Warum machen Menschen Fehler und wie kann man es verhindern

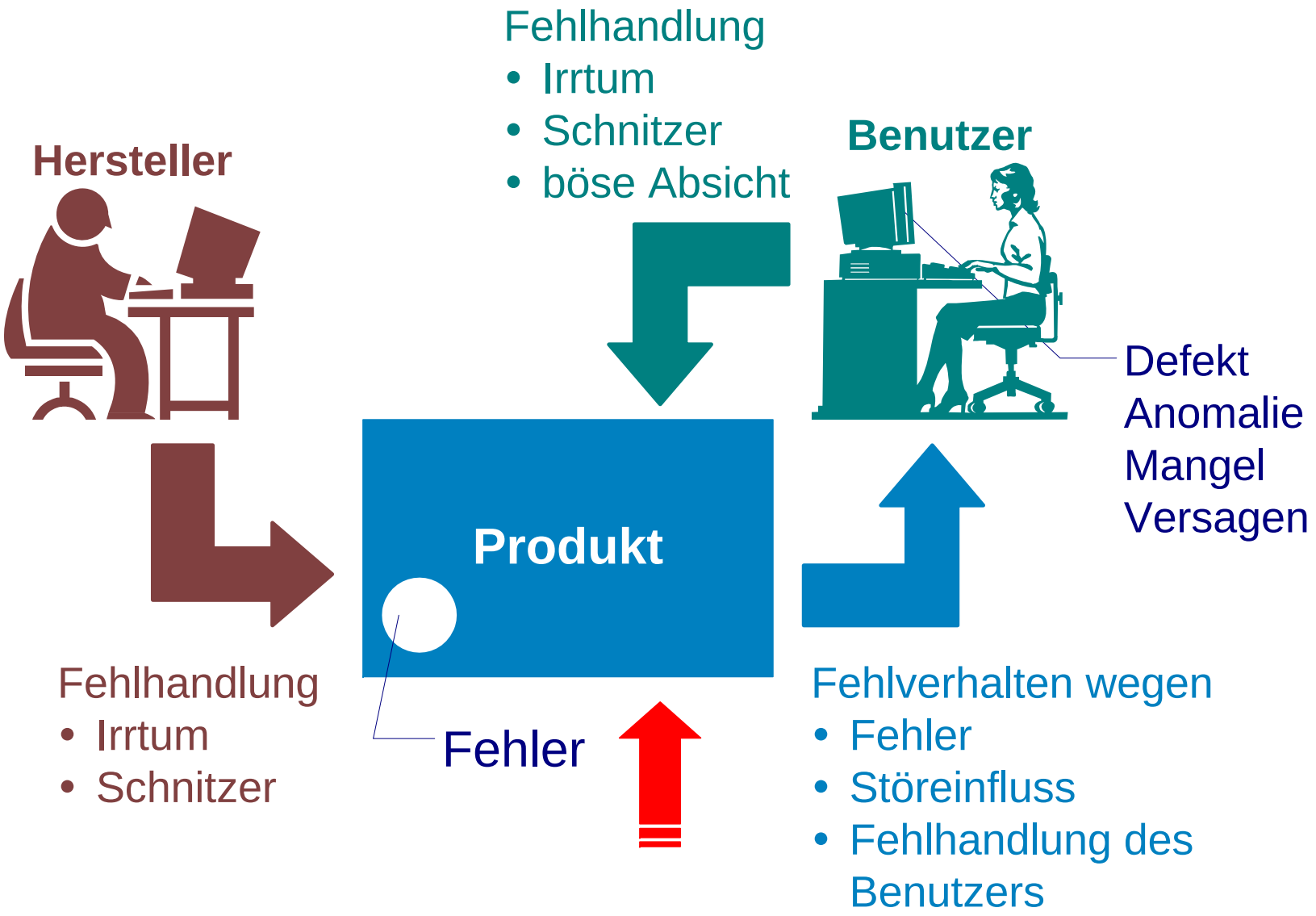
Software Quality Days,
16. Januar 2014

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

Inhalt

- Fehlhandlungen und Fehler
- Warum machen wir Fehler
- Fehlerkultur
- Schlussbemerkungen

Fehlhandlung, Fehler, Defekt



Wie kommt es zum Ärger

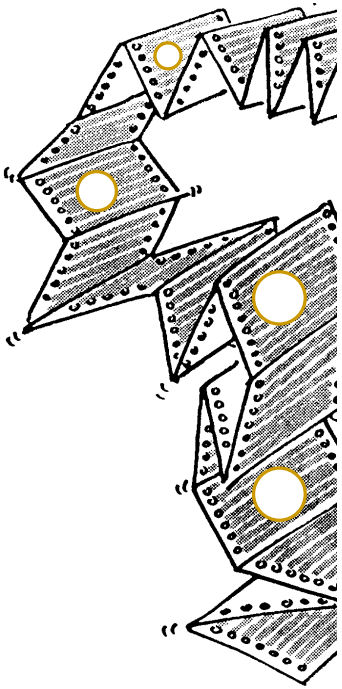
der Benutzer erfährt einen

Defekt (anomaly)

weil

das Produkt enthält einen

Fehler (fault)



wegen

einer vom Hersteller begangenen

Fehlhandlung (error)

Definitionen – Fehlhandlung, Fehler, Defekt

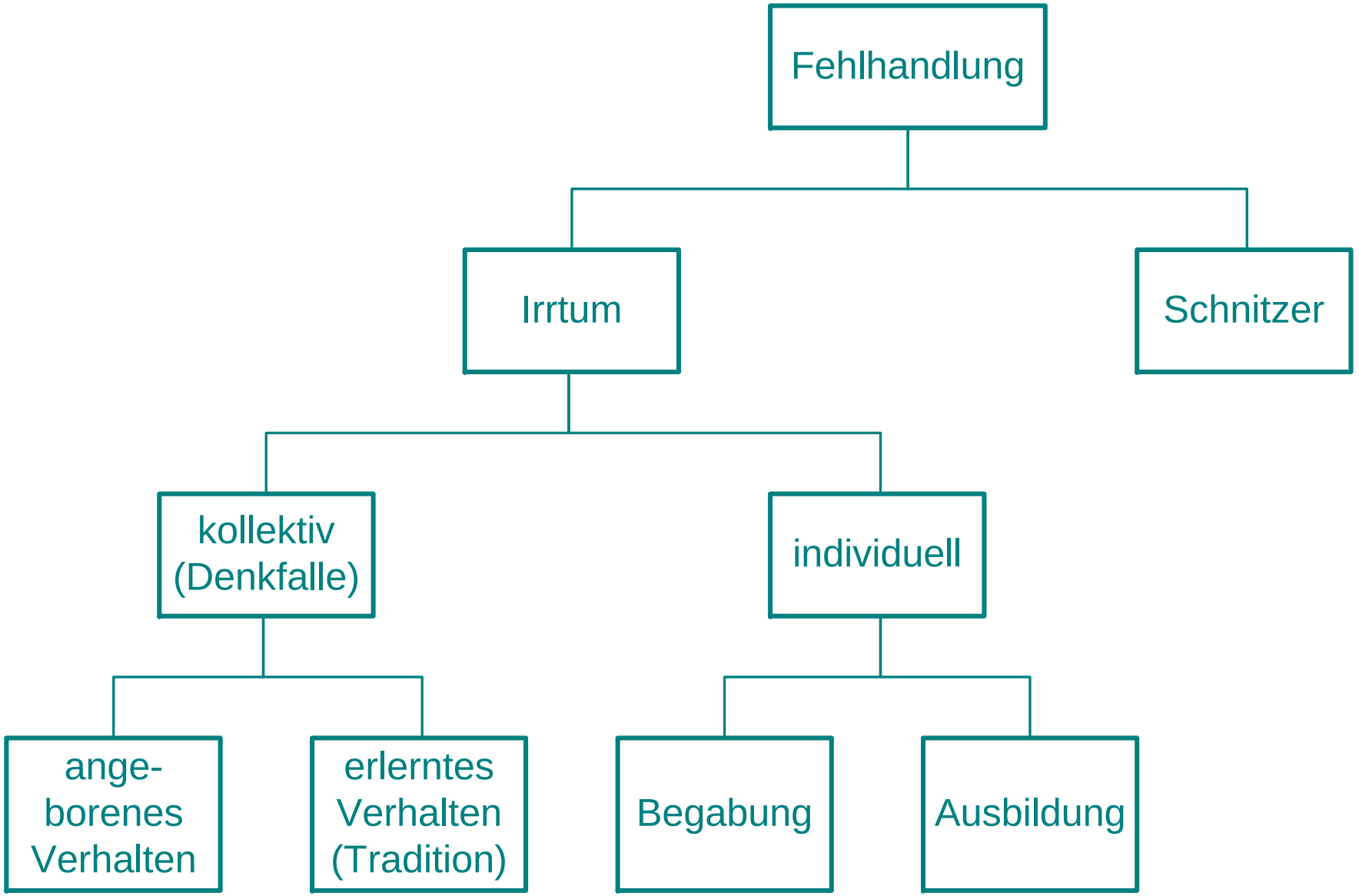
Begriff	Definition	Synonyme
Fehlhand-lung	Menschliche Handlung mit unerwünschtem Ergebnis.	Irrtum, Schnitzer
Fehler	Abweichung der tatsächlichen von der für die Erfüllung der Spezifikation erforderlichen konstruktiven oder fertigungstechnischen Ausführung des Systems (Verdrahtung, Dimensionierung, Programmierung,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

Definitionen – Schnitzer, Irrtum, Denkfalle

Schnitzer	Fehlerhafte menschliche Handlung auf der Ebene des automatisierten (routinierten) Denkens und Handelns.
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.

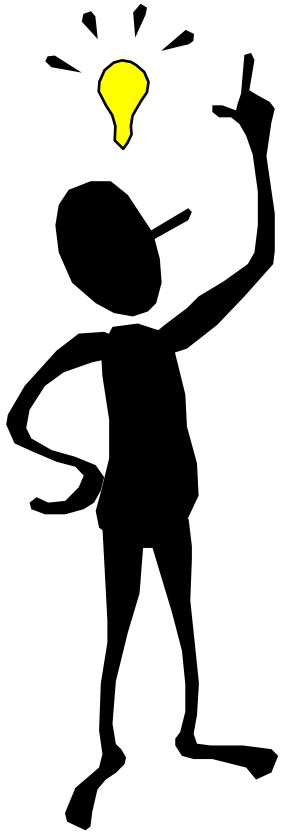
Grams (2001), IEEE-982.2:1988, ISO 9000:2005, Ludewig, Lichter (2007)

Ursachen von Fehlhandlungen



Warum machen wir Fehler

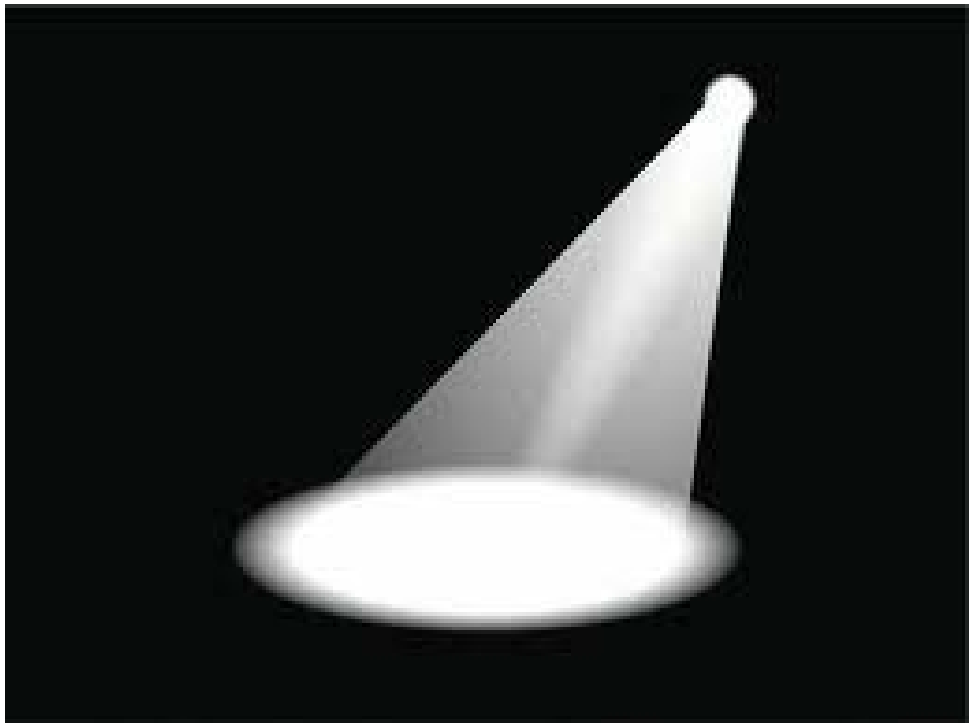
1. weil wir wissen



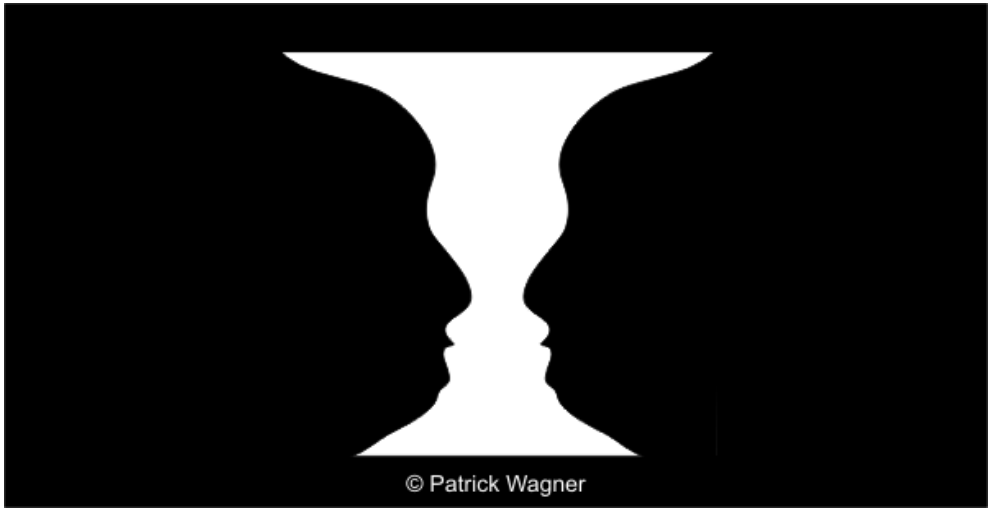
→ wir konzentrieren uns darauf, wovon wir überzeugt sind und blenden alle andere Möglichkeiten aus

Scheinwerferprinzip

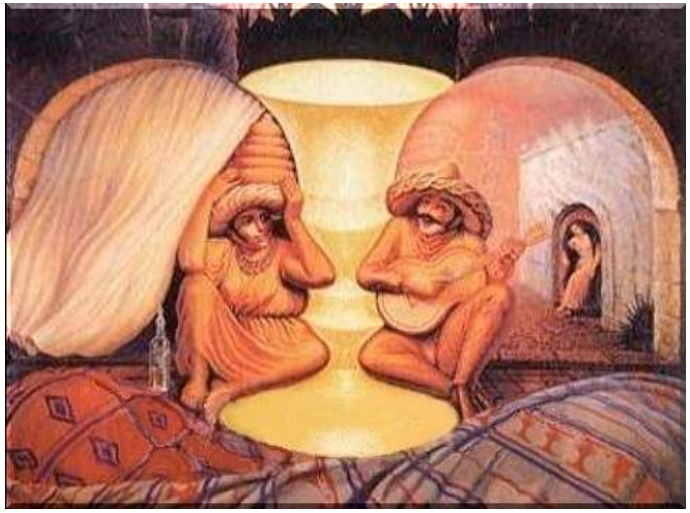
- Wahrnehmung wird durch Erwartung, Vorurteil (= unbegründete Annahme) gelenkt
- nach dem Scheinwerferprinzip liegt stets nur ein kleiner Ausschnitt der momentan zu bearbeitenden Sache im Licht der Aufmerksamkeit, vieles bleibt im Dunkeln



Scheinwerferprinzip



Sehen Sie den Pokal?

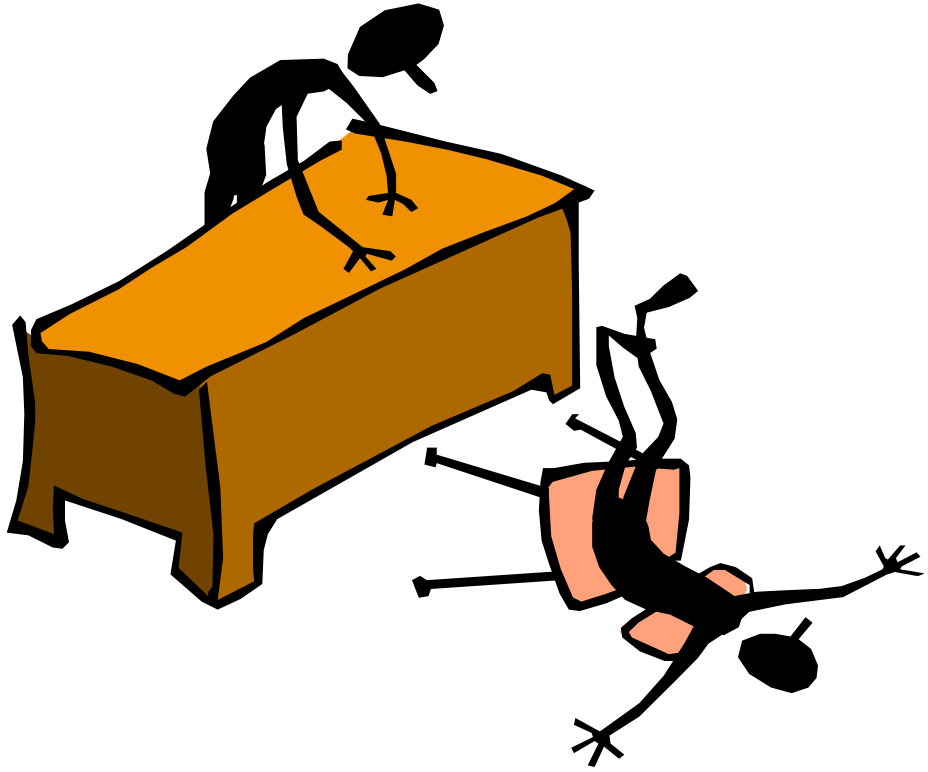


Sehen Sie die Menschen im reifen Alter?

Das Marketing nutzt unsere Fehler aus

Warum machen wir Fehler

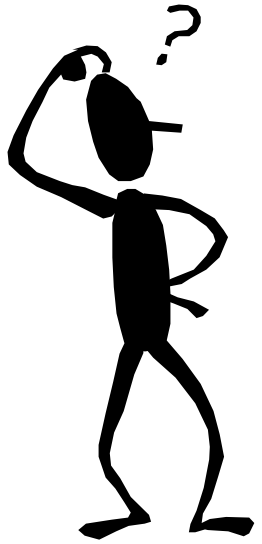
1. weil wir wissen
2. weil wir wissen, uns aber Schnitzer unterlaufen



→ wir beherrschen die Materie, sind unkonzentriert oder es unterläuft uns sonst ein Missgeschick

Warum machen wir Fehler

1. weil wir wissen
2. weil wir wissen, uns aber Schnitzer unterlaufen
3. weil wir nicht wissen



→ tun etwas in der Hoffnung "es wird schon hinhauen" in der Annahme, wie es sein könnte ohne zu wissen, wie es ist

→ da es in gewissen Fällen funktioniert, sind wir zufrieden; es versagt aber in anderen Fällen, die wir nicht bedacht haben

Sparsamkeitsprinzip

- es kommt darauf an, das Ziel mit möglichst geringem Aufwand zu erreichen
- wir sind gezwungen, auf Gesetzmässigkeiten unserer Welt aus einer begrenzten, oft sehr kleinen Anzahl von Beobachtungen zu schliessen
- wir sind gut beraten, zuerst die einfachste aus einer Reihe von Hypothesen zu wählen
- typische Fehler gehen auf falsche Hypothesen über die Funktionsweise / Beschaffenheit der eingesetzten Lösungsmittel zurück

Warum machen wir Fehler

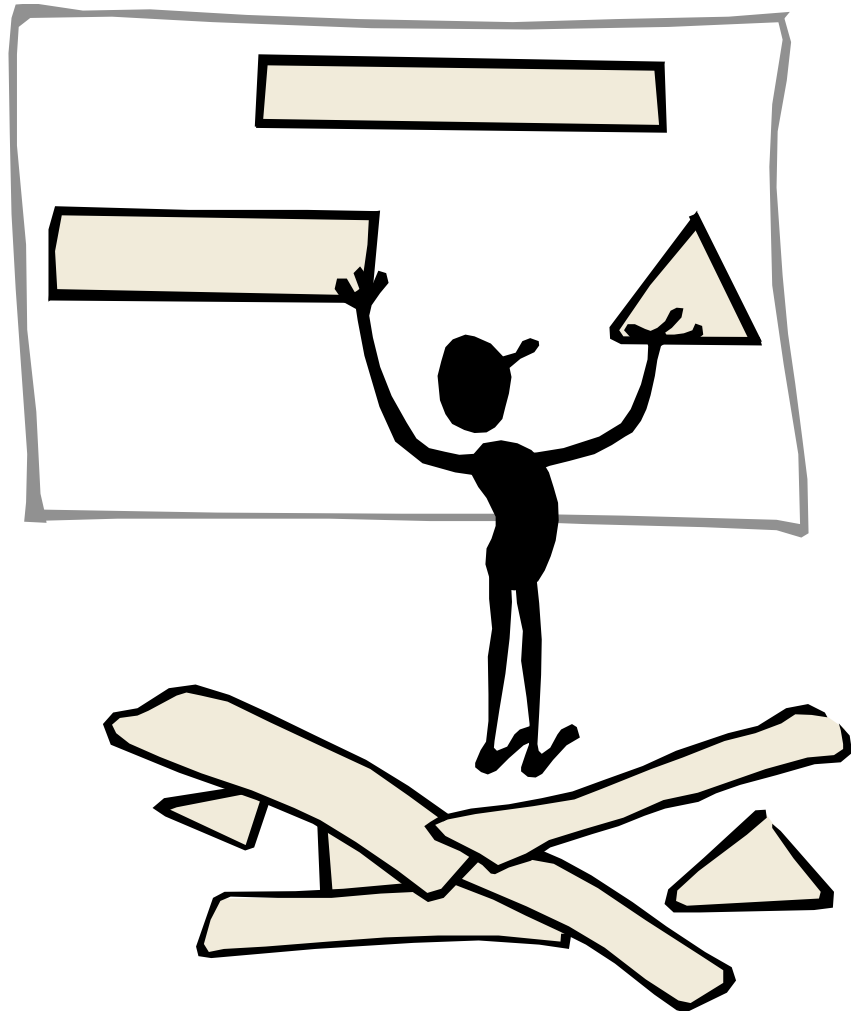
1. weil wir wissen
2. weil wir wissen, uns aber Schnitzer unterlaufen
3. weil wir nicht wissen
4. weil wir nicht wissen, dass wir nicht wissen

→ Selbstüberschätzung

→ wir wählen die erste Lösung, ohne sie anzuzweifeln

→ wiegen uns in falscher Sicherheit

→ ähnlich Scheinwerfer-, Wirkung wie Sparsamkeitsprinzip



Warum machen wir Fehler

1. weil wir wissen
2. weil wir wissen, uns aber Schnitzer unterlaufen
3. weil wir nicht wissen
4. weil wir nicht wissen, dass wir nicht wissen
5. weil wir nicht wissen können

→ Forschung, nicht Entwicklung

→ Sachzwang, etwas zu tun, obwohl wir wissen, "es kann nicht gut herauskommen"

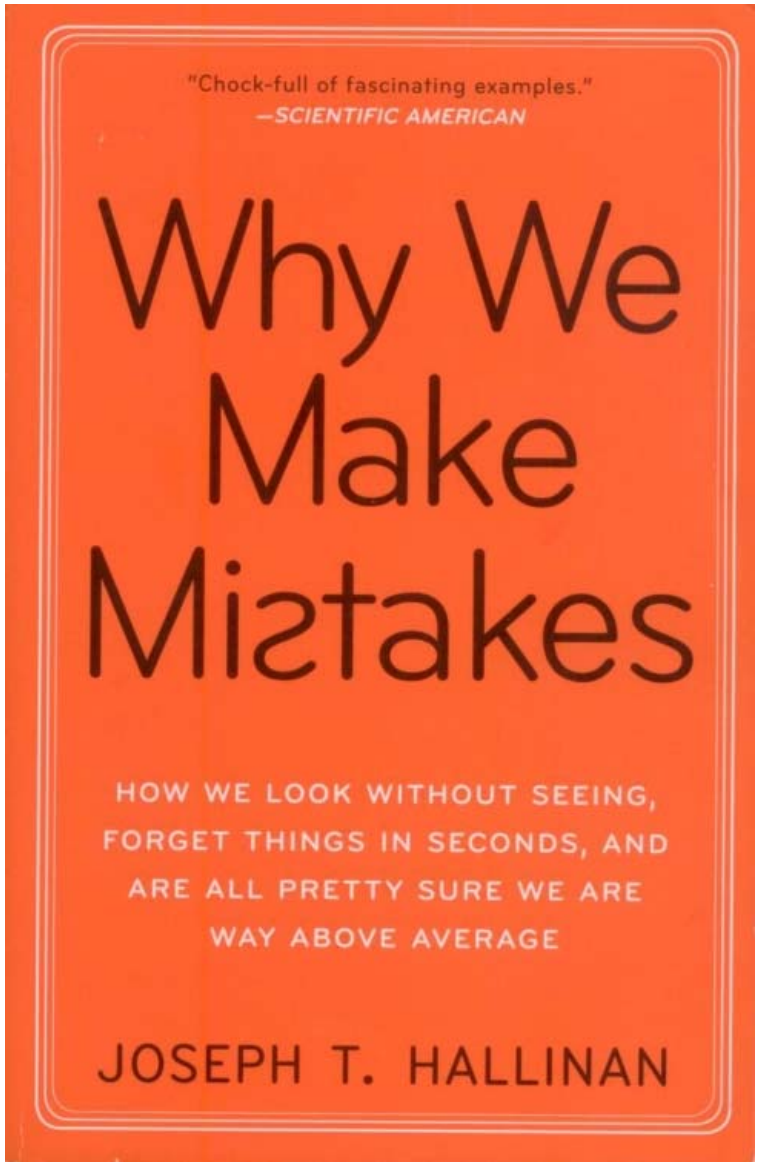
→ z.B. Ersteinsatz neuer Technologie

Warum machen wir Fehler

1. weil wir wissen
2. weil wir wissen, uns aber Schnitzer unterlaufen
3. weil wir nicht wissen
4. weil wir nicht wissen, dass wir nicht wissen
5. weil wir nicht wissen können
6. weil wir eine Aufgabe erledigen, ohne jeglichen 'Handwerkerstolz'

Handwerker?

Als ich mit dem Vortrag fertig war, entdeckte ich ...



... und lernte eine ganze Menge dazu (1)

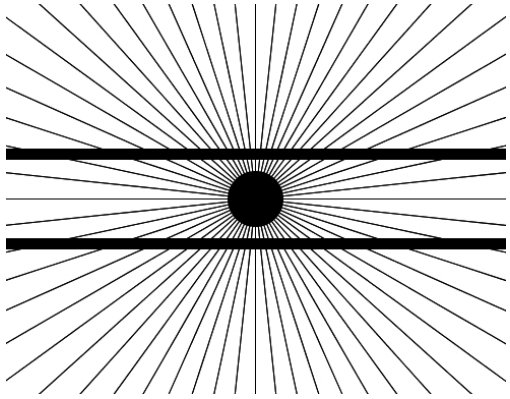
Wir machen Fehler, weil wir

- uns überschätzen (4.)
- uns im anderen Kontext befinden, als derjenige, in dem wir was gelernt haben (3.)
- Sachen überfliegen, skimmen (1. oder 2.)
  wir tauschen die visuellen Details für abstraktes Verständnis ein; mit anderen Worten, wir überfliegen die Sachen und wir wissen nicht, dass wir das tun
  je besser wir sind in etwas, um so wahrscheinlicher ist es, dass wir skimmen
- in der Regel das sehen, was wir sehen wollen (1.)
- uns ablenken lassen (2.)
  wir tun Sachen, die mit unserer Hauptaufgabe nichts zu tun haben
- beim Aufgabenwechsel vergessen, was wir taten oder vor hatten zu tun (*weil wir nicht mehr wissen, was wir wussten*)

... und lernte eine ganze Menge dazu (2)

Wir machen Fehler, weil wir

- die Sachen falsch anschauen (2.)
  schon aus dem Einkaufszentrum rausgeschlendert und versucht den richtigen Schlüssel in ein falsches Auto zu stecken?
- dazu tendieren, Sachen gleich zu tun, funktionale Fixierung (1.)
  wenn wir gelernt haben etwas auf eine bestimmte Art zu tun, tendieren wir dazu, dabei zu bleiben
- wir wissen nicht, dass wir Fehler machen (4.)
  bis uns jemand sagt, dass die zwei dicke Linien gerade sind, gibt es für uns keinen Grund zu mutmassen, dass wir uns irren wenn wir glauben, dass sie Bögen sind



... und lernte eine ganze Menge dazu (3)

Wir lernen nicht aus der Erfahrung, weil wir falsche Fehlerursachen "erkennen" (Rückblick Befangenheit)

- im Rückblick erscheinen Dinge offensichtlich, die vor dem Fakt nicht offensichtlich waren; dies ist der Grund dafür, dass viele unserer Fehler im Rückblick als Dummheiten erscheinen

Ein Weg um Fehler zu vermeiden ist Einschränkungen einzubauen

Design als Quelle der Fehler

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 strukturellen 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

Mit Prüfungen auf Fehlersuche

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*

Beispiel Codierrichtlinien

Codex Programmaticus

Jeder Programmierer, der sich nicht an die standardisierte Namens-, Formatierungs- oder Kommentierungskonventionen hält, sollte erschossen werden.

Wenn es sich so ergibt, dass es lästig ist, ihn oder sie zu erschiessen, dann fordere man ihn oder sie höfflich auf, das Programm so umzuschreiben, dass es den obigen standardisierten Konventionen genügt.

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

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]

Management sorgt für Fehlerkultur

Fehlerblindes Management

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

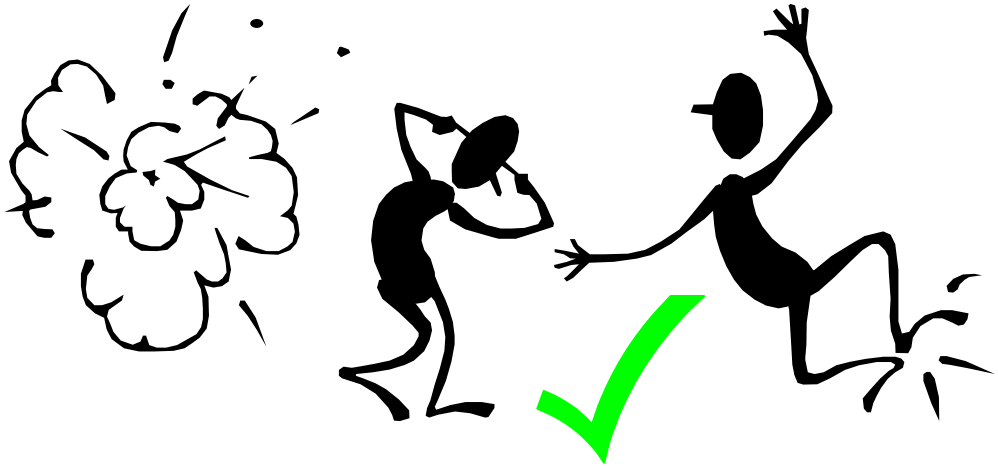
Fehlerbewusstes Management

+ 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, lässt er über Defekte berichten, lässt sie bewerten und verfolgt den Stand ihrer Bearbeitung
+ sorgt für das Lernen aus den Fehlhandlungen
+ wie gut dies gelingt, liest er an den bekannten Fehlerkosten ab

☝ *wenn gesichtet, bitte melden!*

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.



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*

Quintessenz

- Einstellung mitbringen, keine Fehler machen zu wollen, obwohl man weiss, dass dies bei komplexen Aufgabenstellungen kaum möglich ist
- Scheinwerfer ausschalten, alle Optionen berücksichtigen
- bei der Betrachtung der möglichen Versagen die Sicht des Benutzers, des Dienstleistungsempfängers einnehmen
- konzentriert arbeiten und wenn das nicht möglich ist, etwas anderes tun
- beim Sparen nicht grosszügig sein
- up-to-date sein bezüglich Stand der Technik, des Technologie-angebots
- im sicherheitskritischen Bereich keine Kompromisse eingehen, wenn es um die Unterscheidung von Forschung und Entwicklung geht

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 können wir aus ihnen lernen 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

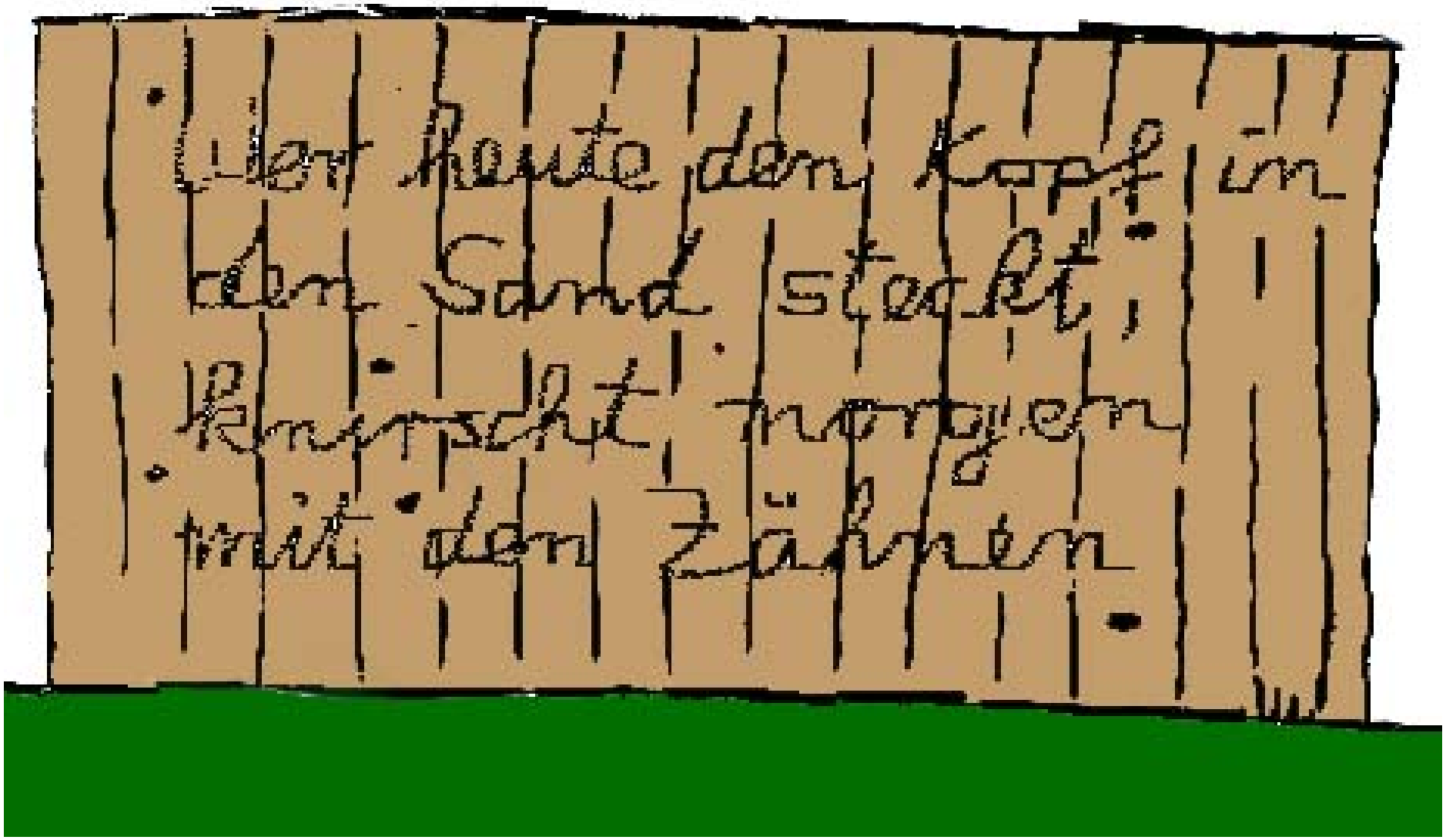
Schlussbemerkungen

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



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

[Hallinan 2009]
Joseph T. Hallinan: Why We Make Mistakes.
Broadway Books, 2009, ISBN 978-0-7679-2806-9

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

Literatur (2)

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

[Leveson 1995]
Nancy Leveson: Safeware: System Safety and Computers.
Addison-Wesley Longman, 1995, ISBN 978-0201119725

[Ludewig, Lichter 2007]
Jochen Ludewig, Horst 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

[Petroski 1994]
Henry Petroski: Design Paradigms – Case Histories of Error and Judgement in Engineering.
Cambridge University Press, 1994, ISBN 0-521-46649-0