

DIN EN 61165

ICS 03.120.01; 29.020

**Anwendung des Markoff-Verfahrens (IEC 61165:2006);
Deutsche Fassung EN 61165:2006**

Application of Markov techniques (IEC 61165:2006);
German version EN 61165:2006

Application des techniques de Markov (CEI 61165:2006);
Version allemande EN 61165:2006

Gesamtumfang 35 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Beginn der Gültigkeit

Die von CENELEC am 2006-07-01 angenommene EN 61165 gilt als DIN-Norm ab 2007-02-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 61165:2003-11.

Für diese Norm ist das nationale Arbeitsgremium K 132 „Zuverlässigkeit“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (<http://www.dke.de>) zuständig.

Die enthaltene IEC-Publikation wurde vom TC 56 „Dependability“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem auf der IEC-Website unter „<http://webstore.iec.ch>“ mit den Daten zu dieser Publikation angegebenen Datum (maintenance result date) unverändert bleiben soll. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe der Norm.

Der Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Anwendung des Markoff-Verfahrens
(IEC 61165:2006)

Application of Markov techniques
(IEC 61165:2006)

Application des techniques de Markov
(CEI 61165:2006)

Diese Europäische Norm wurde von CENELEC am 2006-07-01 angenommen. Die CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Zentralsekretariat oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Zentralsekretariat mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, Ungarn, dem Vereinigten Königreich und Zypern.

CENELEC

Europäisches Komitee für Elektrotechnische Normung
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique

Zentralsekretariat: rue de Stassart 35, B-1050 Brüssel

Vorwort

Der Text des Schriftstücks 56/1096/FDIS, zukünftige 2. Ausgabe von IEC 61165, ausgearbeitet von dem IEC TC 56 „Dependability“, wurde der IEC-CENELEC Parallelen Abstimmung unterworfen und von CENELEC am 2006-07-01 als EN 61165 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem die EN auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2007-04-01
- spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2009-07-01

Der Anhang ZA wurde von CENELEC hinzugefügt.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 61165:2006 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

In der offiziellen Fassung sind unter „Literaturhinweise“ zu den aufgelisteten Normen die nachstehenden Anmerkungen einzutragen:

- | | |
|-----------|---|
| IEC 60812 | ANMERKUNG Harmonisiert als EN 60812:2006 (nicht modifiziert). |
| IEC 61078 | ANMERKUNG Harmonisiert als EN 61078:2006 (nicht modifiziert). |

Inhalt

	Seite
Vorwort	2
Einleitung	5
1 Anwendungsbereich	5
2 Normative Verweisungen	5
3 Begriffe	5
4 Symbole, Formelzeichen und Abkürzungen	8
4.1 Symbole für Zustandsdiagramme	8
4.2 Sonstige Formelzeichen und Abkürzungen	8
4.3 Beispiel	9
5 Allgemeine Beschreibung	10
6 Annahmen und Einschränkungen	11
7 Beziehungen zu anderen Analyseverfahren	11
7.1 Allgemeines	11
7.2 Fehlzustandsbaumanalyse	12
7.3 Zuverlässigkeitsblockdiagramm	12
7.4 Petri-Netze	12
8 Aufstellen von Zustandsübergangsdiagrammen	12
8.1 Voraussetzungen	12
8.2 Regeln zur Entwicklung und Darstellung	13
9 Auswertung	14
9.1 Allgemeines	14
9.2 Berechnung von Maßgrößen für die Funktionsfähigkeit	15
9.3 Berechnung von Maßgrößen für die Verfügbarkeit und Instandhaltbarkeit	15
9.4 Berechnung von Maßgrößen für die Sicherheit	16
10 Dokumentation der Ergebnisse	16
Anhang A (informativ) Grundlegende mathematische Beziehungen bei Markoff-Verfahren	18
Anhang B (informativ) Beispiel: Entwicklung von Zustandsübergangsdiagrammen	21
Anhang C (informativ) Beispiel: Berechnung einiger Zuverlässigkeits- und Sicherheitsmaßgrößen eines 1-von-2-Systems mit funktionsbeteiligter Redundanz	26
Literaturhinweise	31
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	33
 Bild 1 – Diagramm der Übergangswahrscheinlichkeiten im Zeitintervall $(t, t + \Delta t)$ für beliebige t und kleine Δt für ein nicht wiederherstellbares Ein-Element-System mit der konstanten Ausfallrate λ	9
Bild 2 – Zustandsübergangsdiagramm eines nicht wiederherstellbaren Ein-Einheiten-Systems	10
Bild 3 – Interpretation von Ausfall- und Wiederherstellungszeiten in unterschiedlichen Zusammenhängen	15

	Seite
Bild B.1 – Zustandsübergangsdiagramm für ein wiederherstellbares Ein-Element-System	21
Bild B.2 – Zustandsübergangsdiagramm mit drei Zuständen für ein Ein-Element-System	21
Bild B.3 – Zustandsübergangsdiagramm, falls eine Wiederherstellung aus Zustand 2 eines Ein-Element-Systems heraus möglich ist.....	21
Bild B.4 – Zustandsübergangsdiagramm, falls in einem Ein-Element-System ein direkter Übergang berücksichtigt werden muss	22
Bild B.5 – Zustandsübergangsdiagramm für die Berechnung der Überlebenswahrscheinlichkeit eines Ein-Element-Systems	22
Bild B.6 – Zustandsübergangsdiagramm für ein 1-von-2-System mit funktionsbeteiligter Redundanz ohne wiederherstellbare Elemente.....	22
Bild B.7 – Zustandsübergangsdiagramm für ein 1-von-2-System mit funktionsbeteiligter Redundanz mit wiederherstellbaren Elementen, zwei Wiederherstellungsteams und keiner Beschränkung der Wiederherstellungsmittel.....	23
Bild B.8 – Zustandsübergangsdiagramm für ein 1-von-2-System mit funktionsbeteiligter Redundanz mit wiederherstellbaren Elementen, zwei Wiederherstellungsteams und gemeinsamer Ursache für einen Systemausfall.....	23
Bild B.9 – Zustandsübergangsdiagramm für ein 1-von-2-System mit funktionsbeteiligter Redundanz mit nur einem Wiederherstellungsteam und der Wiederherstellungspriorität „erster Ausfall wird als erster wieder beseitigt“	24
Bild B.10 – Zuverlässigkeitsblockdiagramm für ein 2-von-4-System mit funktionsbeteiligter Redundanz	24
Bild B.11 – Zusammengelegtes Zustandsübergangsdiagramm für die Berechnung der Funktionsfähigkeit des Systems in Bild B.10.....	25
Bild C.1 – Zustandsübergangsdiagramm für ein 1-von-2-System mit funktionsbeteiligter Redundanz mit unterschiedlichen Elementen und zwei Wiederherstellungsteams	26
Bild C.2 – Zustandsübergangsdiagramm für ein 1-von-2-System mit funktionsbeteiligter Redundanz mit identischen Elementen, zwei Wiederherstellungsteams und unbegrenzten Wiederherstellungsmitteln	26
Bild C.3 – Zahlenbeispiel für die Nichtverfügbarkeit.....	28
Bild C.4 – Zahlenbeispiel für Gefährdungsrate.....	30

Einleitung

Für die Untersuchung der Zuverlässigkeit und Sicherheit stehen verschiedene analytische Verfahren zur Verfügung. Eines davon ist das Markoff-Verfahren. Die Internationale Norm IEC 60300-3-1 enthält einen Überblick über die verfügbaren Verfahren und deren allgemeine Eigenschaften.

In dieser Norm werden die grundlegende Terminologie und die Symbole für die Anwendung des Markoff-Verfahrens festgelegt. Es werden Grundregeln für die Entwicklung, Darstellung und Anwendung des Markoff-Verfahrens beschrieben sowie die Annahmen und Einschränkungen dieser Vorgehensweise benannt.

1 Anwendungsbereich

Diese Internationale Norm enthält Anleitungen zur Anwendung des Markoff-Verfahrens für die Modellierung und Analyse eines Systems und zur Schätzung der Zuverlässigkeitsmaßgrößen (Funktionsfähigkeit, Verfügbarkeit, Instandhaltbarkeit) und Sicherheitsmaßgrößen.

Diese Norm ist in industriellen Bereichen anwendbar, in denen Zustands-abhängiges Verhalten von Systemen zu analysieren ist. Bei den in dieser Norm behandelten Markoff-Verfahren werden zeitlich konstante Übergangsraten angenommen. Solche Verfahren werden auch als homogene Markoff-Verfahren bezeichnet.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

IEC 60050(191):1990, *International Electrotechnical Vocabulary (IEV) Chapter 191: Dependability and quality of service*.

IEC 60300-3-1, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability: Guide on methodology*.

IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe und Definitionen nach IEC 60050(191):1990 sowie die nachfolgenden.

ANMERKUNG Um bei Sicherheitsbeurteilungen die Anwendbarkeit dieser Norm zu erleichtern, wird die Terminologie von IEC 61508 soweit als möglich verwendet.

3.1

System

Satz von in Wechselbeziehung oder Wechselwirkung stehenden Elementen

[ISO 9000:2000, 3.2.1]

ANMERKUNG 1 Im Zusammenhang mit Zuverlässigkeit besteht ein System aus einem vorgegebenen Zweck, der durch die angeforderten Funktionen beschrieben ist, und festgelegten Betriebs-, Einsatz- und Randbedingungen.

ANMERKUNG 2 Die Struktur eines Systems kann hierarchisch sein.

3.2

Element

Komponente oder Menge von Komponenten, die als Betrachtungseinheit angesehen werden

ANMERKUNG Ein Element kann üblicherweise nur zwei Zustände einnehmen: klar oder unklar (siehe 3.4 und 3.5). Der Einfachheit halber wird der Begriff **Elementzustand** verwendet, um den Zustand einer Einheit zu bezeichnen.

3.3

Systemzustand

$X(t)$

besondere Kombination von Elementzuständen

ANMERKUNG $X(t)$ bezeichnet den Zustand des Systems zur Zeit t . Es gibt weitere Faktoren, die sich auf den Systemzustand auswirken können (z. B. die Betriebsart).

3.4

betriebsfähiger Zustand; Klarzustand

Systemzustand (oder Elementzustand), in dem das System (oder das Element) die geforderte Funktion erfüllen kann

ANMERKUNG Ein System kann aus mehreren unterscheidbaren Klarzuständen bestehen (z. B. voll und eingeschränkt betriebsfähige Zustände).

3.5

nicht verfügbarer Zustand; Unklarzustand

Systemzustand (oder Elementzustand), in dem das System (oder das Element) die geforderte Funktion nicht erfüllen kann

ANMERKUNG Ein System kann aus mehreren unterscheidbaren Unklarzuständen bestehen.

3.6

Gefährdung (en: hazard)

potentielle Schadensquelle für die Gesundheit von Menschen oder für Sachwerte

[IEC 61508-4, 3.1.2 modifiziert]

3.7

gefahrbringender Ausfall

Ausfall mit dem Potential, das sicherheitsbezogene System in einen gefährlichen oder funktionsunfähigen Zustand zu versetzen

[IEC 61508-4, 3.6.7 modifiziert]

ANMERKUNG 1 Ob ein solcher Funktionszustand eintritt oder nicht, kann von der Systemarchitektur abhängen.

ANMERKUNG 2 Der Begriff „gefährlicher Ausfall“ ist in diesem Zusammenhang ebenfalls üblich.

3.8

ungefährlicher Ausfall

Ausfall ohne das Potential, das sicherheitsbezogene System in einen gefährlichen oder funktionsunfähigen Zustand zu versetzen

[IEC 61508 modifiziert]

3.9

Übergang

Veränderung von einem Zustand in einen anderen

ANMERKUNG Ein Übergang ist üblicherweise das Ergebnis eines Ausfalls oder einer Wiederherstellung. Ein Übergang kann auch durch andere Ereignisse hervorgerufen werden, wie beispielsweise durch menschliches Versagen, äußere Ereignisse, Rekonfiguration von Software usw.

3.10

Übergangswahrscheinlichkeit

$$P_{ij}(t)$$

bedingte Wahrscheinlichkeit für den Übergang vom Zustand i in den Zustand j während eines gegebenen Zeitintervalls $(s, s+t)$ unter der Voraussetzung, dass sich das System zu Beginn dieses Zeitintervalls im Zustand i befindet

ANMERKUNG 1 Formal ist $P_{ij}(s, s+t) = P(X(s+t) = j | X(s) = i)$. Im Falle eines zeitlich homogenen Markoff-Prozesses hängt $P_{ij}(s, s+t)$ nicht von s ab und wird mit $P_{ij}(t)$ bezeichnet.

ANMERKUNG 2 Im Falle eines nicht reduzierbaren Markoff-Prozesses (d. h., falls jeder Zustand aus jedem anderen Zustand erreicht werden kann) ist $P_{ij}(\infty) = P_j$, wobei P_j die asymptotische und stationäre Verfügbarkeit des Zustands j ist.

3.11

Übergangsrate

$$q_{ij}$$

Grenzwert, falls er existiert, des Verhältnisses der bedingten Wahrscheinlichkeit, dass sich ein Übergang vom Zustand i in den Zustand j während eines gegebenen Zeitintervalls $(t, t+\Delta t)$ ereignet, und der Dauer des Intervalls Δt , wenn Δt gegen Null geht, vorausgesetzt, das System befindet sich zur Zeit t im Zustand i

ANMERKUNG In diesem Zusammenhang wird auch p_{ij} bzw. c_{ij} verwendet.

3.12

Anfangszustand

Systemzustand zur Zeit $t = 0$

ANMERKUNG Ein System nimmt im Allgemeinen seinen Betrieb bei $t = 0$ in einem Klarzustand auf, dabei funktionieren alle Elemente des Systems. Anschließend geht das System in seinen Endzustand über, also in den Unklarzustand, und durchläuft dabei andere Klarzustände mit abnehmender Anzahl funktionsfähiger Elemente.

3.13

absorbierender Zustand

Zustand, der, falls er einmal eingetreten ist, nicht mehr verlassen werden kann (d. h., aus diesem Zustand sind keine weiteren Übergänge mehr möglich)

3.14

wiederherstellbares System

System, das Einheiten enthält, die ausfallen und danach in ihren funktionsfähigen Zustand wiederhergestellt werden können, ohne dass das System dabei notwendigerweise ausfällt

ANMERKUNG In diesem Zusammenhang wird auch von reparierbar gesprochen.

3.15

nicht wiederherstellbares System

System, dessen Zustandsdiagramm nur Übergänge in Richtung Systemausfall-Zustände enthält

ANMERKUNG In diesem Zusammenhang wird auch von nicht reparierbar gesprochen.

4 Symbole, Formelzeichen und Abkürzungen

4.1 Symbole für Zustandsdiagramme

Markoff-Verfahren werden graphisch durch Zustandsübergangsdiagramme oder durch Übergangsraten-diagramme dargestellt. Beide Begriffe werden in dieser Norm in gleichwertiger Weise verwendet.

Folgende Symbole werden in dieser Norm verwendet. Andere Symbole dürfen nach Bedarf verwendet werden.

4.1.1

Zustandssymbol

Ein Zustand wird durch einen Kreis oder ein Rechteck dargestellt.

ANMERKUNG Zur Verbesserung der Lesbarkeit dürfen Unklarzustände hervorgehoben werden, z. B. durch fette Linien, Einfärbung, Schraffur.

4.1.2

Zustandsbeschreibung

Die Zustandsbeschreibung wird in das Zustandssymbol hineingeschrieben; sie kann aus Worten oder alpha-numerischen Zeichen bestehen und gibt die den Zustand kennzeichnenden Kombinationen ausgefallener und funktionsfähiger Elemente an.

4.1.3

Zustandsmarkierung

Eine Zustandsmarkierung ist eine Zahl oder ein Buchstabe in einem Kreis, neben dem Zustandssymbol oder bei fehlender Zustandsbeschreibung innerhalb des Symbols selbst.

ANMERKUNG Oft ist es ausreichend, den Zustand durch einen Kreis mit der Zustandsnummer bzw. dem Buchstaben anzugeben.

4.1.4

Übergangspfeil

Der Übergangspfeil zeigt die Richtung eines Überganges an (als Ergebnis eines Ausfalls oder einer Wiederherstellung). Die Übergangsrate wird neben den Übergangspfeil geschrieben.

4.2 Sonstige Formelzeichen und Abkürzungen

Die Formelzeichen für Maßgrößen der Zuverlässigkeit und Sicherheit sind, soweit verfügbar, aus IEC 60050(191) entnommen. Die nachfolgenden Verweise mit dem Vorsatz 191 beziehen sich auf IEC 60050(191). In vorliegender Internationaler Norm werden folgende Formelzeichen verwendet:

Formelzeichen/ Abkürzung	Begriff	Verweis
$R(t)$	Überlebensfähigkeit ANMERKUNG In 191-12-01 wird das allgemeine Symbol $R(t_1, t_2)$ verwendet.	
DFR	Gefährdungsrate (en: dangerous failure rate) ANMERKUNG Im Zusammenhang mit Sicherheit wird üblicherweise die Gefährdungsrate HR (en: hazard rate, HR) anstelle von DFR verwendet.	IEC 61508
MTTF	mittlere Dauer bis zum Ausfall	191-12-07
MTTFF	mittlere Dauer bis zum ersten Ausfall	191-12-06
MTTFH	mittlere Dauer bis zur ersten gefährlichen Situation	
PFD	Wahrscheinlichkeit eines Ausfalls bei Anforderung (Nichtverfügbarkeit) (en: probability of failure on demand)	IEC 61508

ANMERKUNG PFD entspricht zu einer gegebenen Zeit t $\sum_j P_j(t)$ für alle Unklarzustände j .

$\lambda(t)$	(momentane) Ausfallrate	191-12-02
$\mu(t)$	Wiederherstellungsrate ANMERKUNG In 191-13-02 wird $\mu(t)$ für die Instandsetzungsrate verwendet.	
$A(t)$	momentane Verfügbarkeit	191-11-01
$U(t)$	momentane Nichtverfügbarkeit	191-11-02
A	asymptotische und stationäre Verfügbarkeit ANMERKUNG Die stationäre Verfügbarkeit hat den gleichen Zahlenwert wie die asymptotische Verfügbarkeit.	
MUT	mittlere Klardauer	191-11-11
MDT	mittlere Unklardauer	191-11-12
$P_i(t)$	Wahrscheinlichkeit, das System zum Zeitpunkt t im Zustand i anzufinden	
P_i	asymptotische und stationäre Wahrscheinlichkeit, das System zum Zeitpunkt t im Zustand i anzufinden	
Δt	ein kleines Zeitintervall	
$P_{ij}(t)$	Übergangswahrscheinlichkeit vom Zustand i in den Zustand j innerhalb der Zeit t	
q_{ij}	Übergangsrate vom Zustand i in den Zustand j , $j \neq i$ ANMERKUNG q_i ist formal definiert als $q_i = \sum_{j \neq i} q_{ij}$. Sie ist die Abgangsrate aus dem Zustand i .	

4.3 Beispiel

Bild 1 zeigt in einem Diagramm beispielhaft die Übergangswahrscheinlichkeit im Zeitintervall $(t, t + \Delta t)$ für beliebige t und kleine Δt für eine nicht wiederherstellbare Einheit mit der konstanten Ausfallrate λ .

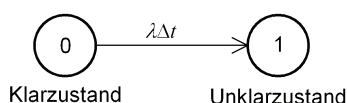


Bild 1 – Diagramm der Übergangswahrscheinlichkeiten im Zeitintervall $(t, t + \Delta t)$ für beliebige t und kleine Δt für ein nicht wiederherstellbares Ein-Element-System mit der konstanten Ausfallrate λ

$\lambda\Delta t$ ist die bedingte Wahrscheinlichkeit für einen Übergang vom Zustand 0 in den Zustand 1 während des kleinen Zeitintervalls $(t, t + \Delta t)$ unter der Voraussetzung, dass sich das System zur Zeit t im Zustand 0 befand. Um die Darstellung zu vereinfachen, wird Δt oft weggelassen, dadurch wird das Diagramm der Übergangswahrscheinlichkeiten in Bild 1 zum Übergangsratendiagramm in Bild 2.