# Normen zum Qualitätsmanagement bei der Softwareentwicklung

**Autoren:**

Dr. Ralf Kneuper (Korrekturaddresse)
Philipp-Röth-Weg 14
64295 Darmstadt

Frank Sollmann
Darmstädter Straße 114
64625 Bensheim

**Kurztitel:** Normen zum Qualitätsmanagement

**Zusammenfassung.** Qualitätsmanagement von Software gewinnt in Wirtschaft und Forschung zunehmend an Bedeutung. Deshalb haben verschiedene Institutionen Normen auf diesem Gebiet entwickelt. Diese sollen die betroffenen Unternehmen unterstützen, geeignete Ansätze und Verfahren auszuwählen, sowie nach außen Vertrauen zu schaffen, daß gewisse Mindestanforderungen erfüllt sind. Die vorliegende Arbeit gibt einen Überblick über die wichtigsten Normen zum Qualitätsmanagement. Ziel ist es, den Leser beim Einstieg in dieses Thema sowie bei der Auswahl der für ihn relevanten Normen zu unterstützen.

**Schlüsselwörter:** Qualitätsmanagement, Qualitätssicherung, ISO 9000, Normen

**Summary.** Software quality management is getting increasingly important in business and research. This has led various institutions to develop norms in this area which are intended to support the businesses concerned to select adequate approaches and procedures, and to provide confidence to externals that certain minimal conditions are met. This paper provides a survey of the most important norms on quality management in software development. It aims to ease the way into this field and support the reader in selecting those norms relevant to him.

**Key words:** Quality management, quality assurance, ISO 9000, norms.

**Computing Reviews Classifications:** D.2.9, K.6.4

# 1. EINLEITUNG

## 1.1 Motivation

Qualitätsmanagement von Software gewinnt in Wirtschaft und Forschung zunehmend an Bedeutung. Dafür gibt es zwei Hauptgründe:

Zum einen ist Qualität bei Softwareprodukten ein immer wichtiger werdender Wettbewerbsfaktor, verursacht vor allem durch das gestiegene Qualitätsbewußtsein der Kunden. Zum anderen ist die Korrektur von Fehlern zu einem erheblichen Kostenfaktor geworden, den man durch frühzeitiges Qualitätsmanagement zu reduzieren sucht.

Aus diesen Gründen, allerdings mit sehr unterschiedlichen Ansatzpunkten, haben verschiedene Institutionen Normen auf dem Gebiet des Qualitätsmanagements entwickelt. Diese sollen die betroffenen Unternehmen unterstützen, geeignete Ansätze und Verfahren auszuwählen, sowie nach außen, also vor allem gegenüber Kunden, Vertrauen zu schaffen, daß gewisse Mindestanforderungen erfüllt sind. Dabei ist zu beachten, daß nicht alle diese Normen sich speziell auf Software und ihre Entwicklung beziehen, sondern teilweise Grundideen des Qualitätsmanagements unabhängig von der betroffenen Branche beschreiben (so z.B. die in Abschnitt 2.1 beschriebenen Normen der ISO 9000-Familie) und also auch bei der Softwareentwicklung anwendbar sind..

## 1.2 Aufbau und Umfang

Nach der Einleitung geben Kapitel 2 und 3 einen Überblick über verschiedene Normen und normenähnliche Dokumente zum Qualitätsmanagement. Nicht behandelt werden jedoch Normen, die nur für bestimmte Branchen oder Kunden gelten, wie z.B. die AQAP-Normen der NATO. Kapitel 4 vergleicht diese verschiedenen Dokumente und die darin verwendeten Ansätze.

Kapitel 5 schließlich zieht ein Fazit und gibt einen Ausblick auf die erwartete zukünftige Bedeutung von Normen für das Software-Qualitätsmanagement.

Ziel ist es, einen Überblick über die wichtigsten Normen in diesem Bereich zu geben, um den Leser beim Einstieg in dieses Thema sowie bei der Auswahl der für ihn relevanten Normen zu unterstützen. Eine wissenschaftliche Auseinandersetzung mit dem Qualitätsmanagement von Software wird hier nicht angestrebt, hierfür sind z.B. die Themenhefte des Informatik Spektrums vom Juni 1987 (Software-Qualitätssicherung) und vom Oktober 1993 (25 Jahre Software Engineering) oder der Tagungsbericht der Fourth European Conference on Software Quality vom Oktober 1994 zu empfehlen.

## 1.3 Begriffe

Qualität wird in ISO 8402 (siehe Tabelle 1) definiert als "*Gesamtheit von Merkmalen einer Einheit bezüglich ihrer Eignung, festgelegte und vorausgesetzte Erfordernisse zu erfüllen*." Merkmale, welche die Qualität mitbestimmen, heißen Qualitätsmerkmale. Dabei ist der Begriff der *Einheit* sehr allgemein zu verstehen: Eine Einheit kann das Endprodukt, aber auch z.B. ein Zwischenprodukt, ein Prozeß, eine Person oder eine Organisation sein.

Nach dieser Definition stellt Qualität kein Absolutum dar, sondern muß in Relation zu den an

die Einheit gestellten Forderungen, den sogenannten "Qualitätsforderungen", gesehen werden. Qualität ist demzufolge ein Maß der Abweichung oder Nichtabweichung von Istdaten zu Solldaten. Die Qualitätsforderungen an eine Einheit ergeben sich aus ihrem Verwendungszweck und können daher sehr unterschiedlich ausfallen.

Gemäß der von der internationalen Normungsorganisation ISO in ISO 8402 (Entwurf 1992) eingeführten Definition wird im folgenden der Oberbegriff Qualitätsmanagement und nicht Qualitätssicherung verwendet. Dies gilt auch dann, wenn in der jeweils beschriebenen Norm noch von Qualitätssicherung die Rede ist.

Laut dieser neuen Definition umfaßt Qualitätsmanagement (QM) "*alle Tätigkeiten der Gesamtführungsaufgabe, welche die Qualitätspolitik, Ziele und Verantwortungen festlegen sowie diese durch Mittel wie Qualitätsplanung, Qualitätslenkung, Qualitätssicherung und Qualitätsverbesserung im Rahmen des Qualitätsmanagementsystems verwirklichen*".

Unter Qualitätssicherung versteht man nun das, was früher als "Darlegung der Qualitätssicherung" bezeichnet wurde, also jene Tätigkeiten, mit denen man Vertrauen in die Qualität eines Objektes schaffen will (beim Produzenten selbst oder beim Kunden, evtl. auch bei dritten wie z.B. staatlichen Institutionen). Im Bereich der Software-Entwicklung sind dies in erster Linie analytische Maßnahmen wie Review oder Test. Qualitätslenkung dagegen, die "*Arbeitstechniken und Tätigkeiten, die zur Erfüllung der Qualitätsforderungen angewendet werden*", umfaßt vor allem konstruktive Maßnahmen wie z.B. den Einsatz von Entwicklungsmethoden oder die Verwendung von Programmierrichtlinien.

Entsprechend spricht man auch nicht mehr von einem Qualitätssicherungssystem, sondern von einem Qualitätsmanagementsystem (QM-System)[1]. Darunter versteht man laut ISO 8402 "*die Organisationsstruktur, Verantwortlichkeiten, Prozesse und erforderlichen Mittel für die Verwirklichung des Qualitätsmanagements*".

## 1.4 Klassen von Normen

Traditionelles Qualitätsmanagement (für Software wie auch für materielle Produkte) basiert auf dem Ansatz, das fertige Produkt mehr oder weniger gründlich auf Erfüllung der Anforderungen zu prüfen (in erster Linie durch Test) und gefundene Abweichungen zu korrigieren. Dieser Ansatz hat sich aber als nicht ausreichend erwiesen. Gründe dafür sind die hohen Kosten sowohl des intensiven Tests eines fertigen Produktes als auch der nachträglichen Korrektur von beim Test gefundenen Fehlern.

Daher geht man heute zunehmend dazu über, die Qualität des Softwareproduktes indirekt über die Qualität des Entwicklungsprozesses zu verbessern. Prüfungen und Tests sind dann Teilaufgaben dieses Prozesses und als solche nur Teil des gesamten Qualitätsmanagements. Dieser Ansatz basiert auf der Hypothese, daß man durch einen qualitativ hochwertigen Prozeß auch voraussagbar qualitativ hochwertige Produkte herstellen kann. Zwar kann man auch durch unstrukturierte Prozesse hohe Produktqualität erreichen, aber die Ergebnisse schwanken in der Regel sehr stark zwischen sehr guten und sehr schlechten Ergebnissen.

Als Folge dieses neuen, prozeßorientierten Ansatzes unterscheiden wir folgende Klassen von Normen:

[1] Gelegentlich auch kürzer von einem Qualitätssystem, entsprechend der in der englischsprachigen Version der ISO 8402 verwendeten Bezeichnung *quality system*.

- Prozeßnormen und Normen zu QM-Systemen
  Hier ist in erster Linie die ISO 9000-Familie zu nennen.
- Produktnormen
  Hierunter fallen Standards, die einheitliche Kriterien für die Beurteilung von Produktqualität zur Verfügung stellen. Diese Normen, wie z.B. ISO 12 119, beziehen sich allein auf die analytische Bewertung von Produkten und nicht auf den Erstellungsprozeß.

Zwischen beiden Klassen gibt es Mischformen, die z.B. Zwischenergebnisse der Softwareentwicklung beschreiben. Hierzu gehören vor allem die IEEE Normen.

## 1.5 Auditierung, Zertifizierung und Akkreditierung

Ein Teil der behandelten Normen ist Basis für eine Zertifizierung, d.h. diese Normen enthalten Forderungen, deren Einhaltung durch ein entsprechendes Zertifikat bescheinigt werden kann. Basis für eine Zertifizierung ist eine meist als (Qualitäts-) Audit[2] bezeichnete Prüfung, ob die jeweiligen Anforderungen erfüllt sind.. Entsprechend den verschiedenen Klassen von Normen unterscheidet man zwischen

- Systemaudits, bei denen ein ganzes (QM-) System überprüft wird
- Produktaudits, bei denen ein einzelnes Produkt überprüft wird.[3]

Außerdem unterscheidet man zwischen

- "First-Party" Audit, bei dem der Produzent selbst oder ein von ihm Beauftragter das Audit durchführt und das vor allem der eigenen Verbesserung und dem Aufdecken von Lücken dient
- "Second-Party" Audit durch einen Kunden oder dessen Beauftragten
- "Third-Party" Audit durch einen neutralen Dritten, z.B. für eine Zertifizierung.

Beim First-Party Audit spricht man auch vom internen Audit, bei Second- oder Third-Party Audits vom externen Audit.

Die Durchführung von Audits von QM-Systemen wird in ISO 10 011 (siehe Tabelle 1) beschrieben.

Third-Party Audits sind offensichtlich nur interessant, wenn die zertifizierende Stelle auch vom Kunden akzeptiert wird. Im gesetzlich geregelten Bereich können natürlich nur staatlich anerkannte Stellen ein solches Zertifikat ausstellen, während es im privatwirtschaftlichen Bereich keine solche Einschränkung gibt. Dies hat zu einer weiteren Ebene der Zertifizierung geführt, nämlich der Zertifizierung der Zertifizierungsstellen, genannt Akkreditierung.

Für Zertifizierungen von QM-Systemen nach ISO 9000 wird das Akkreditierungssystem in Deutschland von der Trägergemeinschaft für Akkreditierung TGA [1] getragen. Die gegenseitige Anerkennung der von akkreditierten Stellen ausgegebenen Zertifikate wird von der EU gefördert als eine Maßnahme zum Abbau von Handelshemmnissen, ist bisher aber nur ansatzweise erreicht. Für Zertifikate über die Einhaltung der Normen ISO 9001-9003 gibt es

---

2 Im engeren Sinne ist ein Qualitätsaudit eine *"unabhängige und systematische Untersuchung"* eines QM-Systems (ISO 8402).

3 Zusätzlich gibt es noch Prozeßaudits, bei denen ein einzelner Prozeß überprüft wird. Da es allerdings kaum Normen gibt, die sich nur auf einen Prozeß beziehen, sind Prozeßaudits üblicherweise auch nicht Basis einer Zertifizierung.

sogar verschiedene konkurrierende Zusammenschlüsse von zertifizierenden Organisationen (z.B. E-Q-Net, itqs) mit dem Ziel der gegenseitigen Anerkennung der Zertifikate. Im Rahmen der freien Marktwirtschaft bleibt es aber letztlich immer dem Kunden überlassen, welchen Wert er einem Zertifikat beimißt. Nur im gesetzlich geregelten Bereich soll in Zukunft die gegenseitige Anerkennung innerhalb der EU garantiert werden.

Für Zertifizierungen nach anderen Normen wurden analoge Akkreditierungssysteme aufgebaut, wobei allerdings aufgrund der geringeren Marktbedeutung meist weniger Zertifizierer zur Auswahl stehen.

# 2. STAND DER NORMUNG

## 2.1 Die ISO 9000-Familie

### 2.1.1 Allgemeines

ISO 9000 ist eine von der "Internationalen Organisation für Normung" (ISO) herausgegebene Familie von Normen und beschreibt den Aufbau von QM-Systemen. Mit dieser Normenfamilie sollen der Industrie und ihren Kunden Kriterien zur Beurteilung der Qualitätsfähigkeit der Unternehmen und damit ein Anhaltspunkt für die Qualität der Produkte gegeben werden.

ISO 9000 ist heute international als *die* Normenfamilie für QM-Systeme anerkannt und wurde von vielen Ländern als nationale Norm übernommen, so z.B. in Deutschland als DIN EN ISO 9000, in Großbritannien als BS 5750, in den USA als ANSI/ASQC Q90. Außerdem wurde sie von der Europäischen Normungsorganisation CEN zur europäischen Norm EN 29000 erklärt. Einen Überblick über die wichtigsten Normen der ISO 9000-Familie gibt Tabelle 1.

Die heute gültige Version der zuerst 1987 herausgegebenen Normenreihe wurde 1994 als sogenannte Kurzzeitrevision verabschiedet. Die Änderungen dienen in erster Linie einer besseren Verständlichkeit und leichteren Anwendbarkeit sowie einer klareren Struktur, während sich die gestellten Anforderungen nur wenig geändert haben. Zur Zeit wird an einer sogenannten Langzeitrevision gearbeitet, in der diese Arbeit fortgesetzt werden soll.

ISO 9000 Teil 1 (ISO 9000-1) gibt eine Einführung in die Normenfamilie, definiert Grundbegriffe und gibt Hilfestellung und Anleitung für die Auswahl zwischen den übrigen Normen der Reihe. ISO 9001 bis 9003 beschreiben Nachweisforderungen an ein QM-System und dienen damit dem externen Nachweis eines angemessenen Qualitätsmanagements gegenüber einem Kunden oder einem neutralen Dritten, z.B. einer Zertifizierungsstelle.

ISO 9004 besteht aus Leitfäden für Aufbau und Struktur eines QM-Systems. Hier wird ein QM-System aus der internen Sicht des betroffenen Unternehmens beschrieben, im Gegensatz zu der externen Sicht in ISO 9001 bis 9003.

Besonders wichtig ist in diesem Zusammenhang noch ISO 9000-3, die die Anwendung von ISO 9001 auf Softwareprodukte beschreibt.

Tabelle 1: Normen der ISO 9000-Familie (Auswahl - Stand August 1995)

| Bezeichnung | Titel |
|---|---|
| DIN ISO 8402 | Qualitätsmanagement und Qualitätssicherung - Begriffe (Entwurf) |
| DIN EN ISO 9000 | Normen zum Qualitätsmanagement und zur Qualitätssicherung/ QM-Darlegung |
| Teil 1 | Leitfaden zur Auswahl und Anwendung |
| Teil 2 | Allgemeiner Leitfaden zur Anwendung von ISO 9001, ISO 9002 und ISO 9003 (Entwurf) |
| Teil 3 | Leitfaden für die Anwendung von ISO 9001 auf die Entwicklung, Lieferung und Wartung von Software |
| DIN EN ISO 9001 | Qualitätsmanagementsysteme - Modell zur Qualitätssicherung/QM-Darlegung in Design, Entwicklung, Produktion, Montage und Wartung |
| DIN EN ISO 9002 | Qualitätsmanagementsysteme - Modell zur Qualitätssicherung/QM-Darlegung in Produktion, Montage und Wartung |
| DIN EN ISO 9003 | Qualitätsmanagementsysteme - Modell zur Qualitätssicherung/QM-Darlegung bei der Endprüfung |
| DIN EN ISO 9004 | Qualitätsmanagement und Elemente eines Qualitätsmanagementsystems |
| Teil 1 | Leitfaden |
| Teil 2 | Leitfaden für Dienstleistungen |
| Teil 7 | Leitfaden für Konfigurationsmanagement (Entwurf) |
| DIN ISO 10 011 | Leitfaden für das Audit von Qualitätssicherungssystemen |
| Teil 1 | Auditdurchführung |
| Teil 2 | Qualifikationskriterien für Qualitätsauditoren |
| Teil 3 | Management von Auditprogrammen |
| DIN ISO 10 013 | Leitfaden für die Erstellung von Qualitätsmanagement-Handbüchern (Entwurf) |

Die Anforderungen der ISO 9000-Normen bestehen im wesentlichen darin, daß alle wichtigen (qualitätsrelevanten) Prozesse und Abläufe definiert und dokumentiert werden, diese Definitionen eingehalten und Ergebnisse dokumentiert werden. Dazu werden eine Reihe von Bereichen aufgelistet, die in einem QM-System geregelt sein müssen, wobei weitgehend offen gelassen ist, wie das getan wird. Man kann diese Normen daher als einen Katalog offener Fragen interpretieren, die beantwortet werden müssen. Wie diese Fragen beantwortet werden, welche Methoden oder Techniken verwandt werden, bleibt weitgehend dem jeweiligen Unternehmen überlassen.

Die wichtigsten Forderungen sind

- Festlegung einer Qualitätspolitik als Grundlage des gesamten QM-Systems
- Definierte Aufbau- und Ablauforganisation mit Regelung von Zuständigkeiten, Befugnissen und Schnittstellen
- Durchführung von internen Audits
- Regelung und Durchführung von Korrekturverfahren
- Definition und Dokumentation aller wichtigen Prozesse und ihrer Ergebnisse. Da diese Anforderung alle im Rahmen der Norm geforderten Prozesse umfaßt, bildet sie eine wichtige Grundlage eines QM-Systems. Aus diesem Grund sollte einer der ersten Schritte bei der Einführung eines QM-Systems die Einführung eines Verfahrens für den Erlaß verbindlicher Regelungen sein (soweit nicht bereits vorhanden)
- Integration der obersten Führungsebene in das QM-System

- Dokumentenlenkung, d.h. kontrollierte Herausgabe, Verteilung, Bekanntmachung und Änderung von verbindlichen Regelungen

Diese Forderungen sind dann auf verschiedene Bereiche anzuwenden, wie z.B. Entwicklung, Korrekturmaßnahmen, Produktion, Schulung der Mitarbeiter, Vertragsprüfung etc.. Hohe Qualität des Endproduktes bzw. des Gesamtprozesses entsteht, so die Grundidee eines QM-Systems, durch das Zusammenwirken und die hohe Qualität all dieser Komponenten.

### 2.1.2 ISO 9001 - 9003

Diese Normen beschreiben drei unterschiedliche Nachweisstufen, die für unterschiedliche Organisationen gedacht sind:

- ISO 9001 gilt für Organisationen, die Produkte im gesamten Lebenszyklus von der Entwicklung über Produktion und Montage bis zur Wartung betreuen.
- ISO 9002 gilt für Organisationen, die Produkte von der Produktion bis zur Wartung betreuen (also ohne Entwicklung).
- ISO 9003 gilt für Organisationen, die Produkte fertigstellen und deren Qualität alleine durch eine Endprüfung sichern.

Daraus ergibt sich eine Hierarchie der Anforderungen, wobei ISO 9001 die umfangreichste und strengste Nachweisstufe bildet. Da ISO 9001 als einzige dieser drei Normen die Entwicklung mit einbezieht, ist sie auch als einzige für die Softwareentwicklung relevant.

### 2.1.3 ISO 9004

Ziel der ISO 9004 ist die Beschreibung eines QM-Systems aus Sicht des betroffenen Unternehmens selbst. Diese Norm gibt also einen Leitfaden für den Aufbau eines QM-Systems, das internen Zwecken und nicht dem Nachweis nach außen, gegenüber einem Kunden oder einem Zertifizierer, dient. Zusätzlich zu den in ISO 9001 betrachteten Anforderungen fließen hier noch Wirtschaftlichkeit sowie Produktsicherheit und Marketing mit ein, die nach Ansicht der Normenautoren für den externen Kunden geringere Bedeutung haben und deshalb nicht Bestandteil der Nachweisforderungen wurden, für das Unternehmen selbst aber lebenswichtig sind. Dafür sind Vertragsprüfung und Lenkung der vom Kunden beigestellten Produkte in ISO 9004 nicht enthalten, die in ISO 9001 bis 9003 gefordert werden.

### 2.1.4 ISO 9000 Teil 3

ISO 9000-3 ist ein Leitfaden für die Anwendung der ISO 9001 bei der Entwicklung von Software, selbst aber keine Basis für eine Zertifizierung.

Abweichend von ISO 9001 gliedert ISO 9000-3 die QM-Maßnahmen in drei Gruppen. Die Zuordnung zu den Forderungen der ISO 9001 läßt sich über eine Tabelle im Anhang der ISO 9000-3 herstellen.[4]

#### 2.1.4.1 QM-System - Rahmen

Hierunter fallen projektübergreifende Tätigkeiten wie die Definition einer Qualitätspolitik sowie die Definition der Verantwortlichkeiten innerhalb der Organisation (Tabelle 8).

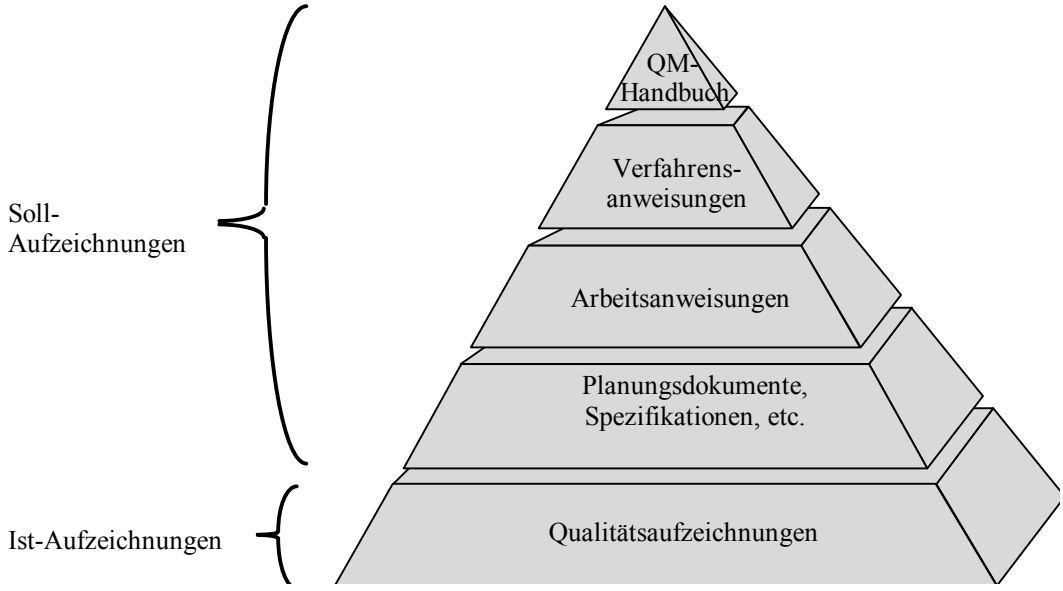
[4] Derzeit allerdings mit Verweis auf die alte Version der ISO 9001 von 1987.

Eine grundlegende Forderung an ein QM-System ist die Dokumentation der zugrundeliegenden Richtlinien und Verfahren. Diese Beschreibung geschieht üblicherweise auf vier Ebenen. Auf der höchsten und abstraktesten Ebene wird der generelle Aufbau des QM-Systems in einem QM-Handbuch beschrieben. Inhalt des QM-Handbuchs sind neben Terminologie die Qualitätspolitik des Unternehmens sowie Verantwortlichkeiten und Abläufe im QM-System. Das QM-Handbuch ist üblicherweise so geschrieben, daß es auch dem Kunden als Nachweis eines angemessenen QM-Systems vorgelegt werden kann und deshalb kein firmenspezifisches Knowhow enthält. Dieses ist auf der Ebene der Verfahrensanweisungen beschrieben, die dann erheblich mehr technische und andere Details enthalten. Noch detaillierter sind die Dokumente der dritten Ebene, meist als Verfahrensanweisungen bezeichnet. Schließlich sind gehören zur Dokumentation noch projektspezifische Planungsdokumente wie z.B. Projektpläne oder Spezifikationen.

Darüber hinaus müssen Qualitätsaufzeichnungen geführt werden, um zu belegen, daß die festgelegten Abläufe auch eingehalten werden. In internen Audits ist dies regelmäßig zu überprüfen.

Die Erstellung und Verwaltung aller solcher Dokumente und Qualitätsaufzeichnungen muß kontrolliert ablaufen, um sicherzustellen, daß sie konsistent sind und alle Beteiligten mit aktuellen Versionen arbeiten. Dazu gehört insbesondere auch ein Konfigurationsmanagement für Dokumente.

Abb. 1: Dokumentation des QM-Systems




### 2.1.4.2 Lebenszyklustätigkeiten

Für die Entwicklung eines Softwareproduktes sollte ein Phasenmodell verwendet werden, in das die verschiedenen qualitätssichernden Tätigkeiten integriert werden. Dabei ist nicht das konkret benutzte Phasenmodell ausschlaggebend, sondern es ist wichtig, daß man sich überhaupt an einem festgelegten und dokumentierten Modell orientiert. Die Norm unterstellt daher auch nicht die Verwendung eines bestimmten Phasenmodells, sie ordnet nur einzelne geforderte Tätigkeiten zeitlich ein (Tabelle 9).

#### 2.1.4.3 Unterstützende Tätigkeiten

Diese unterstützenden, phasenübergreifenden Tätigkeiten (Tabelle 10) umfassen u.a.

- die Einrichtung eines Konfigurationsmanagements
- Verfahren zur Dokumentenlenkung
- Durchführung von Qualitätsmessungen am Produkt und am Prozeß.

### 2.1.5 Anmerkungen

Die ISO 9000-Familie beschreibt einen Rahmen, um ein QM-System in einer Organisation einzuführen und zu betreiben. Die Einführung eines QM-Systems macht es notwendig, sich über alle Vorgänge, Verantwortlichkeiten, Verhaltensweisen und Einstellungen der Mitarbeiter klar zu werden. Diese Dinge müssen offengelegt und dokumentiert werden. Dabei stellt sich oft heraus, daß einzelne Maßnahmen nicht angemessen sind und geändert werden müssen. Dies ist eine große Chance für jedes Unternehmen, seine Abläufe zu optimieren.

Die Allgemeingültigkeit der Normen führt allerdings dazu, daß die Normen sehr vage formuliert sind und daher sehr unterschiedlich interpretiert werden können. Dadurch wird einerseits die Anpassung auf das eigene Unternehmen sehr aufwendig. Andererseits ist es auch möglich, Verantwortlichkeiten und Abläufe auf einem sehr niedrigem Niveau zu regeln, so daß die Anforderungen der Norm zwar formal erfüllt sind, die dadurch erreichte Produktqualität aber trotzdem sehr niedrig ist. Dies ergibt sich auch aus der Tatsache, daß es sich hier um eine Prozeßnorm und keine Produktnorm handelt. Eine weiterer Folge ist, daß Zertifikate verschiedener Zertifizierungsstellen unterschiedlichen Stellenwert auf dem Markt besitzen.

Ein häufig genannter Kritikpunkt ist, daß die Forderungen der ISO 9000 nicht weit genug gehen in Richtung auf eine ganzheitliche Ausrichtung einer Organisation auf das Ziel Qualität, im Sinne des Total Quality Management (TQM). Die Forderungen der ISO 9000 beziehen sich in erster Linie auf die Festlegung von Aufbau- und Ablauforganisation des Unternehmens. Andere Aspekte wie die zentrale Stellung der Kundenzufriedenheit, die Beteiligung und Motivation aller Mitarbeiter sowie die ständige Verbesserung werden nur gestreift.

## 2.2 IEEE Normen zum Qualitätsmanagement

### 2.2.1 Allgemeines

Eine Reihe von Standards des IEEE (Institute of Electrical and Electronics Engineers) beschreibt verschiedene Aspekte des Software Engineering, mit besonderem Schwerpunkt auf Typen und Inhalte von Softwaredokumenten sowie Tätigkeiten und Methoden auf dem Gebiet der Software-Entwicklung. Einige dieser Standards unterstützen das konstruktive QM, indem sie z.B. Vorgaben für Designdokumente oder für die Planung der QM-Aktivitäten machen. Andere beziehen sich stärker auf analytisches QM und beschreiben Aktivitäten wie Test oder Review sowie deren Dokumentation.

Insgesamt sind die IEEE-Standards als Bausteine zu verstehen, mit denen jeweils abgegrenzte Elemente, Tätigkeiten und Maßnahmen innerhalb eines QM-Systems vereinheitlicht werden können. Sie enthalten Vorgaben für einzelne Komponenten eines (Software-spezifischen) QM-Systems, nicht jedoch für das Gesamtsystem.

Für alle diese Standards gilt, daß sie explizit als Hilfestellung gedacht sind und nicht als Nachweisnormen. Deshalb gibt es, im Gegensatz zur ISO 9000, keine Zertifikate für ihre Einhaltung. Dies wäre auch für die meisten wenig sinnvoll, da sie sich jeweils auf einzelne Dokumente und nicht auf allgemeine Abläufe oder Strukturen beziehen.

Tabelle 2: IEEE Standards zu Software-Qualitätsmanagement und Software Engineering (Auswahl)

| Bezeichnung | Titel |
|---|---|
| IEEE Std. 730-1989 | Software Quality Assurance Plans. (IEEE Std. 730.1-1989 wurde umbenannt in IEEE Std. 730-1989.) |
| IEEE Std. 829-1983 | Software Test Documentation (bestätigt 1991.) |
| IEEE Std. 830-1984 | Guide for Software Requirements Specification |
| IEEE Std. 983-1986 | Software Quality Assurance Planning |
| IEEE Std. 1008-1987 | Standard for Software Unit Testing |
| IEEE Std. 1012-1986 | Software Verification and Validation Plans |
| IEEE Std. 1016-1988 | Recommended Practice for Software Design Descriptions |
| IEEE Std. 1028-1988 | Standard for Software Reviews and Audits |
| IEEE Std. 1042-1987 | Guide to Software Configuration Management |
| IEEE Std. 1058.1-1984 | Standard for Software Project Management Plans |
| IEEE Std. 1061-1992 | Standard for Software-Quality Metrics Methodology |

### 2.2.2 IEEE Std. 730 und IEEE Std. 983

Der in diesem Zusammenhang wichtigste Standard ist IEEE Std. 730 in Verbindung mit IEEE Std. 983. Während der erstgenannte Standard den Inhalt eines *Software Quality Assurance Plans (SQAP)* beschreibt, enthält der zweite zusätzlich Hinweise zu Einführung und Umsetzung eines SQAP.

Ein SQAP beschreibt für ein Projekt oder ein Produkt die Tätigkeiten, die innerhalb des Qualitätsmanagements durchzuführen sind. In IEEE Std. 730 ist der Aufbau dieses Dokumentes beschrieben und festgelegt, welche Elemente und Punkte in einem SQAP zu beachten und zu beschreiben sind. Er bezieht sich nicht auf die Aktivitäten des QM selbst, sondern auf deren Planung und Beschreibung.

Gemäß IEEE Std.730 und 983 sollte ein SQAP u.a. die folgenden Punkte enthalten:

- Projektorganisation
- notwendige Dokumente, die die Entwicklung begleiten.
- Standards, Methoden und Konventionen sowie die Überwachung der Einhaltung dieser Vorgaben.
- Reviews und Audits: Festlegung der durchzuführenden Überprüfungen im Software-Entwicklungszyklus
- Test
- Fehlerdokumentation und Korrekturmaßnahmen

IEEE Std. 983 übernimmt (mit einigen Änderungen im Detail) den Aufbau eines SQAP aus IEEE Std. 730 und beschreibt zusätzlich die Ausführung des Plans, Bewertung des Inhalts sowie die Anpassung eines SQAP an sich ändernde Rahmenbedingungen oder Anforderungen.

### 2.2.3 IEEE Std. 829

IEEE Std. 829 enthält Vorgaben für die Dokumentation von Softwaretests. Die Testdokumentation nach dieser Norm umfaßt

- *Testplan*: Testziele, Vorgehensweise und Maßnahmen sowie Personal und Zeitplanung. Der Testplan ist Teil des Qualitätsplanes und damit des Projektplanes.
- *Übergabebericht für Testobjekt*
- *Testentwurfsspezifikation, Testfallspezifikation und Testprozedurspezifikation*: Beschreibung der durchzuführenden Tests. Im Gegensatz zum Testplan bleiben diese Dokumente beim Test neuer Versionen i.A. weitgehend unverändert.
- *Testprotokoll, Testvorfallsbericht und zusammenfassender Bericht* zur Dokumentation der Ergebnisse durchgeführter Tests auf verschiedenen Ebenen

### 2.2.4 IEEE Std. 1012

IEEE Std. 1012 beschreibt Aufbau und Inhalt eines *Software Verification and Validation Plan* (SVVP). Ein SVVP beschreibt die Maßnahmen und Tätigkeiten bei der Verifikation und Validierung und ist damit Teil des SQAP. Ziel ist es,

- Basisanforderungen an die Form und den Inhalt von SVVPs zu stellen
- für kritische Software Mindestanforderungen an die Aufgaben und die dazu notwendigen Daten eines SVVPs aufzustellen
- einen Baukasten für die Auswahl von Tätigkeiten und Maßnahmen im Rahmen einer Verifikation und Validation (V&V) bei nichtkritischer Software bereitzustellen.

Die Norm enthält eine Übersicht über die Aufgaben und organisatorischen Aspekte bei der Durchführung von V&V-Maßnahmen. Zusätzlich werden die V&V-Tätigkeiten in den einzelnen Phasen des Software-Entwicklungszyklus beschrieben, Anforderungen an die Dokumentation der Maßnahmen und Ergebnisse gestellt sowie administrative Aufgaben dargestellt.

### 2.2.5 IEEE Std. 1028

Thema von IEEE Std. 1028 sind die verschiedenen Formen von Software Reviews und Audits:

- *Management-Reviews*, bei denen Projektplanung und Projektstatus relativ zum Projektplan beurteilt werden
- *technische Reviews*, deren Ziel die Prüfung und Bewertung eines Softwareelementes, also eines Entwicklungsdokumentes oder -ergebnisses, sind
- *Software-Inspektionen*, bei denen die Suche nach Fehlern in einem Softwareelement im Vordergrund steht
- *Walkthrough*, bei denen der Autor ein Softwareelement zuerst vorstellt. Anschließend gehen die Teilnehmer es gemeinsam Schritt für Schritt durch und sammeln Fehler und Änderungs- und Verbesserungsvorschläge
- *Audits* zur Überprüfung der Einhaltung von Vorgaben, Standards und Richtlinien.

Für jede dieser Formen von Reviews werden u.a. Ziele, Ein- und Ausgabedaten sowie Anfangs- und Endebedingungen beschrieben. Die verschiedenen Formen von Reviews sind dabei jeweils als Techniken zu betrachten, die auf unterschiedliche Ergebnisse angewandt werden können. Eine mögliche Zuordnung wird in einem Anhang beschrieben.

## 2.3 ISO 9126

Zur Definition von zu erreichenden Qualitätszielen muß der Begriff der Softwarequalität präzisiert werden. Dazu definiert man einzelne Qualitätsmerkmale, deren Gesamtheit die Qualität des SW-Produktes ausmacht. Eine solche Aufschlüsselung von Softwarequalität in einzelne Qualitätsmerkmale liefert z.B. ISO 9126 (Tabelle 3). ISO 9126 definiert die Software-Qualitätsmerkmale Funktionalität, Zuverlässigkeit, Benutzbarkeit, Effizienz, Wartbarkeit und Portierbarkeit. In einem Anhang werden diese Merkmale dann in Untermerkmale gegliedert; so besteht Effizienz z.B. aus den Untermerkmalen Zeitverhalten und Ressourcenverhalten.

Tabelle 3: ISO 9126

| Bezeichnung | Titel |
|---|---|
| ISO/IEC 9126 (1991) | Information technology - Software product evaluation - Quality characteristics and guidelines for their use |
| DIN 66 272 | Informationstechnik; Bewerten von Softwareprodukten; Qualitätsmerkmale und Leitfaden zu ihrer Verwendung (identisch mit ISO/IEC 9126) |

Mit der Definition von Qualitätsmerkmalen ist gleichzeitig eine Basis für die Bewertung der Qualität von Software gelegt. Dieser Aspekt wird in ISO 9126 kurz angerissen und soll in einer zukünftigen Erweiterung weiter ausgearbeitet werden 3.[5] Dabei sollen für die einzelnen Qualitätsmerkmale jeweils verschiedene Techniken wie Funktionstest, Review, Fehlertoleranzanalyse oder formaler Beweis festgelegt werden, die bei einer Bewertung von Software nach dem jeweiligen Merkmal zu benutzen sind. Um unterschiedliche Typen von Software abzudecken, werden dabei verschiedene Bewertungsstufen (von Spielesoftware bis zu Systemen für Flug- oder Zugsicherung) unterschieden. Es ist allerdings innerhalb der zuständigen Gremien noch umstritten, inwieweit dabei konkrete Bewertungsverfahren und Metriken für die einzelnen Qualitätsmerkmale vorgegeben werden sollen.

## 2.4 ISO 12 119

1985 erstellte die Gütegemeinschaft Software (GGS) die Richtlinie RAL-GZ 901 zur einheitlichen Prüfung von Softwareprodukten, die in überarbeiteter Form als DIN 66 285 übernommen wurde. Eine weitere Überarbeitung wurde 1994 als internationale Norm ISO 12 119 herausgegeben und dann wiederum als deutsche Norm übernommen (Tabelle 3). Besteht ein Produkt (in Deutschland) die festgelegten Prüfungen, so wird ihm das RAL-Gütezeichen Software verliehen.

[5] Diese Erweiterung von ISO 9126 basiert u.a. auf Ergebnissen des Esprit-Projektes SCOPE (Software Assessment and Certification Programme Europe).

Tabelle 4: ISO 12 119

| Bezeichnung | Titel |
|---|---|
| DIN 66 285 (1990) | Informationsverarbeitung; Anwendungssoftware; Gütebedingungen und Prüfbestimmungen |
| DIN ISO/IEC 12 119 (1995) | Informationstechnik; Software-Erzeugnisse; Qualitätsanforderungen und Prüfbestimmungen (identisch mit ISO/IEC 12 119:1994; ersetzt DIN 66 285) |

ISO 12 119 besteht aus den Qualitätsanforderungen (früher Gütebedingungen) und den Prüfbestimmungen zur Prüfung der Erfüllung dieser Forderungen. Als reine Produktnorm stellt ISO 12 119 keine direkten Forderungen an den Entwicklungsprozeß und an Maßnahmen während der Entwicklung der Software, sondern bezieht sich lediglich auf eine Endprüfung. Die Qualitätsanforderungen behandeln daher die Produktteile

- Produktbeschreibung zur Information des Kunden vor dem Kauf
- Dokumentation
- Programme und Daten. Diese Qualitätsanforderungen beziehen sich auf die in ISO 9126 genannten Qualitätsmerkmale

Nicht einbezogen sind unterstützende Dienstleistungen wie Beratung, Schulung oder Wartung.

Bei der Prüfung von Programmen und Daten handelt es sich im einen gründlichen Systemtest, der in allen in der Produktbeschreibung angegebenen Soft- und Hardwarekonfigurationen durchgeführt werden muß. Als Hilfestellung wurde von der GMD (Gesellschaft für Mathematik und Datenverarbeitung) ein Rahmenprüfplan [2] erstellt, der sich allerdings noch auf die Vornorm DIN 66 285 von 1985 bezieht.

### 2.4.1 Anmerkungen

ISO 12 119 ist, im Gegensatz zu ISO 9000, eine Produktnorm mit allen damit verbundenen Vor- und Nachteilen. Die Norm basiert auf einer Endprüfung und kann daher Mängel, die während des Entwicklungsprozesses des Produkte entstehen, allenfalls nachträglich aufdecken, aber nicht verhüten. Dem Kunden gegenüber wird damit aber die diesen eigentlich interessierende Produktqualität dokumentiert, im Gegensatz z.B. zu einer Zertifizierung nach ISO 9000, die über die Produktqualität nur wenig aussagt.

Ein großes Problem ist der erhebliche Prüfaufwand schon für kleine Produkte und Softwaresysteme. Für hochkomplexe Softwaresysteme ist eine Endprüfung in dem durch die Norm verlangten organisatorischen Rahmen jedoch aus Aufwandsgründen nur selten durchführbar.

Auf dem Markt konnte sich diese Norm bisher kaum durchsetzen. Laut Aufstellung der GGS gab es im Mai 1995 erst 30 mit dem Gütezeichen Software ausgezeichnete Softwareprodukte. Darüber hinaus wird die Norm allerdings auch als Grundlage für die Abnahme von Individualsoftware verwendet.

# 3. NORMENÄHNLICHE DOKUMENTE

## 3.1 V-Modell des Bundes

Das V-Modell des Bundes ist ein Vorgehensmodell für die Softwareentwicklung, das im Auftrag des Bundesministeriums für Verteidigung entwickelt und 1992 in einer überarbeiteten und mit dem Bundesministerium des Innern abgestimmten Version herausgegeben wurde. Es ist in erster Linie als Grundlage für Ausschreibungen und Verträge gedacht, kann aber auch innerhalb eines Unternehmens ohne Forderung von außen verwendet werden. Bei der Vergabe von größeren Entwicklungsaufträgen schreiben Bundesbehörden häufig den Einsatz des V-Modells vor.

Das V-Modell beschreibt den Entwicklungsprozeß durch eine Reihe von Aktivitäten und Produkten, die im Rahmen dieser Aktivitäten erstellt werden. Es ist in vier sogenannte Submodelle gegliedert, nämlich

- Projektmanagement (PM)
- Softwareerstellung (SWE)
- Qualitätssicherung (QS)
- Konfigurationsmanagement (KM)

Das Submodell SWE ist ein V-förmig strukturiertes Phasenmodell (daher auch der Name V-Modell) mit einer schrittweisen Verfeinerung der Systemanforderungen (top-down) und anschließender Integration der erstellten Komponenten (bottom-up).

In diesem Zusammenhang am wichtigsten ist das Submodell QS, siehe Tabelle 5. Wie alle Submodelle besteht es aus Aktivitäten sowie im Rahmen der Aktivitäten erstellten Produkten, die dann jeweils noch ausführlicher beschrieben sind. Die Beschreibung einer Aktivität besteht aus dem tabellarischen *Produktfluß* sowie der in Prosa beschriebenen *Abwicklung*. Dieses Submodell befaßt sich in erster Linie mit dem *analytischen* Qualitätsmanagement, also der Prüfung von Ergebnissen. Dagegen kann man das gesamte V-Modell als Beitrag zum *konstruktiven* Qualitätsmanagement interpretieren.

Tabelle 5: V-Modell, Submodell QS

| **Aktivität** | | **Produkt** |
|---|---|---|
| QS 1 | QS-Initialisierung | |
| QS 1.1 | QS-Plan erstellen | QS-Plan |
| QS 1.2 | Prüfplan erstellen | Prüfplan |
| QS 2 | Prozeßprüfung von Aktivitäten | Prüfprotokoll |
| QS 3 | Prüfung vorbereiten | |
| QS 3.1 | Prüfmethoden und -kriterien festlegen | Prüfspezifikation |
| QS 3.2 | Prüfumgebung definieren | Prüfplan |
| QS 3.3 | Prüffälle festlegen | Prüfspezifikation |
| QS 3.4 | Prüfprozedur erstellen | Prüfprozedur |
| QS 4 | Produkt prüfen | |
| QS 4.1 | Prüfbarkeit feststellen | Prüfprotokoll |
| QS 4.2 | Produkt inhaltlich prüfen | Prüfprotokoll |
| QS 5 | Durchführungsentscheidung[6] | Protokoll |
| QS 6 | Fertigprodukt[7] prüfen | Prüfprotokoll |
| QS 7 | QS-Berichtswesen | Interne Mitteilung |

Die universelle Einsetzbarkeit des V-Modells hat zur Folge, daß es für jedes konkrete Projekt erst angepaßt werden muß ("Tailoring"). Tailoring umfaßt die Identifizierung der für das konkrete Projekt erforderlichen sowie die Streichung der nicht erforderlichen Aktivitäten und Produkte. Eine Reihe von Streichbedingungen sind als Teil des V-Modells vorgegeben (so entfällt z.B. die Aktivität *QS 2*, wenn im QS-Plan keine Prüfungen von Aktivitäten festgelegt wurden).

Vor allem bei der Verwendung für den Eigenbedarf eines Unternehmens ist es sinnvoll, eine auf die eigene Situation zugeschnittene und mit zusätzlichen Details ausgefüllte Version des V-Modells zu erstellen. So wird es z.B. für *QS 7 QS-Berichtswesen* häufig schon standardisierte Vorgaben innerhalb eines Unternehmens geben, die nicht für jedes Projekt neu erstellt werden.

## 3.2 SEI Capability Maturity Model

Das SEI Capability Maturity Model [4] (CMM) wurde vom Software Engineering Institute im Auftrag des US-Verteidigungsministeriums (DoD) entwickelt. Ein ähnliches, darauf aufbauendes Modell wurde im Rahmen des von der EG unterstützten Projektes *Bootstrap* erstellt. Im Rahmen des SPICE-Projektes wird derzeit eine ISO-Norm auf Basis dieser Arbeiten entwickelt.

Ziel des CMM ist es, Software-Lieferanten und die Qualität ihrer Prozesse (Prozeßreife) zu bewerten. Dabei werden fünf Stufen definiert: Eine Einheit erreicht eine bestimmte Reife, wenn sie die definierten Kriterien dieser Stufe erfüllt (siehe Tabelle 6).

[6] Eine Durchführungsentscheidung ist im wesentlichen die Abnahme einer Aktivität und ihrer Ergebnisse (Produkte).

[7] Unter "Fertigprodukt" versteht man hier eine bereits bestehende Funktionseinheit, die direkt oder nach Modifikationen in das zu entwickelnde System eingebaut wird.

Tabelle 6: SEI Capability Maturity Model (Quelle: Carnegie-Mellon University, Software Engineering Institute)

| Stufe | Charakterisierung | Hauptproblemgebiete |
|---|---|---|
| 5 *Optimizing* | Ständige Prozeßverbesserung auf Basis der ermittelten Parameter und Problemanalysen etc. | • Automatisierung |
| 4 *Managed* | (quantitativ)<br>Wichtige Prozeßparameter werden regelmäßig ermittelt und analysiert | • Neue Technologien<br>• Problemanalyse und Problemvermeidung |
| 3 *Defined* | (qualitativ)<br>Prozesse sind definiert und eingeführt | • Prozeßmessungen<br>• Problemanalyse<br>• Quantitative Qualitätspläne |
| 2 *Repeatable* | (intuitiv)<br>Prozesse sind unter gleichen Bedingungen in etwa wiederholbar, hängen aber noch sehr von einzelnen Personen ab. Grundlegendes Projektmanagement ist vorhanden | • Schulung<br>• Techniken wie Review, Test<br>• Prozeßfokussierung |
| 1 *Initial* | (ad hoc / chaotisch)<br>keine Anforderungen | • Projektmanagement<br>• Projektplanung<br>• Konfigurationsmanagement |

Die Einstufung wird an Hand eines Fragebogens durchgeführt, bei dem jeweils Hauptproblemgebiete (*Key Problem Areas*) abgefragt werden. Von diesem Fragebogen gibt es zwei verschiedene Versionen, die in verschiedenen Formen der Beurteilung eingesetzt werden. *Software Process Assessments* sind Audits von außen, also durch Kunden oder neutrale Dritte, mit dem Ziel der Bewertung des Lieferanten. *Software Capability Evaluations* sind Beurteilungen durch die betroffene Organisation selbst mit dem Ziel der eigenen Verbesserung (mit eigenen oder fremden Auditoren).

In diesem Fall liefert das Modell eine sinnvolle Reihenfolge, in der die verschiedenen Problembereiche angegangen werden sollten. Ist man z.B. auf der ersten Stufe, so sollte zuerst ein systematisches Projektmanagement eingeführt werden, da dieses eine wichtige Grundlage weiterer Verbesserungen bildet. Der Einsatz von Metriken z.B. wird dagegen erst dann sinnvoll, wenn sichergestellt ist, daß ähnliche Meßergebnisse auch auf ähnliche Ursachen zurückzuführen sind. Dazu ist es meist erforderlich, daß die betrachteten Prozesse auch immer gleichartig ablaufen. So erhält man z.B. aus der Anzahl der gefundenen Fehler nur dann eine Aussage über die Qualität eines Produktes, wenn Fehler immer mit der gleichen Intensität gesucht werden und gewährleistet ist, daß alle gefundenen Fehler in die Messung mit aufgenommen werden. Der Prozeß der Meldung gefundener Fehler muß also entsprechend definiert und eingeführt sein.

Vor allem die Stufen 4 und 5 in diesem Modell sind allerdings umstritten, da fast keine Erfahrungen mit ihnen vorliegen und deshalb zweifelhaft ist, inwieweit sie tatsächlich bessere Prozeßqualität beschreiben [5].

## 3.3 IT-Sicherheitskriterien

Die IT-Sicherheitskriterien (siehe Tabelle 7) wurden von der Zentralstelle für Sicherheit in der Informationstechnik (ZSI), jetzt Bundesamt für Sicherheit in der Informationstechnik (BSI), herausgegeben und beschreiben eine Reihe von Kriterien, nach denen Software in verschiedene

Sicherheitsklassen eingeteilt werden kann. Sie sind eine Fortentwicklung des "Orange Book" des US-Verteidigungsministeriums. Im Gegensatz zum Orange Book wird in diesen Kriterien unterschieden zwischen Funktionalitätsklassen, die jeweils bestimmte Anforderungen an die Funktionalität des Systems stellen (z.B. Rechteverwaltung, Fehlerüberbrückung, etc.) und Qualitätsstufen, bei denen Systeme nach der Qualität des Herstellungsprozesses und des Produktes eingestuft werden. Dabei wird eingeteilt in die Stufen Q0 (keine Anforderungen), Q1 (verbale Spezifikation und Beschreibungen) bis Q7 (formale Spezifikation und formale Konsistenzbeweise). Praktisch relevant sind bisher vor allem die Stufen bis Q3 (methodisch getestet und teilanalysiert), gelegentlich auch Q4 (informell analysiert). Die definierten Qualitätsanforderungen beziehen sich allerdings nur auf die Qualität der Sicherheitskomponenten des Produktes. Für eine allgemeine Beurteilung der Qualität von Produkten sind sie weniger geeignet.

Seit 1991 gibt es auch eine vorläufige europäische Version ITSEC dieses Kriterienkataloges, die die IT-Sicherheitskriterien ersetzen soll, allerdings noch sehr umstritten ist [6]. Analog den oben genannten Stufen Q0 bis Q7 werden in ITSEC Evaluationsstufen E0 bis E6 definiert, die jeweils das Vertrauen in die Korrektheit (der Sicherheitsfunktionalität) des evaluierten Systems beschreiben sollen.

Tabelle 7: IT-Sicherheitskriterien

| **Titel** | **Herausgeber** |
|---|---|
| IT-Sicherheitskriterien. Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT) | ZSI - Zentralstelle für Sicherheit in der Informationstechnik (Hrsg.): Bundesanzeiger, Köln, 1989 |
| IT-Evaluationshandbuch. Handbuch für die Prüfung der Sicherheit von Systemen der Informationstechnik (IT) | ZSI - Zentralstelle für Sicherheit in der Informationstechnik (Hrsg.): Bundesanzeiger, Köln, 1990 |
| Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC). Vorläufige Form der harmonisierten Kriterien | Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaft:, Luxemburg, 1991 |

Diese Kriterienkataloge sind vor allem im Bereich der öffentlichen Verwaltung von Bedeutung. Hier sollen laut BSI in Zukunft für alle Anwendungen, bei denen Datensicherheit eine Rolle spielt, nur noch Systeme eingesetzt werden, die für die entsprechende Funktionalitätsklasse und Qualitätsstufe zertifiziert sind. Auch im nichtöffentlichen Bereich hat Sicherheit jedoch bei sehr vielen Anwendungen erhebliche Bedeutung, verursacht z.B. durch Datenschutzforderungen, so daß auch hier Bedarf an nach den genannten Kriterien evaluierten Softwareprodukten besteht.

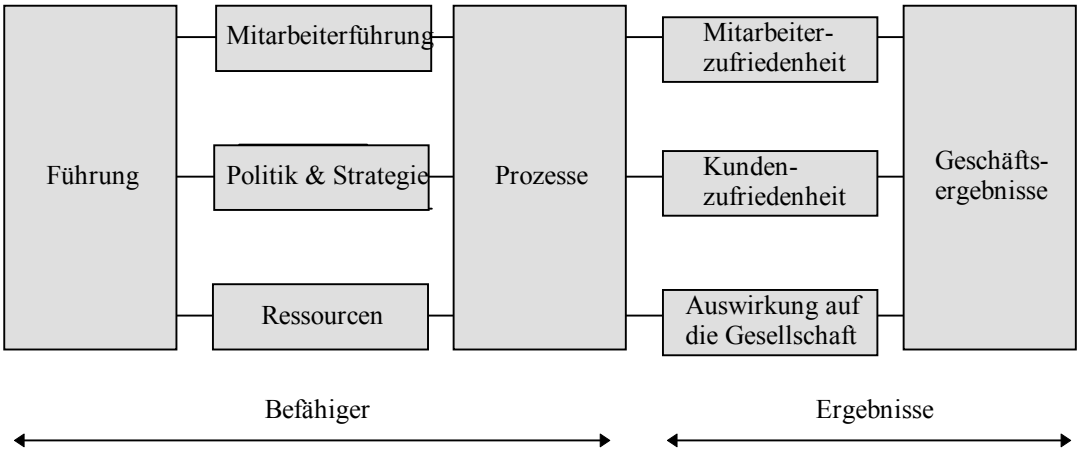
## 3.4 Qualitätspreise

Wesentlich weitergehende, branchenunabhängige Kriterienkataloge wurden im Rahmen von Qualitätspreisen erstellt, die jährlich einem oder einzelnen Unternehmen verliehen werden. Der erste Preis dieser Art war der *Deming Prize* in Japan. Später kam der *Malcolm Baldridge National Quality Award* in den USA dazu, und seit 1992 gibt es auch einen *European Quality Award*. Diese branchenunabhängigen Preise bauen jeweils auf dem Ansatz des Total Quality Management (TQM) auf, also einer ganzheitlichen Ausrichtung des Unternehmens auf das Ziel Qualität, und verwenden Kriterien, nach denen die Umsetzung des TQM in einer Organisation bewertet wird. Der erste Schritt für die Verleihung der Preise ist dabei jeweils eine Selbstbewertung. Damit soll den Unternehmen auch gleichzeitig ein Leitfaden in die Hand gegeben werden, seine Tätigkeiten und Ergebnisse zu überprüfen und Stärken und Schwächen festzu-

stellen. In der öffentlichen Diskussion in den USA hat der Malcolm Baldridge Award ähnliche Bedeutung wie die ISO 9000-Familie.

In dem beim European Quality Award verwendeten Modell beispielsweise werden die Bewertungskriterien in zwei Gruppen eingeteilt, nämlich sogenannte Befähiger und Ergebnisse. Befähiger befassen sich damit, wie Ergebnisse erzielt werden, während Ergebnisse beschreiben, was die Organisation erreicht (hat). In [7] werden diese Kriterien ausführlich dargestellt.

Abb. 2: European Quality Award - Modell




Auch ohne den Anspruch, den jeweiligen Preis zu gewinnen, bilden diese Kriterienkataloge ein Hilfsmittel für ein Unternehmen, seine Stärken und Schwächen aufzudecken. Dabei zeigen sie eine weit über das im Rahmen der oben beschriebenen Normen, insbesondere der ISO 9000-Familie, Geforderte hinausgehende Vision auf.

# 4. BEZIEHUNGEN ZWISCHEN DEN NORMEN

Als Referenzpunkt wird im folgenden ISO 9000-3 verwendet. Die verschiedenen IEEE-Standards sowie ISO 9126 und ISO 12 119 beschreiben jeweils einzelne Aspekte der ISO 9000-3 detaillierter. Die Qualitätspreise dagegen umfassen ein erheblich umfangreicheres Gebiet, nämlich das sogenannte Total Quality Management. Im Vergleich dazu beschränkt sich ISO 9000 weitgehend auf den "Befähiger" Prozesse. Die übrigen Befähiger sowie die Ergebnisse dagegen werden nur andeutungsweise behandelt.

Das V-Modell behandelt einen großen Ausschnitt der Anforderungen von ISO 9000-3, nämlich die phasenabhängigen Tätigkeiten sowie Teile der unterstützenden Tätigkeiten. Da dieser Aspekt bei der Entwicklung des V-Modell berücksichtigt wurde, garantiert die Verwendung des V-Modells auch die Erfüllung dieser (entwicklungsorientierten) Anforderungen der ISO 9000-3.

Das SEI CMM läßt sich nicht auf die gleiche Weise mit ISO 9000-3 vergleichen, da es ja hier fünf verschiedene Stufen gibt. Dabei entsprechen die Anforderungen der dritten Stufe ("Defined") in etwa den in ISO 9000-3 genannten Anforderungen, wobei das CMM sich aber auf den Entwicklungsprozeß konzentriert. ISO 9000-3 dagegen bezieht auch das Umfeld mit ein, z.B. die Formulierung einer Qualitätspolitik oder einen Prozeß wie die Vertragsprüfung. Soweit die Anforderungen der ISO 9000-3 den Entwicklungsprozeß selbst betreffen, entsprechen sie weitgehend denen des CMM. Aufgrund vieler Unterschiede im Detail ist es aber durchaus mög-

lich, nicht einmal Stufe zwei zu erreichen und trotzdem die Anforderungen der ISO 9000-3 zu erfüllen [8].

Abgesehen von dieser eher theoretischen Möglichkeit ist es aber oft sinnvoll, sich bei der Einführung eines QM-Systems nach ISO 9000 am SEI Capability Maturity Model zu orientieren. Dieses gibt eine sinnvolle Reihenfolge der verschiedenen notwendigen Maßnahmen vor, derzufolge z.B. die Einführung eines systematischen Projektmanagements einschließlich Projektplanung und Projektverfolgung Grundlage der weiteren Verbesserung der Prozesse sein muß.

ITSEC behandelt einen ähnlichen Ausschnitt der Anforderungen von ISO 9000-3 wie das V-Modell, allerdings bezogen auf ein einziges Qualitätsmerkmal, nämlich Sicherheit. Außerdem werden hier weniger Anforderungen direkt an den Entwicklungsprozeß gestellt, die meisten Anforderungen beziehen sich auf Zwischen- und Endergebnisse dieses Prozesses. Dafür sind diese Anforderungen zum Teil deutlich konkreter, so werden z.B. für die höheren Stufen nur semiformale bzw. formale Beschreibungen zugelassen.

In Tabelle 8, Tabelle 9 und Tabelle 10 sind die wichtigsten Anforderungen der ISO 9000-3 sowie die sich auf die gleichen Elemente beziehenden anderen Normen zusammengestellt.

Tabelle 8: QM-System Rahmen

| **QM-System Rahmen** | **Nachweis nach ISO 9000-3** | **Andere relevante Normen** |
|---|---|---|
| Verantwortung der obersten Leitung | • Formulierung einer Qualitätspolitik<br>• Festlegung der Organisation<br>• Management Reviews<br>• Qualitätsbeauftragter | |
| QM-System | • Einrichtung, Dokumentation und Aufrechterhaltung eines QM-Systems<br>• Aufstellung eines Qualitätsplanes je Projekt | |
| Interne Qualitätsaudits | • Durchführung und Dokumentation interner Qualitätsaudits<br>• Einleitung von Korrekturmaßnahmen | IEEE 1028-1988<br>ISO 10 011 |
| Korrekturmaßnahmen | • Ursachenanalyse<br>• definierter Korrekturprozeß<br>• Fehlerverhütung,<br>• Überwachung der Wirksamkeit von Korrekturen | |

Tabelle 9: Lebenszyklustätigkeiten

| **Phase der Entwicklung** | **Nachweis nach ISO 9000-3** | **Andere relevante Normen** |
|---|---|---|
| Vertragsüberprüfung | • Inhaltliche Vertragsprüfung, z.B. Annahmekriterien, Behandlung von Änderungen und Problemen, Erfüllbarkeit | V-Modell |
| Spezifikation des Auftraggebers | • Formulierung von funktionalen Forderungen<br>• Definition von Schnittstellen | IEEE 830-1984<br>V-Modell |
| Planung der Entwicklung | • Projektplan (Ziele, Ressourcen)<br>• Phasenmodell mit Meilensteinen<br>• Projektmanagement<br>• Entwicklungsmethoden, Werkzeuge | IEEE 1058.1-1984<br>V-Modell |
| Planung des QM | • Qualitätsziele<br>• Festlegung und Planung von Tests<br>• Validierungs- und Verifizierungsmaßnahmen<br>• Verantwortung für QM-Aktivitäten | IEEE 730-1989<br>IEEE 983-1986<br>IEEE 1012-1986<br>IEEE 1028-1988<br>V-Modell<br>ISO 9126 |
| Design und Implementierung | • Designmethodik<br>• Programmierregeln<br>• Implementiermethoden<br>• Werkzeuge<br>• Durchführung von Reviews | IEEE 1008-1987<br>IEEE 1016-1987<br>V-Modell |
| Test und Validierung | • Testplanung und -durchführung<br>• Validierung<br>• Feldversuch | IEEE 829-1983<br>IEEE 1008-1987<br>IEEE 1028-1988<br>V-Modell |
| Annahme | • Planung und Durchführung der Annahmeprüfung | ISO 12 119<br>V-Modell |
| Vervielfältigung, Lieferung und Installierung | • Sicherungskopien etc.<br>• Möglichkeit zur Verifizierung von Korrektheit und Vollständigkeit der Kopien<br>• Berücksichtigung von Copyright | V-Modell (teilweise) |
| Wartung | • Festlegung von Umfang und Verfahren<br>• Wartungsaufzeichnungen<br>• Freigabeverfahren | |

Tabelle 10: Unterstützende Tätigkeiten (phasenunabhängig)

| Unterstützende Tätigkeiten | Nachweis nach ISO 9000-3 | Andere relevante Normen |
|---|---|---|
| Konfigurations-management | • Geregelte Identifizierung, Lenkung und Rückverfolgung jedes SW-Elementes<br>• Lenkung von Änderungen | IEEE 828-1990<br>IEEE 1042-1987<br>V-Modell |
| Lenkung der Dokumente | • Geregelte Genehmigung, Herausgabe und Änderung von Dokumenten | V-Modell (teilweise) |
| Qualitäts-aufzeichnungen | • Verfahren zur Identifikation, Sammlung, Aufbewahrung, Pflege und Bereitstellung von Qualitätsaufzeichnungen | |
| Messungen | • Verwendung von Meßmethoden für Produkte<br>• Verwendung von Meßmethoden für Prozesse | IEEE 1061-1992 |
| Regeln, Praktiken und Übereinkommen | • Festlegung von Regeln, Praktiken und Übereinkommen, um QM-System wirksam zu machen | |
| Werkzeuge und Techniken | • Nutzung von Werkzeugen und Techniken | |
| Beschaffung | • Beurteilung von Lieferanten<br>• Validierung von beschafften Produkten | |
| Beigestelltes SW-Produkt | • Geregelte Validierung, Lagerung, Schutz und Wartung für vom Kunden zur Verfügung gestellte SW-Produkte | V-Modell |
| Schulung | • Ermittlung des Bedarfs<br>• Durchführung von Schulung für qualitäts-relevante Tätigkeiten | |

# 5. FAZIT

Langfristig halten die Autoren Einführung und Ausbau eines umfassenden Qualitätsmanagements für unumgänglich, um Software angemessener Qualität wirtschaftlich zu produzieren. Die QM-Normen, insbesondere ISO 9000, bieten dafür eine einheitliche Basis. Jedes Unternehmen muß individuell entscheiden, ob es sein Qualitätsmanagement nach einer dieser Normen ausrichtet oder einen eigenen Weg geht - solange der Markt diese Entscheidung nicht vorwegnimmt. In vielen Fällen bieten die QM-Normen Hilfestellung beim Aufbau eines systematischen Qualitätsmanagements, sie sind aber sicher nicht der einzig sinnvolle Weg zum Ziel.

Derzeit gibt es, zumindest in Deutschland, relativ wenige reine SW-Hersteller mit einem zertifizierten QM-System. Es besteht aber hohes Interesse an den entsprechenden Normen, und die Zahl der zertifizierten Unternehmen steigt in allen Branchen einschließlich der SW-Entwicklung rapide an. Dies gilt insbesondere für große SW-Herstellern sowie Unternehmen mit einem Produktmix von Hard- und Software.

Erwähnt werden muß auch, daß eine Zertifizierung des QM-Systems zumindest für kleine Unternehmen ein beträchtlicher Kostenfaktor ist. Nicht jedes Unternehmen wird wirtschaftlich in der Lage sein, eine Zertifizierung und die sich daran anschließenden periodischen Überprüfungen durch unabhängige Stellen durchführen zu lassen. Dies kann dazu führen, daß

Unternehmen mit geringem finanziellen Potential aus dem Markt gedrängt werden. Die Eintrittsbarrieren in den Softwaremarkt würden durch eine solche Tendenz erhöht. (Hier läßt sich natürlich darüber streiten, ob dies ein Vorteil oder ein Nachteil ist.)

Normen bieten eine einheitliche systematische Basis für Einführung und Betrieb eines QM-Systems. Insbesondere die ISO 9000-Familie bildet einen kleinsten gemeinsamen Nenner, der zwar einige Schwachpunkte enthält, andererseits aber einen geeigneten Ausgangspunkt für den Aufbau eines QM-Systems darstellt. Einer unternehmensinternen Erweiterung der Qualitätsmaßstäbe in allen Bereichen steht zudem nichts im Wege. ISO 9000 wird sich nach Einschätzung der Autoren im Bereich der Softwareentwicklung durchsetzen. Es erscheint daher empfehlenswert, sich dieser Tendenz frühzeitig anzupassen und den Schritt zur systematisierten zielorientierten Arbeitsweise mit dem Ziel der Herstellung von Produkten höchster Qualität auf der Basis dieser international anerkannten Normen zu vollziehen.

# 6. LITERATUR


1. Theuer, Andreas: Akkreditierung von Prüflaboratorien und Zertifizierungsstellen aus der Sicht der Industrie. QZ Zeitschrift für industrielle Qualitätssicherung, 5/91, 1991, 263-266
2. Schmidt, K. P.: Rahmenprüfplan für Software, Arbeitspapiere der GMD 312, 1988
3. H.-L. Hausen, D. Welzel: Guides to Software Evaluation, Arbeitspapiere der GMD 746, 1993
4. M. C. Paulk, B. Curtis, M. B. Chrissis: Capability Maturity Model for Software. Software Engineering Institute, Carnegie Mellon University, Technical Report CMU/SEI-91-TR-24, 1991
5. T. B. Bollinger, C. McGowan: A Critical Look at Software Capability Evaluations. IEEE Software, Juli 1991, 25-41
6. Präsidiumsarbeitskreis Datenschutz und Datensicherung der Gesellschaft für Informatik: Stellungname zu den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC) Version 1.2. Inf.-Spektrum *15*, 221-224 (1992)
7. European Foundation for Quality Management: Total Quality Management. Das Europäische Modell für die Selbstbewertung 1992, Eindhoven
8. R. C. Bamford, W. J. Deibler: Comparing, contrasting ISO 9001 and the SEI capability maturity model. IEEE Computer, Oktober 1993, 68-70