch-Maschine-Umwelt-Systems.“*

<sup>1)</sup> Martin Heidegger (1889 – 1976)

## Risiko in der modernen globalen Industriegesellschaft

Wie bereits dargelegt, sind der Mensch in seinem Dasein und die Gesellschaft vielfältigen natürlichen und zivilisationsbedingten Risiken ausgesetzt. Die Herkunft des Begriffs Risiko ist nicht eindeutig geklärt. Vielfach wird von einem arabischen Ursprung mit dem Ausdruck „risqu“ (von Gottes Gnaden abhängiger Lebensunterhalt) bzw. vom im Mittelalter ins Italienische übernommenen „risico“ (Wagnis, Gefahr bei einer Schiffsreise oder militärischen Unternehmen) ausgegangen.

Mit Risiko wird heute in der Regel das Produkt aus der Eintrittswahrscheinlichkeit eines bestimmten Ereignisses und dem Schadensausmaß (Ereignisschwere) bezeichnet (siehe Abschnitt 9.4).

Durch Logarithmierung und Darstellung als Geradengleichung erhält man eine Gerade gleichen Risikos (Bild 9.5). Das heißt, ein formal gleiches Risiko tritt bei geringer Eintrittswahrscheinlichkeit und großen Auswirkungen (z. B. bei einem Flugzeugabsturz), aber auch bei einer großen Eintrittswahrscheinlichkeit und geringeren Auswirkungen (z. B. im Straßenverkehr) ein.

Interessant ist in diesem Zusammenhang, dass in der Bevölkerung bezüglich des Erstgenannten eine Risikoaversion besteht. Es wurde deshalb vorgeschlagen, einen Risikoaversionfaktor in die Risikobeurteilung einzufügen. Allerdings fehlt hierfür die wissenschaftliche Grundlage. Problematisch ist jedoch, dass vielfach von „punktförmigen“ Risiken, z. B. Toten/Jahr und Einwohnern, ausgegangen wird und entsprechende Vergleiche z. B. für tödliche Arbeitsunfälle nach Wirtschaftszweigen oder Vergleiche von statistisch abgesicherten natürlichen Risiken mit probabilistisch ermittelten technischen Risiken (z. B. Kernkraftwerke) erfolgen, um so eine gewisse Akzeptanz zu ermöglichen (siehe deutsche Risiko-studie, „Kernkraftwerke“, siehe Lit.). Geht man davon aus, dass die Eintrittshäufigkeit (Wahrscheinlichkeit) durch eine entsprechende Verteilungsfunktion und die Ereignisschwere durch eine weitere entsprechende Funktion gegeben ist, so ist auch das Risiko durch eine entsprechende Zeit-Orts-Funktion gegeben.

Das zivilisationsbezogene Risiko ist immer mit einer menschlichen Handlung verbunden, deren Folgen nicht absehbar sind. Es müssen vielfach Entscheidungen getroffen werden, auch dann, wenn nicht alle Fakten und Sachverhalte überprüfbar und bekannt sind. Als weiterer Faktor ist die Kontrollierbarkeit der möglichen Folgen (z. B. von Atomkraft, Gentechnik, neuen Technologien → Technikfolgenabschätzung) von großer Bedeutung. Problematisch ist aber auch die Bewertung der zukünftigen Eintrittswahrscheinlichkeit eines Ereignisses aus den bisher ermittelten, zumal sich die Randbedingungen ständig ändern können. Ferner ist die Freiwilligkeit, mit der der Einzelne oder bestimmte gesellschaftliche Gruppierungen ein Risiko eingehen, von Bedeutung. So gesehen stellt das Risiko eine mehrdimensionale Größe dar.

Der Begriff des Risikos wird oft synonym zum Begriff der Gefahr (gevare, mittelhochdeutsch „Hinterhalt“, „Betrug“) verwendet. Die Gefahr als Möglichkeit eines zukünftigen Schadens oder Nachteils ist im Gegensatz zum vordefinierten objektiven Risiko eine qualitative Größe für die Kennzeichnung einer natürlichen oder zivilisationsbedingten Gefahrenquelle. Diese sind nicht immer latent vorhanden und können unbekannt sein.

Als komplementäre Größe wird vielfach der Begriff der Sicherheit verwendet. Im Sinne der Sicherheitstheorie ist die additive Verknüpfung von Sicherheitswahrscheinlichkeit und Gefährdungswahrscheinlichkeit durch eins gegeben (siehe Abschnitt 9.4). Das heißt, wenn

keine Gefährdung vorliegt, z. B. keine Lawinengefahr im Mittelgebirge im Sommer, so ist die Sicherheit durch 100 % (d. h. eine absolute Sicherheit) gegeben.

Mit dem Begriff der Gefahr werden häufig zeitliche Abstände, z. B. eine konkrete Gefahr, eine aktuelle Gefahr, eine Gefahr im Verzug, und Wahrscheinlichkeiten, wie z. B. eine abstrakte Gefahr, miteinander verknüpft. In diesen Fällen ist die Quantifizierung über das objektive Risiko aussagefähiger. Dabei ist zu beachten, dass ein Risiko nur dann vorhanden ist, wenn eine Gefahr und eine Exposition gegenüber derselben gegeben sind. So sind beispielsweise die Gefahren des Straßenverkehrs für den Nichtteilnehmer irrelevant, für die Gesellschaft aber sehr bedeutend. Das heißt, eine Gefahr ist in der Regel immer durch einen örtlich und zeitlich begrenzten Gefahrenwirkungsbereich charakterisiert, wobei dieser jedoch fließend und global wirkend sein kann (z. B. Atomkatastrophen von Tschernobyl, 1986, Fukushima, 2011, Giftgasunfälle in Seveso, 1976, und Bophal, 1984).

Die örtlichen und zeitlichen Auswirkungen können auch den Lebensraum für nachfolgende Generationen stark einschränken. Das bedeutet aber auch, dass zu den global wirkenden natürlichen Katastrophen (Klima, Krankheiten, Seuchen und andere) und den durch die Gesellschaft selbst verursachten Katastrophen (z. B. Krieg, Terrorismus) eine neue Qualität des Risikos, begründet durch den naturwissenschaftlichen und technischen Fortschritt, hinzugekommen ist.

Nach Bieri ist Risiko ein Bestandteil des menschlichen Daseins, eine risikofreie Lebensform ist nicht denkbar und gleichbedeutend mit dem Tod. Ernst Bieri (siehe Lit.) schreibt hierzu treffend:

*„Kein Leben und damit auch keine Technik ohne Risiko: Man kann und soll das Risiko durch den Einsatz des verfügbaren Wissens und Könnens auf ein Minimum herabdrücken, und diese Marschrichtung ist von der Technik eingeschlagen worden, von der Verbesserung der Maschinen in den Fabriken über die Verkehrsmittel aller Art, bis zu den Anlagen für Energiegewinnung und den Umweltschutz. Aber jedes Risiko vollständig und für alle Zukunft ausschalten zu wollen, das wäre Hybris, wäre die Anmaßung der Allmacht durch den Menschen. Das Ende der von uns überblickbaren Risiken tritt mit dem Tod ein. Wer also jedes Risiko ausschalten will, beendet das menschliche Leben, das ohne Risiko, ohne Angst, aber auch ohne den dauernden und über weite Strecken erfolgreichen Kampf dagegen nicht möglich ist.“*

Die Ermittlung von Gefahrenpotenzialen und Risiken bis zu einem gewissen Grad beherrschbar zu machen, ist eine interdisziplinäre Aufgabe der Sicherheits- und Zuverlässigkeitstechnik. Allerdings tritt in diesem Zusammenhang sofort die Frage nach der Akzeptanz eines verbleibenden Risikos auf, d. h. das Abwägen zwischen dem Nutzen (z. B. einer neuen Technologie, eines neuen Medikamentes) und den möglichen Schäden für den Menschen und seinen Lebensraum (Arbeitswelt, Umwelt, Gesundheit und anderes). Als Beispiel hierzu sei die kontrovers geführte Diskussion über das Für und Wider der Kernenergie aufgeführt. Das Beispiel zeigt auch die zeitliche Veränderbarkeit der Bewertung von Risiken durch die Gesellschaft und insbesondere durch bestimmte Gruppierungen der Gesellschaft, unabhängig von neuen wissenschaftlichen Erkenntnissen. Karl Steinbuch schreibt hierzu (siehe Lit.):

*„Die Akzeptanz technischer Risiken hat drei Dimensionen:*

*Erstens die technische Dimension: Die Verminderung technischer Risiken durch Menschen, Methoden oder Material.*

*Zweitens die pädagogische Dimension: Die Aufklärung über die Zwangsläufigkeit mancher Risiken.*

*Drittens die ethische Dimension: Die Erzeugung von Verantwortung und Vertrauen.*

*Auf diesem Gebiet wurde in den letzten Jahren vieles versäumt – wir alle werden hierunter leiden: Das Vertrauenspotential entscheidet über den erreichbaren Wohlstand – die Zerstörung des Vertrauenspotentials (z. B. durch Konfliktideologie oder Skandalpublizistik) führt zwangsläufig zur Verminderung unseres Wohlstandes.“*

Das Erkennen einer Gefahr und die Beurteilung des Risikos mit seiner Eintrittswahrscheinlichkeit und den möglichen Schadensauswirkungen ist a priori immer mit mehr oder weniger großen Unsicherheiten verbunden, da besonders bei seltenen Ereignissen eine statistische Verifizierung nicht möglich ist. Folglich gibt es kein sogenanntes „Restrisiko“ und „Sicherheitsrisiko“. Dies gilt auch für die Schadensauswirkungen.

Thomas A. Jäger schreibt hierzu (siehe Lit.):

*„Die lange Inkubationszeit der physischen Schädigung des Menschen durch schleichend akkumulierende Umwelteinflüsse, wie Wasser- und Luftverschmutzung oder durch in Nahrungsmitteln enthaltene Schadstoffe, macht das Erkennen der Zusammenhänge schwierig. Das gleiche gilt für die physische und psychische Schädigung durch Lärm. Der Nachweis gesundheitlicher Schädigungen ist umso schwieriger, als die Symptome schleichend und nicht eindeutig und ihre Quellen überaus vielfältig sind. Wenn jemand durch schädigende Umwelteinflüsse in seiner Vitalität herabgesetzt oder gar krank ist, so fällt dies lange Zeit nicht weiter auf und die Ursachen bleiben im Nebel.“*

Ungeachtet dessen zeigen die in diesem Zusammenhang vielfältig eingesetzten wissenschaftlichen Methoden, Verfahren, Simulationen und anderes zur Sicherheit, Zuverlässigkeit, Gesundheit, Umweltverträglichkeit, Schutz, dass Risiken objektiviert und minimiert werden können. Das Grundgesetz der Bundesrepublik Deutschland sagt hierzu in Artikel 1 unmissverständlich:

*„(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.“*

### **Zum Paradigma der Sicherheits- und Zuverlässigkeitstechnik**

Aufgrund der zuvor erläuterten engen Verknüpfung der Sicherheits- und Zuverlässigkeitstechnik mit den Natur- und Technikwissenschaften und deren deterministischem Weltbild (jeder Vorgang hat eine Ursache, die Wirkung kann sich höchstens mit der endlichen Lichtgeschwindigkeit ausbreiten) ist dieser Kausalnexus des klassischen Determinismus auch Paradigma der Sicherheits- und Zuverlässigkeitstechnik.

Die Determiniertheit der Welt und des Menschen im Kontext von „Willensfreiheit und bedingtem freien Willen“ ist bis in unsere heutige Zeit Gegenstand philosophischer, psychologischer, neurophysiologischer und anderer Betrachtungen.

Ungeachtet dessen ist der naturwissenschaftliche und technische Fortschritt seit Newton<sup>2</sup> und Laplace<sup>3</sup> durch den Determinismus geprägt. Nach Laplace ist die Zukunft durch die Gegenwart (Anfangsbedingung z. B. einer Differenzialgleichung) eindeutig bestimmt (siehe

<sup>2)</sup> Isaac Newton (1643 – 1727)

<sup>3)</sup> Pierre-Simon Laplace (1749–1827)

auch das Gedankenkonstrukt des „Laplaceschen Dämons“ als einer „Intelligenz“, die befähigt ist, alle Determinationen und Faktoren in Vergangenheit und Zukunft genauestens zu kennen). Dem gegenüber steht das indeterministische Weltbild der Quantenmechanik (Heisenberg<sup>4</sup>, Born<sup>5</sup>, Schrödinger<sup>6</sup> und andere), d. h. die Nichtbestimmtheit der Ursachen bei physikalischen Vorgängen – Zukunft ist nur durch stochastische Modellbildung (Zufalls-Prozess) bestimmbar –, welches in Widerspruch zum Laplaceschen Weltbild steht (siehe auch 2. Hauptsatz der Thermodynamik). Man beachte in diesem Zusammenhang aber auch die streng deterministische Position von Albert Einstein<sup>7</sup> „Gott würfelt nicht“ (sinngemäß aus dem Briefwechsel mit Max Born (siehe Lit.)), die heute jedoch für den Mikrokosmos als widerlegt angesehen wird.

Ähnlich wie in der Physik fand unter anderem durch die Arbeiten von Wöhler, Weibull (siehe Lit.) und weiteren Autoren im Bereich der Werkstoffermüdung und insbesondere in den 40er- und 50er-Jahren durch Pieruschka und Lusser die Stochastik als „Systemdenken“ Einzug in die Ingenieurwissenschaften. So schreibt Pieruschka, der sein Buch Robert Lusser widmete, im Vorwort (siehe Lit.):

*„In the year 1943, the author became, for the first time, aware of the reliability problem during flight testing of the German V-1 missile. Intensive studies of this subject were started in 1954 upon coming to the United States. In the subsequent eight years, the author has completed a great amount of study in the field of reliability theory as research scientist with the Army Rocket and Guided Missile Agency, Redstone Arsenal, Alabama, and with the Lockheed Missile and Space Company, Sunnyvale, California.“*

Weiter heißt es auf Seite 47:

*„The Swiss mathematician Jakob Bernoulli developed the rule which published 1713. Robert Lusser has been stressing the serious consequence of the product rule in the achievement of reliability in complex equipments since the year 1950, and by this insistence has brought into being reliability as a serious profession. Therefore, Formula (siehe Formel 13.1) is called Robert Lusser's reliability formula.“*

Die zweite Auflage des 1962 erschienenen Buches von Igor Bazovsky (siehe Lit.) stellt ebenfalls die Pionierleistungen von Lusser (Seite 275) und Pieruschka (Seiten 60 und 71) heraus.

*„Another historical development in the same direction took place in Germany during the Second World War. Robert Lusser, one of the reliability pioneers, narrates how he and his colleagues, while working with Wernher von Braun on the V1 missile, met with the reliability problem. The first approach they took towards V1 reliability was that a chain cannot be stronger than its weakest link. Thus, the missile will be as reliable as the weakest link can made, or as strong.“*

Nicht unerwähnt sei, dass bereits 1954 (danach jährlich) in den USA das 1. National Symposium on Reliability and Quality Control der IEEE und in Deutschland 1961 (danach alle zwei Jahre) die erste Tagung über Zuverlässigkeit stattfand. Auf Anregung von Ludwig Bölkow, einem der großen Förderer der Deutschen Zuverlässigkeit (siehe Lit.), wurde bereits

---

<sup>4</sup> Werner Heisenberg (1901–1976)

<sup>5</sup> Max Born (1882–1970)

<sup>6</sup> Erwin Schrödinger (1887–1961)

<sup>7</sup> Albert Einstein (1879–1955)

1964 der Fachausschuss „Zuverlässigkeit und Qualitätskontrolle“ beim VDI gegründet. Es entwickelte sich die Zuverlässigkeitstheorie als stochastische Theorie zur Bewertung komplexer Mensch-Maschine-Umweltsysteme. Das Paradigma der Zuverlässigkeitstheorie ist das stochastische Ausfall- bzw. Lebensdauerverhalten von Komponenten und Systemen. Das heißt, die Lebensdauer einer Komponente – wie die des Menschen – ist eine Zufallsvariable. Die Zuverlässigkeitstheorie verfügt wie in diesem Buch dargestellt über ein theoretisches Konzept, einschließlich Methoden, Verfahren und Kenngrößen zur qualitativen und quantitativen Bewertung technischer Systeme gleich welcher Art. Da die Sicherheit als Teilmenge der Ausfall- und Betriebszustände eines Systems angesehen werden kann, ist diese isomorph; das bedeutet, das theoretische mathematische Gebäude der Zuverlässigkeitstheorie bildet auch das theoretische Gebäude der stochastischen Sicherheitstechnik. Die stochastische Modellbildung kann allerdings eine deterministisch orientierte Sicherheits- und Zuverlässigkeitstechnik nicht ersetzen, sondern ermöglicht a priori eine Bewertung im frühen Entwicklungsstadium und im Rahmen des Produktentstehungsprozesses (siehe Kapitel 4) und der Test- und Prüfplanung (siehe Kapitel 27). Die vorangegangenen Betrachtungen zeigen, dass die Paradigmen der Sicherheits- und Zuverlässigkeitstechnik durch den Nexus von Determinismus und Indeterminismus geprägt sind. Allerdings fehlt in diesen Paradigmen eine Unbekannte, und dies ist der Mensch als Individuum und Mittelpunkt des Seins, eingebunden in Gesellschaft, Umwelt, Technik mit all ihren kulturellen und traditionellen Unterschieden. Albert Kuhlmann schlägt deshalb einen „kybernetischen“ Ansatz der Sicherheitswissenschaft vor (siehe Lit.):

*„Die Verknüpfung zwischen Kybernetik und Sicherheitswissenschaft ergibt sich daraus, dass technische Einrichtungen von Menschen bedient und kontrolliert werden, die sich selbst im Wirkungsbereich dieser technischen Einrichtung befinden. Sie nutzen die Maschine, sind aber auch ihren Gefahren für Leib, Leben und Sachen ausgesetzt. Das menschliche Verhalten sowie das Verhalten der Maschine sind wiederum von den Bedingungen der Umwelt abhängig. Die Umwelt technischer Einrichtungen wird ihrerseits oft von ihnen vielfältig beeinflusst, z. B. durch die Abgabe von Abfällen, Abwässern, Lärm und luftfremden Stoffen. Der Mensch wiederum kann Einfluss nehmen auf derartige Umweltfaktoren. Jede technische Einrichtung ist deshalb eingebettet in ein durch Wechselwirkungen gekennzeichnetes Mensch-Maschine-Umwelt-System.“*

Laut Kuhlmann befasst sich die Sicherheitswissenschaft mit der Sicherheit vor möglichen Gefahren bei der Nutzung der Technik, nicht aber mit militärischer und sozialer Sicherheit oder mit der Sicherheit vor Krankheit, die nicht von der Technik verursacht wird.

*„Das Ziel der Sicherheitswissenschaft besteht darin, Schadwirkungen bei der Nutzung der Technik so klein wie möglich oder wenigstens in vorgegebenen Grenzen zu halten. Unter Schadwirkungen sollen dabei sowohl unfallartige als auch solche Schäden verstanden werden, die z. B. infolge von Umweltbelastungen durch technische Anlagen entstehen können.“*

Der Begriff der Sicherheitswissenschaft ist bei Kuhlmann technikbezogen. Das heißt, ein Schutz vor Gefahren, die nicht durch die Technik verursacht sind, ist nicht Gegenstand der Sicherheitswissenschaft. Hierzu ist anzumerken, dass eine klare Trennung zwischen den einzelnen zivilisationsbedingten und den natürlichen Risiken nicht immer möglich ist (zum Beispiel beim Klimawandel). Die Verwendung des Terminus Sicherheitswissenschaft statt Sicherheitstechnik ist strittig. Wie zuvor erläutert, ist die Technik allgemein und damit auch die Sicherheitstechnik eine Wissenschaftsdisziplin, die allerdings als eine interdisziplinäre multifakultative Disziplin anzusehen ist. Unstrittig ist jedoch, wie bereits erwähnt,

dass der Mensch eine besondere Herausforderung für die sicherheits- und zuverlässigkeitstechnische Gestaltung und Nutzung eines Mensch-Maschine-Umwelt-Systems darstellt. Neben den Paradigmen Determinismus und Indeterminismus sei hier von einem **Humankompatibilismus** als drittes Paradigma ausgegangen. Im Gegensatz zum sogenannten „human factor“ – gekennzeichnet durch die Anpassung „Mensch/Maschine“, geprägt durch psychologische, medizinische und andere Erkenntnisse – soll das hier neu eingeführte Paradigma „Humankompatibilismus“ auch die Anpassung „Maschine/Mensch“ (human engineering) durch das Wissensgebiet der Ergonomie und Anthropotechnik mitberücksichtigen. Des Weiteren sollen die Wissenschaftsdisziplinen, die sich mit den Gefahrenpotenzialen und deren Reduzierung bei der Herstellung und Nutzung technischer Systeme gleich welcher Art auseinandersetzen, Bestandteil des Humankompatibilismus sein. Hierzu zählen insbesondere die Verkehrssicherheit, Arbeitssicherheit, Arbeitsmedizin, Arbeitsphysiologie, Pädagogik und andere Disziplinen. Dieses hier neu eingeführte Paradigma „Humankompatibilismus“ berücksichtigt die physischen, psychischen, geistigen und anderen Eigenschaften des Menschen im Sinne einer teleologischen Interaktion mit der Technik und der damit verbundenen Umwelt. Alle drei Paradigmen zusammen charakterisieren aber auch die Bereiche Umweltschutz, Personen- und Objektschutz, Rettungswesen (Sicherungswesen, Brand- und Explosionsschutz, Unfallrettungswesen, persönliche Schutzausrüstung, Katastrophen- und Zivilschutz, Evakuierung und anderes), Qualitätssicherung, Risk-Management, Datenschutz und das sicherheitstechnische Recht als sich stetig verändernde Festschreibung sicherheitstechnischer Erkenntnisse.

## ■ 1.2 Aktuelle Herausforderungen

Die aktuellen Herausforderungen im Kontext Sicherheit und Zuverlässigkeit sind durch die medienwirksamen Schlagwörter „Digitalisierung“, „Industrialisierung 4.0 und Robotik“ und in diesen eingebettet „Künstliche Intelligenz“ (KI) geprägt. Die industriellen Entwicklungen und Innovationen in diesen Bereichen bilden ein großes Potenzial zur Verbesserung der Lebensqualität in allen Bereichen des menschlichen Daseins. Damit eng verbunden sind jedoch auch vielfältige Fragestellungen im Sinne von Safety und Security.

Aufgabe von Staat, Gesellschaft, Industrie, Wissenschaft ist es, diese zu konstatieren und die mit jeder neuen technologischen Entwicklung verbundenen Gefahren, Risiken für den Einzelnen und die Gesellschaft zu bewerten, zu minimieren und in diesem Zusammenhang entsprechende gesetzliche Rahmenbedingungen zu schaffen.

Mit diesen Herausforderungen sind insbesondere die in Forschung und Entwicklung tätigen Wissenschaftler und Ingenieure konfrontiert. Hier gilt es neue Ansätze und Verfahren zur Bewertung, Validierung und Verifizierung der Sicherheit, Zuverlässigkeit, Verfügbarkeit und anderer Kategorien bereitzustellen.

Dabei bildet die sogenannte „Künstliche Intelligenz“ (KI) einen zentralen Baustein, der durch ständig wachsende Entwicklungen und Anwendungen im Kontext des maschinellen Lernens, bei Perzeption, Entscheiden, Handeln, Kommunikation etc. als „schwache KI“ geprägt ist.

Hierzu gehören aktuell unter anderem die Themenkomplexe

- Robotik, Steuerung, Regelung, Expertensysteme,
- autonomes Fahren,
- Sprach- und Textverarbeitung,
- Bild- und Spracherkennung,
- Mustererkennung
- etc.

Für den Bereich der Technischen Zuverlässigkeit gehören hierzu die Themen

- Zuverlässigkeitsplanung und -prüfung (allgemein),
- Predictive Maintenance,
- Fehlerdetektion,
- Ausfallratenbestimmung, Schwachstellenanalyse,
- Struktur- und Systemanalyse
- etc.

Heute wird KI bereits in vielen Branchen wie

- Industrie (Produktion, Fertigung, Qualitätssicherung, Steuerungs- und Regelungstechnik, Robotik und Vernetzung),
- Verkehrsträger (Schiene-, Luft-, Straßenverkehr und autonomes Fahren sowie deren Vernetzung),
- Energiewirtschaft (Steuerung und Optimierung, Netzbetrieb, Kraftwerksteuerung, prädiktive Wartung und Instandhaltung, Vertrieb etc.),
- Wirtschaft und Finanzwelt,
- Medien und Bildungsbereich (Textanalyse, digitale Assistenten, Crawling und Indexierung, Blockchain-Technologie, Video Content Marketing etc.),
- Medizin (Bildgebung, Diagnose, CT, Telemedizin, Neuroprothetik, Exoskelett etc.),
- Militär (autonome Waffensysteme, Strategieentwicklung, Entscheidungsfindung etc.),
- Jurisprudenz (Vertragsgestaltung und -prüfung, Recherche, Prozessvorbereitung, Handlungs- und Entscheidungsempfehlungen)
- etc.

erfolgreich eingesetzt.

Für das multi-fakultative Fachgebiet *Künstliche Intelligenz (KI)* gibt es, aufgrund des nicht fassbaren Begriffs der natürlichen Intelligenz im etymologischen Sinne, zahlreiche Definitionen. Prinzipiell verfolgt KI das Ziel die Attribute der kognitiven analogen Eigenschaften des Menschen durch eine digitale lernfähige Maschine nachzubilden.

Als Begründer der KI wird allgemein der Informatiker John McCarthy<sup>8</sup> angesehen, der 1956 am Dartmouth College in Hanover (New Hampshire, USA) einen Workshop mit dem Titel „Dartmouth Summer Research Project on Artificial Intelligence“ organisierte. McCarthy verweist allerdings selbst auf Alan Turing<sup>9</sup>, einen der Gründungsväter der modernen Computertechnologie, der Informatik und damit der KI (Turing-Maschine, Turing-Test). Im deutschsprachigen Raum wird allgemein Karl Steinbuch<sup>10</sup> als einer der Pioniere der Kybernetik (Begründer Norbert Wiener<sup>11</sup>) und Künstlichen Intelligenz (maschinelles Lernen) und Namensgeber der Informatik als neue akademische Fachdisziplin, hervorgegangen aus der Kybernetik, angesehen (zur Geschichte der Entwicklung siehe Erhard Konrad, siehe Lit.).

Auch wenn die besonders in den letzten Jahren aufgrund verbesserter Rechentechnologien erzielten KI-Erfolge beeindruckend sind, ist der Weg zur sogenannten „starken KI“, d. h. der Adaption der gesamten kognitiven Fähigkeiten des Menschen im Sinne des Analogon Mensch-Maschine, noch durch viele Meilensteine gekennzeichnet. So schreibt Bernd Vowinkel in seinem Buch *Maschinen mit Bewusstsein* (siehe Lit.), Kapitel 1, Natürliche Intelligenz:

*„Bei Fragen der Leistungsfähigkeit und der Eigenschaft von künstlicher Intelligenz wird in der Regel der Mensch als Maß aller Dinge zum Vergleich herangezogen. Das trifft insbesondere auf die Eigenschaften zu, die es bei der künstlichen Intelligenz noch nicht gibt, nämlich Bewusstsein, Vernunft und freier Wille.“*

Ob es jemals eine „starke KI“ geben wird, ist strittig, obwohl ernst zu nehmende Wissenschaftler sich bereits mit dem nächsten Schritt einer „super KI“ und dessen Auswirkungen auf die Menschheit gedanklich auseinandersetzen. Das Gleiche gilt für neurobiologische Forschungen und die Prämissen zur Entwicklung einer „humanen Überintelligenz“ aufgrund von Quantenvorgängen im Gehirn. Unstrittig ist jedoch die Weiterentwicklung von KI und deren Verknüpfung mit der menschlichen Willenskraft (Nervensystem und Gehirnaktivität) zu einer gewissen „hybriden Intelligenz“, die es bereits heute ermöglicht, Schwerstbehinderten eine gewisse Beweglichkeit zurückzugeben, z. B. als Exoskelett-Hand (Neuroprothetik, neuronal gesteuerte Robotik). In diesem Kontext zeigt Bild 1.1 eine mögliche Illustration.

Auch sind sich Wissenschaftler darin einig, dass die Weiterentwicklung und Nutzung von Quantencomputern die KI stark beeinflussen wird (siehe Förderprogramm des BMBF zur Quantentechnologie).

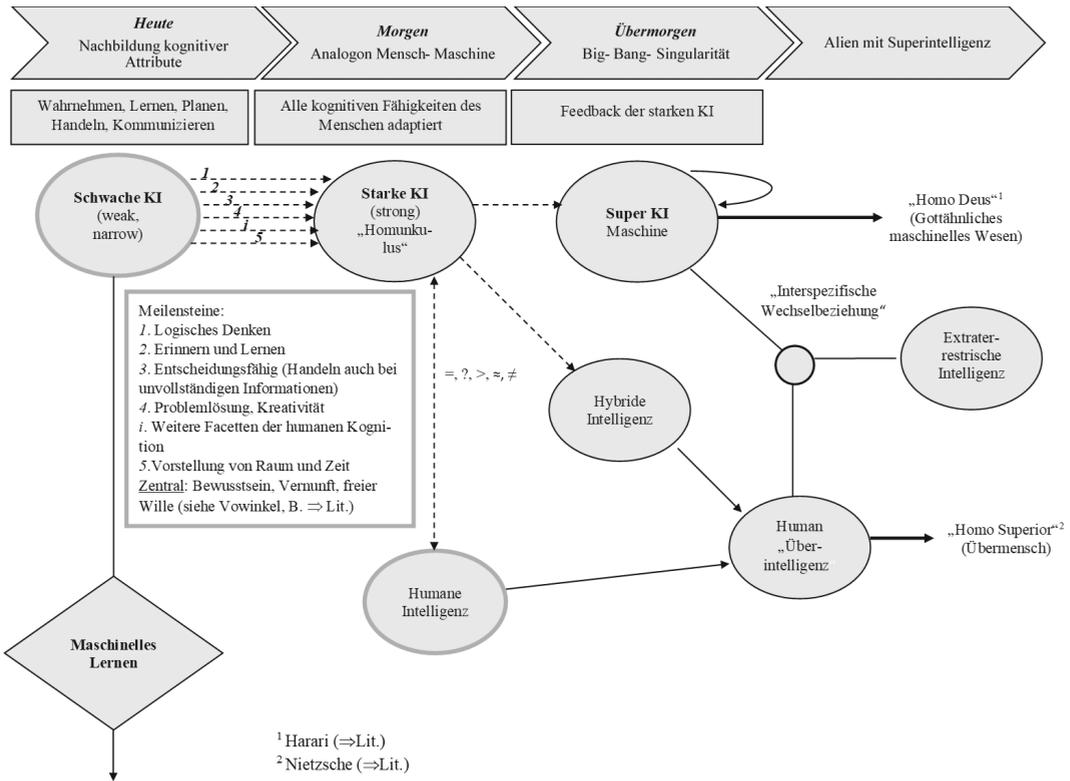
---

<sup>8</sup>) John McCarthy (1927–2011)

<sup>9</sup>) Alan Turing (1912–1954)

<sup>10</sup>) Karl Steinbuch (1917–2005)

<sup>11</sup>) Norbert Wiener (1894–1964)



**Bild 1.1** Evolution der Künstlichen Intelligenz

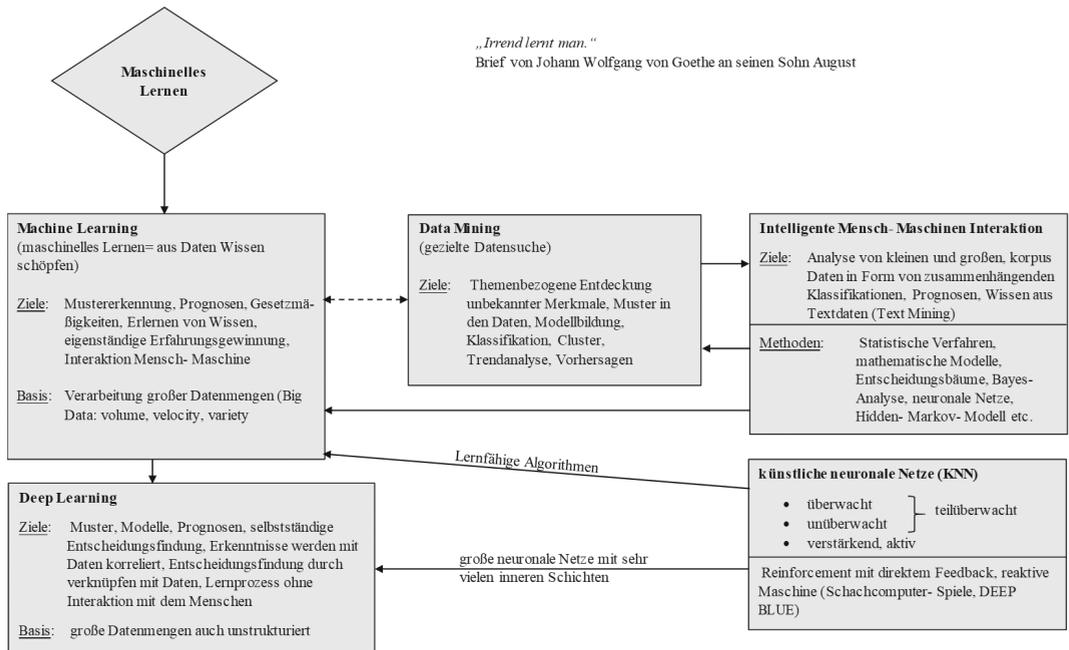
Dass digitale lernfähige Maschinen in vielen speziellen, determinierten Bereichen den intellektuellen Fähigkeiten eines Menschen überlegen sind, ist unstrittig. So gewann der IBM Computer Deep Blue 1997 gegen den damaligen Schachweltmeister Garry Kasparov mit 3,5 zu 2,5 Punkten (d.h., von sechs Partien hat Kasparov zwei verloren, eine gewonnen, drei endeten mit Remis).

Doch zurück zur „schwachen KI“: Der Kernbereich der „schwachen KI“ ist durch das *maschinelle Lernen* geprägt. Hier wurden in den letzten Jahren aufgrund der immensen Weiterentwicklung der Computertechnologie, verbunden mit einer enormen Steigerung der Rechenleistung durch entsprechende Prozessoren und Vernetzung, mit der Möglichkeit sehr große Datenmengen auch in Echtzeit sehr schnell zu verarbeiten, enorme Fortschritte erzielt. *Machine Learning* ist durch lernfähige Algorithmen wie *neuronale Netze* und *Deep Learning* gekennzeichnet. Im Gegensatz hierzu nutzt *Data Mining* statistische Verfahren mit dem Ziel aus den Daten (auch bei einer geringen Anzahl) allgemeine Zusammenhänge und Wissen zu generieren. Bild 1.2 zeigt hierzu einen groben Überblick hinsichtlich *Machine Learning* und *Deep Learning* als inklusive Ausprägung sowie *Data Mining* und die hierzu genutzten algorithmischen Verfahren.

„Niemand formuliert es so, aber für mich ist KI fast eine Geisteswissenschaft. Es ist wirklich der Versuch, menschliche Intelligenz und Kognition zu verstehen.“

Sebastian Thrun (CEO bei Kitty Hawk Coporation and Innovation)

Für weitere Ausführungen hierzu siehe Kapitel 22.



**Bild 1.2** Gegenwärtige Praxis der Künstlichen Intelligenz

Bei aller Euphorie bezüglich der Weiterentwicklung und stetig wachsenden Einsatzbereiche von KI bleibt ein zentrales Thema die Absicherung, d.h. die qualitative und quantitative Bewertung hinsichtlich Sicherheit, Zuverlässigkeit, Verfügbarkeit der durch das maschinelle Lernen geprägten sicherheitskritischen Anwendungsbereiche, wie z.B. Mensch-Roboter-Interaktion, autonomes Fahren, aufgrund der nicht mehr nachvollziehbaren Output-Ergebnisse der zugrunde gelegten und implementierten neuronalen Netze allgemein und insbesondere von *Deep Neural Networks*. Ein Ziel ist es deshalb, neuronale Netze erklärbar zu gestalten. Unter dem Terminus „*Explainable Artificial Intelligence*“, kurz *Explainable AI*, werden hierzu gegenwärtig weltweit Förderprojekte und Forschungen durchgeführt (siehe hierzu unter anderem das Fraunhofer-Institut für Kognitive Systeme, IKS).

Des Weiteren spielt die Qualität der zugrunde gelegten Input-Daten eine entscheidende Rolle. Eine sorgfältige Dateninterpretation und -verarbeitung gelernter Trainingsdaten, aber auch ungelerner Daten als Modellinput ist deshalb unerlässlich für die Robustheit der Modellierung. Diesbezügliche Fehler, insbesondere bei sicherheitskritischen Anwendungen, können naturgemäß mit weitreichenden Auswirkungen und Folgen verbunden sein. Für weitere Ausführungen hierzu siehe Kapitel 6.

Es liegt auf der Hand, dass der Einsatz von KI insbesondere für automatisierte Systeme wie z.B. in automatisierten Prozessen und bei der Nutzung von Robotern sowie bei deren Vernetzung in der Produktion (Industrie 4.0) oder beim autonomen Fahren, aber auch im medizinischen Bereich (Medizintechnik), mit einem stringenten Sicherheitsnachweis verbunden ist. So sind beispielsweise die prinzipiellen Dilemmata beim autonomen Fahren zwar weitgehend bekannt (Meyna/Heinrich, siehe Lit.), allerdings ab Level 3 (Hochautoma-

tisiert) aufgrund der erforderlichen Absicherungen allgemein – von Forschungsfahrzeugen bis Level 5 abgesehen – noch nicht verfügbar. Es ist deshalb äußerst anspruchsvoll, geeignete Strategien wie Fail-Operational Systems für die Behandlung von komplexen Fehlerzuständen wie z.B. bei der Perzeption, der Fahrzeugregelung, der implementierten Hard- und Software, ungewollter oder gewollter Manipulation im Kontext des dynamischen, adaptiven Fehlermanagements inklusive einer Rückfallebene zur Degradation zu entwickeln und diese qualitativ und quantitativ zu bewerten. Nicht zuletzt gilt es, eine systembezogene Resilienz und Verfügbarkeit in Echtzeitanforderungen umzusetzen und zu gewährleisten (Forschungen hierzu siehe unter anderem Fraunhofer IKS und IQZ).

Nach wie vor ungeklärt sind auch die rechtlichen Fragestellungen und Probleme bei den Lern- und Trainingsprozessen der Software im Kontext der damit verbundenen „autonomen“ Handlungs- und Entscheidungsprozesse (Ambivalenz Hersteller vs. Anwender), siehe hierzu unter anderem die juristische Dissertation von Justin Grapentin (siehe Lit.).

Mit dem zunehmenden Einsatz von KI und deren Weiterentwicklung in vielen Bereichen der humanen Existenz spielen auch die damit verbundenen ethischen Fragestellungen eine immer größere Rolle. In diesem Zusammenhang sei auf die in jeder Hinsicht lesenswerte kleine Monographie von Christoph Bartneck et al. des Carl Hanser Verlags (siehe Lit.) verwiesen. Empfehlenswert ist außerdem das Buch „Maschinelles Lernen – Grundlagen und Algorithmen in Python“ von Jörg Frochte (2. Auflage 2019, Carl Hanser Verlag, München).

*„KI ist wahrscheinlich das Beste oder das Schlimmste, was der Menschheit passieren kann.“*

*Stephen Hawking (1942 – 2018)*

# Index

## Symbole

- 2v3-System
- Sicherheitsbetrachtung 259
- $\sigma$ -Algebra 120

## A

- Abbreviated Injury Scale (AIS) 82
- Ablauf einer Zuverlässigkeitsprognose 605
- Abnahmeprüfung
  - attributive 560
  - messende 560
  - zählende 560
- Abnahmerisiko 562
- Abweichungsquadrat 548
- Accelerated Life Test 583
- Acceleration Factor 584
- Acceptable Quality Level 565
- Advanced Product Quality Planning 51
- Akkumulierte Lebensdauer 525
- Allgemeine Erlang-Verteilung 174
- Alternativhypothese 547f., 554
- Analyse von Fehlern gemeinsamer Ursachen 62
- Änderungsmanagement 94
- Anerkennungsverfahren 22
- Anforderungsmanagement 91
- Annahmekennlinienbereich 563
- Annahmewahrscheinlichkeit 561
- Annehmbare Qualitätsslage 565
- Anpassungstest 547
  - Fehlentscheidung 547
  - nach Kolmogorov-Smirnov 542
  - Vergleich 559
  - verteilungs- und parameterfrei 547
- Anwärter
  - Bestimmung der 607
  - korrigierte Berechnung der 612
- Anzahl der Klassen 549
- Approximation 498
  - der Binomialverteilung durch die Normalverteilung 499
  - der Binomialverteilung durch die Poisson-Verteilung 498
  - der hypergeometrischen Verteilung durch die Normalverteilung 500
  - der hypergeometrischen Verteilung durch eine Binomialverteilung 498
  - der Poisson-Verteilung durch eine Normalverteilung 499
- AQL-Wert 565
- Arithmetische Mittel 151
- Arrhenius-Modell 583
- ASIL 85
- ASIL-Ermittlung nach ISO 26262 85
- Assoziativgesetz 119
- Asymptotische Extremwertverteilung 184
- asymptotisch effizient 506
- Attributive Abnahmeprüfung 560
- Attributiver Prüfplan 560
- Ausfalldichte 142
  - Erlang-Verteilung 173
  - Exponentialverteilung 160
  - Normalverteilung 177
  - Weibull-Verteilung 165
- Ausfälle während des Tests 572
- Ausfallfunktion
  - Definition 303
  - Negativlogik 302
- Ausfallmodell 606
- Ausfallrate 142, 544
  - Erlang-Verteilung 173
  - Exponentialverteilung 160
  - kumulative 578
  - logarithmische Normalverteilung 180
  - Normalverteilung 178
  - Weibull-Verteilung 165

Ausfallratenangaben 202  
 Ausfallratendatenhandbücher 204  
 Ausfallratenmodelle 201, 207  
 Ausfallsteilheit 164, 542  
 Ausfallwahrscheinlichkeit 126, 141, 542  
 Ausfallzustände 273  
 Ausgangshypothese 562  
 Ausgangswert  
 – Weibull-Verteilung 164  
 Ausgleichsgerade 542  
 Aussagesicherheit 510  
 Auswahlssatz 492  
 Automotive SPICE 96  
 Automotive-SPICE-Prozessreferenzmodell 97  
 AUTOSAR  
 – Architektur 106  
 – Requirements 107  
 Axiomensystem von Kolmogorov 121

## B

B 10-Wert 544  
 Backpropagation-Algorithmus 475 f.  
 Backpropagation-Regel 475  
 backward-net 472  
 Badewannenkurve 165, 201  
 Barlow-Proschan-Importanz  
 – Definition 322  
 Bayes  
 – Satz von 127  
 Bayes-Statistik 128  
 Bedienungstheorie 172  
 Bedingte Lebenserwartung 144  
 Bedingte Überlebenswahrscheinlichkeit  
 – Exponentialverteilung 162  
 Bedingte Wahrscheinlichkeit 124  
 Belastung-Belastbarkeit-Diagramm 108  
 Berechnung der Zugehörigkeitsgrade 355  
 Bernoulli  
 – Satz von 504  
 Bernoullische Versuche 190  
 Bernoulli-Verteilung 190  
 Beschleunigter Lebensdauertest 583  
 Beschleunigungsfaktor 584  
 Besetzungszahlen 548  
 Bestandungsverläufe 602  
 Betriebssicherheit 36  
 Betriebszeit  
 – kumulative 525  
 Binomialprüfplan 564  
 Binomialverteilung 190  
 – Likelihood-Schätzer 520  
 Black-Gleichung 585

Boolesche Algebra 119  
 – Absorptionsgesetze 281  
 – Assoziativgesetz 280  
 – Axiome 280  
 – Begriffe und Regeln 275  
 – De Morgansche Gesetze 281  
 – Distributivgesetz 280  
 – Einführung von Wahrscheinlichkeiten 297  
 – Grundverknüpfungen 277  
 – Idempotenzgesetze 281  
 – Kommutativgesetz 280  
 – Postulate 280  
 – Shannonsche Zerlegung 290  
 Boolesche Funktion 231, 275  
 – ausgezeichnete disjunktive Normalform 286  
 – ausgezeichnete konjunktive Normalform 288  
 – disjunktive Normalform 284  
 – kanonische Darstellung 284  
 – konjunktive Normalform 284  
 – Maxterm 278  
 – Minterm 279  
 – reelle Variablen 292  
 – Systemfunktion 294  
 Boolesche Grundverknüpfung  
 – Venn-Diagramm 280  
 Boolesche Modellbildung 275  
 BOTTOM-UP-Algorithmus 310  
 Bruchschwingenspielzahl 586  
 Brückenkonfiguration 239  
 Buffonsches Nadelproblem 421

## C

Charakteristische Lebensdauer 164, 542  
 Chi<sup>2</sup>-Verteilung 193  
 Chi-Quadrat-Anpassungstest 542, 547  
 Codex der Haftung 4  
 Coffin-Manson-Gleichung 588  
 Common Cause Analysis (CCA) 62  
 Confirmation Measures 90

## D

Data Mining 14  
 Datenschutz 105  
 Dauerfestigkeit 589  
 Dauerschwingversuch nach Wöhler 586  
 Decreasing Failure Rate 210  
 Decreasing Failure Rate Average 212  
 Deep Learning 14  
 Deep Neural Network 15  
 Defuzzifizierung 331, 343, 357  
 Degradierete Zustände 273

Dehnungs-Wöhlerlinie 588  
 Delta-Regel 474  
 De Morgansche Gesetze  
 – Boolesche Algebra 281  
 De Morgansche Regel 119  
 Derating 254  
 Design for Reliability 113  
 Design-Zielzahlen 113  
 Determinismus 8, 10  
 DFRA-Verteilung 212  
 DFR-Verteilung 210  
 DGQ  
 – Formblatt zur Weibull-Verteilung 544  
 Dichte  
 – hypergeometrische Verteilung 196  
 – logarithmische Normalverteilung 180  
 diehard-test 428  
 Direkte Monte-Carlo-Simulation 431, 440  
 Diskreter Markov-Prozess  
 – lineare Flussgraphen 453  
 Diskrete Verteilungsfunktion 130  
 Diskrete Zufallsgrößen 129  
 Dispersion 135  
 Distributivgesetz 119  
 Dokumentationsmanagement 95  
 Durchschnittswert 151  
 Dynamische Zuverlässigkeitstheorie 422

## E

Echtzeit-Nutzungsdaten 102  
 E/E/S-Architekturen 273  
 E/E/S-Systeme 269  
 Effizienz 506  
 Einfachregression 536  
 Elektrik/Elektronik/Software-  
 Architekturen 273  
 Elektrik/Elektronik/Software-Systeme 269  
 Elementare Miner-Regel 589  
 Empirische Ausfalldichte 150  
 Empirische Ausfallrate 150  
 Empirische Ausfallwahrscheinlichkeit 150  
 Empirischer Erwartungswert 151  
 Empirische Standardabweichung 151  
 Empirische Varianz 151  
 Empirische Zuverlässigkeitskenngrößen 150  
 Endliche Menge 118  
 Endlichkeitskorrekturfaktor 197, 492  
 End-of-Life-Test 581  
 Entwicklungssatz von Shannon 290  
 EOL-Test 581  
 Ereignisablaufanalyse 327  
 Erfolgslauf 569

Erlang-Verteilung  
 – allgemeine 174  
 – Ausfalldichte 173  
 – Ausfallrate 173  
 – Erwartungswert 173  
 – spezielle 172  
 – Varianz 173  
 – Verteilungsfunktion 172  
 Erneuerungsprozesse 371  
 Erneuerungstheorie 172  
 Erwartungstreue Schätzfunktion 506  
 Erwartungswert 133, 144, 491, 505, 548, 577  
 – der Betriebszeit 395  
 – der Reparaturzeit 395  
 – Erlang-Verteilung 173  
 – Exponentialverteilung 161  
 – hypergeometrische Verteilung 197  
 – logarithmische Normalverteilung 180  
 – Weibull-Verteilung 165  
 Erweiterungsprinzip 340  
 event accident process 327  
 event flow 327  
 event tree 327  
 Explainable Artificial Intelligence 15  
 Exponentialverteilung 160  
 – Ausfalldichte 160  
 – Ausfallrate 160  
 – bedingte Überlebenswahrscheinlichkeit 162  
 – Erwartungswert 161  
 – Momentenschätzer 534  
 – Verteilungsfunktion 160  
 Expositionswahrscheinlichkeit  
 – Einstufung nach ISO 26262 83  
 Extremwertverteilung 184  
 – Weibull-Verteilung 186  
 Eyring-Modell 584

## F

Fahrleistungsprognose 606  
 Fail Operational 274  
 Failure Modes and Effects Analysis (FMEA) 62  
 Failures in Time 203  
 Failures per Million Hours 203  
 Farmer-Diagramm 158  
 Fault Tree Analysis (FTA) 62  
 Federal Aviation Regulations 63  
 Feedforward-Modell 473  
 feedforward-net 472  
 Fehler  
 – 1. Art 547, 562  
 – 2. Art 547, 562  
 Fehlerbaumanalyse (FBA) 62, 123, 299

Fehlerbaumauswertung  
 – quantitative 306  
 Fehlerbaumdarstellung 230  
 Fehlermöglichkeits- und Einflussanalyse  
 (FMEA) 62  
 Fehlertoleranz 274  
 Felddaten 102, 593  
 Felddatenanalyse 596  
 Felddatenauswertung 595  
 Felddatenerfassung 593  
 Felddatenquellen 594  
 FIT-Werte 203  
 Flussgraphentheorie 458  
 Folgeprüfung 566  
 Formblatt zur Weibull-Verteilung (DGQ) 544  
 Fraktionale Importanz  
 – Definition 321  
 Fréchet-Verteilung 186  
 Free-Flight-Schätzer 434  
 Freigabeprozess 53  
 Freiheitsgrad 548  
 Frontloading 108  
 Frühausfälle  
 – Weibull-Verteilung 165  
 Functional Hazard Assessment (FHA) 62, 65  
 Funktionale Sicherheit 55  
 – Management 78  
 – Straßenfahrzeuge 74  
 Funktionale Sicherheitsanforderung (FSA) 86  
 – nach ISO 26262 86  
 Funktionales Sicherheitskonzept (FSK) 86  
 Funktionsrisikoanalyse 65  
 Fuzzifizierung 331, 342, 351  
 Fuzzifizierungsprozess 351, 363  
 Fuzzy-Ausfallraten 363  
 Fuzzy Control 330  
 Fuzzy-Ereignisbaumanalyse 365  
 Fuzzy-Fehlerbaumanalyse 357, 362  
 Fuzzy-Fehlermöglichkeiten 358  
 Fuzzy-Inferenz 342  
 Fuzzy-Intervall 358, 363  
 Fuzzy-Logik 330  
 – Anwendung bei der FMEA 348  
 Fuzzy-Markov-Analyse 365  
 Fuzzy-Menge 332  
 Fuzzy-Modell 358  
 Fuzzy-Relation 336 f.  
 fuzzy sets 330  
 Fuzzy-System 331  
 Fuzzy-Wahrscheinlichkeiten 358

## G

Gammaverteilung 173  
 Garantie 19  
 Garantiedaten  
 – Gesamtmodell für zeitnahe 613  
 Gefahr 6 f.  
 Gefährdungsanalyse 62, 65  
 – Luftfahrtindustrie 65  
 Gefährdungsanalyse und Risikobeurteilung  
 – nach ISO 26262 81  
 Gefährdungsbeurteilung  
 – Luftfahrtindustrie 65  
 Gefährdungshaftung 18  
 Gefährdungsidentifikation 81  
 Gefahren- und Risikoanalyse 81  
 Gefährliche Zustände 273  
 Generelle Ausfallratenmodelle 213  
 Generische Norm 31  
 Geometrische Wahrscheinlichkeit 121  
 Gesamtmodell für zeitnahe Garantiedaten 613  
 Gesamtsicherheitsmanagement 78  
 Gesetz der großen Zahlen 498, 502  
 – schwaches 502  
 – starkes 502  
 Gestützte Stichprobe 524  
 Gewährleistung 17, 19  
 Gewährleistungsmanagement 23, 46, 596  
 Gewichtete Maximum-Mittelwert-Methode 345  
 Gewichtete Monte-Carlo-Simulation 435, 437  
 – zur Varianzreduktion 440  
 – zur Varianz- und Zeitreduktion 441  
 Graphentheorie 444  
 – Adjazensliste 447  
 – Adjazensmatrix 446  
 – bewertete Graphen 447  
 – Euler-Weg 446  
 – gerichteter Graph 445  
 – Grad eines Graphen 445  
 – Grundbegriffe 445  
 – Hamilton-Kreis 446  
 – Kante 445  
 – Pfad 446  
 – Schleife 445  
 – Weg 446  
 – Zyklus 446  
 Grenzkurve 542  
 Grenzwertsatz 178, 498  
 – zentraler 501  
 Grenzwertsatz von de Moivre und Laplace 500  
 Gumbel-Verteilung 186  
 Gütekriterien 428  
 Gut-Schlecht-Prüfung 560, 590

## H

Haftung 18  
 Haftungsanspruch 17f.  
 HALT-Methode 590  
 HALT-Test 590  
 HASS-Methode 592  
 HASS-Test 592  
 Häufigkeitssummenlinie 542  
 Hazard Analysis and Risk Assessment (HARA) 81  
 Hebbsche Lernregel 474  
 Heibach-Regel 589  
 Heiße Redundanz 126  
 Herstellerrisiko 562  
 High Cycle Fatigue (HCF) 588  
 Highly Accelerated Life Test (HALT) 590  
 Highly Accelerated Stress Audit 592  
 Highly Accelerated Stress Screen (HASS) 590  
 H-Matrix 386  
 Hochbeschleunigte Testmethoden 590  
 Homogener Markov-Prozess 369  
 Humankompatibilismus 11  
 Hypergeometrische Verteilung 195  
 – Dichte 196  
 – Erwartungswert 197  
 – Varianz 197  
 Hypergeometrisch-verteilte Zufallsgröße 196  
 Hypothesenprüfung 562

## I

IEC 61508 58  
 IFRA-Verteilung 212  
 IFR-Verteilung 207  
 Importance Sampling 424  
 Importanz  
 – marginale 252  
 Importanzkenngrößen 315  
 Increasing Failure Rate 207  
 Increasing Failure Rate Average 212  
 Indeterminismus 9f.  
 Indifferente Qualitätslage 565  
 Indifferent Quality Level 565  
 Induktionsschluss 505  
 Induktive Zuverlässigkeits- und Sicherheitsanalyse 327  
 Industriespezifische Norm 31  
 Inferenz 331  
 Inferenzprozess 355  
 Inhomogener Markov-Prozess 369, 375  
 Inklusions-Exklusions-Methode 308  
 Instandsetzungsdichte 154

Instandsetzungsrate 154  
 Instandsetzungswahrscheinlichkeit 154  
 Instandsetzungszeit 155  
 Institut für Qualitäts- und Zuverlässigkeitsmanagement GmbH (IQZ) XVII  
 Intervallarithmetik 340, 358  
 Intervallschätzung 505  
 Inverse Rangzahl 578  
 Inversionsmethode 429  
 IQL-Wert 565  
 Irrtumswahrscheinlichkeit 507, 549, 553, 562  
 – 2. Art 549  
 Isochronen 596  
 Isochronen-Darstellung 600  
 Isochronous Diagrams 596  
 Item Definition 80

## J

Joint Aviation Requirements 63

## K

Kalte Reserve 172  
 Karnaugh-Veitch-Diagramm 282  
 Kilometerabhängige Lebensdauerprognosen 608  
 Klassen  
 – Anzahl der 549  
 Klassenbesetzung 549  
 Klassenunterteilung 549  
 Klassenwahrscheinlichkeit 549  
 Kolmogorov-Smirnov-Test 552  
 Kolmogorov-Smirnov-Verteilung 554  
 Kommutativgesetz 119  
 Konfidenzintervall 505, 507f.  
 – für den Erwartungswert 508  
 – für den Mittelwert 508  
 – für die Varianz 512  
 Konfigurationsmanagement 95  
 Kongruenzgenerator  
 – linearer 426  
 – nicht-linearer 426  
 Konnektische Modelle 466  
 Konstruktions-FMEA 67  
 Kontrollierbarkeit der Einstufung  
 – nach ISO 26262 84  
 Konvergenz 435  
 Kovarianz 537  
 Kumulative Ausfallrate 578  
 Kumulative Betriebszeit 525  
 Kundencluster 112  
 Kundenrisiko 562

Künstliche Intelligenz 11  
 Kurzzeitfestigkeit 588  
 Kybernetik 10

## L

Lagerhaltungsmodelle 193  
 Laplace-Transformation 398  
 – algebraische Gleichungen 400  
 – Grenzwertsätze 401  
 – Zustandsgleichungen 398  
 Larson-Nomogramm 573  
 Last-Event-Schätzer (LES) 434  
 Latin-Hypercube-Sampling 431  
 Lebensdauer  
 – akkumulierte 525  
 – charakteristische 542  
 Lebensdauerprognose  
 – kilometerabhängige 608  
 – zeitabhängige 609  
 Lebensdauerstest  
 – beschleunigter 583  
 Leere Menge 118  
 Lernverfahren 473  
 Lieferantenrisiko 562  
 Likelihood-Funktion 517  
 Likelihood-Schätzer  
 – Binomialverteilung 520  
 – Exponentialverteilung 521  
 – Lognormalverteilung 521  
 – Poisson-Verteilung 520  
 – Weibull-Verteilung 521  
 Lineare Flussgraphen 447  
 – Anwendung auf diskrete Markov-Prozesse 453  
 – Eintrittswahrscheinlichkeit 457  
 – elementare Rechenregeln 447  
 – Ergodensatz 457  
 – Erwartungswert 457  
 – homogene diskrete Markov-Prozesse 454  
 – Mason-Formel 450  
 – Regeln für die graphische Darstellung stetiger homogener Markov-Prozesse 459  
 – stetiger Markov-Prozess 458  
 Lineare Regression 537  
 Lineare Schadensakkumulationshypothese 587  
 Logarithmische Normalverteilung  
 – Ausfallrate 180  
 – Dichte 180  
 – Erwartungswert 180  
 – Median 181  
 – Modus 181

– Überlebenswahrscheinlichkeit 180  
 – Varianz 180  
 Logarithmisch normalverteilte Zufallsgröße 179  
 Lognormalverteilung  
 – Likelihood-Schätzer 521  
 – Momentenschätzer 536  
 Lognormal-Verteilung 179  
 Low Cycle Fatigue (LCF) 588

## M

Machine Learning 14, 592  
 Majoritätsredundanz 256 f.  
 Marginale Importanz  
 – Definition 318  
 Markov-Bedingungen 368 f.  
 Markov-Kette 381  
 – Ergodensatz 389  
 – homogen absorbierende 385  
 – Verallgemeinerung 405  
 – Zerlegung 385  
 Markov-Prozess 62, 366, 369  
 – diskreter (lineare Flussgraphen) 453  
 – homogener 369, 375  
 – inhomogener 369, 375  
 – mit diskretem Parameterbereich und endlich vielen Zuständen (Markov-Kette) 380  
 – mit kontinuierlichem Parameterraum und diskretem Zustandsraum 392  
 – stetige Eintrittswahrscheinlichkeit 460  
 – stetig mittlere Aufenthaltsdauer 459  
 – stetig stationäre Wahrscheinlichkeit 460  
 Markovsche Erneuerungsprozesse 405  
 Markovsche Modellbildung 380  
 Markovsches Modell 366  
 Markovsche Zeitbedingung 369, 376  
 Markovsche Zustandsbedingung 369  
 Marktanalysen 110  
 Maximale Abweichung 555  
 Maximum-Likelihood-Methode 517, 524  
 Maximum-Mittelwert-Methode 343  
 Max-Min-Komposition 339  
 Max-Min-Methode 355  
 Maxterm 288  
 Mean of Maximum 343  
 Mean Time Between Failures 161, 395  
 Mean Time To Danger 414  
 Mean Time To Failure 161  
 Mean Time To Repair 155, 395  
 Mean Time To System Failure 414  
 Median 138, 577  
 – logarithmische Normalverteilung 181  
 Mehrheitsentscheider 257

- Mehrheitsentscheidungssystem 257
  - Meldeverzug
    - Einfluss 611
  - Mengenalgebra 117
  - Merkmalsausprägungen 548
  - Messende Abnahmeprüfung 560
  - Methode der kleinsten Quadrate 517, 537
  - Methode der relevanten Systemkomponente 240
  - Methodenvergleich 223, 226
    - Aggregierbarkeit 224
    - analytische Sensitivität 224
    - Anwendbarkeit auf komplexe Systeme 223
    - empirische und diskrete Verteilungsfunktionen 224
    - funktionale Sensitivität 224
    - Nachvollziehbarkeit 225
    - Rückverfolgbarkeit 225
    - strukturelle Sensitivität 224
  - Miner-Original 589
  - Miner-Regel 587
  - Minimalpfad
    - Definition 303
  - Minimalschnitt
    - Algorithmus 310
    - Definition 305
  - Minimalschnitte 123
  - Minterm 286
  - Mittelwert 134
    - arithmetischer 489, 544
    - empirischer 489
  - Mittlere quadratische Fehler 505
  - Modalwert 140, 577
  - Modell „Ziehen mit Zurücklegung“ 513
  - Modell „Ziehen ohne Zurücklegung“ 491, 513
  - Modus 140
    - logarithmische Normalverteilung 181
  - Momente 134
  - Momentenmethode 517, 532
  - Momentenschätzer
    - Exponentialverteilung 534
    - Lognormalverteilung 536
    - Weibull-Verteilung 536
  - Monotonieeigenschaft 295
  - Monte-Carlo-Simulation
    - gewichtete 435, 437
    - gewichtete, zur Varianzreduktion 440
    - gewichtete, zur Varianz- und Zeitreduktion 441
  - Monte-Carlo-Simulation (MCS) 421
  - Motorad-Sicherheitsintegritätslevel (MSIL) 86
  - Multiple Zensierung 578
  - Multiplikationssatz 126
  - multiply censored data 578
  - Musterklassifizierung 53
  - mvn-System 256
    - adaptives 257f.
    - einfaches 257f.
    - einfache Zuverlässigkeit 258
- ## N
- Nachweis-Zielzahlen 114
  - Negativlogik 302
  - Neigungsgerade 544
  - Neuronale Netze 14, 466
    - Aktivierungsfunktion 469
    - Arbeitsweise 473
    - Aufbau 472
    - bestärkendes Lernen 473
    - biologisches Paradigma 467
    - Fehlerfunktion 475
    - Grundlagen 467
    - künstliches Neuron 468
    - Netzwerktopologien 472
    - Propagierungsfunktion 468
    - überwachtes Lernen 473
    - unüberwachtes Lernen 473
  - Neuronale Schätzung
    - Verteilungsparameter 477
  - Neuronale Zuverlässigkeitsprognose 481
  - Nicht ausschließende Ereignisse 122
  - Nicht-Boolesche Modelle 366
  - Nichtlineare Regression 537
  - Nicht-Regenerativer Prozess 379
  - Nichtverfügbarkeit 155, 390
  - Nomenklatur zuverlässigkeits- und sicherheitstechnischer Grundgrößen 157
  - Norm 26, 30
  - Normalverteilte Zufallsgröße 177
  - Normalverteilung 176
    - Ausfalldichte 177
    - Ausfallrate 178
    - Likelihood-Schätzer 521
    - standardisierte 177
  - No-Trouble-Found-Prozess 24
  - Nullhypothese 547ff., 553f., 562
  - Nutzungsdaten 101
    - aggregierte 102
  - nvn-System 257, 262
    - Sicherheitsbetrachtung 262
    - Zuverlässigkeitsbetrachtung 262

## O

Oberes Quartil 138  
 O.C.-Kurve 561  
 Operationscharakteristik 561

## P

Palmgrem-Miner-Regel 589  
 Palmgrem-Miner-Modell 587f.  
 Paradigma der Sicherheits- und Zuverlässigkeitstechnik 8  
 Parallel-Seriensystem  
 – bei zwei Ausfallarten 247  
 – Überlebenswahrscheinlichkeit 237  
 Parallelsystem 232  
 – bei zwei Ausfallarten 245  
 – marginale Importanz 253  
 – Zuverlässigkeitskenngößen 233  
 Pass/Fail-Test 592  
 Peck-Modell 585  
 Perzeptron-Lernregel 474  
 Poincarésche Gleichung 123  
 Poincaréscher Algorithmus 308  
 Poisson-Prozess 193  
 Poissonsche Sequentialverhältnis 567  
 Poisson-Verteilung 193  
 – Likelihood-Schätzer 520  
 – Verteilungsdichte 193  
 – Verteilungsfunktion 193  
 Positivlogik 302  
 Predictor 536  
 Preliminary System Safety Analysis (PSSA) 62  
 Prinzipieller Ablauf einer Fuzzy-Anwendung 341  
 Probabilistisch-determinierte Methoden 225  
 Probabilistisch-nicht-determinierte Methoden 225  
 Production Part Approval Process 54  
 Produktbeobachtungspflicht 18  
 Produktentstehungsprozess (PEP) 39, 41  
 Produkthaftungsgesetz 18  
 Produktionsprozess und Produktfreigabe 54  
 Produktlebenszyklus 40  
 Produzentenhaftung 18  
 Profilerstellung 113  
 Prognosemodelle 596  
 Propagierungsregeln 473  
 Proven-in-Use 581  
 Prozess-FMEA 67  
 Prüfgröße 548  
 – maximale Differenz 552  
 Prüfplan 563  
 Prüfplanung 194

Prüfquotient 552  
 Punktschätzung 505

## Q

Qualitätslage  
 – annehmbare 565  
 – indifferente 565  
 – rückzuweisende 565  
 Qualitätsmanagement 596  
 Qualitätssicherung 165  
 Quantil 138, 549

## R

Ranggrößenverteilung 576  
 Rangzahl 575  
 – inverse 578  
 Redundanz  
 – aktive 257  
 – Begriffsdefinition 255  
 – diversitäre 257  
 – Grundprinzipien 256  
 – homogene 257  
 – passive 256  
 Redundanzstrategien 274  
 Referenzmarktprinzip 21  
 Regeln der Technik 28  
 Regel von der totalen Wahrscheinlichkeit 126  
 Regenerativer Prozess  
 – mit einigen Nicht-Regenerationszuständen 377  
 Regenerativer stochastischer Prozess 366  
 Regressant 536  
 Regressionsanalyse 536  
 Regressionsfunktion 536  
 Regressionsgerade 537  
 Regressionskoeffizienten 537  
 Regressor 536  
 Reifegradabsicherung (RGA) 51f.  
 Rejectable Quality Level 565  
 Relative Entropie 256  
 Reliability 31, 36  
 Reliability Block Diagram 230  
 Reparatur 153  
 Reparaturrate 154  
 Repräsentationsschluss 505  
 Residuen 537  
 Restlebensdauer 144  
 Restrisiko 61  
 Risiko 6, 158  
 – Equipment Under Control (EUC) 61  
 – tolerierbares 61

Risikoanalyse  
 – nach ISO 26262 81  
 Risikoaversion 6  
 Risikobeurteilung 81  
 Risikodefinition 61  
 Risikograph 61  
 Risikomanagement 46  
 Risikominderung  
 – nach DIN EN 61508 61  
 Risikoparameter 61  
 Risikopotential 17  
 Risikoprioritätszahl (RPZ)  
 – Ablaufdiagramm 67  
 Risikoreduzierung 61  
 Risikoreduzierung und ASIL  
 – nach ISO 26262 85  
 Rohdatenerfassung 101  
 RQL-Wert 565  
 Rückwärtsgekoppelte Netze 472  
 Rückzuweisende Qualitätslage 565

## S

Sachmängelhaftung 19  
 Safety 31, 33  
 Safety Case 80  
 Safety-Manager 79  
 Satz von Bayes 127  
 Satz von Bernoulli 504  
 Schadensakkumulationshypothese  
 – lineare 587  
 Schadensausmaß  
 – Einstufung nach ISO 26262 82  
 Schadensersatz 20  
 Schadteilanalyse 24  
 Schaltredundanz 172  
 Schätzfunktionen  
 – Eigenschaften von 505  
 – erwartungstreue 506  
 Schätzintervall 505  
 Schichtliniendiagramm 596  
 – Ablauf für die Erstellung 600  
 – Matrix für 598  
 – zur Beurteilung der Qualität 601  
 Schiefe 135  
 Schwaches Gesetz der großen Zahlen 502  
 Schwerpunktmethod 344  
 Screening-Verfahren 590  
 Security 31, 33  
 Semi-Markov-Prozess 376, 405  
 – absorbierender 412  
 – Anfangsverteilung 406  
 – Anzahl der Zustände 406  
 – Charakterisierbarkeit 406  
 – Definition und Grundbegriffe 405  
 – diskreter 405  
 – Einteilung 405  
 – ergodischer 416  
 – ergodischer (Grundbegriffe) 416  
 – Grundgrößen 407  
 – kontinuierlicher 405  
 – mittlere bedingte Verweildauer 416  
 – mittlere Rückkehrzeit 417  
 – mittlere Verweildauer 417  
 – Sonderfälle 405  
 – Vorteile 408  
 – Zeit bis zum Ausgangszustand 417  
 – Zeit bis zur Absorption 414  
 Semi-Markov-Übergangswahrscheinlichkeit 406  
 – Eigenschaften 408  
 – Ermittlung 407  
 Sequentialprüfung 561, 566 f.  
 Sequentialtest 194  
 Seriensystem 232  
 – bei zwei Ausfallarten 244  
 – marginale Importanz 252  
 – Zuverlässigkeitskenngrößen 232  
 Shannon  
 – Entwicklungssatz von 290  
 Shannonsche Zerlegung  
 – Boolesche Algebra 290  
 Sicherheit 6, 31  
 – Begriffsdefinition 55  
 Sicherheitsanforderungen  
 – Hierarchie nach ISO 26262 88  
 Sicherheitsgrundnorm IEC 61508 58  
 Sicherheitsintegritätslevel Automotive (ASIL) 85  
 Sicherheitsintegritätslevel (SIL) 60  
 Sicherheitskenngrößen 156  
 Sicherheitslebenszyklus 59, 78  
 – von Straßenfahrzeugen nach ISO 26262 77  
 Sicherheitsmanagement 79  
 Sicherheitsmechanismen  
 – nach ISO 26262 87  
 Sicherheitsprozess  
 – Wechselwirkungen in der Luftfahrtindustrie 70  
 Sicherheitstechnischer Prozess 55  
 – in der Luftfahrtindustrie 62  
 Sicherheitswissenschaft 10  
 Sicherheitsziel  
 – in der Luftfahrtindustrie 65  
 – nach ISO 26262 86  
 Situationsanalyse 81

- Spannungsamplitude 586
  - Spezielle Erlang-Verteilung 172
  - Spezifikationsprozess
    - in der Luftfahrtindustrie 70f.
  - Standard 30
  - Standardabweichung 135, 544
    - des arithmetischen Mittels 490
  - Standardisierte Normalverteilung 177
  - standby-redundancy 172
  - Standby-System 265, 376
    - Berücksichtigung des Schalters 267
    - Sicherheitsbetrachtung 268
    - Zuverlässigkeitsbetrachtung 266
  - Stand der Technik 20, 28
  - Stand von Wissenschaft und Technik 21, 29
  - Starkes Gesetz der großen Zahlen 502
  - Statistische Schätzung von Parametern 505
  - Statistische Sicherheit 507
  - Stetige Zufallsgröße 129
  - Stichprobe 21
    - gestutzte 524
    - mit Zurücklegung 195
    - ohne Zurücklegung 195
    - zensierte 524
  - Stichprobenumfang 548
    - Bestimmung 513
  - Stichprobenverteilung 489
    - der Mittelwerte bei unbekannter Varianz 494
    - der Varianz 493
    - des Mittelwertes 489
    - des Quotienten zweier Varianzen 497
    - für die Differenz und Summe zweier arithmetischer Mittelwerte 495
  - Stirlingsche Formel 191
  - Stochastik 366
  - stochastisch abhängig 370
  - Stochastische Prozesse
    - anwendungsspezifische Beurteilungskriterien 369
    - Beurteilungskriterien 368, 371
    - definitionsspezifische Beurteilungskriterien 368
    - Einteilung 367
    - Klassifizierungen 371
    - mit diskretem Zustandsraum und endlich vielen Zuständen 368
    - mit kontinuierlichem Parameterraum 368
    - Regenerationspunkte 369
    - Regenerationszustand 369
  - Stochastische Prozesstypen
    - Analysemöglichkeiten (Beispiel) 373
  - Störfallablaufanalyse 327
  - Stratified-Sampling 431
  - Stress-Screening 592
  - Streuung 135, 490
  - Strukturelle Importanz
    - Definition 315
  - Student-Verteilung 422
  - Subsystem 270
  - Success Run 569
  - Success-Run-Test 570, 581
  - Sudden-Death 574
  - Suffizienz 506
  - System
    - Begriffsdefinition 269f.
  - Systemarchitektur 272
  - System-FMEA 67
    - Bewertungszahlen 68
  - Systemfunktion
    - Monotonieeigenschaft 294
    - Negativlogik 295
    - Positivlogik 295, 302
  - Systemkomponente
    - Methode der relevanten 240
  - System Safety Analysis (SSA) 62
  - System Sicherheitsanalyse 62
  - Systemunverfügbarkeit 326
  - Systemverfügbarkeit 324
- ## T
- Technische Norm 26
  - Technische Regel 28
  - Technische Sicherheit 32
  - Technische Sicherheitsanforderungen (TSA) 87
  - Technisches Sicherheitskonzept (TSK)
    - nach ISO 26262 87
  - Technisches System 271
    - Definition 270
  - Teilmenge 118
  - Testentscheidung
    - Hinweise 549
  - Testgröße 549
  - Teststrategie 572
  - Test- und Prüfplanung 560
  - TOP-DOWN-Algorithmus 308, 310
  - Totale Wahrscheinlichkeit
    - Regel von der 126
  - Trinomial-Verteilung 576
  - Tschebyscheffsche Ungleichung 502
  - Typ-II-Zensierung 525
  - Typ-I-Zensierung 524

## U

- Übergangswahrscheinlichkeit 380
- Überlebenswahrscheinlichkeit 141
  - infolge Kurzschluss und Unterbrechung für beliebige Strukturen (Netzwerke) 250
  - logarithmische Normalverteilung 180
- Überwachungsstrategien 274
- Unabhängige Ereignisse 126
- Unendliche Menge 118
- Unschärfe Logik 330
- Unsicherheitsband 542
- Unterbeanspruchung 254
- Unteres Quartil 138
- Unternehmenskultur 41
- Unverfügbarkeit 155
- Use Cases 112
- User Experience 110

## V

- Validationsprozess
  - in der Luftfahrtindustrie 72
- Variablenprüfplan 560
- Variablenprüfung 560
- Varianz 135, 144, 505, 537
  - bekannt 508f.
  - empirische 489
  - Erlang-Verteilung 173
  - hypergeometrische Verteilung 197
  - logarithmische Normalverteilung 180
  - unbekannt 508, 511
  - Weibull-Verteilung 166
- Venn-Diagramm 118
- Verarbeitungsregeln 354
- Vereinigungsmenge 118
- Verfügbarkeit 155, 390
  - stationäre 324, 395
- Vergleichersystem 262
- Verifikationsprozess
  - in der Luftfahrtindustrie 73
- Verkettung von Fuzzy-Relationen 338
- Verknüpfung unscharfer Mengen 334
- Verknüpfung von Fuzzy-Relationen 338
- Verschleißerscheinungen
  - Weibull-Verteilung 165
- Versicherungsschutz 23
- Verteilungsdichte 131
  - Poisson-Verteilung 193
- Verteilungsfunktion 129
  - Erlang-Verteilung 172
  - Exponentialverteilung 160
  - Poisson-Verteilung 193

- Verteilungstest 539
- Vertrauensbereich 505, 541
- Vertrauensgrenzen 542
- Vertrauensintervall 507, 526
- Vertrauenspunkte 542
- Verwerfungsmethode 429
- Very High Cycle Fatigue (VHCF) 589
- V-Modell 88
- Vorläufige Systemsicherheitsanalyse (VSSA) 62
- Vorwärtsgerichtete Netze 472
- Vorwissen und Test 581
- Voter 257

## W

- Wahrscheinlichkeit 121
- Wahrscheinlichkeitsdichte 131
- Wahrscheinlichkeitsnetz 539
  - Konstruktion 539
  - Weibull-Verteilung 540
- Wahrscheinlichkeitsraum 122
- Waldsche Sequentialprüfung 566
- Waldsches Sequentialverhältnis 567
- Wartung 153
- Wartungsfaktor 155
- Weibull-Papier 165
- Weibull-Schätzung
  - Likelihood-Schätzer 521
- Weibull-verteilte Zufallsgröße 164
- Weibull-Verteilung 164
  - Ausfalldichte 165
  - Ausfallrate 165
  - Ausgangswert 164
  - Erwartungswert 165
  - Extremwertverteilung 186
  - Frühausfälle 165
  - Momentenschätzer 536
  - Varianz 166
  - Verschleißerscheinungen 165
  - Wahrscheinlichkeitsnetz 540
  - Zufallsausfälle 165
- „Wenn-Dann“-Regeln 354
- Widrow-Hoff-Regel 474
- Wirtschaftlichkeit (Zuverlässigkeitsziele) 48
- Wissenspyramide 100
- Wähler-Diagramm 586
- Wähler-Versuch 586

## Y

- Yatesche Stetigkeitskorrektur 549

## Z

- Zahlen-Daten-Fakten (ZDF) 100
- Zählende Abnahmeprüfung 560
- Zeitabhängige Lebensdauerprognose 609
- Zeitfestigkeitsgerade 588
- Zeitlich Schwankungen der Ausfallrate 214
- Zeitraffende Prüfung 584
- Zensierte Stichprobe 524
- Zentraler Grenzwertsatz 178, 501
- Zentralmoment 134
- Zentralwert 544
- Zufälliges Ereignis 120
- Zufallsausfälle
  - Weibull-Verteilung 165
- Zufallsgröße 129
- Zufallsvariable 129
- Zufallszahlen 425
- Zufallszahlengenerator 425
  - deterministischer 425
  - nicht deterministischer 425
- Zugehörigkeitsfunktion 331
- Zugehörigkeitsgrade 330, 332
  - Berechnung der 355
- Zulassungsverzug
  - Einfluss 610
- Zustände
  - transiente 384
  - unwesentliche 384
- Zustandsdiagramm 231
- Zustandsgleichungen 392
- Zustandsklasse 383
  - absorbierende 384
  - ergodische 384
- Zustandsmenge
  - irreduzible 384
  - rekurrente 384
  - unzerlegbare 384
  - wiederkehrende 384
- Zustandswahrscheinlichkeit 380
- Zuverlässigkeit 36
- Zuverlässigkeitsanalyse
  - analytische Ebene 221
  - Funktionsebene 220
  - Nutzungs- und Belastungsebene 222
  - Strukturebene 220
- Zuverlässigkeitsbewertung
  - mit Hilfe der Graphentheorie 444
- Zuverlässigkeits-Blockschaltbild 230
- Zuverlässigkeitsfunktion 141
- Zuverlässigkeitskenngrößen 141, 153
  - reparierbarer Systeme 153
- Zuverlässigkeitsmanagement 41, 46
  - präventiv 42
  - reaktiv 46
- Zuverlässigkeitsprognose 46, 604
  - für zeitnahe Garantiedaten 610
- Zuverlässigkeitsprognosemodell
  - für mechatronische Systeme im Kraftfahrzeug bei unvollständigen Daten 605
- Zuverlässigkeitsprozess 39
- Zuverlässigkeitswachstum 41, 44, 604
- Zuverlässigkeitsziele 48