

PT2

Code-Review

Sven Köhler
Hasso-Plattner-Institut
2018-06-26



LIKE YOU READ TURING'S
1936 PAPER ON COMPUTING
AND A PAGE OF JAVASCRIPT
EXAMPLE CODE AND GUESSED
AT EVERYTHING IN BETWEEN.



IT'S LIKE A LEET-SPEAK TRANSLATION
OF A MANIFESTO BY A SURVIVALIST CULT
LEADER WHO'S FOR SOME REASON
OBSESSED WITH MEMORY ALLOCATION.

I CAN GET SOMEONE
ELSE TO REVIEW MY CODE.

NOT MORE THAN
ONCE, I BET.

[<https://xkcd.com/1833/>]

KEEP IN MIND THAT I'M
SELF-TAUGHT, SO MY CODE
MAY BE A LITTLE MESSY.

LEMME SEE-
I'M SURE
IT'S FINE.

...WOW.

THIS IS LIKE BEING IN
A HOUSE BUILT BY A
CHILD USING NOTHING
BUT A HATCHET AND A
PICTURE OF A HOUSE.

IT'S LIKE A SALAD RECIPE
WRITTEN BY A CORPORATE
LAWYER USING A PHONE
AUTOCORRECT THAT ONLY
KNEW EXCEL FORMULAS.

IT'S LIKE SOMEONE TOOK A
TRANSCRIPT OF A COUPLE
ARGUING AT IKEA AND MADE
RANDOM EDITS UNTIL IT
COMPILED WITHOUT ERRORS.

OKAY, I'LL READ
A STYLE GUIDE.

THAT'S THE UGLIEST MESS
OF CODE I'VE EVER SEEN.
WHAT ON EARTH ARE YOU
WORKING ON?

IT'S NOTHING WEIRD
THIS TIME, I SWEAR.
IT JUST LOOKS
BAD BECAUSE IT'S
A SPREADSHEET
FORMULA.

...WHICH ASSEMBLES
A HASKELL FUNCTION.

UHHH.

...FOR PARSING HTML.

...OH MY GOD.

IT'S OK! NOTHING DEPENDS ON THIS.
THAT WALL ISN'T LOAD-BEARING.
DOES THAT MEAN WE CAN JUST
THROW HAMMERS AT IT?

...I MEAN...

WAIT. CRAP.

UGH,
I HATE
READING
YOUR CODE.

I KNOW,
I KNOW.

IT'S LIKE YOU RAN OCR ON
A PHOTO OF A SCRABBLE
BOARD FROM A GAME WHERE
JAVASCRIPT RESERVED WORDS
COUNTED FOR TRIPLE POINTS.

IT LOOKS LIKE SOMEONE
TRANSCRIBED A NAVAL WEATHER
FORECAST WHILE WOODPECKERS
HAMMERED THEIR SHIFT KEYS,
THEN RANDOMLY INDENTED IT.

PT2

Code-Review

Sven Köhler
Hasso-Plattner-Institut
2018-06-26

THE INSPECTION PROCESS

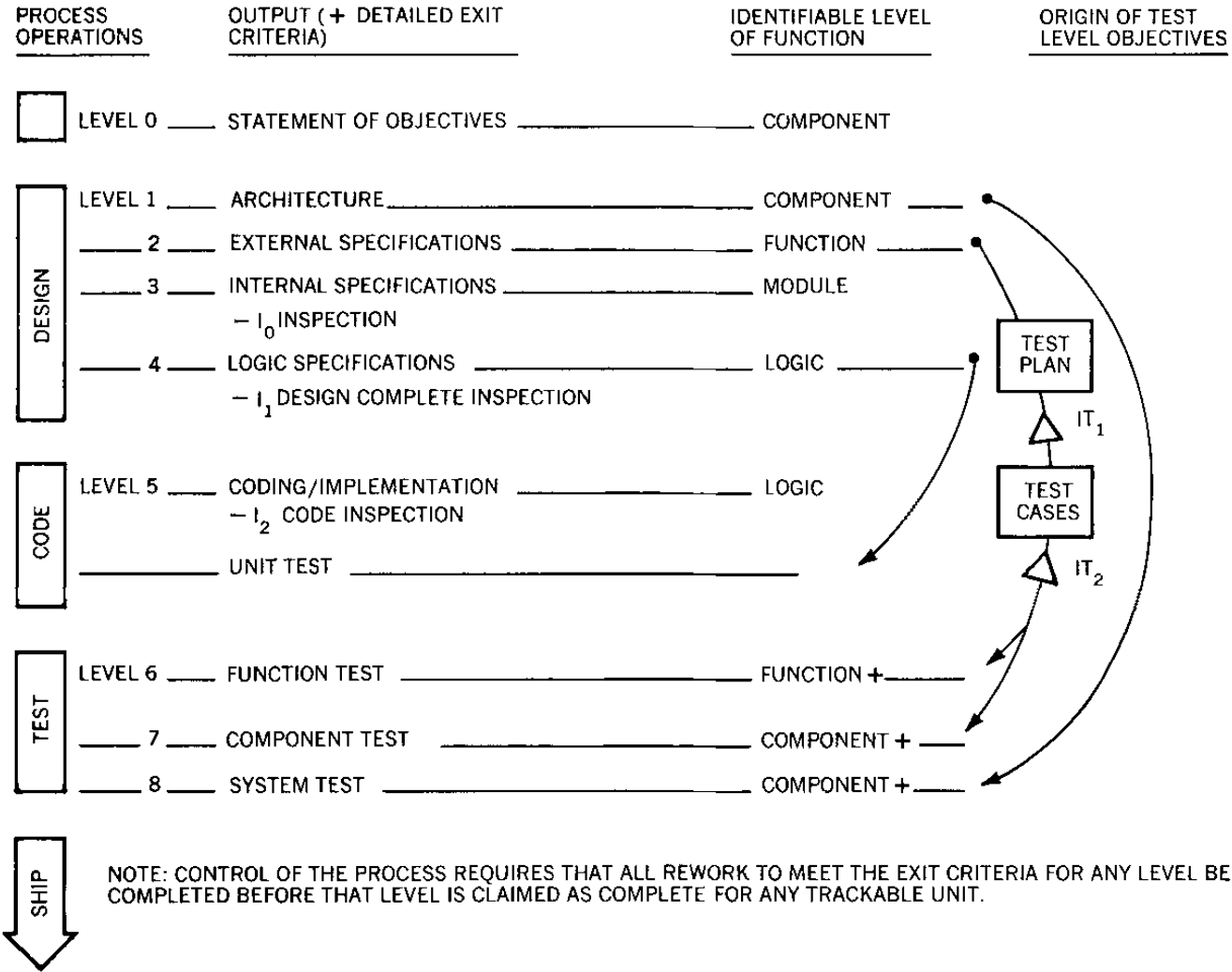
The inspection process follows any development operation whose product must be verified. As shown below, it consists of six operations, each with a specific objective:

<u>Operation</u>	<u>Objectives</u>
PLANNING	Materials to be inspected must meet inspection entry criteria. Arrange the availability of the right participants. Arrange suitable meeting place and time.
OVERVIEW	Group education of participants in what is to be inspected. Assign inspection roles to participants.
PREPARATION	Participants learn the material and prepare to fulfill their assigned roles.
INSPECTION	<i>Find defects.</i> (Solution hunting and discussion of design alternatives is discouraged.)
REWORK FOLLOW-UP	The author reworks all defects. Verification by the inspection moderator or the entire inspection team to assure that all fixes are effective and that no secondary defects have been introduced.



Hintergrund

Figure 1 Programming process



inspected. A clear statement of the project rules and changes to these rules along with faithful adherence to the rules go a long way toward practicing the required project discipline.

A prerequisite of process management is a clearly defined series of operations in the process (Figure 1). The miniprocess within each operation must also be clearly described for closer management. A clear statement of the criteria that must be satisfied to exit each operation is mandatory. This statement and accurate data collection, with the data clearly tied to trackable units of known size and collected from specific points in the process, are



[Fagan, Michael E. *Design and code inspections to reduce errors in program development*. IBM Systems Journal 15, 3 (September 1976), 182-211.]

Code-Durchsicht ::

Formalisierter Arbeitsschritt im Softwareentwicklungsprozess zur Aufdeckung von **Defekten** in bereits geschriebenem Quelltext.

Softwaredefekt ::

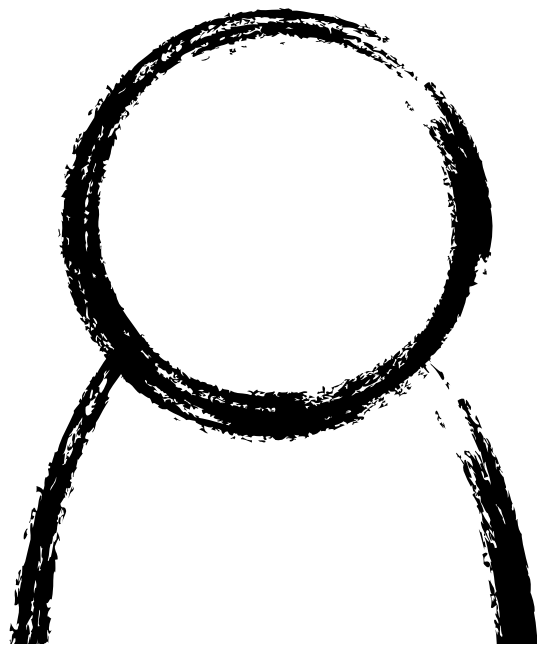
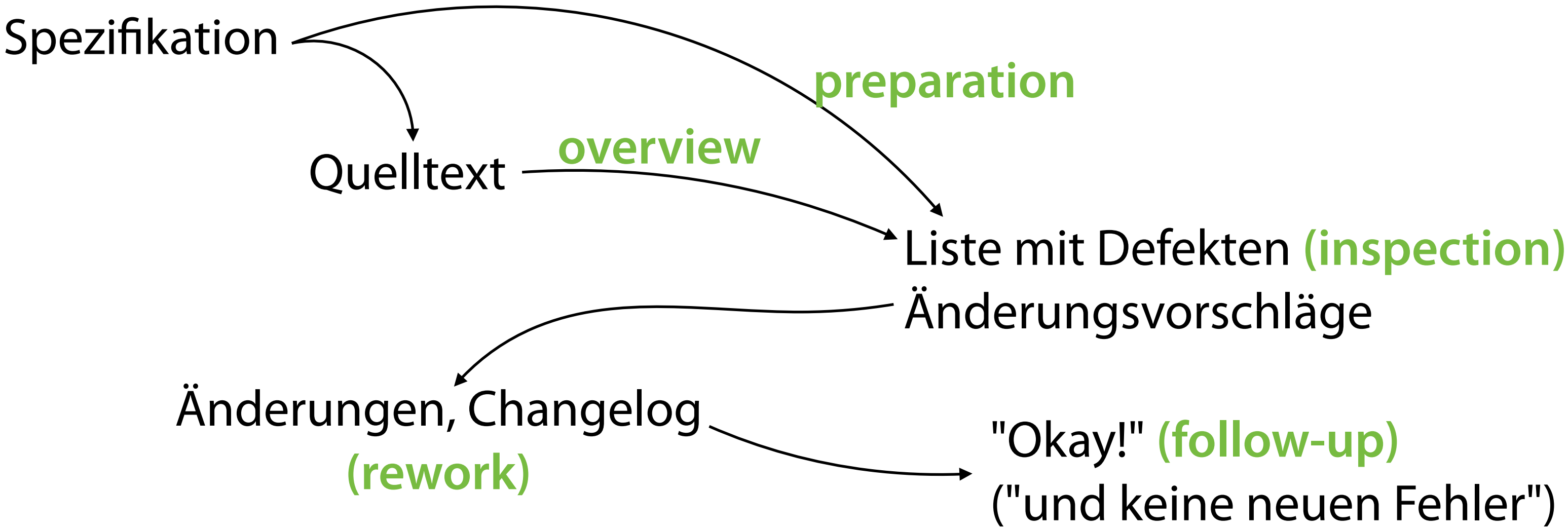
"A defect is an instance in which a requirement is not satisfied." (Fagan)

fehlende Übereinstimmung mit Spezifikation

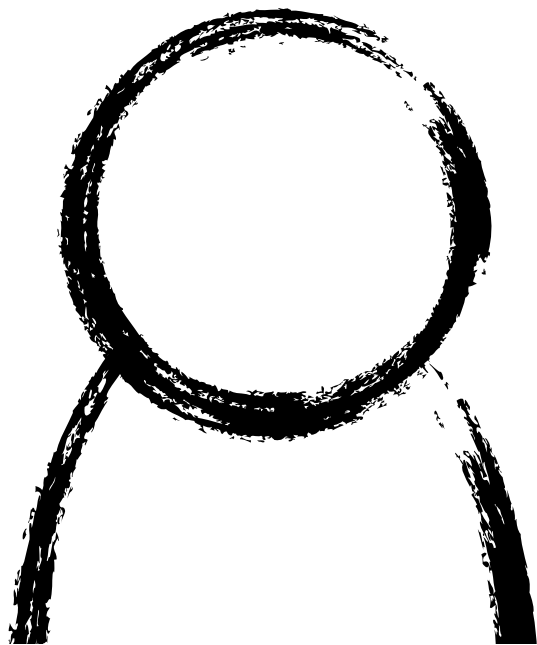


Weiterführende Begriffe (variierender Formalisationsgrad):
formal technical review; (code) inspection (IEEE 1028); walk-through

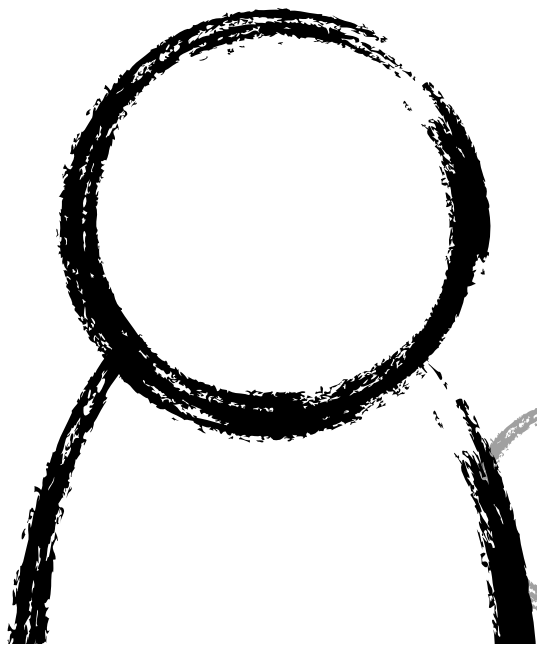
[Formalisierungsgrade variieren
in der Praxis. Was folgt sind Optionen]



Author



Moderator



Reader/Reviewer

(writer)

Rollen
& Phasen

RealDolos commented on Jul 1, 2017 • edited ▾

Let's look if it's actually invalid... Probably not because:

[...]

http://pubs.opengroup.org/onlinepubs/009695399/basedefs/xbd_chap03.html#tag_03_276

So in my humble opinion, it's a valid name and thus systemd has a bug here.


Even if you assume leading numbers are not allowed, systemd running the unit under root is a bug too. It should refuse to run the unit, in particular in the light of:

systemd will validate all configuration data you drop at it


-- @poettering #6237 (comment)


This is clearly not the case, `User=0day` is clearly not properly validated and silently ignored and it's still a bug (or it's just put into something like `atoi` and will try to execute `1day` as uid `1`, not sure about that).

So either way, there is a bug here.

 30

 8

 7

 10

Let's look if it's actually invalid... Probably not because:

[...]

http://pubs.opengroup.org/onlinepubs/009695399/basedefs/xbd_chap03.html#tag_03_276

So in my humble opinion, it's a valid name and thus systemd has a bug here.

Even if you assume leading numbers are not allowed, systemd running the unit under root is a bug too. It should refuse to run the unit, in particular in the light of:





systemd will validate all configuration data you drop at it

-- @poettering #6237 (comment)

This is clearly not the case, `User=0day` is clearly not properly validated and silently ignored and it's still a bug (or it's just put into something like `atoi` and will try to execute `1day` as uid `1`, not sure about that).

So either way, there is a bug here.

	30		8		7		10
--	----	---	---	---	---	---	----

 30	 8	 7	 10
--	---	---	--

© 2014 Pearson Education, Inc. or its affiliate(s). All rights reserved.

de [🔔 Issues 822](#) [🔗 Pull requests 85](#) [📊 Insights](#)

temd can't handle the process previlege that belongs to user name
tswith number, such as Oday #6237

sed mapleray opened this issue on Jun 29, 2017 · 37 comments

mapleray commented on Jun 29, 2017 • edited ▾

10.	Submission type
-----	-----------------

- Bug report

Actual behaviour	Expected behaviour
In case of bug report: Expected behaviour you didn't see	


The process started by systemd should be user privilege


In case of bug report: Unexpected behaviour you saw

The process started by systemd was root privilege

The process started by systemd was root privilege

[...]

 poettering commented on Jun 29, 2017 Member

 poettering commented on Jun 29, 2017 Member



Yes, as you found out "Oday" is not a valid username. I wonder which tool permitted you to create it in the first place. Note that not permitting numeric first characters helps to avoid ambiguities between numeric UID and textual user names.

[...]

So, yeah, I don't think there's anything to fix in systemd here. I understand this is annoying, but still: the username is clearly not valid.

[illegible]

  poettering closed this on Jun 29, 2017

  poettering added the **not-a-bug** label on Jun 29, 2017

Assignees

No one assigned

Labels

not-a-bug

Milestone

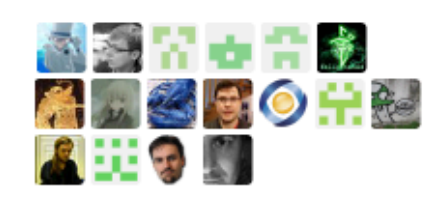
No milestone

Notifications

Subscribe

You're not receiving notifications from this thread.

17 participants



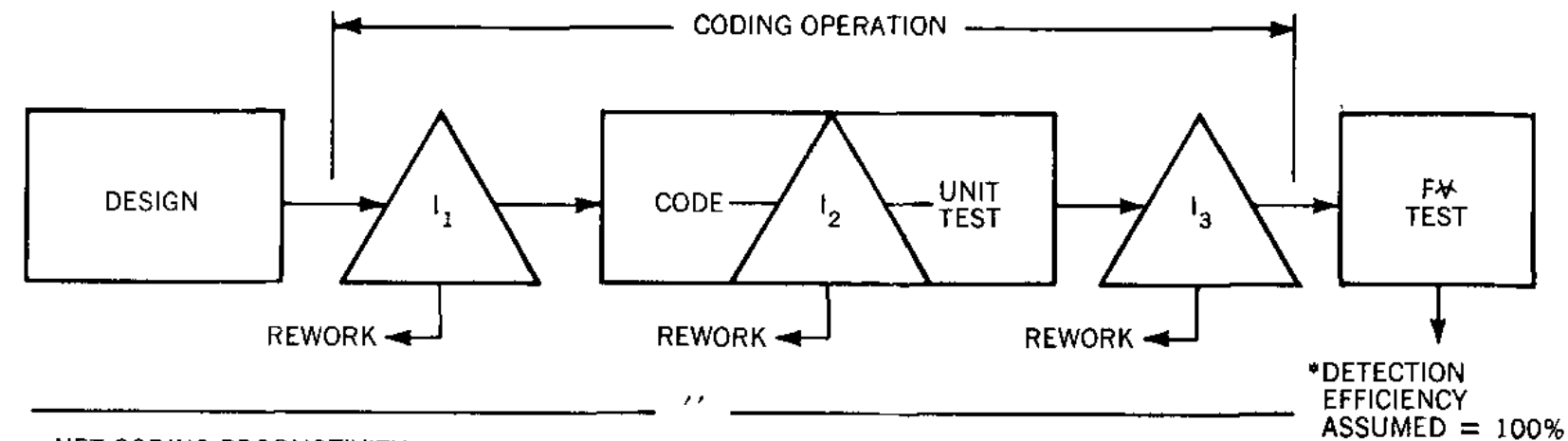
[<https://github.com/systemd/systemd/issues/6237>]

Fehlerkultur

Kritik muss **konstruktiv** und höflich sein ...

... und **dankend** angenommen werden.

Figure 2 A study of coding productivity



• NET CODING PRODUCTIVITY

$I_1 + I_2 + \cancel{I_3} \rightarrow 123\%$ ——— SAMPLE SHOWED 23% NET INCREASE
 $I_1 + \cancel{I_2} + \cancel{I_3} \rightarrow 112\%$ ———
 $\cancel{I_1} + \cancel{I_2} + \cancel{I_3} \rightarrow 100\%$ ——— 122% IN POST STUDY SAMPLE FROM NORMAL PRODUCTION (TO NORMALIZE FOR HAWTHORNE EFFECT)

• NET SAVINGS (PROGRAMMER HOURS/K) DUE TO:

$I_1: 94, I_2: 51, I_3: -20$

• REWORK (PROGRAMMER/HOURS/K. LOC) FROM:

$I_1: 78, I_2: 36, \quad -$

• QUALITY

AN INSPECTION SAMPLE HAD 38% FEWER ERRORS/K. LOC THAN A WALK-THROUGH SAMPLE DURING EQUIVALENT TESTING BETWEEN POST UNIT TEST AND SYSTEM TEST IN THIS STUDY.

Arbeitsweise der Gutachter

Ziel ist: Defekte finden.

Oft: Zurückgreifen auf Wissen um typische Fehler.

Figure 5 Examples of what to examine when looking for errors at I₁

I₁ Logic

Missing

1. Are All Constants Defined?
2. Are All Unique Values Explicitly Tested on Input Parameters?
3. Are Values Stored after They Are Calculated?
4. Are All Defaults Checked Explicitly Tested on Input Parameters?
5. If Character Strings Are Created Are They Complete, Are All Delimiters Shown?
6. If a Keyword Has Many Unique Values, Are They All Checked?
7. If a Queue Is Being Manipulated, Can the Execution Be Interrupted; If So, Is Queue Protected by a Locking Structure; Can Queue Be Destroyed Over an Interrupt?
8. Are Registers Being Restored on Exits?
9. In Queuing/Dequeuing Should Any Value Be Decrement/Incremented?
10. Are All Keywords Tested in Macro?
11. Are All Keyword Related Parameters Tested in Service Routine?
12. Are Queues Being Held in Isolation So That Subsequent Interrupting Requestors Are Receiving Spurious Returns Regarding the Held Queue?
13. Should any Registers Be Saved on Entry?
14. Are All Increment Counts Properly Initialized (0 or 1)?

Wrong

1. Are Absolutes Shown Where There Should Be Symbolics?
2. On Comparison of Two Bytes, Should All Bits Be Compared?
3. On Built Data Strings, Should They Be Character or Hex?
4. Are Internal Variables Unique or Confusing If Concatenated?

Extra

1. Are All Blocks Shown in Design Necessary or Are They Extraneous?

Ändern sich mit der Zeit
(Sprachen, Werkzeuge, Prozesse, Modultests, ...)

Code-Completion, Linter, IDEs und
z.B. Pair-Programming dienen als
kontinuierliches Code-Review

[Fagan, Michael, 1976]

- Lässt sich der Code übersetzen? Besteht er die definierten Testfälle?
- Hat der Gutachter den Code verstanden?
- Folgt der Code den etablierten Codekonventionen?
- Ist er verständlich kommentiert?
- Wird die Spezifikation erfüllt? Auch in Randfällen?
- Trifft der Code nicht-verallgemeinerbare Annahmen?
(z.B. Verwendung von Pfadnamen auf der Autorenmaschine)
- Werden Fehlerfälle korrekt berücksichtigt?
- Gibt es redundanten/unverständlichen Code?

A

ende