Fehler gefunden – Auslöser für größere Fehler

Karol Frühauf
INFOGEM AG, 5400 Baden
Karol.Fruehauf@infogem.ch

Inhalt

- Einleitung
- 9 Gesichtspunkte: An- und Einsichten zu Fehlern
- Schlussbemerkungen

Warum habe ich dieses Thema gewählt?

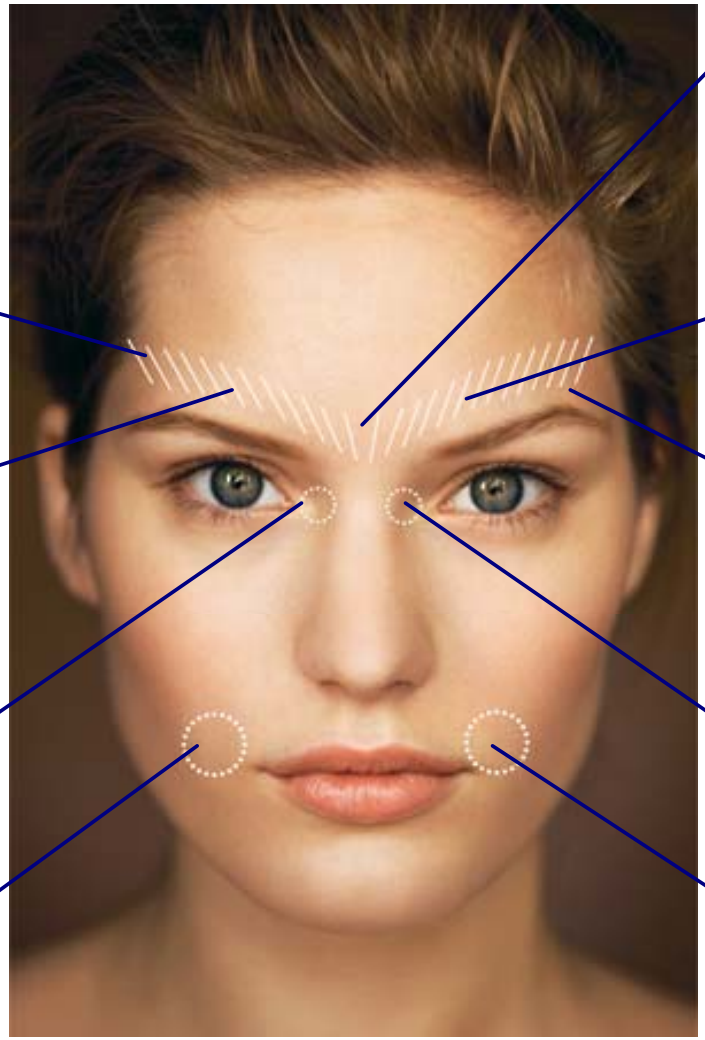
Es gibt 760 Gründe, warum ein Flugkontrollsystem gehackt werden kann

Ein kürzlich in den USA durchgeführtes Audit fand mehr als 760 Schwachstellen mit hohem Risiko in Web-Anwendungen, welche die Flugkontrolle unterstützen. Sie eröffnen den Angreifern eine Möglichkeit, nicht nur auf den Web-Server zuzugreifen, sondern potentiell auch auf die anderen, kritischeren Backend-Systeme.

Software Engineering Notes, Vol. 34, No. 4, pp. 17 (Risk to the Public)

↳ *ich bin ein Sicherheitsbanause,*
also werde ich über Fehler im Allgemeinen reden

Gesichtspunkte, die wir anschauen wollen



Fehlhandlungen und Fehler

Hersteller

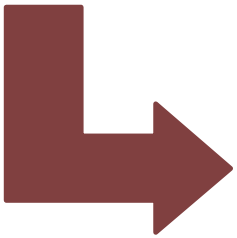
Benutzer
Tester

Software-Produkt

Fehlhandlungen und Fehler

Hersteller

Benutzer
Tester

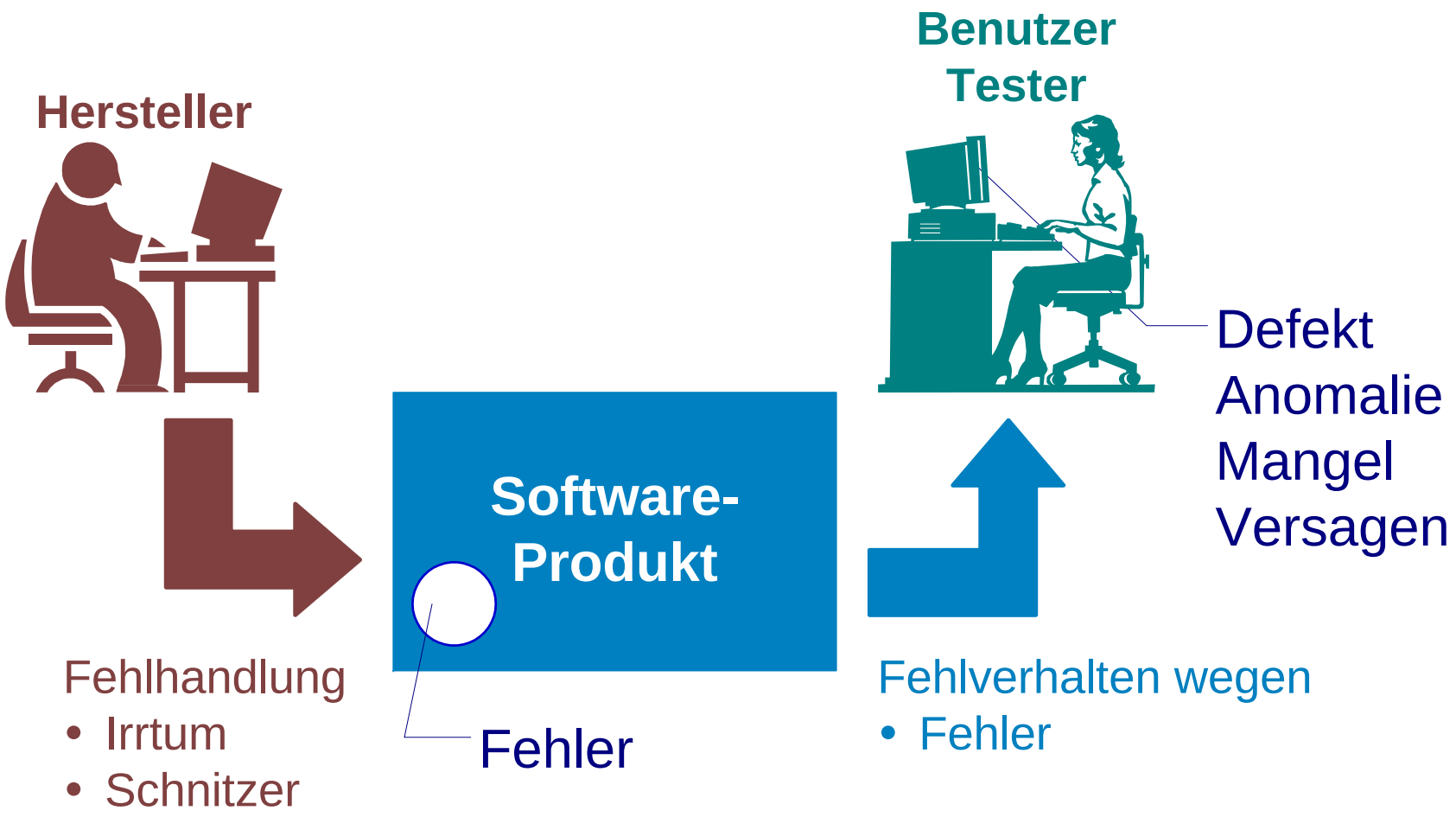


Software-
Produkt

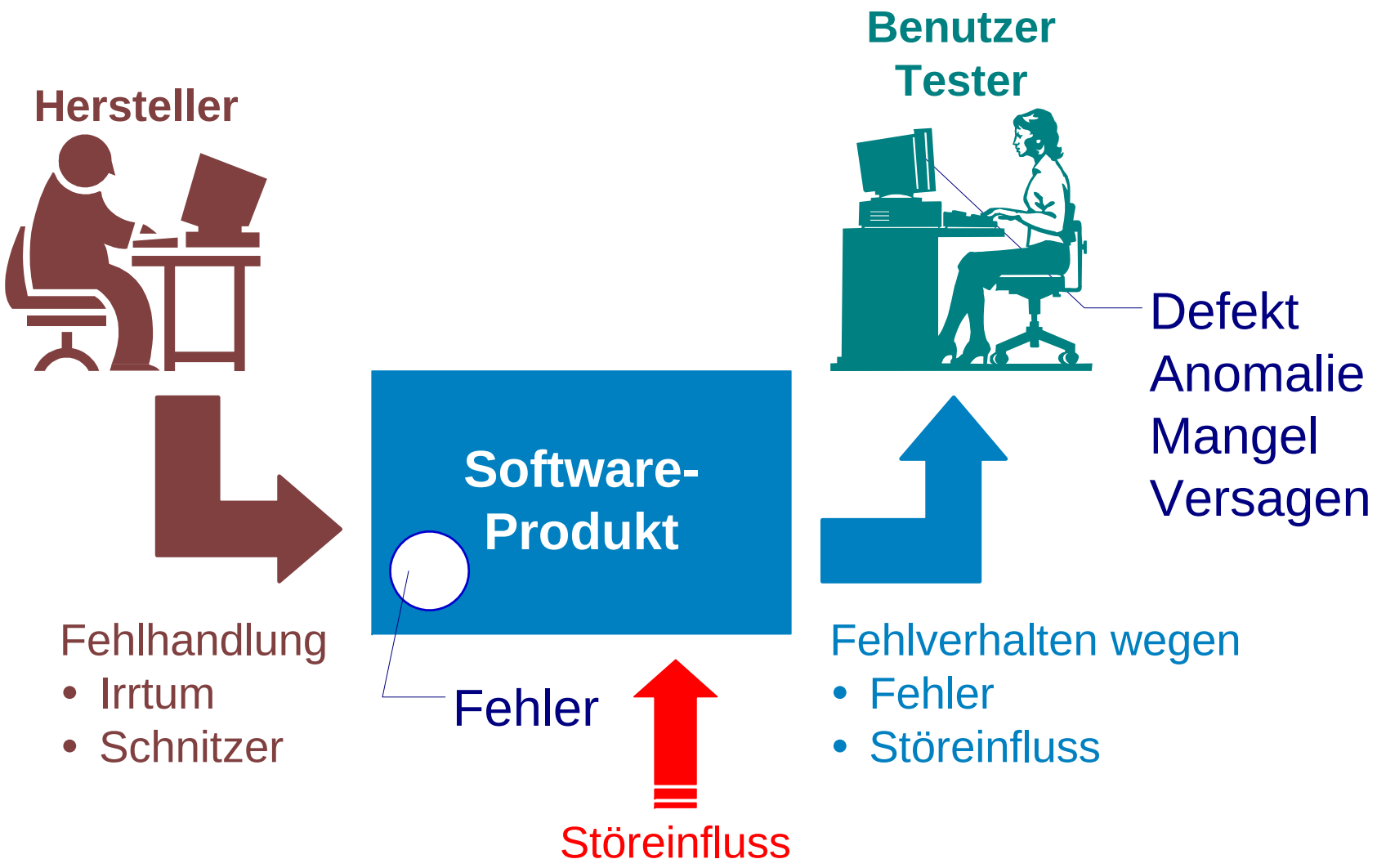
Fehlhandlung
- Irrtum
- Schnitzer

Fehler

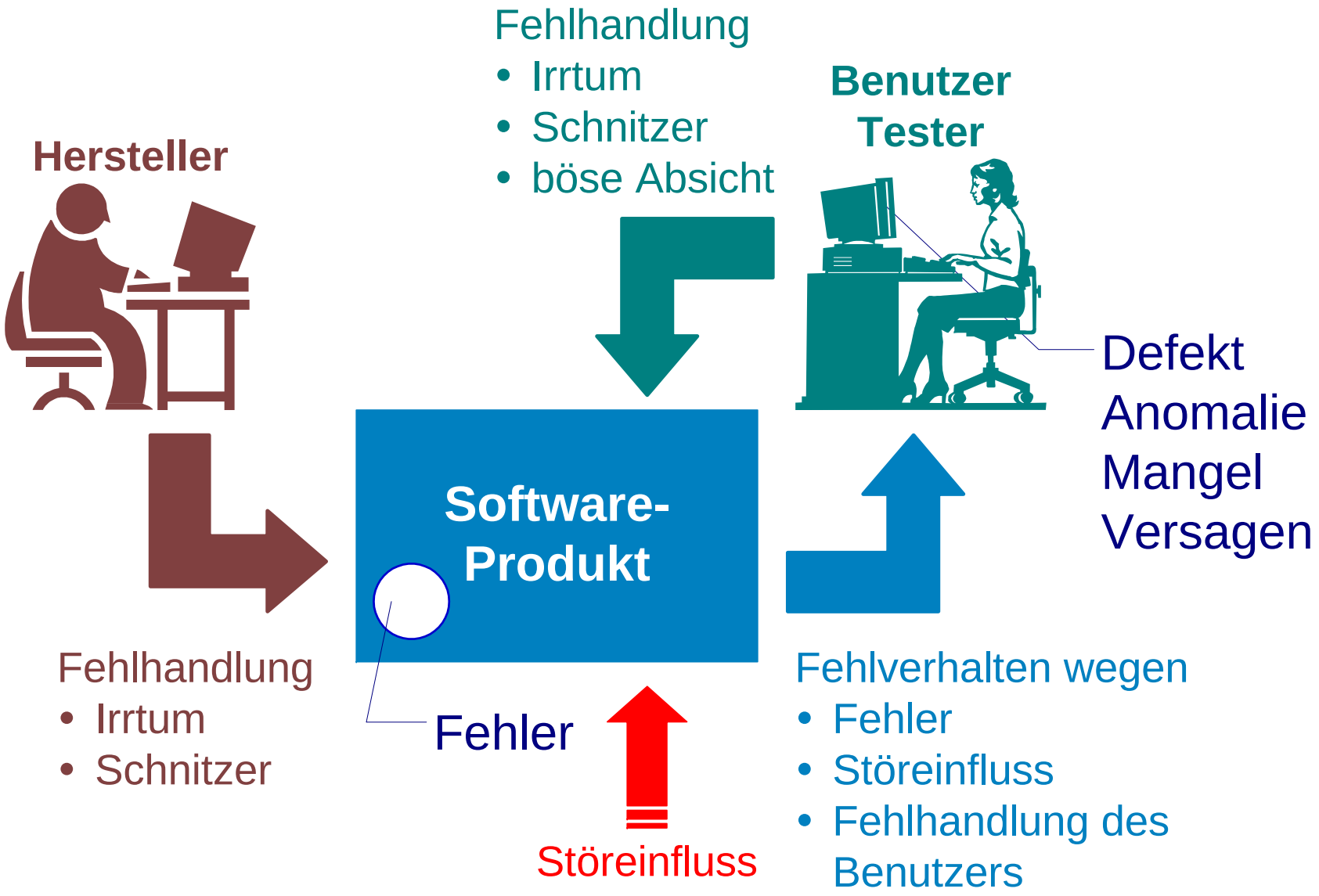
Fehlhandlungen und Fehler



Fehlhandlungen und Fehler



Fehlhandlungen und Fehler



Wie kommt es zum Ärger

der Benutzer erfährt einen

weil

das Programm enthält einen

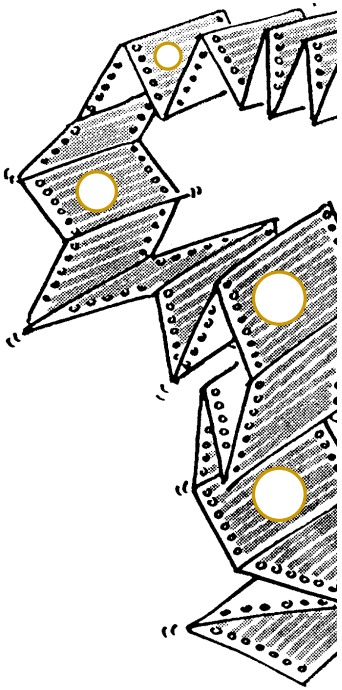
wegen

einer vom Programmierer begangenen

Defekt (anomaly)

⇦

Fehler (fault)



⇦

Fehlhandlung (error)

Definitionen – Fehlhandlung, Fehler, Defekt, Mangel

Begriff	Definition	Synonyme
Fehlhand-lung	Menschliche Handlung mit unerwünschtem Ergebnis.	Irrtum, Schnitzer
Fehler	Abweichung der tatsächlichen von der für die Erfüllung der Spezifikation erforderlichen konstruktiven oder fertigungstechnischen Ausführung des Systems (Verdrahtung, Dimensionierung, Programmierung, usw.).	Fehlerzustand, innerer Fehler
Defekt	Nichterfüllung der Spezifikation. Tatsächliches Systemverhalten abweichend vom spezifizierten. Unkorrektheit.	Anomalie, Versagen, Fehlerwirkung, äußerer Fehler
Mangel	Nichterfüllen der Anforderungen in Bezug auf einen beabsichtigten oder festgelegten Gebrauch.	

Definitionen – Fehlhandlung, Fehler, Defekt, Mangel

Begriff	Definition	Synonyme
Fehlhand-lung	Menschliche Handlung mit unerwünschtem Ergebnis.	Irrtum, Schnitzer
Fehler	Abweichung der tatsächlichen von der für die Erfüllung der Spezifikation erforderlichen konstruktiven oder fertigungstechnischen Ausführung des Systems (Verdrahtung, Dimensionierung, Programmierung, usw.).	Fehlerzustand, innerer Fehler
Defekt	Nichterfüllung der Spezifikation. Tatsächliches Systemverhalten abweichend vom spezifizierten. Unkorrektheit.	Anomalie, Versagen, Fehlerwirkung, äußerer Fehler
Mangel	Nichterfüllen der Anforderungen in Bezug auf einen beabsichtigten oder festgelegten Gebrauch.	

☞ *Eine Spezifikation kann nur Mängel aufweisen*

Und wo sind die Bugs geblieben?

Definitionen – Irrtum, Denkfalle, Schnitzer

Irrtum	Auf inadäquates Wissen zurückführbare fehlerhafte menschliche Handlung. Typische und weit verbreitete – also überindividuelle – Irrtümer gehen auf *Denkfallen* zurück.
Denkfalle	Das Hintergrundwissen ist einer Aufgabenstellung oder einer zu meisternden Situation nicht angemessen. Hintergrundwissen ist Wissen, das von einer größeren Gruppe – beispielsweise allen Menschen einer Zivilisation – geteilt wird. Eine Denkfalle wird offenbar, wenn ein *Irrtum* in der betrachteten Gruppe weit verbreitet ist.
Schnitzer	Fehlerhafte menschliche Handlung auf der Ebene des automatisierten (routinierten) Denkens und Handelns.

Grams (2001), IEEE-982.2:1988, ISO 9000:2005, Ludewig, Lichter (2007)

Soziologische Aspekte

Menschen haben es nicht gern, wenn ihre Irrtümer, Versehen oder Unzulänglichkeiten für alle sichtbar herumhängen.
Anwälte sind bereit sich draufzustürzen,
Mitbewerber sind darauf erpicht, daraus ihren Vorteil zu ziehen,
Arbeitsplätze sind in Gefahr und
die Sorge um die nationale Sicherheit schaltet die Freimütigkeit aus.

In einer Umwelt, in der Firmen und Einzelne nur ihre beste Seite zeigen dürfen, bleiben viele Fehler und deren Urheber versteckt im Schatten der Berechnung.

Und das macht die Verbesserung der Rechnersysteme durch Lernen aus Irrtümern – eine ehrwürdige Strategie im Ingenieurwesen – sehr viel schwieriger, als es sein sollte.

(Petersen 1996)

Soziologische Aspekte – Offenheit

Menschen haben es nicht gern, wenn ihre Irrtümer, Versehen oder Unzulänglichkeiten für alle sichtbar herumhängen.
Anwälte sind bereit sich draufzustürzen,
Mitbewerber sind darauf erpicht, daraus ihren Vorteil zu ziehen,
Arbeitsplätze sind in Gefahr und
die Sorge um die nationale Sicherheit schaltet die Freimütigkeit aus.

In einer Umwelt, in der Firmen und Einzelne nur ihre beste Seite zeigen dürfen, bleiben viele Fehler und deren Urheber versteckt im Schatten der Berechnung.

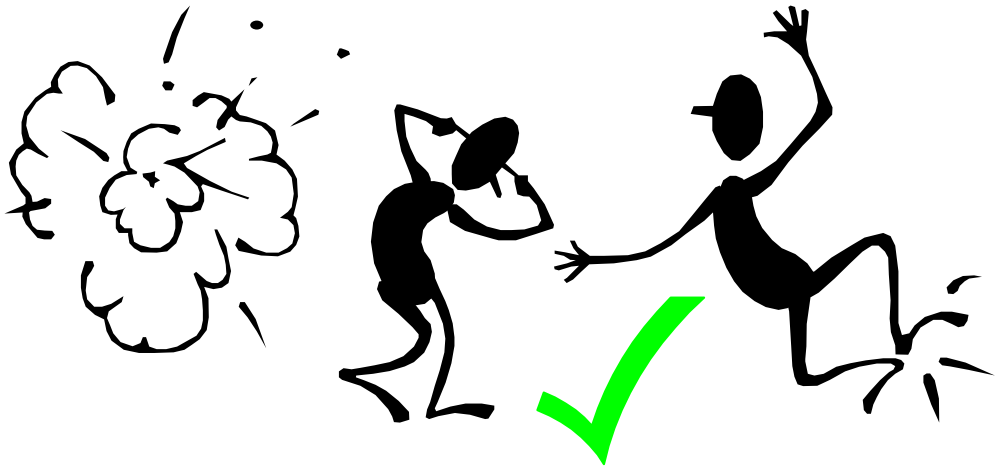
Und das macht die Verbesserung der Rechnersysteme durch Lernen aus Irrtümern – eine ehrwürdige Strategie im Ingenieurwesen – sehr viel schwieriger, als es sein sollte.

(Petersen 1996)

☝ *Hat jemand Unternehmenskultur gesagt?*

Fehlerkultur

1. Es ist erlaubt Fehler zu machen.
2. Es ist lobenswert, Fehler zu finden.
3. Es ist lohnenswert, Fehler so früh wie möglich aufzuspüren.
4. Es ist förderungswürdig, aus den Fehlern zu lernen.
5. Es ist statthaft, neue Art von Fehlern zu entdecken.
6. Es ist ehrenhaft, Fehler zu vermeiden.



Soziologische Aspekte – Prüfungen

Es ist die Essenz des modernen Ingenieurwesens nicht nur fähig zu sein, die Ergebnisse eigener Arbeit zu prüfen, sondern sie auch von anderen prüfen zu lassen und fähig zu sein, die Ergebnisse der Arbeit anderer prüfen zu können.

- *1. Ich mache Fehler, ich brauche Hilfe.*
  2. Meine Kollegen machen Fehler, sie brauchen meine Hilfe.

Um dies zu bewerkstelligen, müssen sich die Arbeitsergebnisse nach gewissen Konventionen richten, gewissen Normen genügen und ein verständliches Teilstück der technischen Kommunikation sein.

(Petroski 1996)

- *Einstellung zur Arbeit & Handwerk beherrschen*

Codex Programmaticus

> Codex Programmaticus
>
> Jede Person, die beim Programmieren die Konventionen für Benennung, Formatierung und Kommentierung nicht befolgt, soll erschossen werden.
>
> Wenn es zufällig ungelegen kommt sie zu erschießen, dann soll sie höfflich gebeten werden, das Programm neu zu schreiben und dabei den obigen Standard zu befolgen.

Technical report, D.E.C. Maynard, Ma (1974)

Rechtliche Aspekte – Vertragliches

Vertrag

- Trägt er der unvermeidbaren Tatsache Rechnung, dass es Fehler in der Lieferung geben wird? Oder bekommt man bei ihm den Eindruck, als ob so was noch nie vorgekommen wäre?
- Sind die Verantwortlichkeiten für Mängel und Fehler gerecht zugewiesen?

Gewährleistung

- Garantiert der Lieferant nur die Richtigkeit der Speichermedien, auf denen die Lieferung erfolgt? Oder gibt es eine Regelung, wie die in der Garantiezeit erkannten Defekte behandelt werden?
- Garantiert der Lieferant die Wartung des gelieferten Produkts für eine spezifizierte Frist? Wie ist die Bereitschaft geregelt?

Rechtliche Aspekte – Produkthaftung

Die große Bürde des Ingenieurs im Vergleich mit anderen Berufsgattungen ist, dass die Ergebnisse seiner Arbeit öffentlich sind, alle können sie sehen.

Er kann seine Irrtümer nicht begraben, wie es Ärzte tun können.
Er kann sie durch Argumente nicht in der Luft auflösen lassen oder die Richter beschuldigen, wie die Rechtsanwälte es tun können.
Er kann sein Versagen nicht mit Bäumen oder Kletterpflanzen verdecken, wie es Architekten gegönnt ist.
Er kann nicht, wie Politiker, seine Schwächen durch Beschuldigung des Opponenten verdecken und hoffen, dass die Menschen vergessen werden.

Der Ingenieur kann einfach nicht leugnen, dass er es getan hat.
Wenn das Ergebnis seiner Arbeit nicht funktioniert, dann wird er verdammt.

[Petroski 1985]

Ethik

Die Moral erhebt einen Anspruch auf allgemeine Verbindlichkeit.
Sie appelliert in Form von Geboten (Du sollst ..; Es ist Deine Pflicht ..)
oder Verboten (Du sollst nicht ..) an die Gemeinschaft der Handelnden.

[Thurnherr 2000]

Ethik ist jedoch der Bereich, in dem wir Verantwortung für unsere Entscheidungen übernehmen: "Ich soll ...", "Ich soll nicht ..".

[Von Foerster, 1993]

? **Soll ich** in der Waffenindustrie arbeiten?

? **Soll ich** etwas unternehmen, wenn der Test des medizinischen Geräts nach meinem Wissensstand nicht streng genug war?

? **Soll ich** etwas tun, um die Auslieferung des Programms zu verhindern, das die Haben-Zinsen immer ab- und die Soll-Zinsen immer aufrundet?

Management

Fehlerblindes Management

– Interessiert sich um Fehler nur, wenn der Kunde direkt bei ihm reklamiert, natürlich lautstark

Fehlerbewusstes Management

+ kümmert sich darum, dass keine Fehler gemacht werden
+ wenn das nicht ganz gelingt, sorgt dafür, dass die Fehler wenigstens möglichst früh entdeckt und beseitigt werden
+ um den Erfolg messen zu können, werden die Defekte berichtet, bewertet und der Stand ihrer Bearbeitung verfolgt
+ sorgt für das Lernen aus den Fehlhandlungen
+ wie gut dies gelingt, liest er an den bekannten Fehlerkosten ab

Management

Fehlerblindes Management

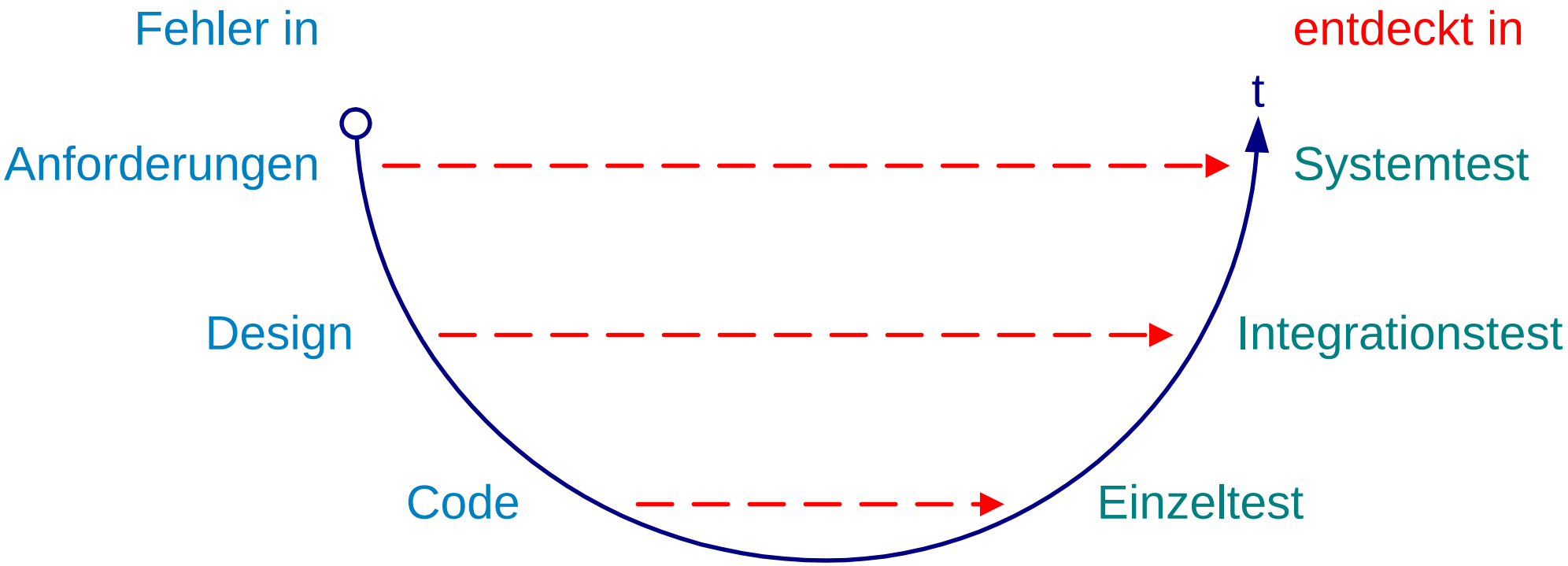
– Interessiert sich um Fehler nur, wenn der Kunde direkt bei ihm reklamiert, natürlich lautstark

Fehlerbewusstes Management

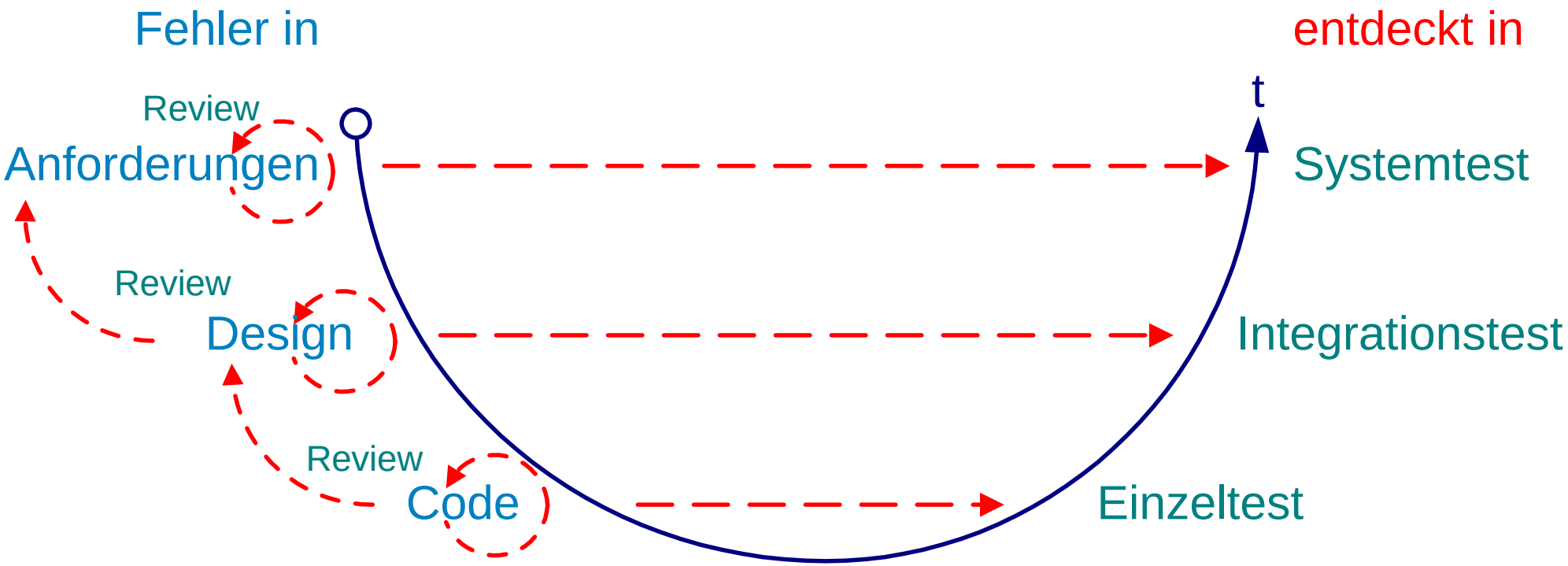
+ kümmert sich darum, dass keine Fehler gemacht werden
+ wenn das nicht ganz gelingt, sorgt dafür, dass die Fehler wenigstens möglichst früh entdeckt und beseitigt werden
+ um den Erfolg messen zu können, werden die Defekte berichtet, bewertet und der Stand ihrer Bearbeitung verfolgt
+ sorgt für das Lernen aus den Fehlhandlungen
+ wie gut dies gelingt, liest er an den bekannten Fehlerkosten ab

☝ *wenn gesichtet, bitte melden!*

Lebensdauer des Fehlers



Lebensdauer des Fehlers



Wirtschaftlichkeit von Prüfungen – ein Beispiel

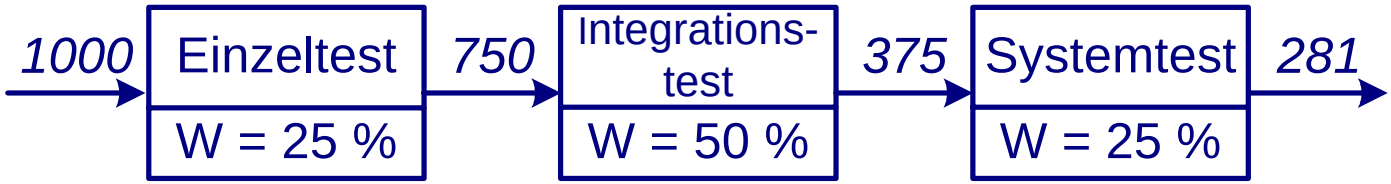
- Größe der Anwendung: 320 Function Points
- Kostenansatz: 100 € / Stunde
- Annahme für Kosten der Fehlerentdeckung
  - → Lineare Zunahme je Prüfschritt, bei höherer Wirksamkeit vergleichsweise teurer
- Annahme für Kosten der Fehlerbehebung
  - → Verdoppelung nach jedem Prüfschritt
- Annahme für die ausgelieferten Fehler
  - → alle werden von den Benutzern entdeckt und dann behoben

Vergleich der Fehlerkosten

1. Fall A: Ausgangslage
2. Fall B: Verdoppelung der Wirksamkeit vom Systemtest
3. Fall C: Verdoppelung der Wirksamkeit vom Einzeltest
4. Fall D: Einsatz von Reviews

Wirtschaftlichkeit – Beispiel Fall A

Fall A

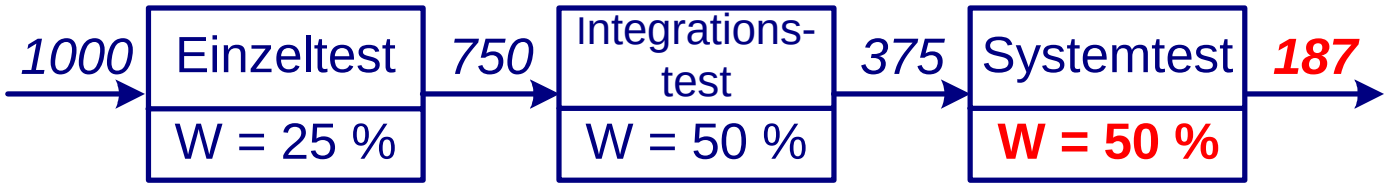


Kosten	Einzeltest	Integrationstest	Systemtest	Wartung
Entdeckung / FP [h/FP]	0.50	1.25	1.5	–
Entdeckung [€]	320*0.5*100 = 16k	320*1.25*100 = 40k	320*1.5*100 =48k	–
Beseitigung / Fehler [h/Fehler]	2.5	5	10	20
Beseitigung [€]	250*2.5*100 = 62.5k	375*5*100 = 187.5k	94*10*100 = 94k	281*20*100 = 562k

Fehlerkosten Fall A = 1'010'000 €

Wirtschaftlichkeit – Beispiel Fall B

Fall B

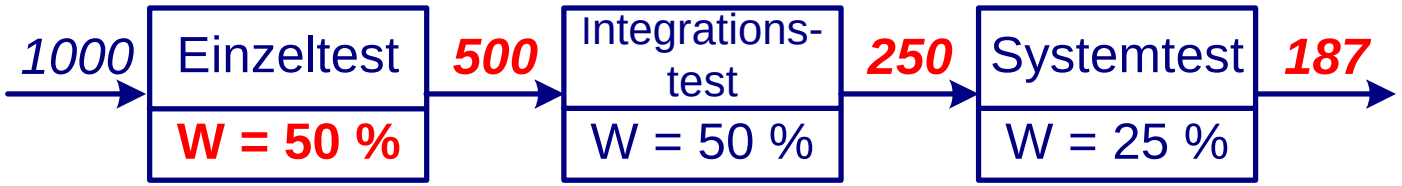


Kosten	Einzeltest	Integrationstest	Systemtest	Wartung
Entdeckung / FP [h/FP]	0.50	1.25	**1.75**	–
Entdeckung [€]	320*0.5*100 = 16k	320*1.25*100 = 40k	320***1.75***100 = **56k**	–
Beseitigung / Fehler [h/Fehler]	2.5	5	10	20
Beseitigung [€]	250*2.5*100 = 62.5k	375*5*100 = 187.5k	**187***10*100 = **187k**	**187***20*100 = **374k**

Fehlerkosten Fall B = 923'000 € = 91.4% von Fall A

Wirtschaftlichkeit – Beispiel Fall C

Fall C

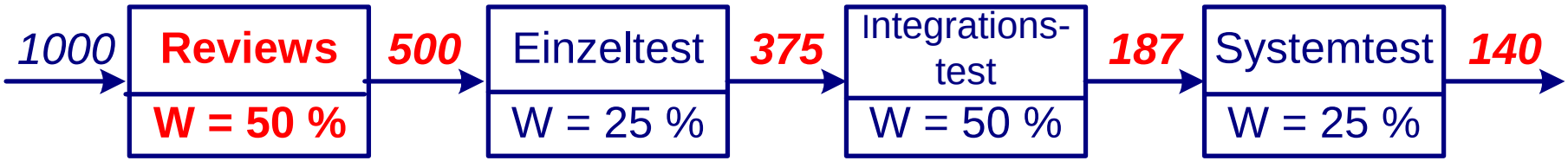


Kosten	Einzeltest	Integrationstest	Systemtest	Wartung
Entdeckung / FP [h/FP]	**0.75**	1.25	1.5	–
Entdeckung [€]	320*__0.75__*100 = **24k**	320*1.25*100 = 40k	320*1.5*100 = 48k	–
Beseitigung / Fehler [h/Fehler]	2.5	5	10	20
Beseitigung [€]	**500***2.5*100 = **125k**	**250***5*100 = **125k**	**125***10*100 = **125k**	**187***20*100 = **374k**

Fehlerkosten Fall C = 861'000 € = 85.2% von Fall A
93.3% von Fall B

Wirtschaftlichkeit –Beispiel Fall D

Fall D



Kosten	Reviews	Einzeltest	Integrationstest	Systemtest	Wartung
Entdeckung / FP [h/FP]	**0.5**	0.50	1.25	1.5	–
Entdeckung [€]	**320*0.5*100 =16k**	320*0.5*100 = 16k	320*1.25*100 = 40k	320*1.5*100 = 48k	–
Beseitigung / Fehler [h/Fehler]	**1.25**	2.5	5	10	20
Beseitigung [€]	**500*1.25*100 = 62.5k**	**125***2.5*100 = **31.25k**	**187***5*100 = **93.5k**	**47***10*100 = **47k**	**140***20*100 = **280k**

Fehlerkosten Fall C = 634’250 € = 62.9% von Fall A

73.7% von Fall C

Entwicklung

Wenn die Erinnerung an das Scheitern für bessere Brücken sorgen kann, können bauliche Erfolge für bessere Brückenbauer sorgen.

Natürlich führt der Erfolg letztendlich zum Versagen, zum ästhetischen, funktionalen oder strukturellem Versagen. Das erste kann uns die Lust am Leben rauben, das zweite die Qualität des Lebens und das dritte das Leben selbst.

Der Zweck des Designs ist Versagen zu vermeiden, ein nicht antizipiertes Versagen ist ein klares Zeichen nicht angemessenen Designs. Aber das Versagen kann man nur vermeiden, wenn man ihn antizipiert. Die grundlegende Fragenfolge im Design ist demnach:

1. Wie kann es zu einem Versagen kommen?
2. Welcher Lösungsansatz kann dieses Versagen verhindern ohne die Gefahr eines anderen Versagens heraufzubeschwören?

[Petroski 1985]

Entwicklung

Wenn die Erinnerung an das Scheitern für bessere Brücken sorgen kann, können bauliche Erfolge für bessere Brückenbauer sorgen.

Natürlich führt der Erfolg letztendlich zum Versagen, zum ästhetischen, funktionalen oder strukturellem Versagen. Das erste kann uns die Lust am Leben rauben, das zweite die Qualität des Lebens und das dritte das Leben selbst.

Der Zweck des Designs ist Versagen zu vermeiden, ein nicht antizipiertes Versagen ist ein klares Zeichen nicht angemessenen Designs. Aber das Versagen kann man nur vermeiden, wenn man ihn antizipiert. Die grundlegende Fragenfolge im Design ist demnach:

1. Wie kann es zu einem Versagen kommen?
2. Welcher Lösungsansatz kann dieses Versagen verhindern ohne die Gefahr eines anderen Versagens heraufzubeschwören?

[Petroski 1985]

☝ *wer an Risikoanalyse denkt, denkt richtig*

Risikoanalyse und Reviews

Defekt und Testen

Defekt entdecken

- Programm zum Fehlverhalten verleiten

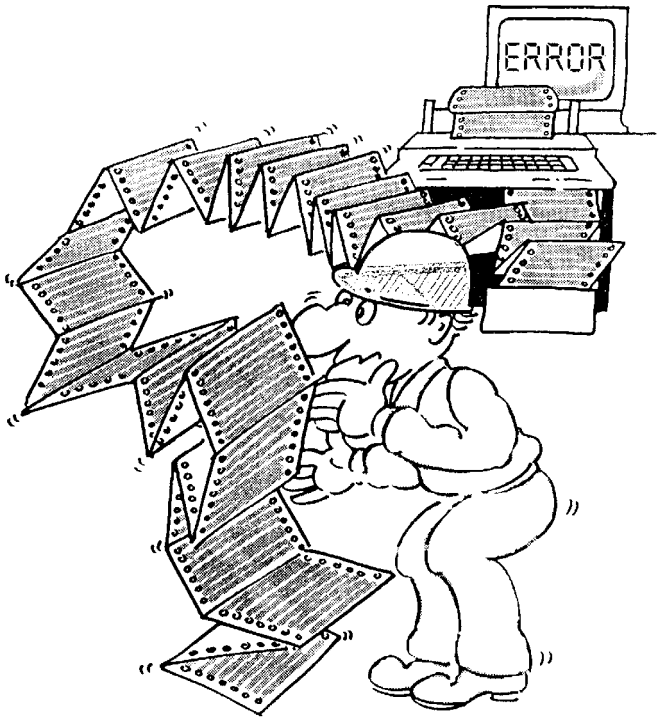
Defekt berichten

- umfassende Information über das Fehlverhalten und die Bedingungen, unter denen es vorkam
- Schwere, Priorität des Defekts
- Hemmnisse, Defekte zu berichten

Defekt behandeln, Fehler beseitigen

Fehlerbeseitigung testen

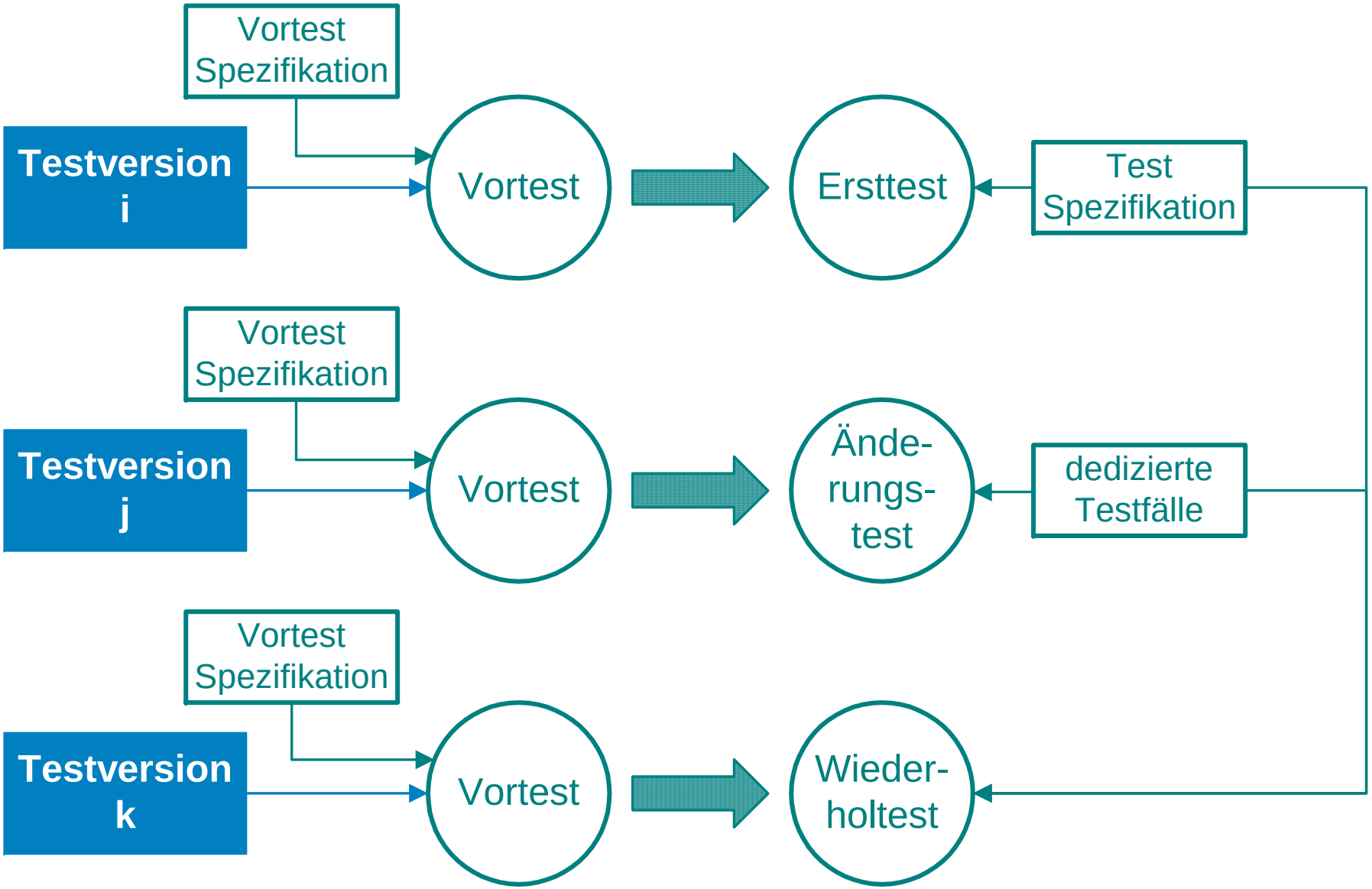
- eine andere Test-Art



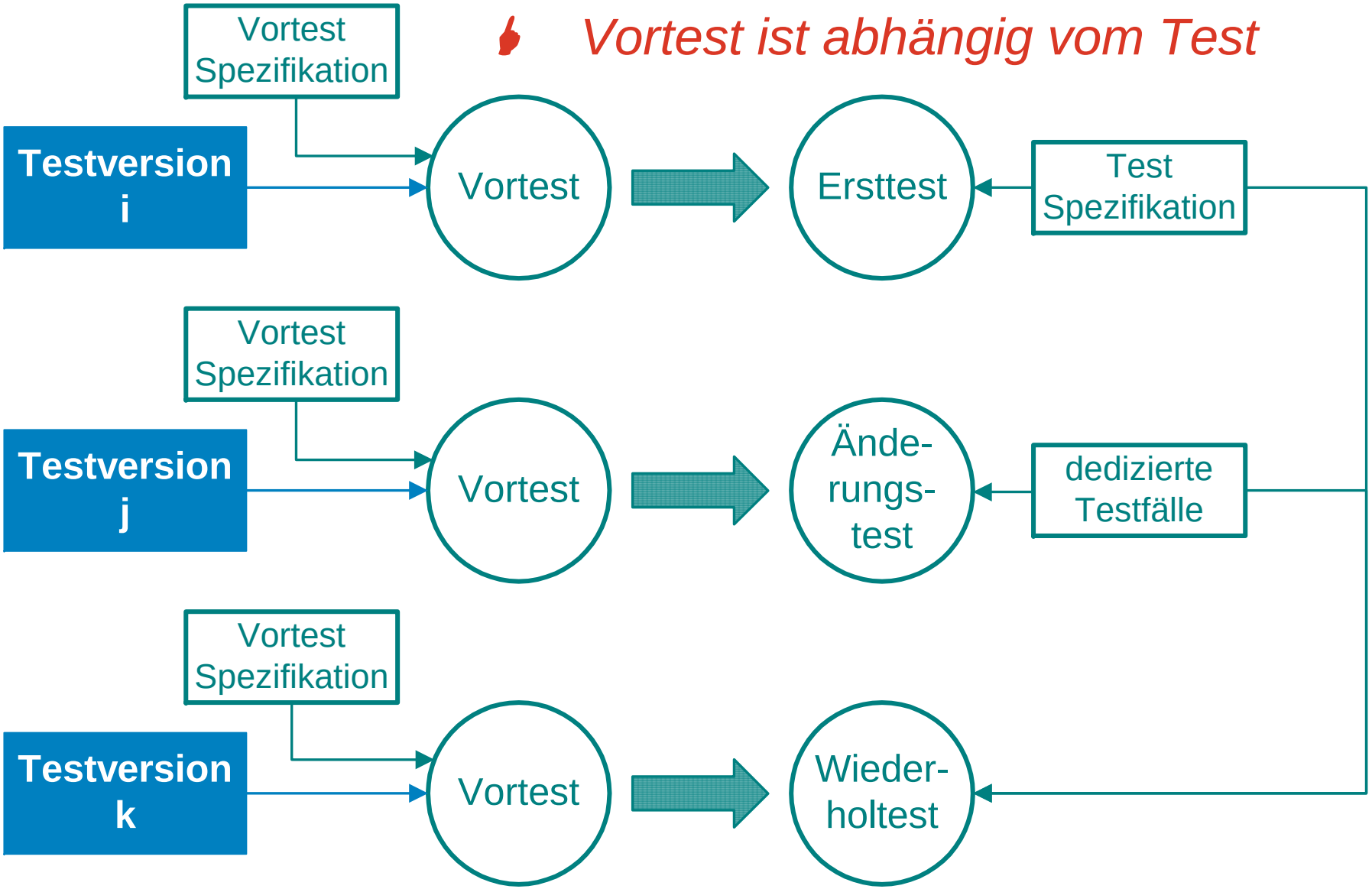
Testarten nach Zweck und Umfang des Tests

Testart	Zweck und Umfang	Synonyme
Vortest	herausfinden, ob es sich lohnt, mit dem Test zu beginnen; weniger als 3% des geplanten Testaufwands	smoke test, sanity check
Ersttest	die Reife eines Testgegenstands bestimmen; definierter Satz von Testfällen	
Änderungs-test	herausfinden, ob eine Änderung (neue Anforderung, Fehlerbeseitigung) korrekt implementiert ist; ein dedizierter Satz von Testfällen	
Wiederhol-test	herausfinden, ob Änderungen keine unbeabsichtigte Wirkung zeitigen; von den bereits ausgeführten Testfällen alle: vollständiger dedizierte Untermenge: partieller	regression test

Testarten nach Zweck und Umfang des Tests



Testarten nach Zweck und Umfang des Tests



Was gilt als Defekt?

Ein Defekt ist das, was als Defekt deklariert wurde, nachdem alle Argumente ausgetauscht wurden. Solche Deklarationen können und sollen aufgezeichnet und gezählt werden.

[Beizer 1984]

- *definiere, (ab) wann gilt eine Beobachtung als Defekt mit allen Konsequenzen, die diese Tatsache mit sich bringt*
- *lieber einen Defekt zu viel als einen zu wenig berichten*

Warum Defekte nicht berichtet werden (Stahl 2008)

Hemmnisse sind bedingt durch die

- Arbeitsweise in der Organisation
  - → nicht reproduzierbar – nicht melden
  - → sofort behoben – nicht melden, z.B. Integrationsfehler
  - → unmögliche Fehler – sie passieren doch
  - → zwei Fehler in einer Meldung
  - → ich werde zurück kehren – oder auch nicht
- Psychologie des Testers
  - → Märchen weben – keinen Fehler finden wollen
  - → stecken bleiben – Kampf mit den Voraussetzungen
  - → Frustration – "die werden es sowieso nicht reparieren (wollen)"
- Auffassung des Testers über das Testen
  - → "Es ist die gleiche Ursache" – oder doch nicht?
  - → "Es ist in der Spezifikation" – sie kann auch falsch sein
  - → "Benutzerfreundlichkeit ist nicht mein Job" – von wem denn?

Warum Fehler nicht berichtet werden (Stahl 2008)

Hindernisse bedingt durch die

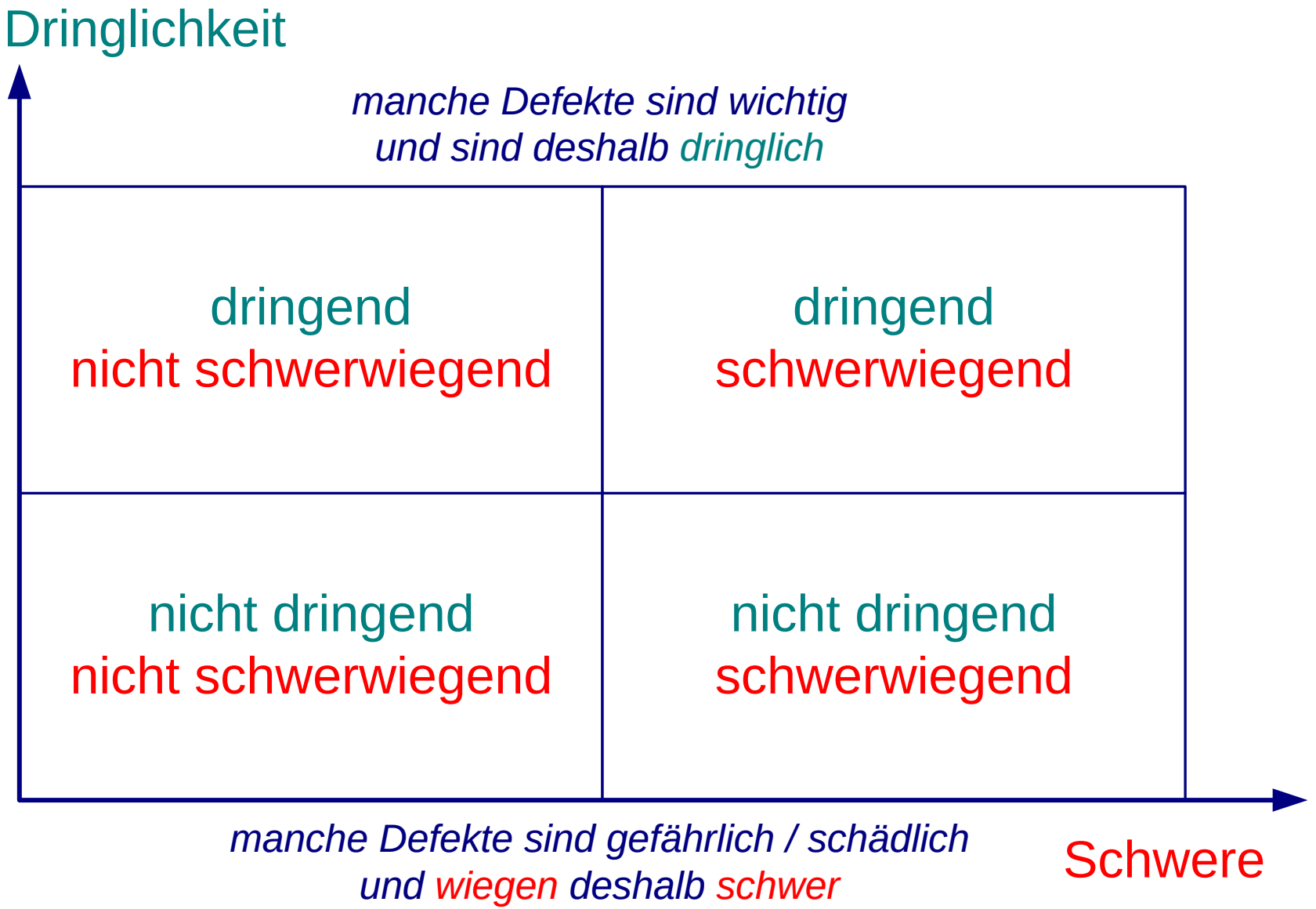
- Arbeitsweise in der Organisation
  - → nicht reproduzierbar – nicht melden
  - → sofort behoben – nicht melden, z.B. Integrationsfehler
  - → unmögliche Fehler – sie passieren doch
  - → zwei Fehler in einer Meldung
  - → "ich werde zum Fehler zurück kehren" – oder auch nicht
- Psychologie des Testers
  - → Märchen weben – keinen Fehler finden wollen
  - → stecken bleiben – Kampf mit den Voraussetzungen
  - → Frustration – "die werden es sowieso nicht reparieren (wollen)"
- Auffassung des Testers über das Testen
  - → "Es ist die gleiche Ursache" – oder doch nicht?
  - → "Es ist in der Spezifikation" – sie kann auch falsch sein
  - → "Benutzerfreundlichkeit ist nicht mein Job" – von wem denn?

    ☝ *nicht gemeldete Defekte werden nicht behandelt*

Abweichungsmeldung (Defektmeldung)

- eindeutige Identifikation der Meldung
- eindeutige Identifikation des Testobjekts
- eindeutige Identifikation des Testgeschirrs
- Zeit, wann die Abweichung beobachtet wurde
- Referenz auf den (erfolgreichen) Testfall
- Problembeschreibung
- Schwere
- Name des Melders
- Name des (nächsten) Bearbeiters
- Status
- Dringlichkeit (Priorität)
- Referenz auf die betroffene Anforderung
- Art der Tätigkeit, die den Fehler verursacht hat
- Stellungnahme / Korrekturmaßnahme des Bearbeiters

Schwere und Dringlichkeit



Schwere (Defektklasse)

Aussage über die Folgen für die Benutzer

Schwere	Bedeutung	Einsatz eingeschränkt
kritischer Defekt	betriebsverhindernd: System kann seinen Zweck nicht erfüllen; z.B. Datenverlust, blockierte Funktion	ganz
wesentlicher Defekt	wesentliche Funktion ist fehlerhaft; Anforderung nicht beachtet oder falsch implementiert; Umweg möglich	merklich
normaler Defekt	alle anderen Fälle	kaum bis wenig

- *mehr als drei Klassen sind üblich, aber nicht sinnvoll*
- *betriebsverhindernd kann auch testbetriebsverhindernd sein*

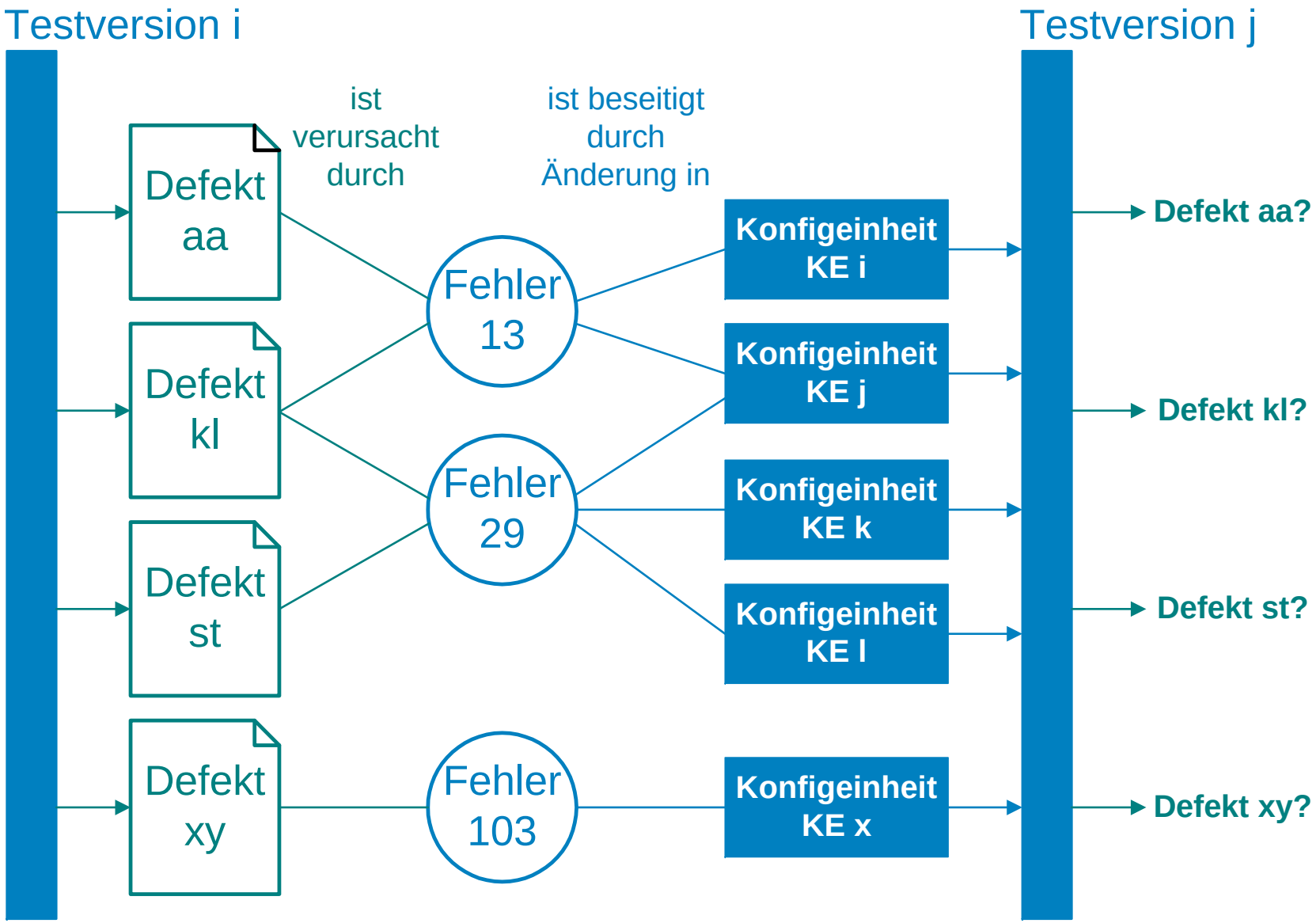
Dringlichkeit (Priorität)

Aussage darüber, wann der den Defekt verursachende Fehler beseitigt werden soll

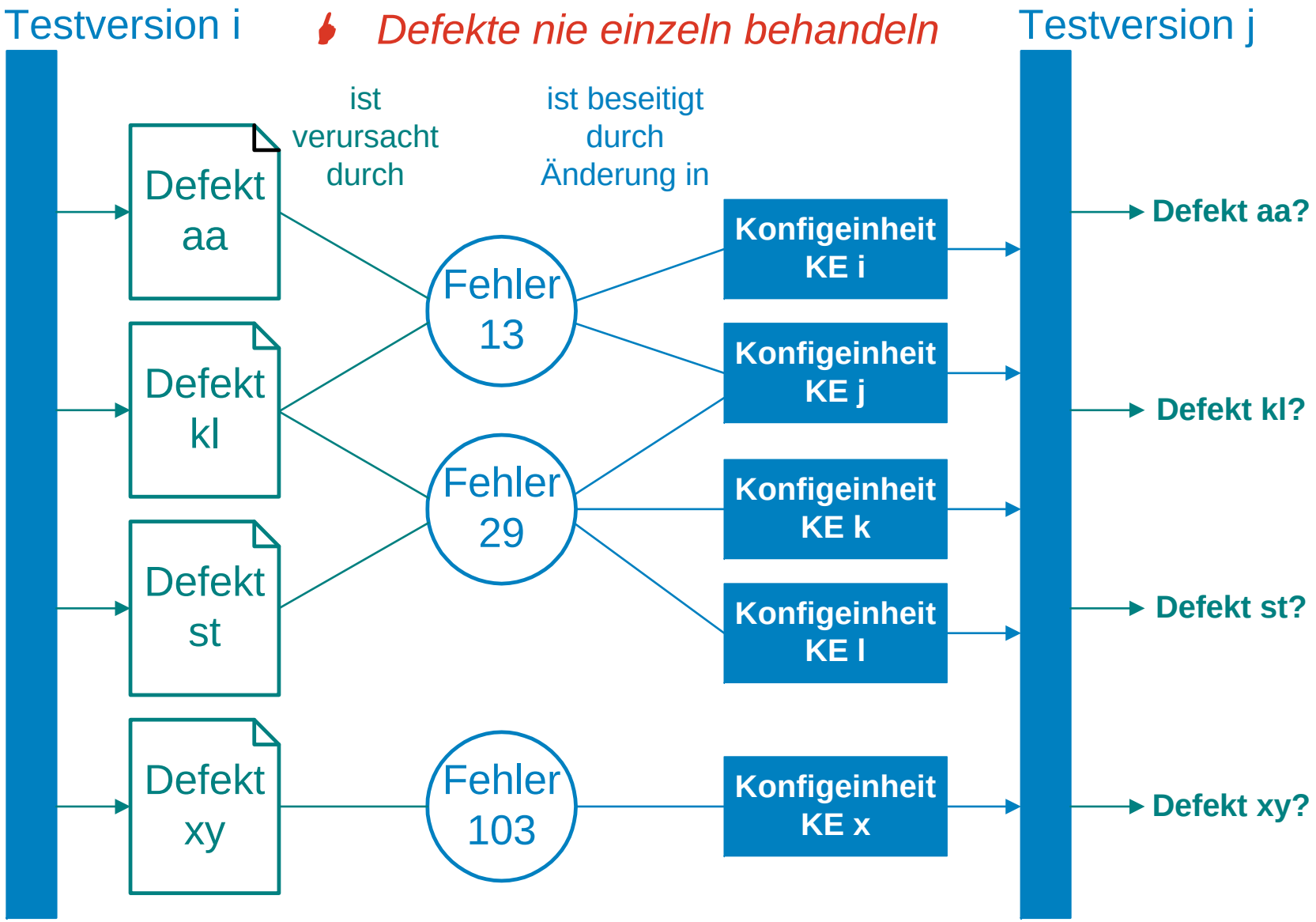
Dringlichkeit	Bedeutung
Patch	Fehler muss sofort, evtl. nur provisorisch, beseitigt und die Korrektur unmittelbar (zum Kunden, zum Test) ausgeliefert werden
nächstes Release	Fehler muss bis zur nächsten geplanten Auslieferung (zum Kunden, zum Test) behoben sein
späteres Release	Fehler soll in einem der für später vorgesehenen Releases beseitigt werden

- *keine Prioritätszahl vergeben, Plangrößen verwenden*

Defekte, Fehler und Testversionen



Defekte, Fehler und Testversionen



Gebote für Beseitigen von Fehlern

I	verstehe das System	understand the system
II	lasse das System scheitern	make it fail
III	höre auf zu denken und schaue	quit thinking and look
IV	teile und herrsche	divide and conquer
V	ändere immer nur ein Ding	change one thing at a time
VI	schreibe auf, was du tust	keep an audit trail
VII	prüfe den Stecker	check the plug
VIII	sorge für einen anderen Blick	get a fresh view
IX	wenn du's nicht repariert hast, dann ist es nicht repariert	if you didn't fix it, it ain't fixed

David Agans (2001)

Gebote für Beseitigen von Fehlern

I	verstehe das System	understand the system
II	lasse das System scheitern	make it fail
III	höre auf zu denken und schaue	quit thinking and look
IV	teile und herrsche	divide and conquer
V	ändere immer nur ein Ding	change one thing at a time
VI	schreibe auf, was du tust	keep an audit trail
VII	prüfe den Stecker	check the plug
VIII	sorge für einen anderen Blick	get a fresh view
IX	wenn du's nicht repariert hast, dann ist es nicht repariert	if you didn't fix it, it ain't fixed

David Agans (2001)

☝ *Annahmen sind verboten; die Annahme "es ist o.k." ist verheerend*

Benutzer unterstützen

First Level Support

- muss instruiert werden
  - → über die bekannten Defekte und mögliche Abhilfen
  - → vom Benutzer präzise und vollständige Information über den gemeldeten Defekt einzuholen
- muss informiert werden über
  - → den Stand der Bearbeitung von Defekten
  - → die Art der Lösung des Problems
  - → geplanten Auslieferungstermin (Release)
- muss die Benutzer
  - → regelmässig informieren, wenn die Behandlung des gemeldeten Defekts länger dauert

Benutzer unterstützen

First Level Support

- muss instruiert werden
  - → über die bekannten Defekte und mögliche Abhilfen
  - → vom Benutzer präzise und vollständige Information über den gemeldeten Defekt einzuholen
- muss informiert werden über
  - → den Stand der Bearbeitung von Defekten
  - → die Art der Lösung des Problems
  - → geplanten Auslieferungstermin (Release)
- muss die Benutzer
  - → regelmässig informieren, wenn die Behandlung des gemeldeten Defekts länger dauert

☞ *die Entwicklung kümmert sich um viele ihrer Kunden wenig, aber um keinen weniger als den First Level Support*

Schlussbemerkungen

Niemand will aus Irrtümern lernen, aber wir können aus Erfolgen nicht genug lernen, um den Stand der Technik zu überwinden.

Jedoch keine Katastrophe muss sich wiederholen, weil durch Reden und Schreiben über die begangenen Irrtümer lernen wir aus ihnen und durch das Lernen aus ihnen können wir ihre Wiederholung vermeiden.

[Petroski 1985]

Ariane V Flug 501

Jungfernflug am
4. Juni 1996

Untersuchungskommission

Beginn der Arbeit:
13. Juni 1996

Ausgabe des Berichts:
19. Juli 1996

Schlussbemerkungen

Und weil Versagen mehr eindeutige Information beinhalten als Erfolge, sind Fallstudien über Versagen oder über das explizite Vermeiden des Versagens die fruchtbarsten Daten für jeden Designer.

[Petroski 1985]

Unser Ziel ist es anderen helfen aus unserer Erfahrung zu lernen, nicht den Gerätehersteller oder irgendjemanden sonst zu kritisieren. Die Irrtümer die hier passierten sind nicht speziell für diesen Hersteller, sondern sind, unglücklicherweise, ziemlich häufig auch in anderen sicherheitskritischen Systemen.

Zitat aus Leveson, Turner: Therac 2 Report in [Peterson 1996]

- *Über Erfolg zu reden ist Silber, über Versagen Gold, Fehler zu verschweigen ist töricht*

Schlussbemerkungen

Peter Neumann ist vertraut mit den vielfältigen Schwächen der Computerei und bleibt der Idee verpflichtet, dass es hilft die Software-Entwicklung zu verbessern und fördert die Sorgfalt bei der Automatisierung, wenn die Öffentlichkeit auf die Computer Probleme aufmerksam gemacht wird.

[Peterson 1996]

http://catless.ncl.ac.uk/risks

THE RISKS DIGEST

Forum On Risks To The Public In Computers And Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Vol 25 Issue 76 (Saturday 15 August 2009)

Seit 1. August 1985 ca. 2200 Ausgaben mit je ca. 15 Beiträgen

... eine Art Schlusswort

Tester
entdeckt
Defekt

Wesen des Defekts
verbergen
wenn er meldet
Tester Versehen

Tester
merkt
Defekt

bewegt er keene Feder
Tester Fehler der Fehler
wehe Tester! trete weg!
besser gehst den Weg des Verfemten

Literatur (1)

[Agans 2002]
David J. Agans: Debugging. AMACOM, 2002, ISBN 0-8144-7168-4

[Beizer 1984]
Boris Beizer: Software System Testing and Quality Assurance. Van Nostrand Reinhold Electrical/Computer Science Series,1984, ISBN 0-442-21306-9

[Frühauf, Ludewig, Sandmayr]
K. Frühauf, J. Ludewig, H. Sandmayr: Software-Prüfung – Eine Anleitung zum Test und zur Inspektion; VdF Verlag, 5. Auflage, 2004, ISBN 3 7281 2906 2

[Grams 2001]
Timm Grams: Grundlagen des Qualitäts- und Risikomanagements. Vieweg Praxiswissen, 2001, ISBN 3-528-03945-0

[IEEE 982.2-1988]
EEE 982.2-1988 IEEE Guide for the Use of Standard Dictionary of Measures to Produce Reliable Software

[ISO 9000:2005]
ISO 9000:2005 Qualitätsmanagementsysteme, Grundlagen und Begriffe, 2005.

Literatur (2)

[Ludewig, Lichter 2007]
J. Ludewig, H. Lichter: Software Engineering. dpunkt.verlag, 2001, ISBN 3-89864-268-2

[Peterson 1996]
Ivars Peterson: Fatal Defect - Chasing Killer Computer Bugs. Vintage Books, 1996, ISBN 0-679-74027-9

[Petroski 1985]
Henry Petroski: To Engineer is Human – The Role of Failure in Successful Design. St. Martin's Press, New York, 1985, ISBN 0-312-80680-9

[Stahl 2008]
M. Stahl: Roadblocks to Bug Reporting
Proceedings of CONQUEST 2008, pp. 297-403

[Thurnherr 2000]
Urs Thurnherr: Angewandte Ethik, zur Einführung. Junius Verlag, 1000, ISBN 3-88506-322-0

[von Foerster 1993]
Heinz von Foerster: KybernEthik, Merve Verlag, Berlin, 1993, ISBN 3- 88369-111-6