SEMINARARBEIT

Konzeptentwicklung Akkreditierte Software Prüfstelle

durchgeführt am
Studiengang Angewandte Informatik

an der
Naturwissenschaftlichen Fakultät
der Universität Salzburg

Fachbereich Computerwissenschaften

vorgelegt von:
Josef Maier
Thomas Pfeiffenberger

Betreuer: Uni.-Prof. Dipl.-Ing. Dr. Wolfgang Pree

Salzburg, Februar 2008

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1

Einleitung

Die vorliegende Seminararbeit beschäftigt sich mit der Konzeptentwicklung *Akkreditierte Software Prüfstelle*. Diese Konzeptentwicklung soll als Basis und Leitfaden für die Akkreditierung von Prüflaboratorien dienen, welche ihre Kompetenzen und Prüfdienstleistungen im Bereich Softwaretests, -sicherheit und Softwarequalitätsmanagement anbieten. Diese Konzeptentwicklung kann durchaus teilweise für andere Branchen, wie zum Beispiel für EMV Prüflaboratorien verwendet werden, da die Grundlagen der Akkreditierung Branchenunabhängig ist. Weiters wird darauf hingewiesen, dass im Bezug auf rechtliche Rahmenbedingungen, Kosten und Durchführung eines derartigen Akkreditierungsverfahrens, sich diese Konzeptentwicklung auf Österreich beschränkt.

Das erste Kapitel wird im Folgenden die Problemstellung, sowie den Lösungsansatz beschreiben. Im nächsten Kapitel werden die Grundlagen der Akkreditierung behandelt. Hier werden im Wesentlichen zwei Themenbereiche angesprochen. Erstens, die Anforderungen an das Qualitätsmanagementsystem und zweitens die Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien. Im dritten Kapitel wird die Spezialisierung im Softwarebereich beschrieben. Hier werden schwerpunktmäßig die Themen Qualitätsmerkmale für Softwareprodukte, funktionale Sicherheit sicherheitsbezogener *elektrischer, elektronischer, programmierbar elektronischer Systeme* (E/E/PES) und IT Sicherheitsverfahren behandelt. Im vierten Kapitel werden die Kosten und der betriebswirtschaftliche Effekt einer derartigen Akkreditierung betrachtet. Im letzten Kapitel erfolgt eine Zusammenfassung der gesamten Seminararbeit.

1.1 Problemstellung

Qualitätsmanagement von Software gewinnt in der Wirtschaft und der Forschung zunehmend an Bedeutung. Zum einem 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 versucht. Ein klassisches Beispiel, welche Auswirkungen fehlerhafte Software haben kann, ist der Absturz der Ariane-5 Trägerrakete vom Jahr 1996.

Neben möglichen strafrechtlichen Konsequenzen bei Todesfällen oder etwaigen Haftungsansprüchen bei Personen-, Sach- oder Vermögensschäden sollte auch die nicht versicherbare Gewährleistung eines Softwareproduktes über die Einführung und konsequente Umsetzung eines Prozessmanagement im Bereich der Softwareentwicklung und -tests sichergestellt werden. Software nimmt insofern eine Sonderstellung ein, da Software ein Produkt ist, bei dem nur die Entwicklung schwierig ist, die Produktion dagegen aus bloßem, völlig unproblematischem Kopieren besteht. Darüber hinaus ist Software aufgrund ihres immateriellen Charakters schwierig zu überprüfen.

1.2 Lösungsansatz

Aus diesen Gründen, allerdings mit sehr unterschiedlichen Ansatzpunkten, haben verschiedene Institutionen, Normen und Standards auf dem Gebiet des Qualitätsmanagement entwickelt. Diese sollen Unternehmen unterstützen, geeignete Ansätze und Verfahren auszuwählen, so dass gewisse Mindestanforderungen an die Software erfüllt werden. Bei sicherheitskritischen, softwareintensiven Systemen ist trotz Einsatz des Qualitätsmanagementsystems eine Prüfung der erstellten Software gefordert. Alle Prüfungen und Kalibrierungen müssen nach standardisierten Regelwerken und Methoden durchgeführt werden und müssen in einem gemäß nach ISO/IEC 17025 akkreditierten Prüf- und Kalibrierlaboratorium erfolgen.

Im folgenden Kapitel werden die Grundlagen der Akkreditierung für ein Prüf- und Kalibrierlaboratorium behandelt.

2

Grundlagen der Akkreditierung

Prüf- und Kalibrierlaboratorien müssen ein Managementsysteme betreiben, technisch kompetent und fähig sein um fachlich fundierte Ergebnisse zu erzielen. Prüf- und Kalibrierlaboratorien die der ISO/IEC 17025 entsprechen, werden teilweise auch übereinstimmend mit der ISO 9001 arbeiten. Die Konformität mit der ISO 9001 bedeutet aber nicht notwendigerweise, dass das Qualitätsmanagementsystem mit allen Anforderungen der ISO 9001 übereinstimmt. Wenn ein Prüf- und Kalibrierlaboratorium die Akkreditierung wünscht, muss eine Akkreditierungsstelle gewählt werden, die nach ISO/IEC 17011 arbeitet. [17005]

Da für die Akkreditierung eines Prüf- und Kalibrierlaboratorium eine Zertifizierung nach ISO 9001 nicht zwingend erforderlich, aber hilfreich ist, wird im Folgenden zuerst ein Überblick über die Anforderungen an das Qualitätsmanagement im Allgemeinen gegeben und danach der Schwerpunkt auf die Anwendung der ISO/IEC 17025 gelegt.

2.1 Anforderung an das Qualitätsmanagementsystem

Die in der ISO 9001 festgelegten Anforderungen sind allgemeiner Natur und auf alle Organisationen anwendbar, unabhängig von deren Art und Größe und von der Art der bereitgestellten Produkte. Die Organisation muss entsprechend den Anforderungen dieser Norm ein Qualitätsmanagementsystem aufbauen, dokumentieren, verwirklichen, aufrechterhalten und dessen Wirksamkeit ständig verbessern.

Dies umfasst im Wesentlichen die Schwerpunkte *Verantwortung der Leitung*, *Management von Ressourcen*, *Produktrealisierung* und *Messung, Analyse und Verbesserung.* [90000a] [90000b] [90000c]

2.1.1 Prozessorientierter Ansatz

Heutige Qualitätsmanagementsysteme orientieren sich an der Selbstverantwortung aller Beteiligten, sowie an der Kundenzufriedenheit. Dieser Ansatz wurde hauptsächlich von Deming [1] entwickelt und propagiert.

Die Normenreihe der ISO 9000 Familie, fördert die Wahl eines prozessorientierten Ansatzes für die Entwicklung, Verwirklichung und Verbesserung der Wirksamkeit eines Qualitätsmanagementsystems um die Kundenzufriedenheit durch Erfüllung der Kundenanforderungen zu erhöhen.

Ein Modell eines prozessorientierten Qualitätsmanagementsystems ist im Anhang A auf Seite 29 in Abbildung 1 schematisch dargestellt.

2.1.2 Grundsätze des Qualitätsmanagements

Im Qualitätsmanagementsystem gelten folgende wesentliche Grundsätze: [LJSH00]

1. Qualität in der Entwicklung, sowie in der Produktion muss erzeugt werden, sie kann nicht erprüft werden.

2. Qualität bezieht sich immer auf die hergestellten Produkte, sowie auf die Prozesse zur Herstellung dieser Produkte.

3. Die Qualitätsverantwortung liegt immer bei den gleichen Personen, welche auch die Sach-, Termin- und Kostenverantwortung haben, eben bei den Führungskräften und Entwicklern.

[1] William Edwards Deming war ein US-amerikanischer Physiker, Statistiker sowie Wirtschaftspionier im Bereich des Qualitätsmanagements.

4. Das Qualitätswesen ist verantwortlich für die Ermittlung der Qualität. Es erbringt Dienstleistungen in allen Belangen der Qualität sowohl für die Entwickler als auch für die Führungskräfte.

5. Das Qualitätswesen muss einen unabhängigen Berichterstattungspfad haben, der bis zur Geschäftsleitung geht.

6. Die Mitarbeiter müssen über die Qualität ihrer Arbeit informiert werden. Jeder Vorgesetzte muss die Qualität der Arbeit seiner Mitarbeiter in deren Beurteilung mit einbeziehen.

Im folgenden Abschnitt wird nun ein Überblick über die ISO/IEC 17025 gegeben, welche für die Umsetzung und Durchführung einer Akkreditierung von Prüf- und Kalibrierlaboratorien zwingend erforderlich ist. Die wesentlichen Unterscheidungsmerkmale der ISO/IEC 17025 sind die technischen Anforderungen, welche in der ISO 9001 nicht behandelt werden.

2.2 Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien

Die ISO/IEC 17025 legt die allgemeinen Anforderungen an die Kompetenz für die Durchführung von Prüfungen oder Kalibrierungen, einschließlich Probennahmen fest und ist auf alle Organisationen, die Prüfungen oder Kalibrierungen durchführen, anwendbar. [17005]

2.2.1 Anforderungen an das Managementsystem

Managementarbeiten erstrecken sich auf feste Einrichtungen des Prüf- und Kalibrierlaboratoriums und auf mobile Einrichtungen vor Ort. Wenn das Prüf- und Kalibrierlaboratorium Teil einer Organisation ist, dürfen keine Interessenskonflikte auftreten. Die oberste Leitung muss geeignete Kommunikationsprozesse zur Verfügung stellen. Das Laboratorium muss seine grundsätzlichen Tätigkeiten in dem erforderlichen Umfang

schriftlich niederlegen, um die Qualität der Prüf- oder Kalibrierergebnisse zu sichern. Aussagen zur Qualitätspolitik müssen in einem Qualitätsmanagement-Handbuch festgelegt sein.
Die wesentlichen Anforderungen an das Managemensystem behandeln die Themen *Anfragen, Angebote und Verträge*. Weiters werden die *Dienstleistungen für den Kunden*, die *Lenkung von Aufzeichnungen* und *Interne Audits* behandelt. [17005]

Weiterführende Information zu diesen Themen befindet sich im Anhang B auf Seite 30
Im folgenden Abschnitt werden die technischen Anforderungen näher betrachtet.

2.2.2 Technische Anforderungen

Die Leitung des Laboratoriums muss sicherstellen, dass alle Mitarbeiter qualifiziert und kompetent sind. Weiters muss sie den Schulungsbedarf der Mitarbeiter ermitteln. Ausbildungsprogramme müssen sich an den gegenwärtigen und zukünftigen Aufgaben des Laboratoriums orientieren. Das Laboratorium muss Aufzeichnungen über Befugnisse, fachliche Kompetenz, Ausbildungs- und Berufsqualifikation, Schulung, Fertigkeiten und Erfahrungen aller technischen Mitarbeiter führen.

Die Laboratoriumsausstattung für Prüfungen oder Kalibrierungen muss so sein, dass sie die korrekte Durchführung dieser ermöglicht. Querkontaminationen müssen ausgeschlossen werden. [17005]

2.2.2.1 Prüf- und Kalibrierverfahren und deren Validierung

Anleitungen, Normen, Handbücher und Referenzdaten müssen auf dem neuesten Stand gehalten und dem Personal leicht zugänglich gemacht werden. Abweichungen von den Prüf- und Kalibrierverfahren sind nur dann zulässig, wenn sie dokumentiert, technisch begründet und durch den Kunden genehmigt sind. Das Laboratorium muss sicherstellen, dass die gültigen Ausgaben von Normen verwendet werden. Durch das Laboratorium entwickelte Verfahren dürfen verwendet werden, wenn sie dafür validiert wurden. Weiters muss das Laboratorium bestätigen, dass es die Normen richtig anwenden kann. Ein Kalibrierlaboratorium oder Prüflaboratorium, muss über ein Verfahren zur Schätzung der Messunsicherheit verfügen. [17005]

2.2.2.2 Mess- und Prüfeinrichtungen

Das Laboratorium muss mit Mess- und Prüfeinrichtungsgegenständen ausgestattet sein, die für die ordnungsgemäße Durchführung der Prüfungen oder Kalibrierungen erforderlich sind. Einrichtungen dürfen nur von befugtem Personal bedient werden. Gebrauchs- und Wartungsanleitungen müssen für das Personal leicht zugänglich sein. Alle Mess- und Prüfeinrichtungen sind mit einem Kalibrierstatus zu kennzeichnen.

Alle Mess- und Prüfeinrichtungsgegenstände müssen vor ihrer Inbetriebnahme kalibriert werden. Bei Kalibrierlaboratorien muss für die Kalibrierung sichergestellt sein, dass die vom Laboratorium durchgeführten Kalibrierungen und Messungen auf SI-Einheiten [2] rückgeführt sind.

Das Laboratorium ist verantwortlich für die Unversehrtheit der Prüf- und Kalibriergegenstände, sowie der Interessen des Laboratoriums und des Kunden. Das Laboratorium muss über ein System für die Kennzeichnung von Prüf- oder Kalibriergegenständen verfügen. Die Kennzeichnung muss während des gesamten Zeitraumes, für die sich der Gegenstand im Laboratorium befindet, beibehalten werden. [17005]

2.2.2.3 Qualität von Prüf- und Kalibrierergebnissen

Das Laboratorium muss über Qualitätslenkungsverfahren zur Überwachung der Gültigkeit von durchgeführten Prüfungen und Kalibrierungen verfügen. Diese Überwachung ist zu planen und zu prüfen und kann durch die Teilnahme an Programmen von Vergleichen zwischen Laboratorien durchgeführt werden. Weiters besteht die Möglichkeit der Wiederholungsprüfungen, unter Anwendung derselben oder unterschiedlicher Verfahren. Auch die erneute Prüfung von aufbewahrten Gegenständen und die Korrelation von Ergebnissen für verschiedene Merkmale eines Gegenstandes, kann zur Überwachung herangezogen werden. [17005]

[2] Internationales Einheitensystem

2.2.2.4 Ergebnisberichte

Ergebnisse müssen genau, klar, eindeutig und objektiv sowie in Übereinstimmung mit den in den Prüf- oder Kalibrierverfahren enthaltenen Anweisungen berichtet werden. Die Ergebnisse müssen in einem Prüfbericht oder Kalibrierschein dargestellt werden und haben alle Informationen zu enthalten, die der Kunde verlangt hat und die für die Interpretation erforderlich sind, sowie alle Informationen, die nach dem verwendeten Verfahren erforderlich sind. Im Falle von internen Prüfungen oder Kalibrierungen oder im Falle einer schriftlichen Vereinbarung mit dem Kunden können die Ergebnisse in vereinfachter Weise berichtet werden. Die dem Kunden nicht mitgeteilten Ergebnisse müssen in dem Laboratorium leicht verfügbar sein. Wenn in einem Prüfbericht Meinungen und Interpretation enthalten sind, müssen die Grundlagen, auf denen diese beruhen, schriftlich niedergelegt sein und müssen im Prüfbericht eindeutig als solche gekennzeichnet werden. Auch müssen Ergebnisse von Prüfungen, die von Unterauftragnehmer durchgeführt wurden, klar gekennzeichnet sein. Der Aufbau von Prüfberichten oder Kalibrierscheinen muss so gestaltet sein, dass die Gefahr von Missverständnissen oder Missbrauch auf ein Minimum reduziert ist. Inhaltliche Änderungen an einem Prüfbericht oder Kalibrierschein nach der Ausstellung dürfen nur in Form eines gesonderten Schriftstücks gemacht werden. Wenn es erforderlich ist, einen vollständig neuen Prüfbericht oder Kalibrierschein auszustellen, muss dieser eine eindeutige Bezeichnung haben und den Hinweis enthalten, welches Original er ersetzt. [17005]

3

Spezialisierung im Softwarebereich

Im folgenden Abschnitt werden drei verschiedene Bereiche diskutiert, die sich mit der Qualität der Software, beziehungsweise mit der Qualität des Softwareentwicklungsprozesses in sicherheitskritischen Softwareprodukten beschäftigen.

3.1 Qualitätsmerkmale für Softwareprodukte

In der ISO/IEC 9126 sind verschiedene Qualitätsmerkmale eines Softwareprodukts spezifiziert. Die Gesamtqualität eines Softwareprodukts kann mit diesen Qualitätsmerkmalen beurteilt und getestet werden.

Ein Softwaresystem kann nicht alle Qualitätsmerkmale gleich gut erfüllen. Teilweise kann die Erfüllung eines Qualitätsmerkmales die Nichterfüllung eines anderen Merkmales bedingen. Ist ein Softwaresystem hocheffizient in Bezug auf das Zeitverhalten, kann es unter Umständen in der Portierbarkeit erhebliche Einschränkungen aufweisen. Welche Qualitätsmerkmale und -eigenschaften in einem Softwareprodukt umgesetzt werden, sollte in einer Prioritätenliste definiert werden. Diese Prioritätenliste dient bei der Umsetzung als Anhaltspunkt für die Erfüllung bestimmter Qualitätsmerkmale und zur Überprüfung.

Die wesentlichen Softwarequalitätsmerkmale nach ISO/IEC 9126 sind *Funktionalität*, *Zuverlässigkeit*, *Benutzbarkeit*, *Effizienz* und *Änderbarkeit und Übertragbarkeit*, welche im Folgenden näher erläutert werden. [91206]

3.1.1 Funktionalität

Das Qualitätsmerkmal Funktionalität beschreibt alle definierten Fähigkeiten des Systems, es wird auch die Wirkung und Reaktion des Systems auf entsprechende Eingabeparameter beschrieben. Nach der ISO/IEC 9126 gliedert sich das Merkmal Funktionalität in die *Teilmerkmale*, *Angemessenheit*, *Richtigkeit*, *Interoperabilität*, *Ordnungsmäßigkeit* und *Sicherheit*.

Von einer angemessenen Umsetzung spricht man, wenn jede geforderte und definierte Fähigkeit umgesetzt wurde und vom System unterstützt wird. Es ist immer darauf zu achten, dass die geforderten, beziehungsweise richtigen Reaktionen und Wirkungen vom System erbracht werden. Mit Interoperabilität wird das Zusammenspiel mit vorgegebenen Systemen und Umgebungen bezeichnet. Erfüllt das System Anforderungen, anwendungsspezifische Normen oder gesetzliche Bestimmungen, spricht man von einer ordnungsgemäßen Funktionalität. Ein vorsätzlicher oder versehentlicher Zugriff auf das System oder auf die Daten, muss unter allen Umständen verhindert werden. [91206]

3.1.2 Zuverlässigkeit

Zuverlässigkeit beschreibt die Fähigkeit eines Systems, ein Leistungsniveau unter festgelegten Bedingungen über einen definierten Zeitraum zu bewahren. Die Zuverlässigkeit wird unterteilt in *Reife*, *Fehlertoleranz* und *Wiederherstellbarkeit*. Die Reife eines Systems gibt Auskunft wie häufig ein Versagen der Software durch Fehlerzustände vorkommt. Die Wiedererlangung eines spezifizierten Leistungsniveaus nach einer Fehlerwirkung, ausgelöst durch einen Defekt oder Fehlbedienung des Systems, wird als Fehlertoleranz bezeichnet. Die Dauer und der Aufwand zur Erreichung des spezifizierten Leistungsniveaus definiert die Wiederherstellbarkeit. [91206]

3.1.3 Benutzbarkeit

Bei interaktiven Softwaresystemen spielt die Benutzbarkeit eine wesentliche Rolle für die Akzeptanz der Systeme. *Verständlichkeit*, *Erlernbarkeit* und *Bedienbarkeit* sind Teilaspekte der Benutzbarkeit. Zur Benutzbarkeit gehören aber auch Aspekte wie die Einhaltung von Standards, Konventionen oder anderen Schnittstellendefinitionen. [91206]

3.1.4 Effizienz

Der benötigte Aufwand an Zeit und der Verbrauch an Betriebsmittel für die Erfüllung einer Aufgabe, wird mit dem Qualitätsmerkmal Effizienz beschrieben. Betriebsmittel umfassen dabei andere Softwaresystem (zur Konfiguration des Systems, der Hardware und der Software) sowie andere Materialien (Speichermedien, Papier). [91206]

3.1.5 Übertragbarkeit

Softwaresysteme werden oft über einen längeren Zeitraum und auf unterschiedlichen Plattformen eingesetzt. Eine Änderbarkeit für eine andere Plattform ist deshalb Grundvoraussetzung zur Erfüllung dieses Softwarequalitätsmerkmal. Änderbarkeit umfasst die einzelnen Aspekte *Analysierbarkeit*, *Modifizierbarkeit*, *Stabilität* und *Prüfbarkeit*.

Anpassbarkeit, *Installierbarkeit*, *Konformität* und *Austauschbarkeit* sind bei der Übertragbarkeit der Softwaresysteme zu berücksichtigen. Übertragbarkeit von Softwaresystemen definiert die Übertragung auf eine andere Software- oder Hardwareumgebung, sowie die Übertragung in verschiedenen organisatorischen Umgebungen. [91206]

3.2 Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme

Die IEC 61508 ist eine Sicherheitsgrundnorm zur funktionalen Sicherheit von elektrischen, elektronischen und programmierbar elektronischen sicherheitsbezogenen Systemen. Diese Norm ist anzuwenden, *wenn elektrische, elektronische, programmierbar*

elektronische Systeme (E/E/PES) zur Ausführung von Sicherheitsfunktionen eingesetzt werden. [61503] [Bel05]

Die IEC 61508 wird als so genannte Grundnorm verwendet, sie kann also für weitere Anwendungsgebiete als Vorlage dienen. Implementierungen der IEC 61508 für bestimmte Anwendungsgebiete sind zum Beispiel die *Anforderungen für sicherheitsrelevante Systeme in einem Kernkraftwerk*, oder die *Anforderungen für Eisenbahn-Signalanlagen.*

Auch Software, die einen Teil eines sicherheitsbezogenen Systems bildet, sollte nach EN 61508 entwickelt werden. Sie wird hier als sicherheitsbezogene Software bezeichnet. Sicherheitsbezogene Software beinhaltet *Betriebssysteme*, *Systemsoftware*, *Software in Netzwerken*, *Mensch-Maschine-Schnittstellen*, *Hilfswerkzeuge*, *Firmware* sowie *Anwenderprogramme.*

3.2.1 Softwareentwicklungsprozess nach IEC 61508

Die Phasen des Softwareentwicklungsprozesses werden in der IEC 61508 als Software-Sicherheitslebenszyklen bezeichnet.

3.2.1.1 Sicherheitsanforderung

Es müssen alle Anforderungen an die Software, bezüglich den Funktionen, den E/E/PES Systemen und dem Sicherheits-Integritätslevel spezifiziert werden. Die Spezifikationen müssen hinreichend genau sein, um die erforderliche Sicherheitsintegrität zu erreichen. Definiert werden:

- Die Sicherheitsfunktionen.
- Die Konfiguration oder Architektur des Systems.
- Die Anforderungen der Sicherheitsintegrität der Hardware.
- Die Anforderungen der Sicherheitsintegrität der Software.
- die Leistungsfähigkeit und die Reaktionszeit.

- Die Einrichtungen und Schnittstellen zum Anwender.
- Beziehungen zwischen Hard- und Software.

Je nach Sicherheits-Integritätslevel, müssen auch die folgenden Punkte berücksichtigt werden:

- Selbstüberwachung der Software und Überwachung der Hardware.
- Ermöglichen der Testbarkeit der Sicherheitsfunktionen und periodische Tests der Sicherheitsfunktionen während des Betriebs des Systems.
- Anforderungen der Software, die es ermöglichen einen sicheren Zustand zu erreichen oder aufrecht zu erhalten.
- Funktionen bezüglich der Erkennung, Anzeige und Handhabung von Fehlern in der Hardware, der programmierbaren Elektronik, der Sensoren und Aktoren und der Software selbst.
- Funktionen bezüglich der periodischen On-Line und Off-Line Tests der Sicherheitsfunktionen.
- Funktionen, die es erlauben Modifikationen am PES sicher durchführen zu können.
- Schnittstellen zu nicht sicherheitsbezogenen Funktionen und zwischen der Software und dem PES.
- Leistungsfähigkeit und Reaktionszeit.
- Sicherheits-Integritätslevel für jede der oben angeführten Funktionen.

Darüber hinaus, müssen auch Verfahren zum Lösen von Meinungsverschiedenheiten definiert werden. [61503]

3.2.1.2 Validierung

Um zeigen zu können, dass die Software ihre Sicherheits-Integrität erfüllt, wird ein Plan für die Validierung entworfen, welcher folgende Punkte enthalten muss:

- Zeitplan und Vorgehensweise der Validierung und verantwortliche Personen.
- Kennzeichen der wichtigen Betriebsarten (inklusive abnormaler Zustände).
- Entsprechend der Vorgehensweisen, Maßnahmen und Verfahren, die eingesetzt werden.
- Kriterien für bestanden und nicht bestanden (erforderliche Eingangssignale, erwartete Ausgangssignale, Speicherbelegung, Toleranzen, ...), sowie die Umgebungsbedingungen.
- Verfahrensweisen um die Ergebnisse (besonders das Versagen) zu bewerten.

Die technischen Vorgehensweisen, je nach Sicherheits-Integritätslevels, werden ebenfalls in der IEC 61508 definiert. [61503]

3.2.1.3 Softwareentwurf und Softwareentwicklung

Ein Ziel im Softwareentwurf und -entwicklungsprozess ist es, die Wechselwirkungen zwischen Hard- und Software zu überprüfen und zu bewerten. Ein weiteres Ziel ist, einen geeigneten Satz von Werkzeugen (Programmiersprache, Compiler) auszuwählen, die Software zu entwerfen, zu implementieren und zu verifizieren ob die Anforderungen bezüglich der Sicherheit erreicht worden sind.

Je nach Art der Softwareentwicklung, muss die Verantwortung im gesamten Softwareentwurf und -entwicklungsprozess klar definiert und dokumentiert werden. Dies muss während der Sicherheitsplanung festgelegt werden.

Während des Entwurfs müssen die Testbarkeit und Möglichkeit für sichere Modifikationen betrachtet werden und der sicherheitsbezogene Teil der Software möglichst gering gehalten werden. Wenn sowohl sicherheitsgerichtete, wie auch nicht sicherheitsgerichtete Funktionen enthalten sind, muss die gesamte Software als sicherheitsbezogen behandelt werden, es sei denn, es kann eine ausreichende Unabhängigkeit der Funktionen bewiesen werden.

Wenn standardisierte, oder bereits früher entwickelte Software als Teile des Entwurfs verwendet werden, so müssen diese eindeutig gekennzeichnet sein. Die Eignung dieser Teile für sicherheitsbezogene Software muss begründet und belegt werden. [61503]

3.2.1.4 Test der Softwaremodule

Jedes Softwaremodul muss getestet werden. Diese Tests müssen zeigen, dass jedes Softwaremodul seine bestimmungsgemäße Funktion und keine andere ausführt. Mögliche Tests sind unter anderem der Test aller *Äquivalenzklassen*, *Tests auf Strukturebene*, *Grenzwertanalysen*, *Kontrollflussanalysen* oder *Nebenpfadanalysen*. Wenn formale Beweise oder Plausibilitäten verwendet wurden, kann der Umfang der Tests reduziert werden. Die Durchführung der Tests und dessen Ergebnisse müssen dokumentiert werden und die Verfahren bei versagen im Test spezifiziert werden. [61503]

3.2.1.5 Softwareintegrationstest

Der Softwareintegrationstest muss während der Entwurfs- und Entwicklungsphase spezifiziert werden. Die Spezifikation muss Folgendes beschreiben:

- Die Aufteilung der Software in handhabbare Integrationsarbeiten.
- Testfälle und Testdaten.
- Arten der Tests, die durchzuführen sind.
- Testumgebung, Werkzeuge, Konfiguration und Programme.
- Testkriterien, nach denen die Vollständigkeit der Tests beurteilt werden.
- Verfahren für Korrekturen bei Versagen im Test.

Ergebnisse und Aussagen über das Erreichen der Ziele müssen dokumentiert werden. Sollte ein Versagen festgestellt werden, so sind die Gründe zu dokumentieren. Während der Softwareintegration, muss jede Modifikation einer Einflussanalyse unterzogen werden. Dies ist notwendig um den entsprechenden Einfluss auf alle Softwaremodule zu ermitteln.

Auch diese Integrationstests werden während der Entwurfs- und Entwicklungsphase spezifiziert. Die Spezifikation enthält über die Aufteilung des Systems in Integrationsstufen hinaus auch noch alle relevanten Informationen, wie in der Softwareintegration. Die gesamte Integration läuft proportional zur Integration der Software. [61503]

3.2.1.6 Softwaremodifikation

Eine Modifikation darf nur dann durchgeführt werden, wenn eine autorisierte Softwaremodifikationsanforderung, unter denn während der Sicherheitsplanung spezifizierten Verfahren, besteht. In der Modifikationsanforderung müssen die vorgeschlagenen Änderungen, sowie die Gründe für die Änderungen (zum Beispiel, funktionale Sicherheit zu niedrig, Fehler entdeckt, ...) und die Gefahren die betroffen sein könnten, beschrieben werden.

Weiters muss eine Analyse der Auswirkungen der Modifikation auf das E/E/PES System ausgeführt und dokumentiert werden. Sofern ein Einfluss auf die funktionale Sicherheit auftritt, muss zu einer angemessenen Phase des Sicherheitslebenszyklus zurückgekehrt werden und von dort alle folgenden Phasen ausgeführt werden. Eine Sicherheitsplanung, die die Modifikation der sicherheitsbezogenen Software spezifiziert, muss folgende Informationen enthalten, und sollte immer ausgeführt werden:

- Die Benennung des Personals und Festlegung dessen benötigter Fähigkeiten.
- Eine genaue Spezifikation der Modifikation.
- Die Planung der Verifikation.
- Den Anwendungsbereich von Neuvalidierung und Test der Modifikation, in dem durch den Sicherheitsintegritätslevel geforderten Umfang.

Die Modifikation muss exakt nach dieser Planung erfolgen und ausreichend dokumentiert werden. [61503]

3.2.1.7 Validierung bezüglich der Sicherheit

Die Validierung der Software muss wie geplant durchgeführt und dokumentiert werden. Folgende Ergebnisse müssen für jede Sicherheitsfunktion dokumentiert werden:

- Die chronologische Aufzeichnung der Validierungstätigkeiten.
- Die Version des verwendeten Plans der Validierung der Software bezüglich der Sicherheit.
- Die validierte Sicherheitsfunktion, zusammen mit dem Bezug zum Plan zur Validierung der Software bezüglich der Sicherheit.
- Die verwendeten Werkzeuge und Betriebsmittel mit den Daten der Kalibrierung und die Ergebnisse der Validierungstätigkeiten.
- Die Abweichungen zwischen den erwarteten und den tatsächlichen Ergebnissen.

Die verwendeten Hilfsmittel und Betriebsmittel müssen ebenfalls einer Norm entsprechen.

Die Validierung muss zeigen, dass die Anforderungen an die Software bezüglich der Sicherheit richtig durchgeführt wurden und das System keine undefinierten Funktionen ausführt. Die Testfälle und Ergebnisse müssen für nachfolgende Analysen und unabhängige Beurteilungen dokumentiert werden. [61503]

3.2.1.8 Verifikation

Die Verifikation, stellt außer der Gesamtverifikation, keine eigenständige Phase des Sicherheitslebenszyklus dar, sondern wird in jeder Phase durchgeführt. [61503]

3.3 IT Sicherheitsverfahren und Evaluationskriterien

Die ISO/IEC 15408 *Common Criteria* (CC) ist ein internationaler Standard zur Bewertung der Sicherheit von IT-Systemen. Die CC basiert auf mehreren internationalen

Standards. Durch die Zusammenführung der europäischen Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), des Orange-Book (TCSEC) der USA und der kanadischen Kriterien (CTCPEC) wurde eine international anerkannter Standard geschaffen. [15407b] [15407a] [CV07] [V.05]

3.3.1 Ziele der Common Criteria

Durch die Definition von Sicherheitskriterien ermöglicht die CC den Nachweis und die Evaluation von geforderter Sicherheitsfunktionalität in Bezug einer definierten Vertrauenswürdigkeit eines IT Sicherheitsproduktes. Es ermöglicht die neutrale und vertrauenswürdige Prüfung und Bewertung. Das Ergebnis der Bewertung ist ein international anerkanntes Zertifikat, das von einer staatlich anerkannten Prüfstelle (ISO/IEC 17025) vergeben wird. Diese Zertifikat umfasst die Sicherheitsfunktionalität in Bezug auf das Konfigurationsmanagement, die Auslieferung und den Betrieb, den Entwicklungsprozess, die Qualität der Handbücher, die Lebenszyklusunterstützung, das unabhängige Testen der Funktionalität, die Schwachstellenbewertung und die Erhaltung der Vertrauenswürdigkeit. [15407b] [15407a] [CV07]

3.3.2 Schutzprofil

Im Schutzprofil sind die Anforderungen an die Funktionalität sowie an die Vertrauenswürdigkeit vom bestimmten Produktgruppen definiert. Es enthält eine ausführliche Beschreibung und Gegenüberstellung des Sicherheitskonzepts und der Bedrohung. Schutzprofile definieren einen gewissen Sicherheitsstandard aus der Sicht des Anwenders. Anwender und Hersteller können unabhängig von bereits existierenden Produkten Schutzprofile nach ihren Anforderungen und Standardsicherheitsprobleme einer Produktgruppe definieren.

Bedingt durch das allgemeine Sicherheitskonzept eines Schutzprofiles ist für den IT-Anwender somit eine gute Vergleichbarkeit verschiedener Produkte gewährleistet.

Schutzprofile werden durch ein internationales Registrierungsverfahren evaluiert und zertifiziert und sind dadurch international anerkannt. [15407b] [15407a] [CV07]

3.3.3 Vertrauenswürdigkeitsstufen

Die CC umfasst sieben Stufen für die Vertrauenswürdigkeit, die *Evaluation Assurance Level* (EAL). Die Auswahl der Vertrauenswürdigkeitsstufe beruht im Wesentlichen auf dem geplanten Verwendungszweck des Produktes. Die Vertrauenswürdigkeitsstufe ist ebenfalls von rechtlichen Faktoren abhängig. [V.05]

Da die Auswahl der Vertrauenswürdigkeitsstufe eine wichtige Grundlage für den Umfang und Aufwand der Evaluation ist, sollten auch Kostenaspekte Einfluss auf die Auswahl der Vertrauenswürdigkeitsstufe haben. Höhere Vertrauenswürdigkeitsstufen können oft als Wettbewerbsvorteil oder auch als qualitätssichernde Maßnahme betrachtet werden.

Folgende Vertrauenswürdigkeitsstufen (EAL) sind in der CC definiert, wobei jede höhere Vertrauenswürdigkeitsstufe die vorangegangenen inkludiert:

- EAL0 unzulängliche Vertrauenswürdigkeit.
- EAL1 funktionell getestet.
- EAL2 strukturell getestet.
- EAL3 methodisch getestet und überprüft.
- EAL4 methodisch entwickelt, getestet und durchgesehen.
- EAL5 semiformal entworfen und getestet.
- EAL6 semiformal verifizierter Entwurf und getestet.
- EAL7 formal verifizierter Entwurf und getestet.

Die Common Criteria ist ein internationales Kriterienwerk für die Sicherheitsbewertung von Softwareprodukten. Es ermöglicht damit die internationale Vergleichbarkeit von Softwareprodukten. Die CC bildet für Anwender die Grundlage für einen gemeinsamen Bewertungsmaßstab von Sicherheitsprodukten. [15407b] [15407a] [CV07]

4

Kostennutzen Rechnung

Im diesem Abschnitt erfolgt die Darstellung der externen und internen Kosten für die Akkreditierung von Prüf- und Kalibrierlaboratorien gemäß ISO/IEC 17025. Anschließend werden diese Daten kritisch betrachtet und die betriebswirtschaftlichen Vor- und Nachteile diskutiert.

4.1 Externe und interne Kosten

Die jeweilige Organisation erstellt anhand der Norm ISO/IEC 17025 und des Leitfadens L05 [L0507], Version 9/2005, ein Qualitätsmanagementhandbuch und die erforderlichen Prüf- und Kalibrierverfahren. Der Leitfaden L05 ist auf der Homepage des Bundesministeriums für Wirtschaft und Arbeit erhältlich. [BWA07]

Das erstellte Qualitätsmanagementhandbuch und die Prüf- und Kalibrierverfahren müssen dann zur Begutachtung an das Bundesministerium für Wirtschaft und Arbeit weitergeleitet werden. Nach positiver Bewertung erfolgt die Überprüfung der im Qualitätsmanagementhandbuch definierten Qualitätsmanagementprozesse, Prüf- und Kalibrierverfahren im Unternehmen. Dies erfolgt durch zwei Sachverständige, wobei diese immer ein Techniker und ein Qualitätsmanager sind. Die Überprüfungen sind im optimalen Fall in zwei Tagen abgeschlossen.

Die anfallenden externen Kosten für eine Akkreditierung gemäß ISO/IEC 17025, im Idealfall, sind in Tabelle 4.1 aufgelistet. Die dazugehörigen internen Kosten sind in Tabelle 4.2 aufgelistet.

Erfahrungswerte zeigen, dass für die Erstellung des Qualitätsmanagementhandbuchs und aller benötigter Verfahren, im Idealfall, ein Mannjahr benötigt wird.

Einmaliger Verwaltungsaufwand (5-Jahreszyklus)	EURO 5.595,-
Für jedes Prüf- und Kalibierverfahren	EURO 36,-
Sachverständige (Überprüfung der Verfahren im Unternehmen)	EURO 4.400,-
Gesamtsumme	EURO 10.031,-

Tabelle 4.1: Externe Kosten für Akkreditierung im Idealfall

Aufbau des Qualitätsmanagementsystem und aller benötigter Verfahren. (ca. 1 Mannjahr)	EURO 73.000,-
Betreuung des Qualitätsmanagementsystem pro Jahr	EURO 14.600,-
Laufende Validierungen und Kalibrierungen der Mess- und Prüfmitteln (keine Erfahrungswerte im Softwarereich)	-
Mess- und Prüfmitteln müssen dem aktuellen Standard entsprechen (keine Erfahrungswerte im Softwarereich)	-
Personalschulungen pro Mitarbeiter	EURO 5.000,-

Tabelle 4.2: Interne Kosten für Akkreditierung im Idealfall

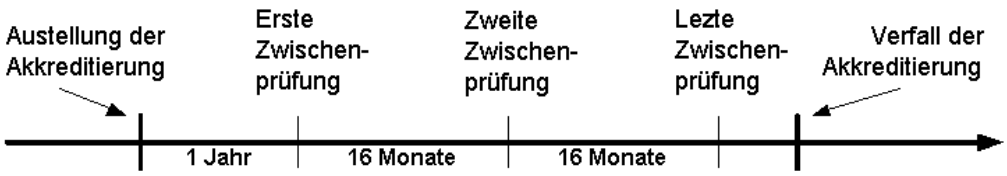

Abbildung 4.1: Nachhaltigkeit der Akkreditierung

Die Akkreditierung ist ab Ausstellung fünf Jahre gültig. Nach Ausstellung der Akkreditierung werden im Abstand von einem Jahr und danach zweimal im Abstand von 16 Monaten, Überprüfungen durchgeführt. Falls bei diesen Zwischenüberprüfungen keine Mängel auffallen, fallen dementsprechend auch keine Kosten an. Abbildung 4.1 zeigt eine schematische Darstellung der Nachhaltigkeit einer Akkreditierung im Idealfall.

4.2 Betriebswirtschaftlicher Effekt

Qualität ist nicht umsonst. Die Durchführung von Qualitätsmanagement Maßnahmen in Projekten belastet diese terminlich sowie kostenmäßig.

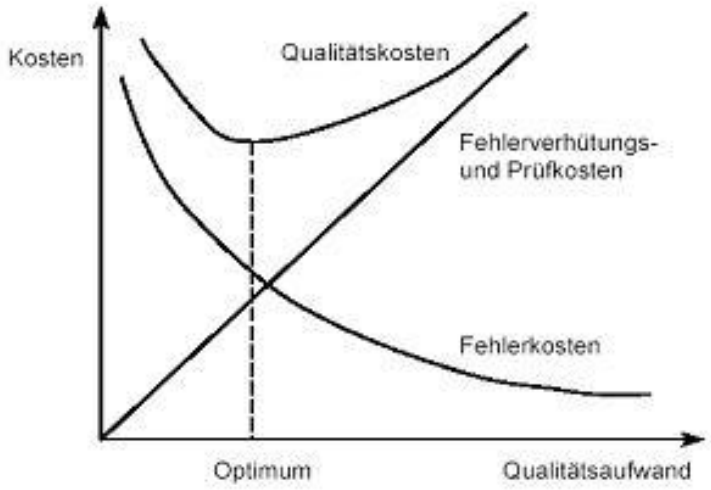

Abbildung 4.2: Darstellung der Qualitätskosten [LJSH00]

Welcher Nutzen steht diesen Kosten gegenüber? Qualitätsmanagement bedeutet Verhinderung und rechtzeitige Entdeckung von Fehlern. Jeder nicht entdeckte oder zu spät entdeckte Fehler ist mit erheblichen Fehlerbeseitigungskosten und mögliche Folgekosten verbunden. Die Wirtschaftlichkeit des Qualitätsmanagementsystems ergibt sich also aus der Gegenüberstellung von Qualitätsmanagementkosten einerseits und Fehlerkosten andererseits, siehe dazu Abbildung 4.2.

Wesentliche Vorteile, die sich durch eine Akkreditierung nach ISO/IEC 17025 ergeben sind, Erweiterung des Portfolios, Wettbewerbsvorteil und der Informationsvorsprung. Zu den wesentlichen Nachteilen zählen die doch sehr hohen Implementierungskosten und die allgemeinen Einbußen im Bereich der Flexibilität.

5

Zusammenfassung

Als Grundlage für eine unabhängige Softwareprüfstelle dient die Akkreditierung nach ISO/IEC 17025. Sie definiert den gesamt prozesstechnischen Ablauf eines Prüfverfahrens.

Nach welchen speziellen Regelwerken oder Normen ein Softwareprodukt evaluiert oder geprüft wird, hängt hauptsächlich von dem wirtschaftlichen Interesse ab.

Qualitätssicherung im Entwicklungsprozess und die Evaluierung durch einen unabhängigen Dritten sind die Grundlagen für die Steigerung der Vertrauenswürdigkeit gegenüber den Anwendern. Durch die Möglichkeit einer Evaluierung nach bestimmten Normen und Regelwerke können Softwareprodukte erst verglichen werden. Die ISO/IEC 9126 bildet dabei die Grundlage der Qualitätssicherung. Durch die Definition bestimmter Softwarequalitätsmerkmale ist es erst möglich eine Evaluierung und Test durchzuführen. Der Test dient dabei zur Sicherstellung, dass die festgelegten Anforderungen erfüllt wurden.

Die ISO/IEC 61508 bildet ein Regelwerk um den gesamten Softwarelebenszyklus von Softwareprodukten in sicherheitskritischen Anwendungen zu definieren. Es werden dabei sämtliche Phasen des Softwareentwicklungsprozess bis zur Außerbetriebnahme des Softwareprodukts berücksichtigt.

In der ISO/IEC 15408 Common Criteria ist ein Kriterienkatalog definiert, um eine systematische Evaluation von Sicherheitsmaßnahmen in Softwareprodukten durchzuführen. Die in der CC definierten und formulierten Sicherheitsanforderungen sind auf einem

sehr generischen Niveau. Dadurch ist es möglich bestimmte Sicherheitsanforderungen in konkreten Sicherheitsfunktionen verschiedenster Produktkategorien umzusetzen.

Die betriebswirtschaftlichen Aspekte sind aus der Sicht der vorliegenden Arbeit nicht vollständig beantwortet. Eine Erhebung des Marktpotentials sollte unbedingt durchgeführt werden. Ein nicht zu vernachlässigender betriebswirtschaftlicher Effekt ist sicherlich der Kompetenzaufbau im Softwareentwicklungsprozess und die daraus resultierenden Effekte.

Literaturverzeichnis

[15407a] DIN ISO/IEC 15408. *Anforderungen an die Vertrauenswürdikeit.* Europäisches Komitee für Normung, 2007.

[15407b] DIN ISO/IEC 15408. *Funktionale Sicherheitsanforderungen.* Europäisches Komitee für Normung, 2007.

[17005] EN ISO/IEC 17025. *Allgemeine Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien.* Europäisches Komitee für Normung, 2005.

[61503] ISO/IEC 61508. *Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme.* Europäisches Komitee für Normung, 2003.

[90000a] EN ISO 9000. *Qualitätsmanagementsysteme - Grundlagen und Begriffe.* Europäisches Komitee für Normung, 2000.

[90000b] EN ISO 9001. *Qualitätsmanagementsysteme - Anforderungen.* Europäisches Komitee für Normung, 2000.

[90000c] EN ISO 9004. *Qualitätsmanagementsysteme - Leitfaden zur Leistungsverbesserung.* Europäisches Komitee für Normung, 2000.

[91206] ISO/IEC 9126. *Software Quality Model.* Europäisches Komitee für Normung, 2006.

[Bel05] Ron Bell. *Introduction to IEC 61508.* UK Crown Copyright, This paper appeared at the ACS Workshop on Tools and Standards Sydney, 2005.

[BWA07] Bundesministerium für wirtschaft und arbeit. http://www.bmwa.gv.at/BMWA/Schwerpunkte/Unternehmen/Akkreditierung/default.htm. Dezember2007, 2007.

[CV07] CCMB-2007-09-004:V3.1R2. *Evaluation methodology*. 2007.

[L0507] Bundesministerium für wirtschaft und arbeit, leitfaden l05. http://www.bmwa.gv.at/NR/rdonlyres/7CF4F714-1E3F-46BD-9068-4138327568A0/0/LeitfadenL05AkkreditierungsantragsPstelleV91CD.pdf, 2007.

[LJSH00] Frühauf K. Ludedwig J. Sandmayr H. *Software-Projektmanagement und Qualitätssicherung*. vdf Hochschulverlag, 2000.

[V.05] Bhansali P. V. *Universal Software Safety Standard*. ACM SIGSOFT, 2005.

Abkürzungsverzeichnis

CC	Common Criteria
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
EAL	valuation Assurance Level
EMV	Elektromagnetische Verträglichkeit
EN	Europäische Norm
E/E/PES	elektrischer/elektronischer/programmierbar elektronischer Systeme
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ITSEC	Information Technology Security Evaluation Criteria
TCSEC	Trusted Computer System Evaluation Criteria

Anhang

Anhang A

Prozessorientierter Ansatz der ISO 9001

Damit eine Organisation wirksam funktionieren kann, muss sie zahlreiche miteinander verknüpfte Tätigkeiten erkennen, leiten und lenken. Eine Tätigkeit, die Ressourcen verwendet und die ausgeübt wird, um die Umwandlung von Eingaben in Ergebnisse zu ermöglichen, kann als Prozess angesehen werden. Oft bildet das Ergebnis des einen Prozesses der direkte Eingabe für den nächsten. [90000b]

Die Anwendung eines Systems von Prozessen in einer Organisation, gepaart mit dem Erkennen und den Wechselwirkungen dieser Prozesse sowie deren Management, kann als prozessorientierter Ansatz bezeichnet werden, siehe dazu Abbildung 1.

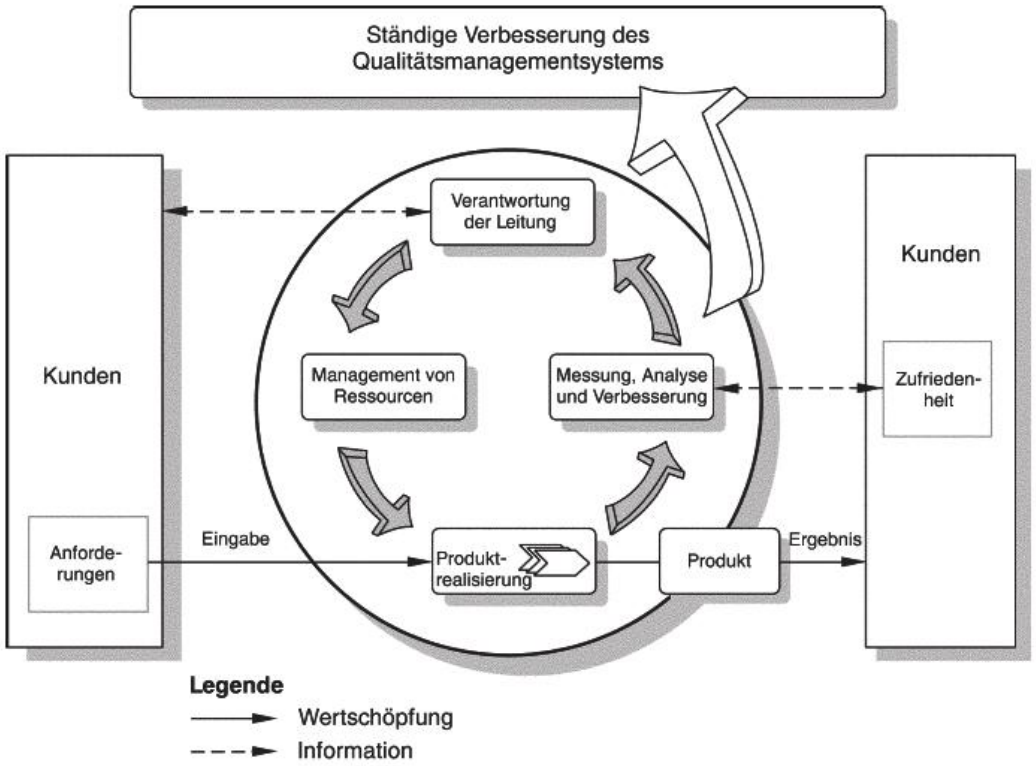

Abbildung 1: Modell eines prozessorientierten Qualitätsmanagementsystems [90000b]

Anhang B

Anforderungen an das Managementsystem gemäß ISO/IEC 17025

Alle Dokumente und auch Änderungen, die an das Personal im Laboratorium herausgegeben werden, müssen vor der Ausgabe von befugtem Personal geprüft und für den Gebrauch genehmigt werden, um auszuschließen, dass ungültige Dokumente verwendet werden. Es muss sichergestellt werden, dass die entsprechenden Dokumente eindeutig gekennzeichnet sind, verfügbar sind und regelmäßig überprüft werden. [17005]

Anfragen, Angebote und Verträge

Die Prüfungen die zu einem Vertrag über eine Prüfung führen, müssen sicherstellen, dass die Anforderungen, einschließlich der zu verwendeten Methoden, verstanden, festgelegt, schriftlich niedergelegt und von Laboratorium erfüllt werden können. Die Prüfung muss auch alle Arbeiten einschließen, die das Laboratorium als Unterauftrag vergibt. Der Kunde muss über jede Abweichung vom Vertrag unterrichtet werden. Unterauftragnehmer müssen für die in Frage kommenden Prüfungen und Kalibrierungen der ISO/IEC 17025 entsprechen. [17005]

Dienstleistung für den Kunden

Das Laboratorium muss mit dem Kunden eng zusammenarbeiten, ist Verantwortlich für den Informationsrückfluss, muss aber die Vertraulichkeit gegenüber anderen Kunden bewahren. Der Informationsrückfluss dient zur Verbesserung des Managementsystems. Über Beschwerden und vom Laboratorium ergriffenen Korrekturmaßnahmen müssen Aufzeichnungen geführt werden. [17005]

Lenkung von Aufzeichnungen

Das Laboratorium muss sicherstellen das bei fehlerhaften Prüf- oder Kalibrierarbeiten, die Verantwortlichkeiten und Befugnisse zur Behandlung dieser fehlerhaften Arbeiten

festgelegt sind. Wo erforderlich ist auch der Kunde zu unterrichten. Qualitätsaufzeichnungen sind interne Audits, Managementbewertungen, Korrekturmaßnahmen und vorbeugende Maßnahmen. Die Aufzeichnungen müssen leserlich sein und es müssen Aufbewahrungsfristen festgelegt werden. Aufzeichnungen können in Papierform oder auf elektronischen Medien abgelegt werden. Aufzeichnungen von Prüfungen oder Kalibrierungen müssen alle Informationen enthalten um die Prüfung oder Kalibrierung unter den gleichen Bedingungen zur wiederholen. [17005]

Interne Audits

Das Laboratorium muss regelmäßig seine Tätigkeiten einem internen Audit unterziehen, um nachzuweisen, dass seine Abläufe den Anforderungen der ISO/IEC 17025 entsprechen. Diese Audis müssen von qualifiziertem Personal durchgeführt werden. [17005]