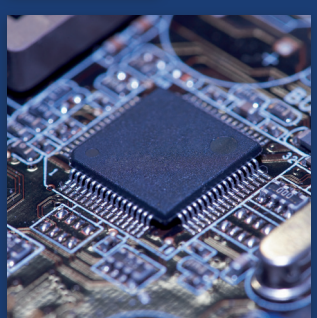
Verifysoft TECHNOLOGY

Softwaretest- & Analysetools für Produktivität und Qualität



- Statische Codeanalyse
- Dynamische Codeanalyse
- Software-Komplexitätsmessung
- Code Coverage

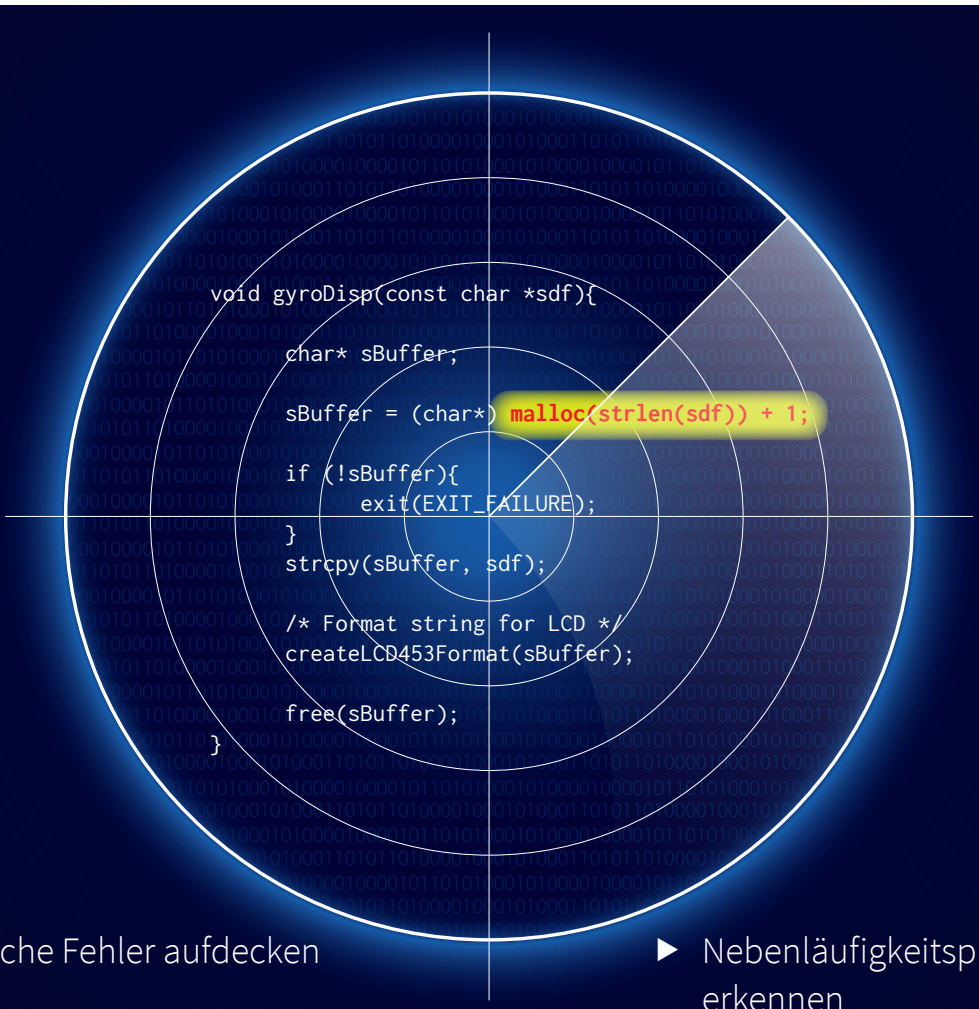
www.verifysoft.com

GrammaTech CodeSonar® – Wenn Softwarequalität zum Prinzip erhoben wird

Statische Analyse von Quell- und Binärcode

Da die statische Analyse eine Ausführung der zu analysierenden (Teil-) Applikation nicht erfordert, kann CodeSonar bereits früh im Entwicklungsprozess kritische Softwarefehler aufdecken.

Risiken, hervorgerufen durch z.B. gefährliche Sicherheitslücken, nichtdeterministische Nebenläufigkeitsfehler und Speicherlecks können so minimiert und hohe Wartungskosten, verursacht durch schwer lesbaren Code, vermieden werden.



- Kritische Fehler aufdecken
- Sicherheitsschwachstellen eliminieren
- Codierrichtlinien überprüfen
- Nebenläufigkeitsprobleme erkennen
- Reports zur Zertifizierung nach ISO 26262 / DO-178C generieren

Statische Quellcodeanalyse

Als führendes Werkzeug zur statischen Quellcodeanalyse weist CodeSonar im Vergleich zu vielen anderen statischen Analyse-Tools nicht nur eine bessere Fehlererkennung auf, es zeichnet sich zudem durch eine vergleichsweise geringe Rate an Fehlwarnungen (False Positives) aus

Statische Binäranalyse

Vielfach werden in Applikationen von Drittanbietern gelieferte Komponenten (Bibliotheken) eingebunden. Da diese oft nur als Binärdateien vorliegen, lassen sich Zweifel an deren Qualität nur schwer ausräumen und die Stabilität und Sicherheit der Gesamtapplikation steht in Frage. CodeSonar for Binaries geht mit seiner Analyse über den Quellcode hinaus und detektiert kritische Fehler auch in Binärdateien.

Hohe Anzahl von Prüfungen

CodeSonars große Anzahl von Checkern ermöglicht das Auffinden einer Vielzahl von kritischen Fehlern.

Sicherheitsprüfungen

Sicherheit von Applikationen spielt durch zunehmende Vernetzung eine immer wichtigere Rolle. CodeSonar führt umfangreiche Überprüfungen Ihrer Software im Hinblick auf Sicherheitsschwachstellen durch und hilft damit Angriffe abzuwehren.

Nebenläufigkeitsprüfungen

Nebenläufigkeitsprobleme wie Race Conditions und Synchronisationsfehler wie Deadlocks deckt CodeSonar durch Verwendung interner Laufzeitmodelle zuverlässig auf.

Floating Point Warnungsklassen

CodeSonars Analyse arbeitet auf Basis von Fließkommaarithmetik. Es ist damit Werkzeugen, die innerhalb einer Integer-Domäne arbeiten, in vielen Bereichen überlegen.

HINTERGRUNDWISSEN

Unterstützte Programmiersprachen

- C/C++
- Java
- C#

Unterstützte Betriebssysteme

- Windows
- Linux
- Solaris (SPARC)
- OS X
- NetBSD
- FreeBSD

Unterstützte Compiler

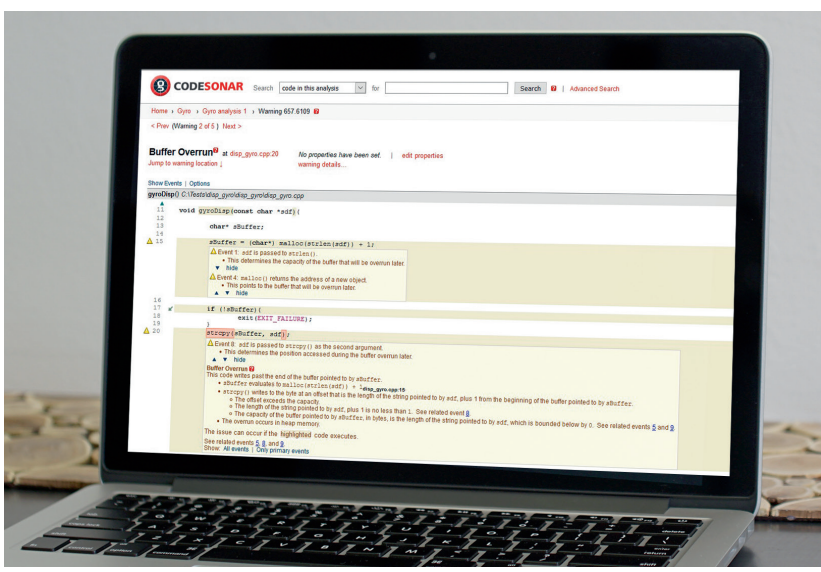
CodeSonar arbeitet mit nahezu allen aktuellen Compilern problemlos zusammen. Zur Verwendung mit werksseitig nicht unterstützten Typen und Derivaten ist eine Konfigurationsanpassung meist schnell und unkompliziert möglich.

- ARM RealView
- Intel C/C++
- CodeWarrior
- MacOS
- Free BSD
- Microsoft Visual Studio
- GCC
- G++
- Keil
- Renesas
- Green Hills
- Sun C/C++
- HI-TECH
- Texas Intruments CodeComposer
- IAR
- Wind River

… und viele mehr

Gut dokumentierte Ergebnisse

CodeSonar gibt seine Ergebnisse als Warnungen aus, die durch eine gute Dokumentation leicht verständlich sind.



INTEGRATION

Eclipse Integration
Ein mitgeliefertes Plug-in ermöglicht den Entwicklern sich die Analyseergebnisse direkt in Eclipse anzeigen zu lassen. Änderungen können so leicht an der ausgewiesenen Stelle im Code vorgenommen werden.

Microsoft Visual Studio Integration
Eine Integration in Microsoft Visual Studio erlaubt CodeSonar aus dem Visual Studio heraus zu starten und die Analyseergebnisse direkt im Visual Studio auszuwerten.

Continuous Integration
CodeSonar arbeitet problemlos mit Hudson und Jenkins zusammen. Zur komfortablen Anbindung an Jenkins ist zudem ein Plug-in verfügbar

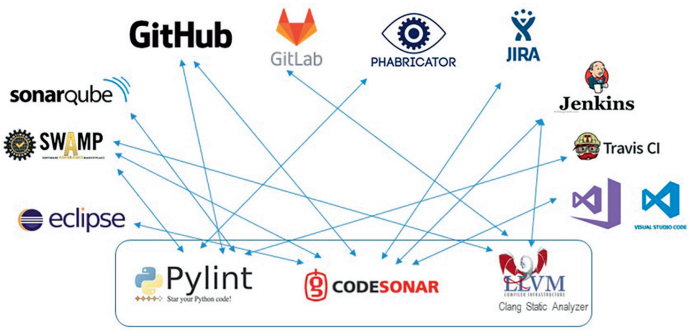
Anbindung an Bug-Tracking Tools
Mittels sogenannter „Warning Processors" können diverse Bug-Tracking Tools problemlos angebunden werden. Ein Python Beispiel-Script zur Bugzilla Integration wird mitgeliefert. Es kann leicht an andere Systeme angepasst werden. Für JIRA ist ein Plug-in erhältlich.

Integration von JULIA

Mit der optionalen Integration des JULIA Static Analyzers sind weitreichende Analysen von Java und .NET Applikationen möglich.

SARIF Importer Plug-in

SARIF (Static Analysis Results Interchange Format) ist ein neuer offener Standard der OASIS (Organization for the Advancement of Structured Information Standards). CodeSonars SARIF Importer Plug-in ermöglicht den Import von SARIF-Dateien.



Performance

CodeSonars Checker sind im Hinblick auf hohe Performance optimiert. CodeSonar skaliert gut auf Multicore- und Mehrprozessormaschinen und erlaubt zudem die Verteilung von Analysen auf mehrere Maschinen. So können schnelle Analyseergebnisse auch großer Projekte von mehreren Millionen Codezeilen ermöglicht werden.

Inkrementelle Analyse

CodeSonars Fähigkeit bei Projektaktualisierungen lediglich die Änderungen unter Berücksichtigung bereits bestehenden Analysedaten zu bearbeiten, ermöglicht die Analysezeiten deutlich zu reduzieren.

Überprüfung auf Einhaltung von Coding Standards

CodeSonar überprüft Applikationen auf die Einhaltung von Coding Standards. Folgende Regelwerke werden unterstützt:

- MISRA C 2012
- MISRA C++ 2008
- Power Of Ten
- JPL
- SEI CERT

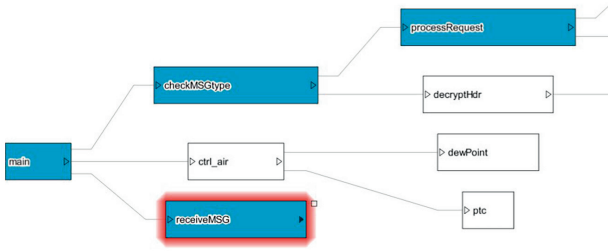
Die Implementierung eigener Regeln ist möglich.

Architekturvisualisierung

CodeSonars Fähigkeit auch komplexen Quellcode hoher Verschachtelungstiefe grafisch als Diagramm aufbereitet darzustellen, erleichtert das Verständnis von Applikationen.

Taint Data Tracking

CodeSonars Taint Data Tracking Analysefunktion identifiziert Sicherheitsschwachstellen, die eine eventuelle Einspeisung von Schadcode in die Applikation ermöglichen und weist die davon direkt oder indirekt betroffenen Abschnitte sowohl farblich markiert im Quellcode als auch in einer graphischen Repräsentation im Diagramm aus. Präventivmaßnahmen sind so einfach zu treffen.



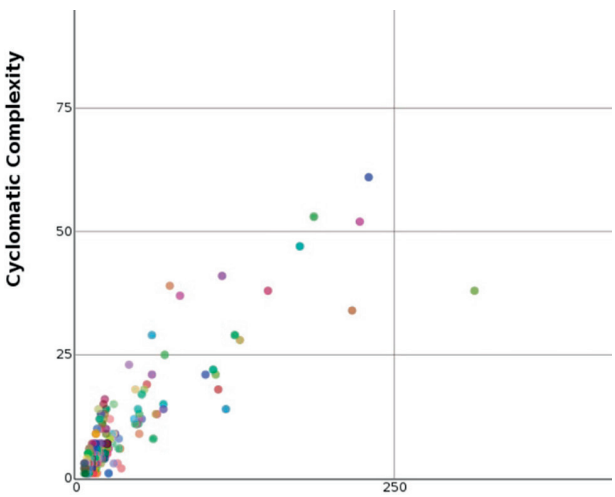
Erhebung von Metriken

Zur Beurteilung der Wartungsfreundlichkeit von Quellcode berechnet CodeSonar eine Vielzahl verschiedener Metriken wie z.B.

- Modifizierte zyklomatische Komplexität
- Zyklomatische Komplexität
- Halstead Metriken
- Watson und McCabe

...und viele mehr.

Auch die Erhebung eigener, zusätzlicher Metriken lässt sich Implementieren bzw. durch Aggregation bestehender Metriken mittels Konfiguration realisieren.



Plug-in API

Zur Implementierung eigener Checker stehen gut dokumentierte APIs der Sprachen C, C++, Python, Scheme, C# und Java zur Verfügung

HINTERGRUNDWISSEN

Zertifizierung

CodeSonar wurde von der SGS TÜV Saar GmbH zertifiziert als ein geeignetes Werkzeug zur Erlangung von Zertifizierungen nach:

- ISO 26262
- DO 178-C
- IEC 61508
- IEC 62304
- EN 50128

Qualifizierung

Im Hinblick auf eine Zertifizierung Ihrer Applikationen ist, abhängig vom Ergebnis der Klassifizierung, in den meisten Fällen eine Qualifizierung von CodeSonar als Teil der eingesetzten Toolchain nötig.

Hierfür ist ein Qualification Kit verfügbar, das die erforderlichen Reports generiert. Das CodeSonar Qualification Kit unterstützt Sie bei Qualifizierungen nach:

- ISO 26262
- DO 178-C
- IEC 61508

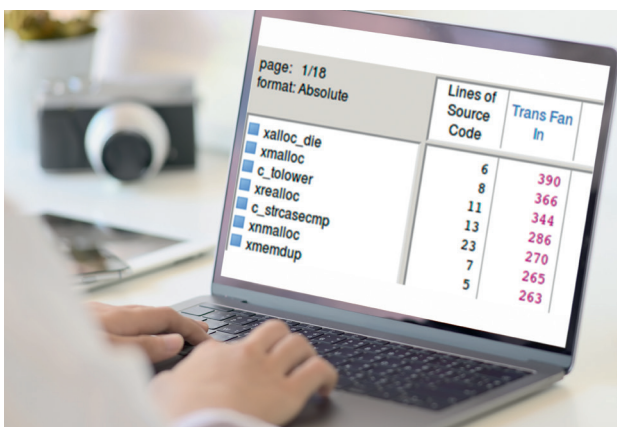
Für sicherheitskritische Anwendungen ist eine tiefgehende statische Analyse unverzichtbar.

Imagix 4D – Das Werkzeug für alle Fälle

Werkzeug zur Visualisierung und Überprüfung von C, C++ und Java Projekten

Imagix 4D ist ein Werkzeug, um komplexen, in C, C++ und Java geschriebenen Third-Party- und Legacy Source Code zu verstehen, zu dokumentieren und zu verbessern. Imagix 4D automatisiert die Analyse des Kontrollflusses und der Abhängigkeiten. Das Werkzeug deckt Probleme in der Datennutzung und bei Task-Interaktionen auf.
Mit Imagix 4D steigern Sie Ihre Produktivität und Qualität und reduzieren Risiken.

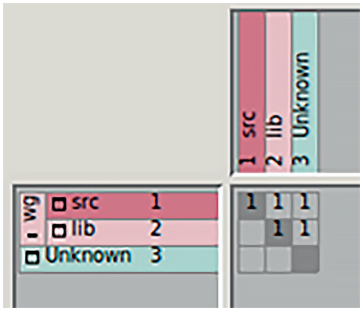
Finden Sie Brennpunkte und verbessern Sie die Qualität

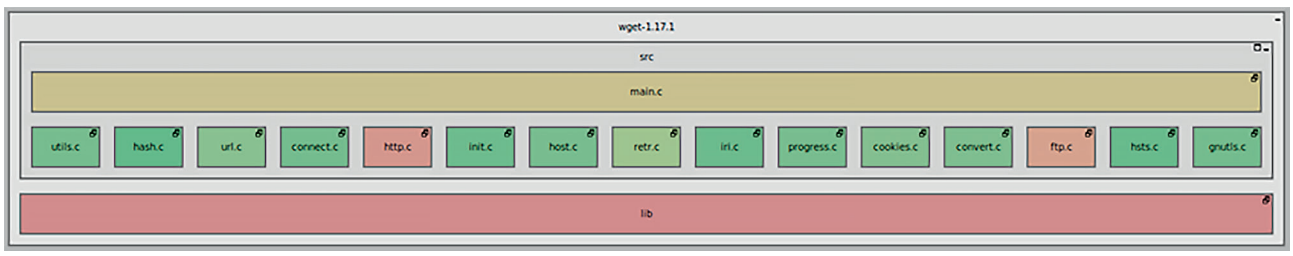


- Automatische Checker finden Anomalien im Quellcode
- Die Erhebung diverser Metriken (z.B. zyklomatische Komplexität, Decision Density u.v.m.) lässt Sie kritische Komponenten schnell identifizieren
- Teilautomatisierte Reviews ermöglichen eine effiziente Durchführung qualitativer Analysen nach CWE oder nach eigenen Vorgaben

Behalten Sie die Kontrolle auch bei umfangreichen Projekten

- Aussagekräftige Diagramme ermöglichen Sichten von einer globalen Perspektive bis zu den granularen Eigenschaften einzelner Datentypen
- Δ-Analysen erlauben eine detaillierte Nachverfolgung von Änderungen zwischen Revisionen
- Anhand von Architekturdiagrammen ist eine effiziente Prüfung der bestehenden Architektur auf strukturelle Anforderungen problemlos möglich





Wie ein Schweizer Taschenmesser

Imagix 4D beinhaltet eine Fülle von nützlichen Werkzeugen zur Beurteilung von Quellcode: Architekturdiagramme, Berichte, Δ-Analyse, Profiler-Integration, Testabdeckungsintegration für Testwell CTC++, Function Call-Diagramme, Include-Hierarchie-Diagramme, Fehlersuche, Vererbungsdiagramme, Klassen-Aufrufs-Graphen, Datentyp-Hierarchie-Graphen, UML-Task-Diagramme, Reviews, Refactoring, Datei-Aufrufs-Graphen, Flussdiagramme, CWE, Kontrollflussdiagramme, Variablen-Metriken, Funktions-Metriken, Klassen-Metriken, Datei-Metriken, Verzeichnis-Metriken, Architektur-Metriken, Design-Struktur-Matrizen, Diff-Tool, Datei-Editor, Calculation-Trees, Datenbankabfragen, Dokumentgenerator, , Diagrammexport, statische Quellcodeanalyse, UML-Datei-Diagramme, UML-Klassen-Diagramme, Symbol-Listen und Filter-Funktionen, Grep-basierte Dateisuche, Nebenläufigkeitsanalyse, Include-Analyse, Function- und Call-Coverage-Berichte, kundenspezifische Diagramme des vorliegenden Quellcodes geben stets den tatsächlichen Ist-Stand des Projektes wieder. Der Aufwand einer manuellen Erstellung entfällt.

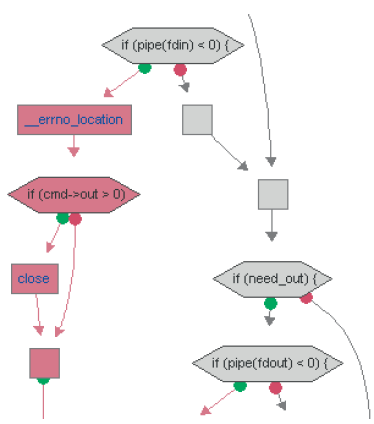
Verbessern Sie den Entwicklungsprozess

Datenbankabfragen beschleunigen das Auffinden von Informationen zu spezifischen Symbolen

- Unbekannter Quellcode kann mit Imagix 4D leicht verstanden und bewertet werden
- Die automatisch generierten Dokumente auf Basis des vorliegenden Quellcodes geben stets den tatsächlichen Ist-Stand des Projektes wieder. Der Aufwand einer manuellen Erstellung entfällt.

Profitieren Sie von der Testwell CTC++ Integration

- Visualisierung der Testabdeckung im Kontrollflussdiagramm
- Zusammenhänge zwischen Tests und Testabdeckung werden verständlicher, was die Entwicklung passender Testfälle beschleunigt
- Function- und Call-Coverage-Berichte ergänzen das Portfolio von Testwell CTC++



Verbessern Sie Ihre Produktivität und evaluieren Sie Imagix 4D jetzt!

Testwell CTC++
Test Coverage Analyser

Testabdeckung für alle Coverage-Stufen, alle Compiler, alle Embedded Targets

Testwell CTC++ ist ein leistungsfähiges und einfach zu benutzendes Code-/Test-Coverage Tool, welches alle Teile Ihres Quelltextes zeigt, die bereits ausgeführt/getestet wurden.
Testwell CTC++ unterstützt alle Coverage-Stufen und kann auch in sicherheitskritischen Projekten eingesetzt werden.

Einfache Nutzung

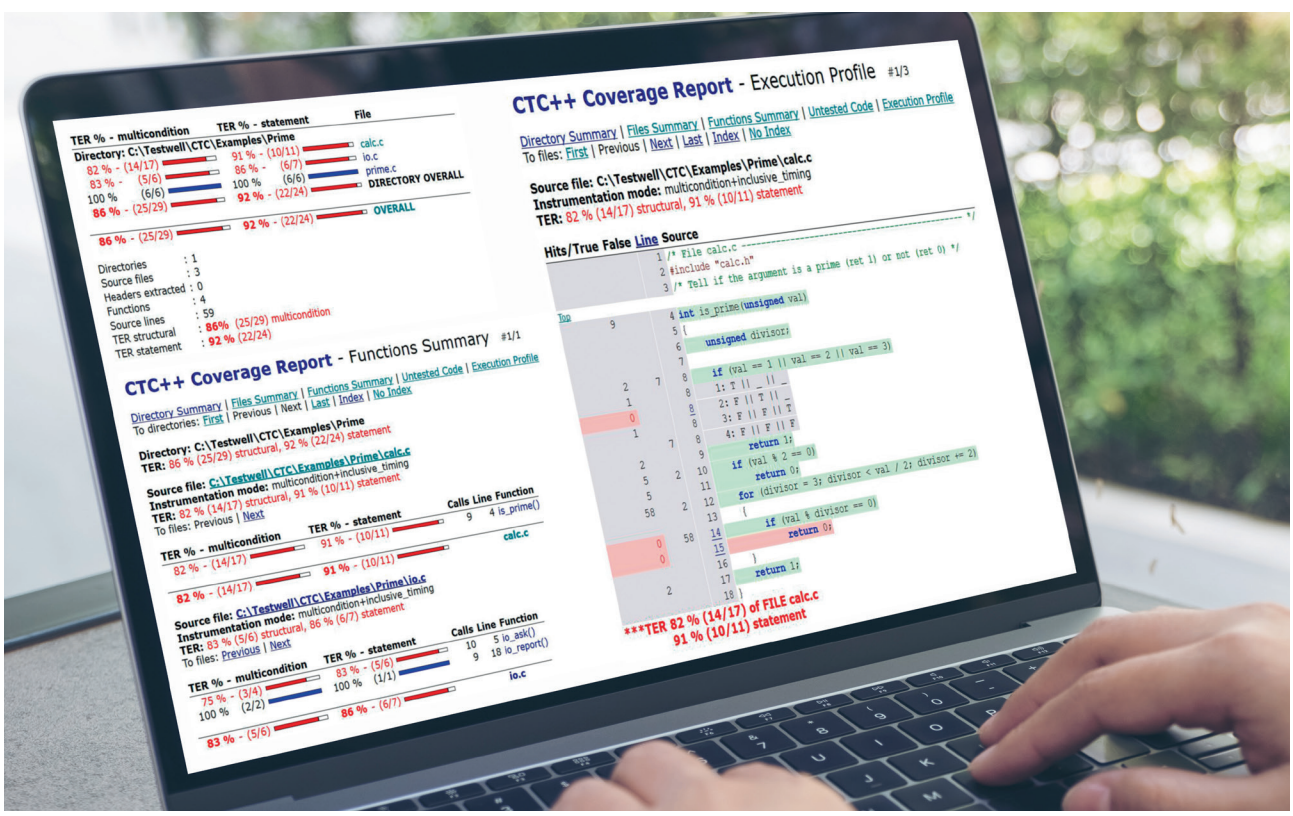
- Keine Modifikationen an existierendem Code
- Unterstützung bereits existierender Makefiles
- Sehr schnell in der Ausführung
- Nahtlose Integration in viele IDEs
- Unterstützung von C und C++

Add-ons für Testwell CTC++

- Unterstützung von Java/Android
- Unterstützung von C#

Die Testabdeckung in aussagekräftigen, klaren Berichten

- HTML-Bericht für die Anwender
- Diverse Formate zur automatisierten Weiterverarbeitung (XML, JSON etc.)



Testwell CTC ++
Test Coverage Analyser

Code Coverage für alle Coverage-Stufen

- Statement Coverage
- Function Coverage
- Decision Coverage/Branch Coverage
- Condition Coverage
- Modified Condition/Decision Coverage (MC/DC)
- Multicondition Coverage (MCC)

Testwell CTC++ ist das ideale Tool, um die Testüberdeckung Ihrer Embedded Targets und Microcontroller zu analysieren. Es kann sowohl auf Hosts, wie auch direkt auf Ihren Targets eingesetzt werden.

- Sehr kleiner Instrumentation-Overhead
- Analysiert die Testüberdeckung in allen Targets
- Arbeitet auch mit kleinsten Targets
- Arbeitet mit jedem Compiler/Cross-Compiler

Code Coverage mit Testwell CTC++

- Erfüllen Sie die Anforderungen von Normen
- Formulieren Sie bessere Testfälle
- Vermeiden Sie redundante Testfälle
- Weisen Sie die Test-Coverage gegenüber Ihren Kunden nach
- Decken Sie Dead-Code auf
- Fordern Sie von Lieferanten den Nachweis der Testabdeckung
- Finden Sie Bottlenecks durch das Untersuchen des Laufzeitverhaltens

Qualification-Kit

Vereinfachen Sie die Zertifizierung Ihrer Projekte mit dem Qualification-Kit für Testwell CTC++. Folgende Normen werden durch Testwell CTC++ unterstützt:

- **DO-178C / ED-12C**
  Software Considerations in Airborne Systems and Equipment Certification
- **IEC 61508**
  Functional Safety of Electrical/Electronic Programmable Electronic Safety-related Systems
- **EN 50128**
  Railway applications - Communication, signalling and processing systems
- **ISO 26262**
  Road vehicles - Functional safety
- **IEC 60880**
  Nuclear Power

Alle Testwell-Tools sind verfügbar für:
Windows, Linux, MacOS, Solaris, HP-UX und AIX

Qualification-Kit für die Normen:
DO-178C - IEC 61508 - EN50128 - ISO 26262

Testwell CMT++ und Testwell CMTJava

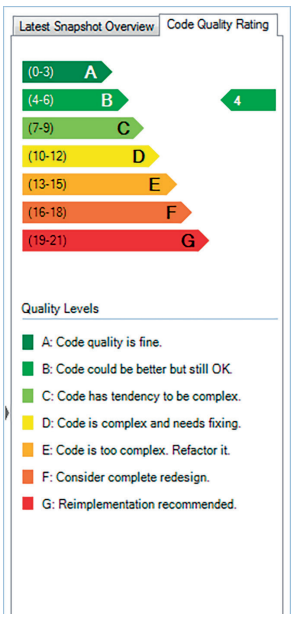
Softwarekomplexitätsanalyse für die Sprachen C, C++, C# und Java

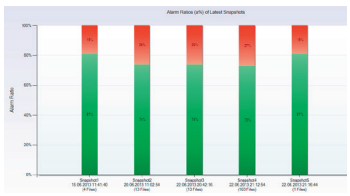
Testwell CMT++ und Testwell CMTJava sind Tools zur Softwarekomplexitätsanalyse von C, C++, C# und Java Quellcode. Beide Tools analysieren Ihren Quellcode und geben Ihnen sofortige Rückmeldung über Ihre innere Softwarequalität, auch bei größeren Softwareprojekten. Durch eine gute Struktur der Software, wird Software-Erosion vermieden. Die Code-Qualität, Wartbarkeit und Testbarkeit wird deutlich verbessert.

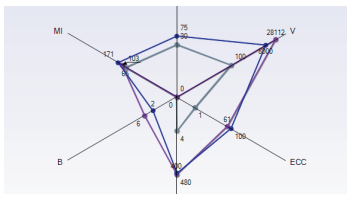
Software-Komplexitätsanalyse

- McCabe Cyclomatic Complexity
- Alle Lines-of-Code Metriken
- Alle Wartbarkeitsindizes (Maintainability Indexes)
- Alle Halstead Metriken

Die Komplexität Ihres Quellcodes hat direkten Einfluss auf die Robustheit und Fehleranfälligkeit Ihrer Software. Komplexer Quellcode ist schwierig zu testen und die Wartung von komplexem Quellcode ist schwierig und kostenintensiv.







Grafisches Add-on für Testwell CMT++

Verybench for CMT++ ist ein grafisches Frontend für Testwell CMT++. Es ermöglicht Ihnen, Ihren Quellcode grafisch in einem standardisierten User-Interface zu analysieren, zu bewerten und zu dokumentieren.

- **Alarme für Metriken**
  Verybench zeigt alle Alarme, die in Testwell CMT++ für Metriken definiert wurden und zeigt wenn Metriken außerhalb der empfohlenen Werte liegen.
- **Snapshots**
  Um die Qualität Ihres Quellcodes über die Zeit erfassen zu können, fertigt Verybench Snapshots aller berechneten Metrikwerte für jede Komplexitätsanalyse an
- **Quality-Baseline**
  Alle über die Zeit entstandenen Snapshots bilden eine Quality-Baseline und fördern Ihr Verständnis für den Komplexitätszuwachs/-rückgang Ihrer Code Base.
- **Code-Quality-Rating**
  Verybench bewertet Ihren Quellcode nach jeder Komplexitätsanalyse für eine sofortige Qualitätseinschätzung Ihres Quellcodes.
- **Reports**
  Verybench unterstützt Sie bei der Dokumentation Ihrer Qualitätsanalyse durch PDF-, HTML-, XML-, CSV- und Text-Reports.

Unsere Referenzen

Über 600 Kunden auf allen Kontinenten

Unsere Test- und Analysetools sind erfolgreich bei über 600 Kunden auf allen Kontinenten im Einsatz. Neben Großunternehmen setzen zahlreiche kleinere und mittelständische Entwicklungsfirmen unsere Software für Test und Qualitätssicherung ein.




ABB
COMARCH
HITACHI
NXP
ST
AKKA
Continental
Honeywell
PHILIPS
AMG
DAIMLER
iav
Texas Instruments
AOA
DGA
Infineon
PORSCHE
THALES
AIRBUS DEFENCE & SPACE
dSPACE
Raytheon
AIRBUS HELICOPTERS
EATON
intel
RENESAS
TOMTOM
EMBRAER
jenaoptronik
SAFRAN
VIESMANN
arianeGROUP
esa
KNORR-BREMSE
Sagem
ATTENSITY
LIEBHERR
VORWERK
ESO
SAMSUNG
Audi
LUK
Schindler
framatome
MAGNETI MARELLI
Schneider Electric
Westinghouse
MAQUET
SICK
ZEISS
Giesecke & Devrient
MBtech
SIEMENS
BOMBARDIER
gemalto
Mentor Graphics
Sopra group
ZF
Bundesamt für Sicherheit in der Informationstechnik
HELLA
SPIE
ZODIAC AEROSPACE
BOSCH

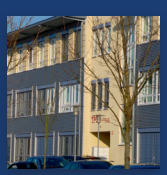
Verifysoft
TECHNOLOGY

Die Verifysoft Technology GmbH ist auf Entwicklung, Vertrieb und Support von Softwaretest- und Analysetools spezialisiert. Neben den eigenen Testwell-Tools vertreiben wir auch komplementäre Werkzeuge unserer Partner.

Verifysoft Technology GmbH wurde im Jahr 2003 von einer Gruppe privater Investoren und Softwarespezialisten im Technologiepark Offenburg (Baden-Württemberg) gegründet.

Mit einem internationalen Team betreuen wir mehrere hundert Kunden weltweit. Unsere Entwicklungs- und Supportmitarbeiter haben langjährige Erfahrung im Testtool-Bereich.

Finden Sie Softwaredefekte und -probleme vor dem Release und garantieren Sie höchste Softwarequalität mit Tools von Verifysoft Technology.



Verifysoft Technology bietet Seminare zu Themen der Entwicklung und dem Test von Software an.

Aktuelles Seminarprogramm unter:
www.verifysoft.com/de_events.html

Weitere Informationen und weitere Tools finden Sie unter:
www.verifysoft.com

Evaluieren Sie unsere Tools – Jetzt!

Ausgabe: Januar 2019 Fotos: www.fotolia.de, www.aeroweb-fr.net, www.heinzalbers.org, www.mev.de, NASA, Verifysoft Technology GmbH

Technologiepark, In der Spöck 10-12 | 77656 Offenburg (Deutschland)
Tel. +49 781 127 8118 - 0 | quality@verifysoft.com | www.verifysoft.com