Prüforganisation

- Organisation der Qualitätssicherung und des Qualitätsmanagements
- Personelle Trennung von Entwicklung und QS
- Dokumentation und Auswertung der Prüfung
- Standards
  - Bedeutung von Standards
  - Prozessorientierte Standards
  - Technische Standards
- Literatur

Organisation der Qualitätssicherung und des Qualitätsmanagements

Alternative Organisationsformen für das Qualitätsmanagement:

- Totales Qualitätsmanagement (TQM)
  - Verteilte Qualitätsverantwortung
  - Keine unabhängige Qualitätssicherung
- Klassische Qualitätssicherung
  - Unterscheidet deutlich zwischen der Rolle des Entwicklers und der Rolle Qualitätssicherers
  - Die Qualitätsverantwortung nimmt der Qualitätssicherer wahr, der aus diesem Grund eine starke unabhängige Position benötigt.
  - In der Regel ist die Qualitätssicherung in dieser Organisation nicht der Projektleitung unterstellt.

Organisation der Qualitätssicherung und des Qualitätsmanagements

- Mehrzahl der Software-Unternehmen verwendet Organisationsformen, die einen Kompromiss aus TQM und der klassischen Qualitätssicherung darstellen.
- In sicherheitskritischen Anwendungen: unabhängige Qualitätssicherung zusätzlich zu den qualitätssichernden Maßnahmen durchgeführt, die die Entwickler verantworten (Forderung einschlägiger Standards)
- Z.B. DIN EN 50128 „Bahnanwendungen – Software für Eisenbahnsteuerungs- und Überwachungssysteme“ unterscheidet in der Qualitätssicherung die Rollen des Verifizierers und des Validierers.
  - Verifikation: Überprüfung der fehlerfreien Umsetzung der Anforderungen einer Phase in das Ergebnis der Phase
  - Validation: Demonstration, dass das Produkt seine Anforderungen erfüllt.

Organisation der Qualitätssicherung und des Qualitätsmanagements: Die Norm DIN EN 50128

Die Norm enthält die folgenden Forderungen:

- Für Software, die nicht sicherheitsrelevant ist (Software-Sicherheitsanforderungsstufe 0) dürfen Entwerfer, Implementierer, Verifizierer und Validierer dieselbe Person sein.
- Für Software der mittleren Sicherheitsanforderungsstufen 1 und 2 dürfen Verifizierer und Validierer dieselbe Person, aber nicht identisch mit dem Entwerfer/Implementierer sein. Diese Regelung stellt das „Vieraugenprinzip” sicher. Die Entwicklung und die Qualitätssicherung werden von unterschiedlichen Personen durchgeführt. Beide Personengruppen dürfen jedoch an den gleichen Projektleiter berichten. Daher hat der Projektleiter die Möglichkeit, Warnungen der Qualitätssicherung zu ignorieren.
- Für Software der hohen Sicherheitsanforderungsstufen 3 und 4 existieren zwei alternative Organisationsformen der Qualitätssicherung:
  - Verifizierer und Validierer können identisch sein. Sie dürfen aber nicht gleichzeitig Entwerfer/Implementierer sein. Verifizierer und Validierer berichten nicht der Projektleitung und müssen die Möglichkeit haben, die Freigabe zu verhindern.
  - Entwerfer/Implementierer, Verifizierer und Validierer sind unterschiedliche Personen. Der Entwerfer/Implementierer und Verifizierer berichten an die Projektleitung. Der Validierer muss einen unabhängigen Berichtsweg haben. Es muss ihm möglich sein, die Freigabe zu verhindern.

Organisation der Qualitätssicherung und des Qualitätsmanagements: Die Norm DIN EN 50128

- Den Regeln liegt das folgende Prinzip zugrunde: Mit ansteigender Sicherheitskritikalität einer Software muss die personelle und organisatorische Unabhängigkeit der Qualitätssicherung zunehmen.
- Bei sicherheitskritischer Software wird die klassische Organisation der Qualitätssicherung den Prinzipien des Total Quality Managements vorgezogen. Diese Regel ist vereinfacht, weil die Existenz einer unabhängigen Qualitätssicherung eine in die Entwicklung integrierte Qualitätssicherung nicht ausschließt. Im Gegenteil: Insbesondere in einer sicherheitskritischen Entwicklung ist dafür zu sorgen, dass der Entwicklung die Qualitätsziele bekannt sind und Verfahren genutzt werden, um sie zu erreichen und die Erreichung zu prüfen. Die Qualität muss in die Software hineinentwickelt werden. Sie kann nicht hineingeprüft werden.

Organisation der Qualitätssicherung und des Qualitätsmanagements: Personelle Trennung von Entwicklung und QS

- Eine personelle Trennung zwischen der Tätigkeit des Entwickelns und des Prüfens scheint auf den ersten Blick stets sinnvoll zu sein. Bei näherer Betrachtung erweist sich dies als nicht korrekt:
  - Falls z. B. der Modultest durch eine unabhängige Person durchführt wird, so ist die Aufgabe des Programmierers lediglich, sein Modul fehlerfrei zu compilieren. Wenn alle Syntaxfehler beseitigt sind, so wechselt die Verantwortung zum unabhängigen Modultester. Dieser kann bestimmte Fehler erkennen, die der Programmierer nicht bemerken kann, weil ihre Ursache z. B. Missverständnisse der Modulspezifikation sind, die einem unabhängigen Tester nicht in gleicher Weise unterlaufen. Nachteilig ist, dass der unabhängige Tester nicht über die präzise Kenntnis des Programmierers bezüglich der Struktur des Moduls verfolgt. Der Programmierer weiß, warum er bestimmte Kontrollstruktur verwendet, welche Funktionen die Variablen besitzen, und wie bestimmte Testfälle verarbeitet werden müssen. Diese Kenntnisse des Programmierers werden nicht genutzt, während der unabhängige Tester sie nicht besitzt. Das Beispiel zeigt, dass es Argumente für die Durchführung der Prüfung durch den Entwickler und andere Argumente für die Prüfung durch eine andere Person geben kann. Systematische Testtechniken bieten eine Lösung für das skizzierte Problem. Man kann beispielsweise folgendermaßen vorgehen:

Organisation der Qualitätssicherung und des Qualitätsmanagements: Personelle Trennung von Entwicklung und QS

Beispiel einer Regel für Zuständigkeiten:

- Falls im Modultest ein Zweigüberdeckungstest durchgeführt wird, so hat der Programmierer eine bestimmte Zweigüberdeckungsrate zu erreichen (z. B. 80 %). Dies nutzt die Sachkenntnis des Programmierers zu Beginn des Tests und gewährleistet, dass ein Modul an den unabhängigen Tester weitergegeben wird, das bereits im Wesentlichen funktioniert. Anschließend wird ein unabhängiger Tester zuständig. Das kann z. B. die gleiche Person sein, die den Integrationstest für das Modul durchführt. Die Verantwortung wechselt in diesem Fall bereits vor dem Abschluss der Phase. Der unabhängige Tester führt den Test zu Ende und gewährleistet dabei die Einhaltung des „Vieraugenprinzips“. Der Integrationstest und Systemtest wird in der Regel von unabhängigen Personen durchgeführt. In großen Software-Entwicklungen ist der Systemtest darüber hinaus oft nicht der Projektleitung unterstellt.

Organisation der Qualitätssicherung und des Qualitätsmanagements: Personelle Trennung von Entwicklung und QS

- Es ist sinnvoll, jene Personen, die die Prüfung durchführen, in die zugeordneten Entwicklungsphasen einzubinden. Der Systemtester sollte in die Analyse, der Integrationstester in den Entwurf und der Modultester in die Implementierung eingebunden sein. Die gleiche Regel gilt auch invers. In die Planung der Systemtestfälle sollte jemand eingebunden sein, der in die Analyse involviert war. Ebenso sollte ein Entwerfer in die Planung des Integrationstests und der Programmierer in den Modultest eingebunden sein.
- In einer reifen Organisation existieren systematische Arbeitsweisen, definierte Ziele und Möglichkeit zur Überprüfung ihrer Erreichung. Die Zielerreichung ist in der Vorantwortung der Entwickler. Die Aufgabe einer starken organisatorisch unabhängigen Qualitätssicherung ist lediglich, unabhängig vom Projektleiter zu prüfen, ob die definierten Ziele erreicht sind. Eine derartige Organisation der Qualitätssicherung kombiniert die Vorteile der klassischen Qualitätssicherung und des Total Quality Managements.

Dokumentation und Auswertung der Prüfung

- Alle Standards zum Qualitätsmanagement und zur Qualitätssicherung betonen die Bedeutung einer systematischen Vorgehensweise bei der Prüfung. Prüfungen müssen systematisch geplant, durchgeführt, kontrolliert, ausgewertet und dokumentiert werden. Die Norm DIN EN ISO 9000-3 /DIN EN ISO 9000-3 97/ fordert – wie auch zahlreiche andere Normen – die Existenz eines Qualitätssicherungsplans, der die folgenden Inhalte besitzen soll:
  - Messbare Qualitätsziele
  - Kriterien für die Vorgaben und Ergebnisse jeder Entwicklungsphase
  - Festlegung der Arten von Prüfungen
  - Detailplanung der Prüfungen einschließlich Terminen, Mitteln und Genehmigungsinstanzen
  - Verantwortlichkeiten

Dokumentation und Auswertung der Prüfung

- Prüfungen sind insbesondere als Nachweis ihrer ordnungsgemäßen Durchführung zu dokumentieren.
- Bei dynamischen Tests umfasst die Dokumentation in der Regel
  - die Testplanung,
  - den Nachweis der Durchführung der Testfälle,
  - die Dokumentation der Testergebnisse,
  - Eine Fehlerschreibung.
- Diese Dokumente können in Abhängigkeit der verwendeten Testtechnik unterschiedlich beschaffen sein
- Funktionsorientierter Test:
  - Testplanungsunterlage: Äquivalenzklassenaufstellung mit zugeordneten Testfällen
  - Nachweis der Durchführung und der Testergebnisse:Protokoll
- Strukturorientierter Test:
  - Protokoll eines Testwerkzeugs

Dokumentation und Auswertung der Prüfung

- Erfassung der Fehlverhalten:
  - Zeitpunkt
  - Testfall
  - Einschätzung der Schwere des Fehlerverhaltens
  - Klassifikation des Fehlverhaltens

Nr.	Datum	Testfall	Schwere (1 - 4)	Klassische Fehlverhalten	Korrektur-datum	Klassische Fehler	Korrektur-aufwand (MT)
1	05.08.2002	218	1	Totalausfall	12.08.2002	Programmier-Fehler	0,5
2	08.08.2002	279	3	Zeitanfordung verletzt			
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Standards
Bedeutung von Standards

- Standards entscheiden im Zweifelsfall, welche Verfahrensweisen, Methoden und Techniken als Stand der Technik bzw. als Stand von Wissenschaft und Technik zu betrachten sind.
- Standards und Normen:
  - Keine Rechtsnorm , aber antizipierte Sachverständigengutachten
- Gesetzliche Regelungen:
  - z.B. Produkthaftungsgesetz, Schadensersatz nach BGB
- Europäische Richtlinien
  - Haben den Charakter eines Gesetzes, weil sie von den Mitgliedsstaaten zwingend in nationales Recht umzusetzen sind
- Verordnungen
  - werden meistens von Behörden – der Exekutive – erlassen und sind in der Regel verbindlich

Standards
Bedeutung von Standards

- Normung ist in Deutschland die planmäßige, durch die interessierten Kreise gemeinschaftlich durchgeführte Vereinheitlichung von materiellen und immateriellen Gegenständen zum Nutzen der Allgemeinheit. Deutsche Normen werden in einem privatrechtlichen Verein durch interessierte Kreise erstellt (z. B. DIN Deutsches Institut für Normung e.V., Verband Deutscher Elektrotechniker (VDE) e.V.). Standards und Normen sind keine Rechtsnormen. Sie sind – im Unterschied zu Gesetzen – nicht rechtsverbindlich, aber sie können als antizipierte Sachverständigengutachten verstanden werden. Durch Einhaltung der jeweils relevanten Normen kann ein Hersteller sicherstellen, dass der Stand der Technik erreicht ist, und er damit seine Sorgfaltspflicht erfüllt hat.

Prozessorientierte Standards

- Regeln z. B. die Verfahrensweisen, Abläufe, Aufgaben und Verantwortlichkeiten in der Software-Entwicklung und Software-Qualitätssicherung.
- Im Wesentlichen enthalten sie organisatorische Forderungen.
- Sie schließen kaum genaue technische Forderungen ein.
- Beispiele:
  - DIN ISO 9000-Reihe
  - V-Modell
  - ISO/IEC TR 15504 zum Assessment-Verfahren SPICE
  - AQAP-Century-Standards für den militärischen Anwendungsbereich

Technische Standards

- Technische Standards können entweder einen bestimmten Anwendungsbereich betreffen – z. B. Luftfahrt oder Schienenverkehr – oder auf bestimmte Arten von Systemen anwendbar sein, die in einer Vielzahl von Anwendungsbereichen auftreten können.
- Enthalten oft explizite Regelungen der einzusetzenden Techniken
- Beispiele:
  - IEC 61508 /IEC 61508 98/ ist ein sehr umfassender Standard zum Thema Sicherheit elektrisch bzw. elektronisch programmierbarer, sicherheitskritischer Systeme. Software wird insbesondere in der IEC 61508-3 behandelt.
  - Die Standards DIN EN 50128 /DIN EN 50128 01/ und Mü 8004 /Mü 8004 99/ sind für die Anwendung auf Schienenverkehrssysteme vorgesehen.
  - Der Standard /RTCA/DO-178B 92/ betrifft Software-Anforderungen im Bereich der Avionik.

Literatur

/DIN EN 50128 01/: DIN EN 50128, Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Software für Eisenbahnsteuerungs- und Überwachungssysteme, Berlin: Beuth Verlag 2001

/DIN EN ISO 9000-3 97/: DIN EN ISO 9000-3, Normen zum Qualitätsmanagement und zur Qualitätssicherung/QM-Darlegung – Teil 3: Leitfaden für die Anwendung von ISO 9001 auf Entwicklung, Lieferung, Installation und Wartung von Computer-Software, Berlin: Beuth Verlag 1997

/IEC 61508 98/: IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems: Parts 1 – 7, International Electrotechnical Commission, 1998

/RTCA/DO-178B 92/: RTCA/DO-178B, Software Considerations in Airborne Systems and Equipment Certification, RTCA, Inc., 1992