Einführung

Prof. Sven Apel

Universität des Saarlandes



Teil I

Warum Software Engineering?

Warum Software Engineering?

Naive Sicht:

Implementierung

Problemspezifikation



Finales Programm

Aber:

Woher kommt die *Spezifikation*?

Wie korrespondiert die Spezifikation zu den Nutzeranforderungen?

Wie entscheidet man, wie das Programm strukturiert wird?

Wie weiß man, dass das Programm tatsächlich der Spezifikation entspricht?

Wie weiß man, dass das Programm immer korrekt arbeitet?

Was macht man, wenn die Nutzeranforderungen sich ändern?

Wie teilt man Aufgaben auf, falls man mehr als ein 1-Personen-Team hat?

Softwarekrise

Begriff während der NATO Software Engineering Konferenz 1968 geprägt:

"[The major cause of the software crisis is] that the machines have become several orders of magnitude more powerful! To put it quite bluntly: as long as there were no machines, programming was no problem at all; when we had a few weak computers, programming became a mild problem, and now we have gigantic computers, programming has become an equally gigantic problem."

– Edsger Dijkstra, 1972

- > Kosten für Software überstiegen Kosten für Hardware
- → Nur 34% der Softwareprojekte erfolgreich abgeschlossen

Ariane 5

Ariane 5 Flight 501: 4.6.1996

Selbstzerstörung nach 39 Sekunden

~ \$ 500 Million Schaden



However, problems began to occur when the

software attempted to *stuff this 64-bit variable*, which can represent billions of potential values,

Therac-25

Medizinische Strahlentherapie

Durch Softwarefehler zu hohe Strahlendosis, 3 Tote

Ein einziger Entwickler schrieb Software und benutzte vorhandene Komponenten

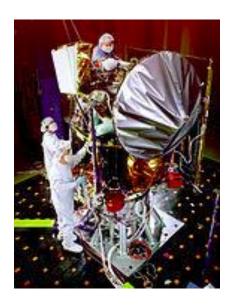


Mars Climate Orbiter

Verloren 1999 beim Anflug auf den Mars

~ \$ 330 Millionen Schaden

Grund: Einheitenfehler im Navi (metrische Einheiten vs. imperiale Einheiten)



Zwischenfall mit Patriot-Rakete

Fehler im Zielsuchsystem führte zum Verfehlen der abzufangenden Rakete und somit zum Tod von 28 Menschen während des Golfkriegs 1991

Grund: Fehlerhafte Zeitberechnung durch ungenaue arithmetische Berechnungen (Kommastellen wurden bei 24 Bit abgeschnitten, was zu Ungenauigkeiten führte)



AT&T Netzwerkausfall

AT&T-Telefonnetzwerk kollabierte am 15.1.1990

11 h Ausfall, ~ \$ 60 Millionen Schaden

"The fault was in the code" of the new software that AT&T loaded into front-end processors of all 114 of its 4ESS switching systems in mid-December, said Larry Seese, AT&T's director of technology development.



Los Angeles Flugkontrolle

Flugkontrolle in LAX stürzte am 30.4.2014 ab

10 gestrichene und 500 verspätete Flüge

Grund: US-Spionageflugzeug verwirrte Software



2003 Northeast Blackout

Über 2 Tage Stromausfall in USA/Kanada

~ 10 Opfer, 45 Millionen Menschen betroffen

Software-Fehler verhinderte lokalen Alarm, so dass sich das Problem ausbreitete

Toyota Motosteuerung

Verursacht "unerwünschte Beschleunigung"

89 Tote zwischen 2001 und 2010



Boeing 737 Max





Absturz Lion Air (189 Tote)

Jo Atlee @ ESEC/FSE'19 https://vimeo.com/356373889/dcb19424f9

Absturz Ethiopian Airlines (157 Tote)



The angle of attack sensor, at bottom center, is seen on a 737 Max aircraft at the Boeing factory in Renton, Washington, U.S., March 27, 2019. REUTERS/Lindsey Wasson

"The anti-stall system [...] has been pinpointed by investigators as a possible cause in a fatal Lion Air crash in Indonesia and the one in Ethiopia."

Software Fail Watch (5th Edition)

606 erfasste Softwarefehler im Jahr 2017

Betroffen

3.7 Milliarden Menschen

\$1.7 Billiarden Kosten

314 Unternehmen



LOSSES FROM SOFTWARE FAILURES (USD)

1,715,430,778,504

Warum scheitern Softwareprojekte?

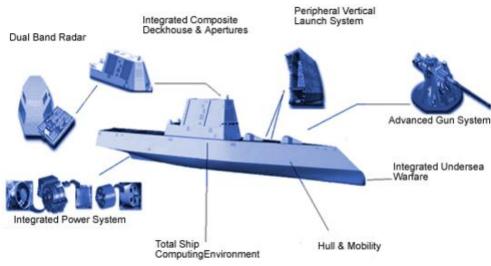
Extreme Komplexität

Beispiel: DDX Zumwalt (US Navy)

Viele, vernetzte eingebettete Systeme

Zusammen 30.000.000.000 Zeilen Code (Schätzung)

in 142 Programmiersprachen



Variabilität





SOLITE_OMIT_LOOKASIDE

Exclusive Locking

Case Sensitivity

Thread Safety

Atomic Write

Konfigurationen:

1.1 Options To Set Default Param	
SQLITE_DEFAULT_AUTOMATIC_INDEX=<0 or	
This macro determines the initial setting for $\underline{\text{PF}}$ SQLite.	
See also: SQLITE OMIT AUTOMATIC INDEX	
SQLITE_DEFAULT_AUTOVACU	SOLITE MAX SO
This macro determines if SQI command.	Whenever the any real work
SQLITE_DEFAULT_CACHE_SIZ	SQLITE_POWERS
This macro sets the default s	This option ch
SQLITE_DEFAULT_FILE_FORM	YYSTACKDEPTH:
The default schema format n	This macro se
All versions of SQLite since 3 schema format was set to 1 f	1.2 Options
The schema format number f	There are compile
SQLITE_DEFAULT_FILE_PERM	The compile-time
The default numeric file perm	 SQLITE MAX SQLITE MAX
SQLITE_DEFAULT_FOREIGN_K	
This macro determines wheth is normally off by default, bu	SQLITE MAX SQLITE MAX
SQLITE_DEFAULT_MMAP_SIZE	 SQLITE MAX SQLITE MAX SQLITE MAX
This macro sets the default li sqlite3 config(SQLITE CONF	
SQLITE_DEFAULT_JOURNAL_S	SQLITE_4_BYTE
This option sets the size limit	On most syste
be changed at run-time using	SQLITE_CASE_S
SQLITE_DEFAULT_LOCKING_M	II tills option
If set to 1, then the default lo	DQLITE_DIRECT
SQLITE_DEFAULT_MEMSTATUS	When this opt

This macro is used to deter

This macro is used to set the

SOLITE DEFAULT PAGE SIZE

Use memory by default but allow the <u>PRAGMA ten</u> neter Values The default setting is 1. Additional information can be found in tempfiles.html RAGMA automatic SQLITE_TRACE_SIZE_LIMIT=N SQLITE_USE_URI This option causes the UR CHEMA RETRY=N 1.4 Options To Enab e database schema cl k done. This paramete SQLITE_ALLOW_URI_AUTHO SAFE OVERWRITE: URI filenames normally th hanges the default as Some future versions of SI power loss. With SOL SOLITE ALLOW COVERING =<max_depth> applications to break. Henc ets the maximum dep ctoring their SQL as it SOLITE ENABLE 8 3 NAME To Set Size Li default but may be disable e-time options that wil SQLITE_ENABLE_ATOMIC_W options for setting up If this C-preprocessor mad filesystems that support at ATTACHED SOLITE_ENABLE_COLUMN_M EXPR DEPTH LENGTH LIKE PATTERN LEN sqlite3_column_datab sqlite3_column_table sqlite3_column_origin To Control Op SOLITE ENABLE FTS3 ALIGNED MALLOC When this option is defined SQLITE_ENABLE_FTS3_PARE ems, the malloc() sys

ENSITIVE LIKE is present, then the b

OVERFLOW READ

tion is present, conte

SOLITE HAVE ISNAN

If this option is present, then SOLit

SOLITE OS OTHER=<0 or 1>

The option causes SQLite to omit it

SOLITE ENABLE STAT2

This option used to cause the ANALYZE cor SOLITE_ENABLE_STAT3

his option controls whether temporary files are stored on disk or in memory.

SQLITE_ENABLE_TREE_EXPLAIN

This whole mechanism is highly experimental

If this option is defined, then it must also be

This option modifies the qu

SOLITE ENABLE FTS4

SQLITE_TEMP_STORE=<0 through 3>

SOLITE DISABLE FTS3 UNICODE

SOLITE DISABLE FTS4 DEFERRED

If this C-preprocessor macro disables the "de

When this option is define SOLITE_ENABLE_ICU -DSQLITE_OMIT_ALTERTABLE -DSQLITE_OMIT_ALTERTABLE=1

This option causes the Int -DSOLITE OMIT ALTERTABLE=0 SOLITE ENABLE TOTRACE If any of these options are defined, then the same When both the SQLite core

SQLITE_ENABLE_LOCKING_ Special versions of the SQLite amalgamation that of This option enables addition

SOLITE_OMIT_AUTOINCREMENT

If this option is defined, then foreig

This option adds additional logic to the ANAL

QLITE_OMIT_AUTOVACUUM This option adds support for the SQLITE_TEST

SQLITE_ENABLE_UPDATE_DELETE_LIMIT This option enables an optional ORDER BY an

SQLITE_ENABLE_UNLOCK_NOTIFY OLITE_OMIT_BUILTIN_TEST This option enables the sqlite3_unlock_notif-

SOLITE SOUNDEX SOLITE OMIT CAST This option enables the soundex() SQL funct

SOLITE OMIT CHECK YYTRACKMAXSTACKDEPTH

This option causes the LALR(1) parser stack d SOLITE OMIT COMPILEOPTION DI 1.5 Options To Disable Feature SOLITE OMIT COMPLETE

SQLITE_DISABLE_LFS If this C-preprocessor macro is defined, large SOLITE OMIT COMPOUND SELECT This option is used to omit the com SQLITE_DISABLE_DIRSYNC

As INCEST statement with multiple If this C-preprocessor macro is defined, dir OLITE OMIT DATETIME FUNCS If this notion is defined, SOLIte's b OLITE OMIT DECLTYPE

QLITE_OMIT_DEPRECATED

QLITE_OMIT_DISKIO 1.6 Options To Omit Features

The following options can be used to reduce the six OLITE OMIT EXPLAIN employing any of these compile-time options. You

OLITE_OMIT_FLOATING_POINT

Important Note: The SOLITE_OMIT_* optio

SOLITE OMIT OR OPTIMIZATION

SQLITE_OMIT_PAGER_PRAGMAS

This option omits the lookaside memory allocato

This option is used to omit the PRAGMA command from the

SQLITE_OMIT_PROGRESS_CALLBACK This option may be defined to omit the capability to issue "

SOLITE OMIT OUICKBALANCE

SOLITE OMIT TCL VARIABLE

SOLITE OMIT TEMPOR

Defining this antion amits support for TRIGGER objects. Neith SOLITE_OMIT_TRUNCATE_OPTIMIZATION

This macro is used to omit support for UTF16 text encoding SQLITE_OMIT_VACUUM

When this option is defined, the VACIJUM command is not inc

This option omits support for the Virtual Table mechanism in

. "WAL") capat

<u>llocator</u> and the nst a system libr

260,532,200,783,961,400,000,000,000,000,000,000,000, 000,000,000,000,000,000,000,000,000,000,000,000

> The value of SOLITE THREADSAFE When SOLite has been compiled wit

> > SQLITE CONFIG SINGLETHREAD

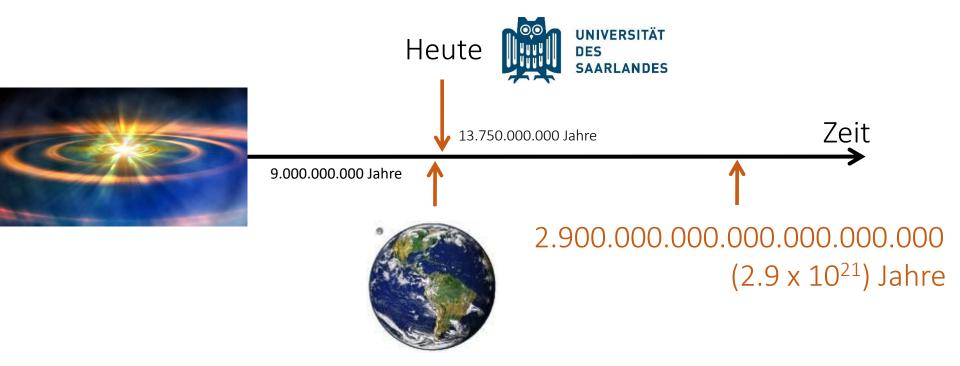
SQLITE CONFIG MULTITHREAD
 SQLITE CONFIG SERIALIZED

SOLITE OMIT AUTHORIZATION Defining this option omits the authorization callback feature from the library. Th

SQLITE_DEBUG also turns on some other debugging features. SQLITE_MEMDEBUG

The SOLITE_MEMDEBUG option causes an instrumented debu









Linux-Kernel

~ 6.000.000 Zeilen Quelltext

Weitgehend konfigurierbar

> 10.000 Konfigurationsoptionen! (x86, 64bit, ...)

Fast aller Quelltext ist "optional"





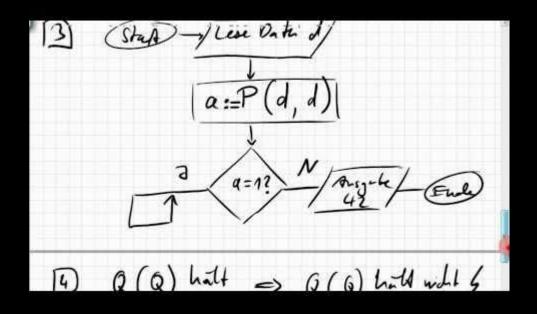




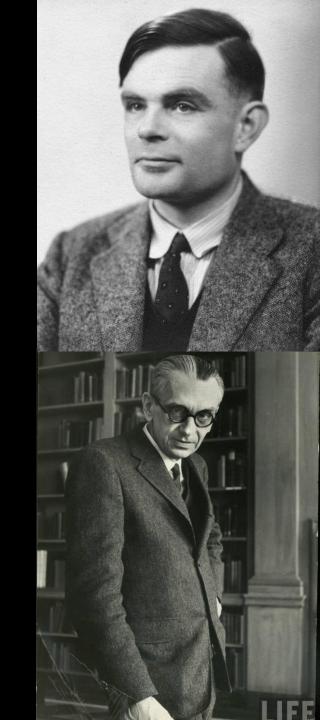








Unentscheidbarkeit + Unstetigkeit



Teil II

Was ist Software Engineering?

Begriff: Software Engineering

SOFTWARE ENGINEERING

Report on a conference sponsored by the

NATO SCIENCE COMMITTEE

Garmisch, Germany, 7th to 11th October 1968

Chairman: Professor Dr. F. L. Bauer

Co-chairmen: Professor L. Bolliet, Dr. H. J. Helms

Editors: Peter Naur and Brian Randell

January 1969

Definition (1)

"state of the art of developing quality software on time and within budget "

Aktuellster Stand der Technik:

Entscheidet Community

Lebenslanges Lernen

Ressourcenbeschränkung

Definition (2)

"multi-person construction of multi-version software "

Teamwork!

Erfolgreiche Softwaresysteme müssen sich weiterentwickeln

Änderung ist der Normalfall, nicht die Ausnahme

Definition (3)

"software engineering is an *engineering* discipline that is concerned with *all aspects* of software production"

Software ist ein *Produkt*, das für einen bestimmtem Kunden entwickelt wird

Nicht nur Programmierung, sondern *alle Aspekte des Softwarelebenszyklus*

Software Engineering vs. Informatik

Informatik beschäftigt sich mit der Theorie und den Grundlagen von Computersystemen

Software Engineering beschäftigt sich mit theoretischen und praktischen Themen der Entwicklung und Wartung "guter" Software

Was ist "gute" Software?

Maintainable (Wartbar)

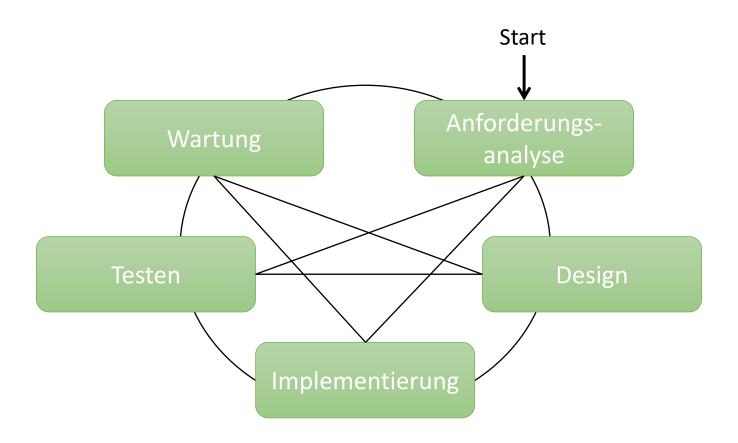
Dependable (Verfügbar, Zuverlässig)

Efficient (Effizient)

Usable (Nutzbar, Anwendbar)

Secure, Safe (Sicher)

Phasen Softwarelebenszyklus



Programmierung ist nur ein kleiner Teil von Softwareentwicklung!

Abgrenzung: Ingenieursdisziplin

Software hat praktisch *keine physischen* Eigenschaften

Keine zugrundeliegende physikalische Theorie

Kein Verfall, trotzdem existiert nach 10 Jahren typischerweise keine einzige Zeile des ursprünglichen Quellcodes mehr

Software kann (fast) beliebig komplex werden