

Jmetrika

Handbuch

Analyse sicherheitsrelevanter Software

Ansprechpartner:

Berufsgenossenschaftliches Institut
für Arbeitsschutz – BGIA

Zentralbereich

Prof. Dr. Dietmar Reinert

53754 Sankt Augustin

Tel.: 02241 231-2750

Fax: 02241 231-2234

Dietmar.Reinert@HVBG.de



Inhaltsverzeichnis

1 Inhalte	3
2 Nutzung	3
3 Haftung.....	3
4 Installation und Start der Anwendung.....	4
5 Bedienebenen.....	4
5.1 Projektverwaltung	4
5.2 Projekteinstellungen	5
5.3 Metriken.....	7
5.4 Kennzahlen	8
6 Bericht.....	8
7 Kontrollflussgraph.....	10
8 Kiviatgraph.....	11

1 Inhalte

„Jmetrika“ ist eine Software, die zur Erstellung von Metriken, Qualitätskriterien und Strukturgraphen sicherheitsrelevanter Software dient. Ziel der Anwendung ist es, den Gutachtern solcher kritischer Anwendungen einen schnellen Einstieg in die Prüflinge zu ermöglichen. Berechnete Daten dienen als Beurteilungs- und Diskussionsgrundlage für Softwarezertifizierungen und Reviews, in denen die zu prüfenden Anwendungen untersucht werden.

Das Programm „Jmetrika“ wurde für mehrere Programmiersprachen entwickelt. Diese Anleitung beschreibt die Nutzung von „Jmetrika“ im Allgemeinen und geht nicht auf die Besonderheiten der zu untersuchenden Programmiersprache ein. Hinweise für die entsprechende Programmiersprache entnehmen Sie bitte der zusätzlichen Information zu dieser Programmiersprache. Im Folgenden wird immer nur der Programmname „Jmetrika“ verwendet, welcher dem Werkzeug zur Analyse von Java-Quelltexten entspricht. Bei anderen Programmiersprachen wurde der Programmname entsprechend erweitert:

AWL jmetrikaAWL

C jmetrikaC

C++ jmetrikaCPP

Das Werkzeug kann kostenlos heruntergeladen werden. Es baut auf den Abschlussarbeiten an der Fachhochschule Bonn-Rhein-Sieg der Informatiker *Michael Krell*, *Christian Staron*, *Vitali Maurer*, *Martin Ley*, *Thomas Breuer* und *Daniel Paurat* auf, die auf den [Hochschulseiten](#) zur Verfügung stehen. Die Einzelmetriken lassen sich grundsätzlich anpassen. Die voreingestellten Werte für die Metriken sind weitgehend der Literatur entnommen. Insbesondere für die Metriken von Breuer (nur für Programmiersprache AWL) und Krell sind die Autoren an einer Rückmeldung aus der industriellen Praxis sehr interessiert, um das Werkzeug weiter zu optimieren.

2 Nutzung

Die Software wurde gemäß dem Stand von Wissenschaft und Technik sorgfältig erstellt. Sie wird dem Nutzer unentgeltlich zur Verfügung gestellt. Die Benutzung der Software erfolgt auf eigene Gefahr.

3 Haftung

Eine Haftung – gleich aus welchem Rechtsgrund – ist, soweit gesetzlich zulässig, ausgeschlossen. Insbesondere für Sach- und Rechtsmängel der Software sowie der damit zusammenhängenden Dokumentationen und Informationen wird – vor allem im Hinblick auf deren Richtigkeit, Fehlerfreiheit, Freiheit von Schutz- und Urheberrechten Dritter, Aktualität, Vollständigkeit und/oder Verwendbarkeit, außer bei Vorsatz oder Arglist – nicht gehaftet.

Das BGIA ist bemüht, sein Internetangebot virenfrei zu halten, gleichwohl kann keine Virenfreiheit der zur Verfügung gestellten Software und Informationen zugesichert werden. Dem Nutzer wird daher empfohlen, vor dem Herunterladen von Software,

Dokumentationen oder Informationen selbst für angemessene Sicherheitsvorkehrungen und Virens Scanner zu sorgen.

4 Installation und Start der Anwendung

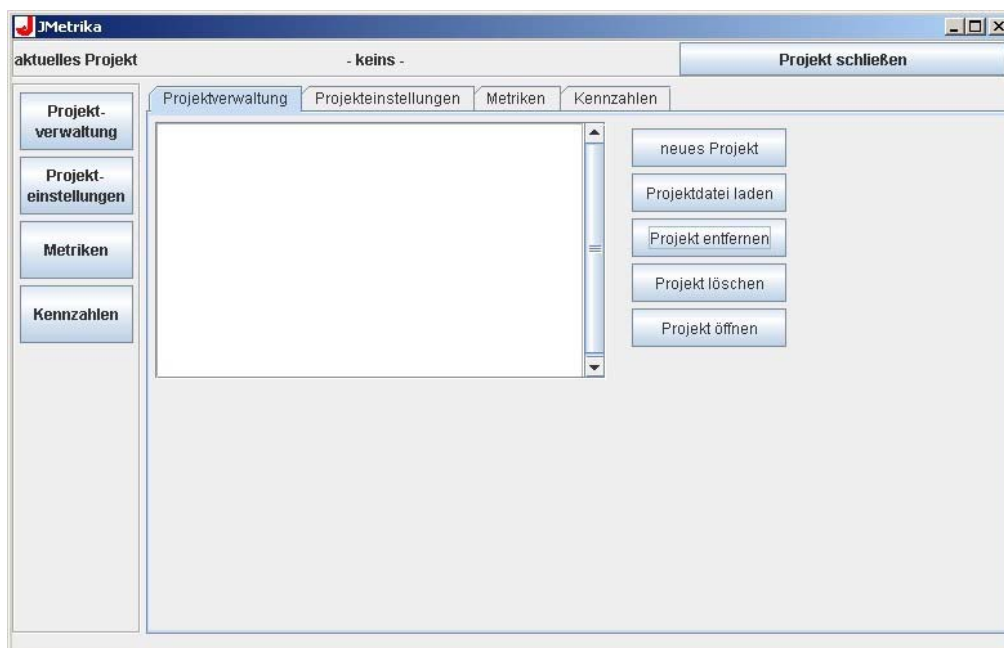
Zur Installation der Anwendung ist doppelt auf die Setup-Datei zu klicken und den Installationsanweisungen zu folgen. Im Startmenü wird unter „Programme/ Berufsgenossenschaftliches Institut für Arbeitsschutz – BGIA/“ ein Eintrag mit der entsprechenden Programmversion angelegt. Bei Klick auf „Jmetrika“ wird das Programm gestartet und kann verwendet werden.

Das Programm hat vier Bedienebenen, die entweder über die Buttons links im Programm erreicht werden können **oder** direkt über die entsprechenden Reiter gleichen Namens. Die Bedienebenen werden im Folgenden näher erläutert.

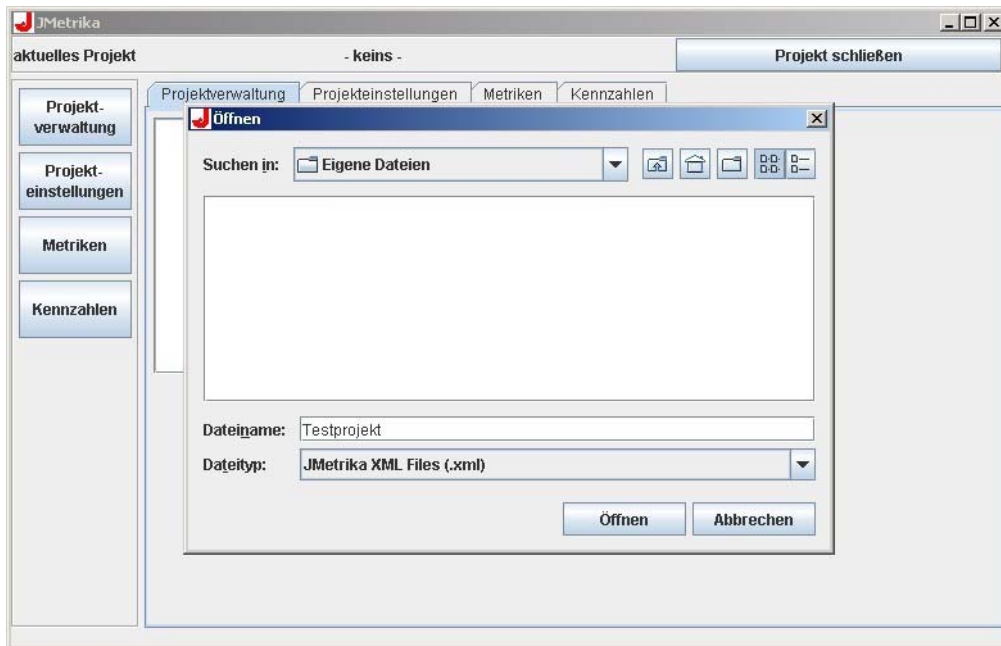
5 Bedienebenen

5.1 Projektverwaltung

Nach dem Start des Programms erscheint die Projektverwaltung. Hier können Projekte angelegt, geladen und wieder gelöscht werden.



Über den Button „neues Projekt“ können Sie ein neues Projekt anlegen, das daraufhin automatisch geöffnet wird.



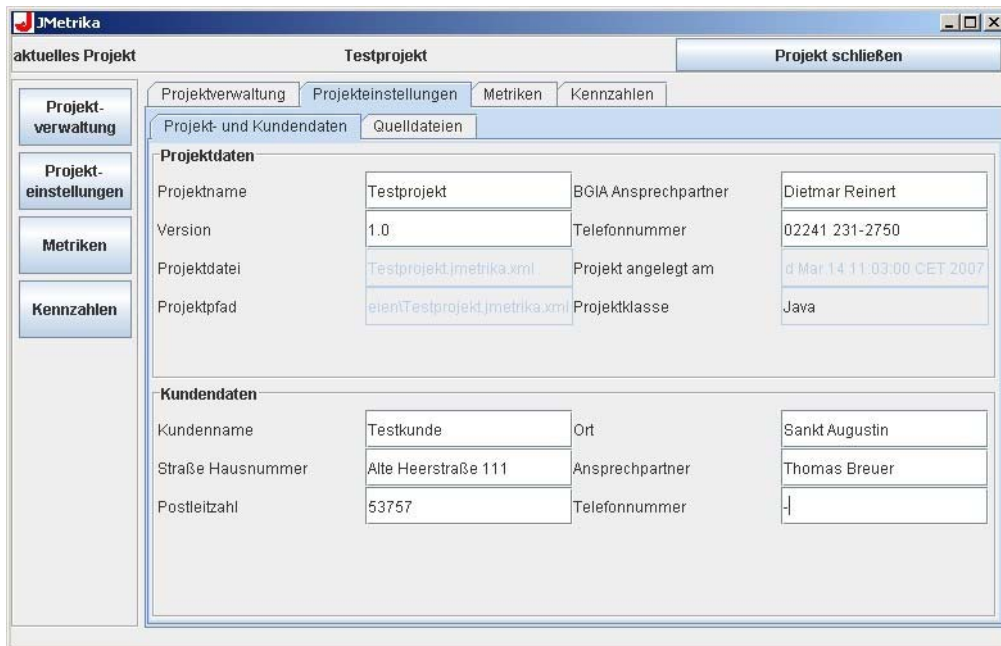
Des Weiteren können Sie über den Button „Projektdatei laden“ ein bereits erstelltes Projekt in die Auswahlliste (weißes Feld neben den Buttons) laden. Dieses Projekt wird dann auch automatisch geöffnet. Falls vorher ein anderes Projekt geöffnet war, wird dieses automatisch geschlossen und alle relevanten Daten des Projektes werden gespeichert.

Über den Button „Projekt entfernen“ können Sie ein Projekt aus der Auswahlliste entfernen (Projektdatei bleibt am Speicherort erhalten). Wenn Sie ein Projekt sowohl aus der Auswahlliste als auch auf der Festplatte löschen möchten, müssen Sie den Button „Projekt löschen“ betätigen.

Mit dem Button „Projekt öffnen“ können Sie ein Projekt öffnen, das Sie zuvor in der Auswahlliste angewählt haben. Falls vorher ein anderes Projekt geöffnet war, wird dieses automatisch geschlossen und alle relevanten Daten des Projektes werden gespeichert.

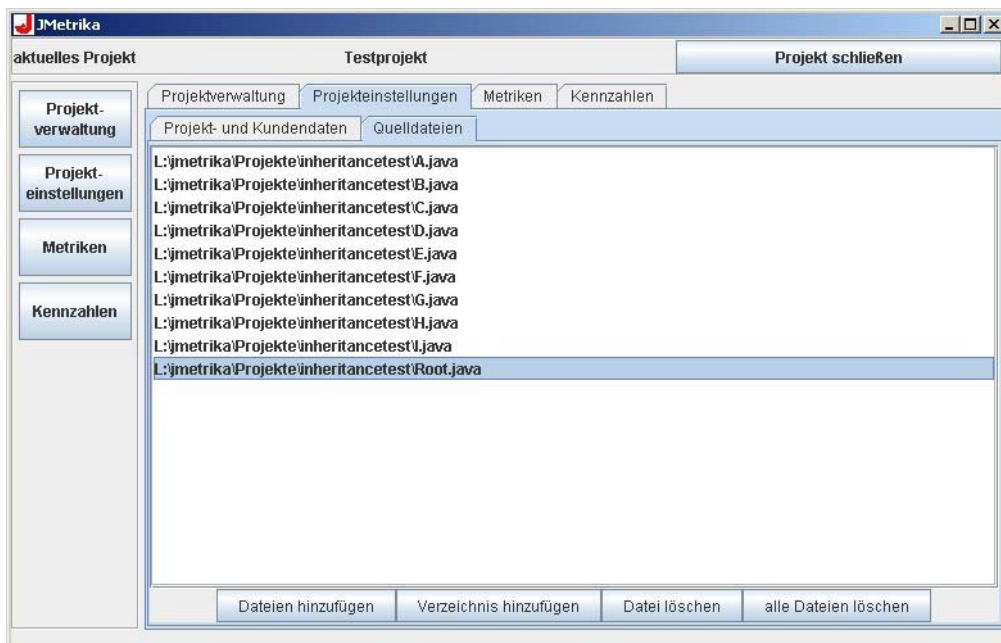
5.2 Projekteinstellungen

Über den Button „Projekteinstellungen“ links im Programm oder direkt durch Anwahl des Reiters „Projekteinstellungen“ erreichen Sie die Bedienebene zur Eingabe/Änderung der Projekt- und Kundendaten und Auswahl der zu untersuchenden Quelldateien.



Im Reiter „Projekt- und Kundendaten“ können Sie alle relevanten Daten eingeben. Diese Daten werden später an oberster Stelle im erzeugten Bericht angezeigt.

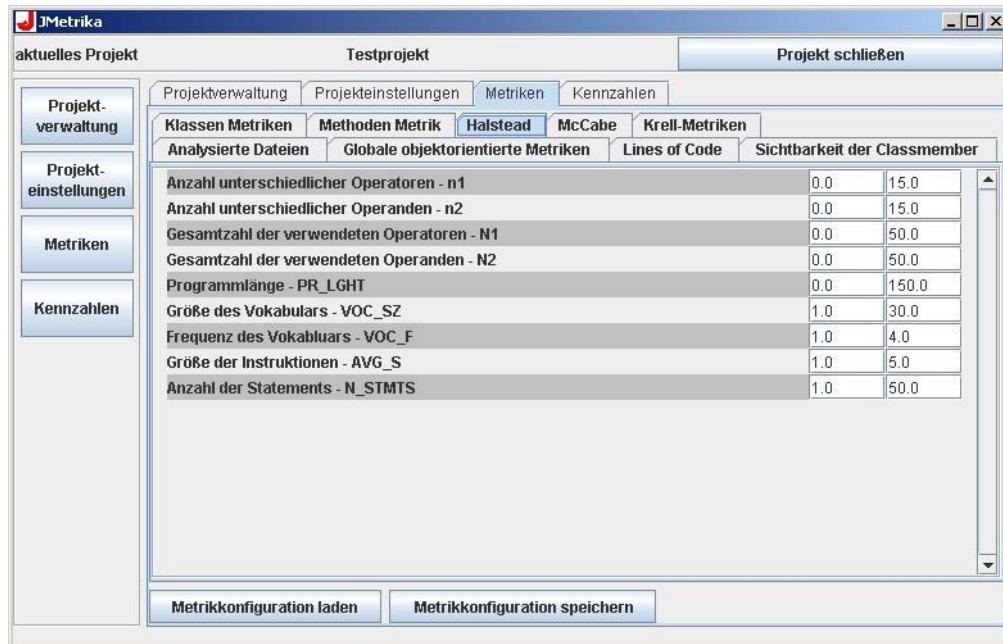
Um die zu untersuchenden Quelldateien auszuwählen oder zu ändern, müssen Sie in den Reiter „Quelldateien“ wechseln. Wenn Sie einzelne Dateien in die Auswahlliste hinzufügen möchten, müssen Sie den Button „Dateien hinzufügen“ betätigen. Über den Button „Verzeichnis hinzufügen“ können Sie ein ganzes Verzeichnis hinzufügen, das rekursiv (auch Dateien in sämtlichen Unterordnern) alle Dateien hinzufügt. Bitte prüfen Sie an dieser Stelle noch einmal nach, ob Sie auch wirklich nur zu untersuchende Quelltexte in die Auswahlliste aufgenommen haben. Andernfalls wird im später erzeugten Bericht ggf. ein Vermerk auftauchen, dass die Datei(en) nicht eingelesen werden konnte(n).



Über die Buttons „Datei löschen“ und „alle Dateien löschen“ können Sie Dateien wieder aus der Auswahlliste entfernen. Die entsprechenden Dateien werden nur aus der Auswahlliste entfernt und nicht auf der Festplatte gelöscht.

5.3 Metriken

Über den Button „Metriken“ links im Programm oder direkt durch Anwahl des Reiters „Metriken“ erreichen Sie die Bedienebene zur Betrachtung/Veränderung der verwendeten Metriken und deren Grenzwerte.



Jede Gruppe von Metriken hat an dieser Stelle einen eigenen Reiter. Links zu sehen ist immer sowohl der Name der entsprechenden Metrik als auch deren Kurzschreibweise. Die hier angezeigten Metriken haben immer eine untere (linker Zahlenwert) und eine obere (rechter Zahlenwert) Schranke. Liegt der errechnete Wert einer Metrik außerhalb dieser Schranken/Grenzwerte, so wird die Metrik im Bericht farblich (rot) hervorgehoben. Außerdem führt das Überschreiten der Grenzen bei einigen Metriken dazu, dass eine bestimmte Aussage zur Qualität der Software getroffen wird.

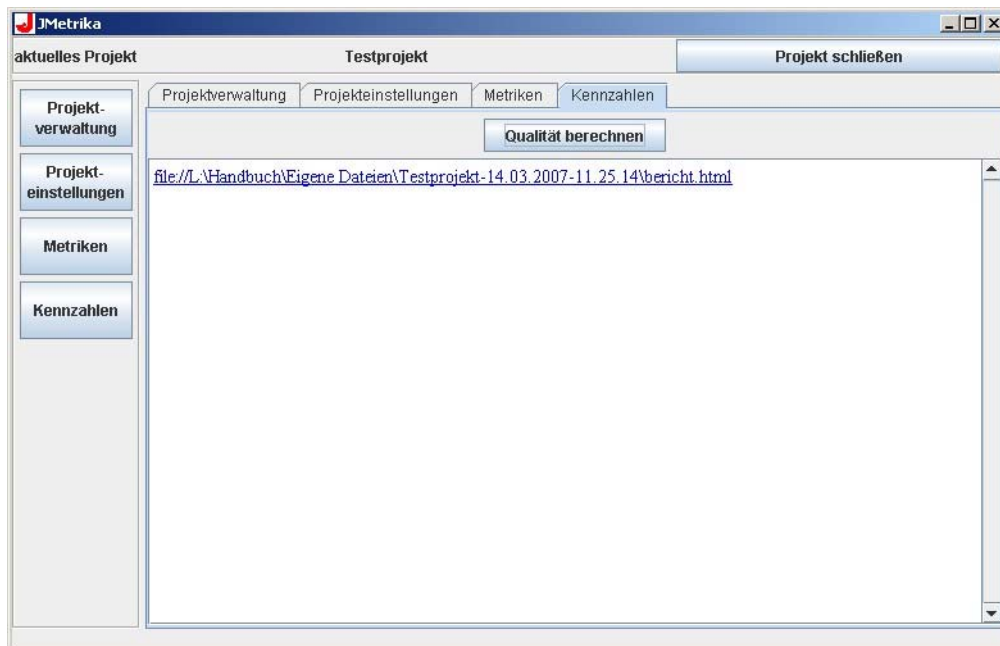
Die Grenzwerte wurden zum Teil aus der Literatur entnommen, zum Teil aber auch an die Besonderheiten sicherheitskritischer Anwendungen angepasst. Die Metrikgrenzwerte lassen sich an dieser Stelle aber auch an die eigenen Bedürfnisse anpassen und werden automatisch für das aktuell geöffnete Projekt gespeichert. Wenn die veränderten Metrikgrenzwerte auch in anderen Projekten verwendet werden sollen, können Sie die Konfiguration speichern über den Button „Metrikkonfiguration speichern“ und in einem anderen Projekt laden über den Button „Metrikkonfiguration laden“. Wenn Sie eine Metrikkonfiguration laden, werden die neuen Grenzwerte automatisch für das aktuelle Projekt gespeichert.

WICHTIG: Eine Metrikkonfiguration gilt immer nur für eine bestimmte Programmiersprache und kann somit nicht z. B. in Jmetrika für Java erzeugt werden und in JmetrikaC für die Programmiersprache C geladen werden!

Näheres zu den Metriken und Qualitätskriterien für eine bestimmte Programmiersprache erfahren Sie in der Dokumentation der entsprechenden Jmetrika-Version .

5.4 Kennzahlen

Über den Button „Kennzahlen“ links im Programm oder direkt durch Anwahl des Reiters „Kennzahlen“ erreichen Sie die Bedienebene zum Auslösen der Berechnung der Qualität.



Wenn Sie auf den Button „Qualität berechnen“ klicken, werden die Berechnung der Metriken, die Berechnung der Qualitätskriterien und die Berichtserzeugung gestartet. Für den Bericht wird im gleichen Ordner, in dem die Projektdatei liegt, ein Unterordner mit folgender Namensgebung erzeugt:

Projektname-Datum-Uhrzeit

Nach der Erzeugung des Berichts wird dieser automatisch in ihrem Webbrowser geöffnet. Da das Erzeugen eines Berichts mitunter sehr lange dauern kann, wird in einem Projekt immer der Link zu dem zuletzt erzeugten Bericht gespeichert. Bei Klick auf den entsprechenden Link wird der letzte erzeugte Bericht angezeigt und keine neue Berechnung der Metriken angestoßen.

6 Bericht

Der Bericht wird als HTML-Datei im gleichen Ordner, in dem die Projektdatei liegt, ein Unterordner mit folgender Namensgebung erzeugt (s.o.):

Projektname-Datum-Uhrzeit

Die Hauptseite des Berichts heißt „bericht.html“ und kann aus einem Webbrowser heraus geöffnet werden. Dieser Bericht ist der Überblicksbericht über das Projekt. Er umfasst immer zuerst die Projekt- und Kundendaten sowie einen Link zu den beiden Druckversionen des vollständigen Berichts (Druckbericht mit und ohne Kiviatgraphen). Die Druckversionen skalieren die eingebundenen Graphen auf Seitenbreite und fassen alle Berichte in einer Datei zusammen, sodass diese problemlos gedruckt werden kann.

Als nächstes folgen die Aussagen über die globale Qualität. Da sich die Metriken und Qualitätskriterien in den verschiedenen Programmiersprachen unterscheiden, wird auf

diese Besonderheiten für die jeweilige Programmiersprache in der zugehörigen Dokumentation eingegangen.

The screenshot shows a web browser window titled "JMetrika Bericht - Mozilla Firefox". The address bar shows the file path: file:///L:/Handbuch/Eigene%20Dateien/Testprojekt-14.03.2007-11.25.14/bericht.html. The page content is as follows:

Projektdaten

Projektname	Testprojekt
Version	1.0
BGLA Ansprechpartner	Dietmar Reinert
Telefonnummer	02241 231-2750
Projekt angelegt am	Wed Mar 14 11:03:00 CET 2007

Kundendaten

Kundenname	Testkunde
Straße Hausnummer	Alte Heerstraße 111
Postleitzahl	53757
Ort	Sankt Augustin
Ansprechpartner	Thomas Breuer
Telefonnummer	-

Druckversionen des Berichts:

[Vollständiger Bericht](#)
[Bericht ohne Kiviat-Graph](#)

Fertig

Bei objektorientierten Programmiersprachen umfasst der Überblicksbericht außerdem die errechneten Werte für die globalen Metriken und einen Überblick über die Qualität aller Klassen. Für jede Klasse wird ein eigener Bericht erzeugt, der jeweils im Überblicksbericht verlinkt ist.

The screenshot shows a web browser window titled "JMetrika Bericht - Mozilla Firefox". The address bar shows the file path: file:///L:/Handbuch/Eigene%20Dateien/Testprojekt-14.03.2007-11.25.14/bericht.html. The page content is as follows:

GlobALE QUALITÄT

TESTBARKEIT	ACCEPTED
EINFACHHEIT	ACCEPTED
LESBARKEIT	ACCEPTED
SELBSTBESCHREIBUNG	ACCEPTED

Globale Metriken:

Analysierte Dateien	Wert	min	max
Anzahl analysierter Dateien - NUM_ANALYSED_FILES	10	0	1.000
Globale objektorientierte Metriken			
	Wert	min	max
Tiefe des Vererbungsbaums - DIT	4	0	6
Durchschnittliche Tiefe des Vererbungsbaums - MEAN_DIT	1,9	0	3

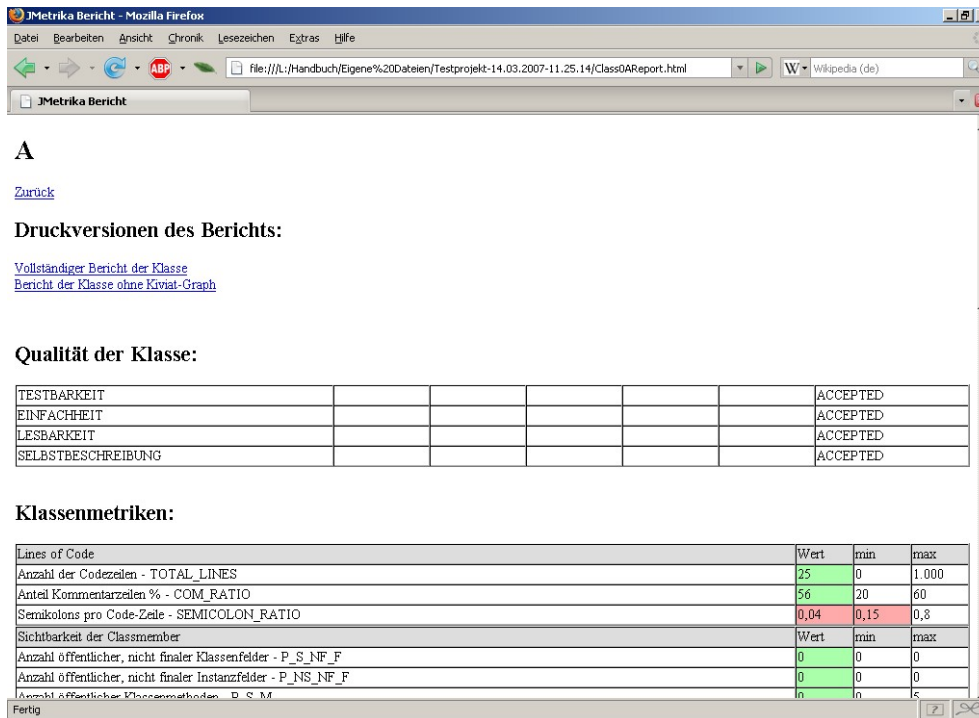
Übersicht über Klassen des Projekts:

[A](#)

TESTBARKEIT					ACCEPTED
EINFACHHEIT					ACCEPTED
LESBARKEIT					ACCEPTED
SELBSTBESCHREIBUNG					ACCEPTED

Fertig

Der Bericht jeder Klasse ist wieder ein Überblicksbericht: Zuerst enthält er die verlinkten Druckversionen, dann die Aussagen über die Qualität der Klasse, als nächstes die Klassenmetriken und zuletzt den Überblick über die jeweiligen Module der Klasse.

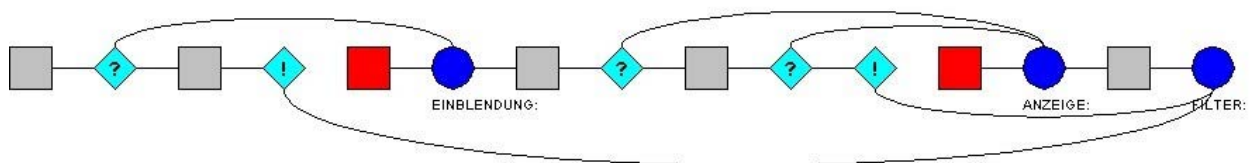


Für jedes Modul wird ein eigener Bericht erzeugt mit dessen Qualitätsaussagen, Kontrollflussgraph, Metriken und Kiviatgraph.

In nicht objektorientierten Programmiersprachen wird in dem Überblicksbericht direkt eine Übersicht über die Qualität der Module und deren Kontrollflussgraph dargestellt. Der Bericht einer Klasse entfällt für nicht objektorientierte Programmiersprachen.

7 Kontrollflussgraph

Für jedes Modul wird ein Kontrollflussgraph erzeugt und dem Bericht hinzugefügt (sowohl dem Bericht für das Modul als auch dem Überblicksbericht über alle Module). Dieser Kontrollflussgraph zeigt den Kontrollfluss durch ein Modul. Bei jedem bedingten Sprung (bedingter Sprung zu einem Label, If-Struktur, Switch-Struktur) einer Schleife (while, do while, for) oder einer Schleife entsteht ein zusätzlicher Pfad durch das Programm.



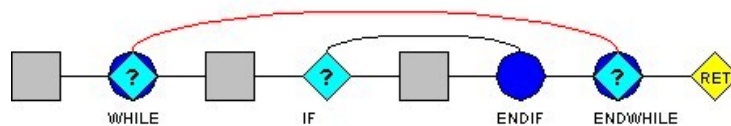
Sequentieller Code (Code ohne Sprünge, Verzweigungen oder andere Kontrollstrukturen) wird als graues Quadrat dargestellt. Ein bedingter Sprung wird als türkisfarbene Raute mit einem Fragezeichen, ein unbedingter Sprung als türkisfarbene Raute mit einem Ausrufezeichen dargestellt. Wenn ein Programmteil z. B. wegen eines Sprunges nicht mehr erreichbar ist, wird dieser Teil im Graph rot hinterlegt. In diesem Beispiel ist das für zwei Stellen sequentiellen Codes der Fall. Beide werden durch einen unbedingten Sprung übersprungen. Sprungziele (Labels) werden als blauer Kreis incl. ihres Namens dargestellt.

Des Weiteren werden Kontrollstrukturen rot hinterlegt, wenn diese mindestens zwei nachfolgende Komponenten haben sollten, aber nur eine nachfolgende Komponente

im Graph auftaucht. Dies kann vorkommen, wenn z. B. das Sprungziel zu einem bedingten Sprung nicht gefunden wird. Insbesondere tritt dieser Fall auch auf, wenn solch ein bedingter Sprung die letzte Komponente des Kontrollflussgraphen ist.

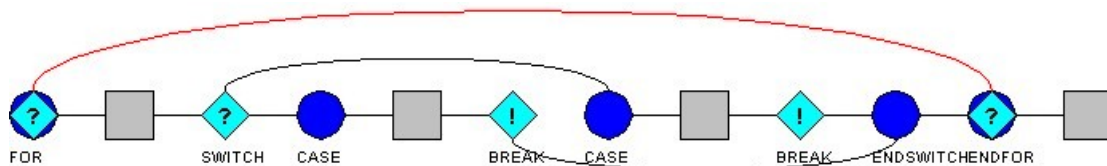
Ein Rücksprung im Kontrollflussgraphen ist immer als rote Linie dargestellt. Ein Rücksprung kann ein bedingter oder unbedingter Sprung zu einem Label sein, das im Code vor dem Sprungaufruf liegt, oder aber auch eine For- oder While-Schleife. Da der Beginn und das Ende einer Schleife sowohl als Sprungziel als auch als bedingter Sprung zu werten sind, ist das Zeichen für eine Schleife ein blauer Kreis, auf dem eine türkisfarbene Raute mit einem Fragezeichen liegt.

Hier ein Beispiel für eine While-Schleife, in deren Körper sich eine If-Abfrage befindet:



Die gelbe Raute, die mit „RET“ beschriftet ist, steht für eine Return-Anweisung in dem Programm.

Folgendes Beispiel zeigt eine For-Schleife, in deren Körper sich eine Switch-Anweisung befindet, deren zwei Fälle (Labels mit „CASE“ beschriftet) mit einem Break beendet werden.



8 Kiviatgraph

Der Kiviatgraph listet alle Metriken eines Typs (alle Klassenmetriken bzw. alle Modulmetriken) in einem Graphen auf. Der äußere Kreis des Graphen repräsentiert die obere Grenze der entsprechenden Metrik, der innere Kreis die untere Grenze der jeweiligen Metrik. Für jede Metrik werden die Kurzschreibweise und deren Wert dargestellt. Der Wert wird in Proportion zu den Grenzen der Metrik gesetzt und entsprechend in den Graphen eingezeichnet. Liegt eine Metrik außerhalb ihrer Grenzen, so werden die zugehörige Linie, deren Name und Wert rot in den Graphen gezeichnet.

Am Kiviatgraph erkennt man, ob die Metrik ihre Grenze über- oder unterschreitet. Anhand der Proportionen kann man schnell abschätzen, ob der Grenzwert weit über- oder unterschritten wird oder eben nur wenig.

