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 iv

Tabellenverzeichnis v

1 Einleitung 1
   1.1 Problemstellung ........................................ 2
   1.2 Lösungsansatz ........................................... 2

2 Grundlagen der Akkreditierung 3
   2.1 Anforderung an das Qualitätsmanagementsystem .......... 3
       2.1.1 Prozessorientierter Ansatz ......................... 4
       2.1.2 Grundsätze des Qualitätsmanagements ............... 4
   2.2 Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien 5
       2.2.1 Anforderungen an das Managementsystem ............. 5
       2.2.2 Technische Anforderungen ........................... 6
           2.2.2.1 Prüf- und Kalibrierverfahren und deren Validierung . 6
           2.2.2.2 Mess- und Prüfeinrichtungen ..................... 7
           2.2.2.3 Qualität von Prüf- und Kalibrierergebnissen ......... 7
           2.2.2.4 Ergebnisberichte .............................. 8

3 Spezialisierung im Softwarebereich 9
   3.1 Qualitätsmerkmale für Softwareprodukte .................. 9
       3.1.1 Funktionalität ...................................... 10
       3.1.2 Zuverlässigkeit .................................... 10
       3.1.3 Benutzerbarkeit .................................... 11
       3.1.4 Effizienz .......................................... 11
       3.1.5 Übertragbarkeit .................................... 11
Abbildungsverzeichnis

<table>
<thead>
<tr>
<th>4.1 Nachhaltigkeit der Akkreditierung</th>
<th>21</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2 Darstellung der Qualitätskosten [LJSH00]</td>
<td>22</td>
</tr>
<tr>
<td>1 Modell eines prozessorientierten Qualitätsmanagementsystems [90000b]</td>
<td>29</td>
</tr>
</tbody>
</table>
# Tabellenverzeichnis

| 4.1 Externe Kosten für Akkreditierung im Idealfall | 21 |
| 4.2 Interne Kosten für Akkreditierung im Idealfall | 21 |
Einleitung


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. Einleitung

1.1 Problemstellung


1.2 Lösungsansatz


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


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

Dies umfasst im Wesentlichen die Schwerpunkte *Verantwortung der Leitung, Management von Ressourcen, Produktrealisierung* und *Messung, Analyse und Verbesserung*.

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: \([\text{LJSH00}]\)

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 Geschäftsführung geht.


### 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 Managementsystem behandeln die Themen Anfragen, Angebote und Verträge. Weiters werden die Dienstleistungen für den Kunden, die Lenkung von Aufzeichnungen und Interna 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 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

2. Grundlagen der Akkreditierung

2.2.2.2 Mess- und Prüfeinrichtungen


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 zurückgeführt 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. Weiter 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

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.


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

3.1.1 Funktionalität


3.1.2 Zuverlässigkeit

3.1.3 Benutzbarekeit

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

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).

3.1.5 Übertragbarkeit


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
Spezialisierung im Softwarebereich 12

elektronische Systeme (E/E/PES) zur Ausführung von Sicherheitsfunktionen eingesetzt werden. [61503] [Be05]

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.


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:
3. Spezialisierung im Softwarebereich

- 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


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.

3.2.1.4 Test der Softwaremodule


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.

3. Spezialisierung im Softwarebereich

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 denen 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 (TC-SEC) 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


4. Kostennutzen Rechnung

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

4.2 Betriebswirtschaftlicher Effekt

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

![Diagram of Quality Costs](image)

Abbildung 4.2: Darstellung der Qualitätskosten [LJSH00]


Zusammenfassung


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


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
5. Zusammenfassung

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

Literaturverzeichnis


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


<table>
<thead>
<tr>
<th>Abkürzung</th>
<th>Deutscher Begriff</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC</td>
<td>Common Criteria</td>
</tr>
<tr>
<td>CTCPEC</td>
<td>Canadian Trusted Computer Product Evaluation Criteria</td>
</tr>
<tr>
<td>EAL</td>
<td>valuation Assurance Level</td>
</tr>
<tr>
<td>EMV</td>
<td>Elektromagnetische Verträglichkeit</td>
</tr>
<tr>
<td>EN</td>
<td>Europäische Norm</td>
</tr>
<tr>
<td>E/E/PES</td>
<td>elektrischer/elektronischer/programmierbar elektronischer System</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>ITSEC</td>
<td>Information Technology Security Evaluation Criteria</td>
</tr>
<tr>
<td>TCSEC</td>
<td>Trusted Computer System Evaluation Criteria</td>
</tr>
</tbody>
</table>
Anhang
Anhang A

Prozessorientierter Ansatz der ISO 9001


Abbildung 1: Modell eines prozessorientierten Qualitätsmanagementsystems
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

**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 Audits müssen von qualifiziertem Personal durchgeführt werden. [17005]