

QA, bugtracking, debugging, valgrind a profiling

Tomáš Švec, Jan Doležal, Jaroslav Dytrych a Petr Veigend

Fakulta informačních technologií Vysokého učení technického v Brně
Božetěchova 1/2. 612 66 Brno - Královo Pole
dytrych@fit.vut.cz veigend@fit.vut.cz



1. dubna 2026

Quality Assurance



„They’re only yours until they stop working, Bernie. Then they’re mine.“ – Theresa Cullen (Westworld)

- Proces zajišťování kvality
- Týká se všech fází vývoje, pro procesy i pro výstup
- Kvalitní == splňuje požadavky

Kontrola kvality procesů

- ISO 9001, CMM, SPICE
- certifikovat lze i proces výroby nekvalitních produktů

Kontrola kvality výstupu (software)

- code review
- testování
- QA inženýr kontroluje práci vývojářů

1 – Počáteční (Initial)

- Procesy jsou realizovány adhoc

2 – Opakované (Repeatable)

- Dodržuje se určitá kázeň nezbytná pro provádění základních opakovaných procesů

3 – Definovaná (Defined)

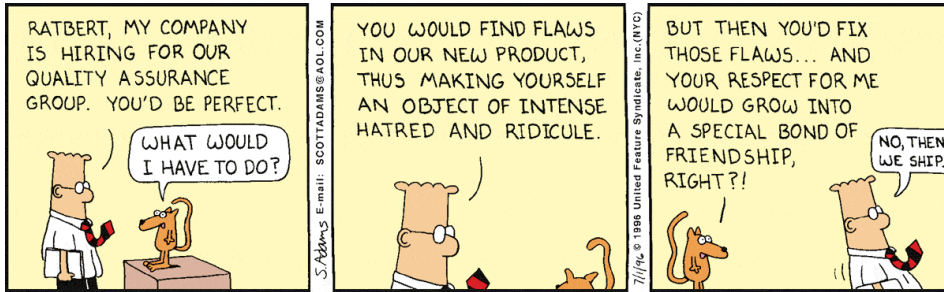
- Procesy organizace jsou zdokumentovány

4 – Řízená (Managed)

- Procesy jsou řízeny a provádí se měření jejich výkonnosti pomocí KPI (Key Performance Indicators)

5 – Optimalizovaná (Optimized)

- Procesy jsou trvale zlepšovány, existuje inovační cyklus na procesech a řízení

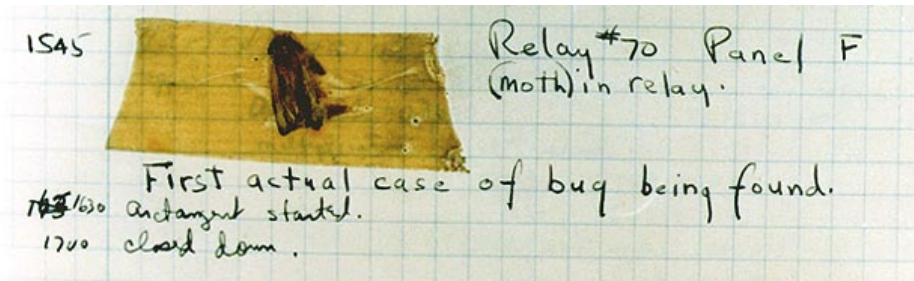


<https://www.youtube.com/watch?v=baY3SaIhf10>

Původ slova bug?

Thomas Edison v dopise z roku 1878. „*You were partly correct, I did find a 'bug' in my apparatus, but it was not in the telephone proper. It was of the genus 'callbellum.'* The insect appears to find conditions for its existence in all call apparatus of telephones.“

Historka o molu v relé počítače Mark II v roce 1947.



Mariner 1 (1962)

- Americká sonda určená k průzkumu Venuše
- Chyba při přepisu vzorce navigačního programu
- Z původního $\overline{R_n'}$ se během přepisu stalo R_n'
- Čára znamená „vyhlazená data“
(nevýznamné odchylky by neměly být brány v potaz)
- Ztráta 18,5 milionů dolarů
(cca 150 milionů dnešních dolarů)

<https://www.wired.com/2009/07/dayintech-0722/>



Mars Climate Orbiter (1999)

- Software od Lockheed Martin předával výsledky v imperiálních jednotkách
- Software od NASA je očekával v jednotkách SI
- Výsledkem byla chybně vypočítaná trajektorie vstupu na oběžnou dráhu (po 286 dnech letu)
- Cena: 328,6 milionů dolarů (cca 507 milionů dnešních dolarů)

<https://kosmonautix.cz/2015/08/top-5-faily-a-chyby-v-kosmonautice/>

PSS! HEY KID

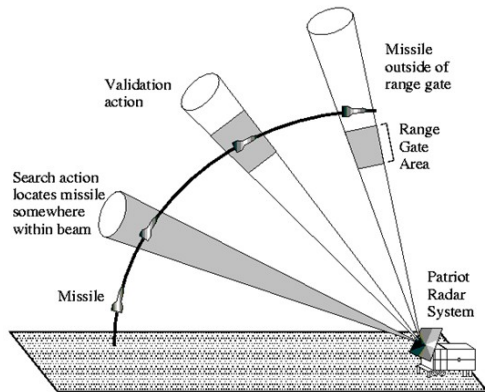
WANNA TRY
SOME
INTERNATIONAL
STANDARDS?



Protiraketové střely Patriot (25. 2. 1991)

- 28 mrtvých, 98 zraněných
- systémové hodiny měřily čas v desetinách sekundy (jako celé číslo)
- čas se pak převáděl na desetinné číslo (tzn. vydělil se 10) na 24 bitech
- po 100 hodinách odchylka 0,34 s
- za tuto dobu irácká raketa Scud uletěla cca 800 metrů (a proto ji Patriot minul)

https://medium.com/@emma_programmer/r-17-vs-patriot-a-rounding-issue-d6b8021334e2
<https://barrgroup.com/blog/lethal-software-defects-patriot-missile-failure>



USS Yorktown CG-48 (1997)

- Smart Ship, síť 27 počítačů
- Po zadání nuly na nesprávné místo v datech došlo k dělení nulou, přetečení bufferu a výpadku na 2,5 hodiny



<https://www.wired.com/1998/07/sunk-by-windows-nt/>

https://medium.com/@bishr_tabbaa/when-smart-ships-divide-by-zero-uss-yorktown-4e53837f75b2

Therac-25 (80. léta), <https://www.youtube.com/watch?v=Ap0orGCiou8>

- Minimálně 5 mrtvých (údajně až 22)
- Obsluha omylem zvolila použití vysokoenergetického paprsku, po opravě na nízkoenergetický se ale přesto spustil vysokoenergetický paprsek
- Chybějící code review
- Chybějící hardwarové pojistky (odstraněny při přechodu na čistě SW řízení)
- První testy proběhly až v nemocnici
- Systém poznal, že něco nesedí, ale chyby byly časté a šlo je ignorovat
- Race condition, pokud byl operátor moc rychlý
 - jedna proměnná pro více účelů

<https://medium.com/enjoytechweb/the-importance-of-software-testing-f4904753c8e>



Boeing 787 Dreamliner

- Po 248 dnech přejdou elektrické generátory do nouzového režimu (2015)
- Po 22 dnech se bez varování restartují všechny tři řídicí moduly (2016)



<https://www.nytimes.com/2015/05/01/business/faa-orders-fix-for-possible-power-loss-in-boeing-787.html>

Boeing 737 MAX, <https://www.youtube.com/watch?v=NDEkH0zd3F8>


- 2 nehody v rozmezí 5 měsíců, 346 mrtvých (2018-2019)
- Maneuvering Characteristics Augmentation System (MCAS)
- Může způsobit neočekávaný let střemhlav – chyběl v manuálech a školení
- Certifikace FAA – kroky delegované Boeingu
- Cena cca 18,6 miliard dolarů (březen 2020)



https://www.idnes.cz/technet/technika/faa-boeing-737-max-regulace-certifikace-mcas.A190730_044921_tec_technika_pka


Sčítání lidu 2021!

- Je potřeba sečíst přes 10 000 000 lidí za 14 dní
- Dopady na důvěře v IT kompetence
- „Robotické testování“ neodhalilo skutečné chování uživatelů
- Chyba v modulu pro vyhledávání adres
- Výpadek systému v řádu jednotek hodin

 **čsú** @statistickyurad · 27. 3. 2021

Odpověď uživateli @statistickyurad

Online sčítání je opět funkční. Náš dodavatel @OKsystemCZ provedl opravy a aplikaci plně obnovil. Zároveň jsme přijali další opatření k posílení kapacity systému na vyšší zátěž.
[▶ Více se dozvíte na \[scitani.cz/csu/scitani2021...\]\(https://scitani.cz/csu/scitani2021...\)](#)

 **čsú** @statistickyurad

Systém je v současnosti velmi vytižen, doporučujeme sečíst se později. Zájem o sčítání online je v tuto chvíli enormní (přibližně 170 tis. lidí najednou). Omlouváme se za případná zdržení a děkujeme za trpělivost.

6:51 odp. · 27. 3. 2021

19 88 Sdílet tento Tweet

Omlouváme se za dočasnou nedostupnost elektronického sčítacího formuláře, na zprovoznění se pracuje. Děkujeme za pochopení.





Sčítání 2021 Aktuality Časté dotazy Nápověda Ke stažení Kontakty Čeština 🔍

[Jak se sečíst](#) [Průběh sčítání](#) [Přínos sčítání](#) [Ochrana dat](#) [Výsledky](#)

Vážení uživatelé,

omlouváme prosím dočasnou nedostupnost aplikace pro vyplnění elektronického sčítacího formuláře. Všechny informace o Sčítání lidu, domů a bytů 2021 najdete na stránkách www.scitani.cz.

Děkujeme za pochopení.

[Mapa webu](#) [Ochrana osobních údajů](#)
[Přístupnost](#) [Podmínky užívání](#)

dat

Log4j v prosinci 2021

- Logovací knihovna na spoustě veřejných serverů (open source)
- Možnost získat kontrolu nad CMD
- Apple, Amazon, Cisco, IBM, Microsoft
- Je nutné vše patchovat
- ... a pak znovu.

Chyby jsou **nevyhnutelné**.

- vytvořit bezchybný kód je téměř nemožné
- pro většinu aplikací není nutná absolutní bezchybnost
- ale jsou výjimky: zdravotnictví, vojenství, aerospace

Péče věnovaná testování by měla být úměrná náročnosti, důležitosti a nebezpečnosti zakázky.

Metodologie: extrémní programování (XP), programování řízené testy (TDD), lean development, Crystal, Adaptive Software Development, ...

Pád programu

- i laik pozná, že je něco špatně

Nekonečný cyklus či rekurze

- nemusí být jasné, jestli program něco dělá

Chyby ve výsledných hodnotách

- program zdánlivě funguje správně

Syntaktické chyby

- prohřešky proti gramatice jazyka
- program nelze přeložit
- u interpretovaných jazyků se odhalí až za běhu
- chytrý editor je označí už během psaní

Sémantické chyby

- program nedělá, co má
- obtížná autodetekce



<https://xkcd.com/371/>

Syntaktické:

- chybějící středník či závorka (v Pythonu odsazení)
- překlep v názvu proměnné, funkce, ...

Sémantické:

- chybný přístup do paměti
- dělení nulou
- chyba o jedničku
- přetečení
- nekonečný cyklus
- chyby v synchronizaci vláken

- Textové = překlepy
- Pády aplikace → debugger / valgrind
 - segmentation fault, buffer overflow ...
- Úniky paměti (memory leak) → valgrind
- Problémy s výkonem → profiler / vyšší výkon v cloudu?
- Neočekávané chování
 - program dělá něco jiného, než by měl
 - chyba v programu nebo dokumentaci?
- Bezpečnostní problémy
 - např. neošetřené vstupy (SQL injection, CSRF, XSS, ...)

Bug tracking

Také Issue Tracking, Ticket System . . .

- Aby mohl vývojář vyřešit problém, musí o něm vědět
- Více kódu → více chyb → potřeba lepší evidence

- Hlášení chyb a požadavků
- Přiřazování vývojářům či testerům
- Sledování životního cyklu chyb
- Sledování závislosti chyb
- Lze provázat s verzovacím systémem (např. GitHub)

- JIRA, Azure DevOps Server, Bugzilla, Trac, Redmine, MantisBT . . .

Podle závažnosti:

- blokující
- kritický
- významný
- normální
- méně důležitý
- triviální (drobnosti, chyby v překladu, ...)
- rozšíření (požadavek na vylepšení) – „Change Requests“ (CRs)

Požadavky jsou zpracovávány dle priority

- dle závažnosti, množství výskytů, ...

Závažnost (severity)

- Označuje dopad výskytu chyby
- V různých organizacích různé úrovně (viz následující slide)
- Většinou lze určit podle sady pravidel
 - „Existuje workaround?“
 - „Postihuje určité procento uživatelů?“
 - „Ovlivňuje klíčovou funkcionalitu systému?“

Priorita (priority)

- Označuje jak brzy se s chybou vypořádáme
- Můžou existovat dvě chyby se stejnou závažností, ale v různých modulech
- Opravě kterého modulu pak dáme větší přednost?
- Většinou se určuje po dohodě s týmem/zákazníkem

- S1 Blocker – ovlivňuje klíčovou funkcionalitu nebo data, brání v dalším testování, nelze obejít (např. nefunguje přihlášení)
- S2 Critical – ovlivňuje klíčovou funkcionalitu nebo data, nelze obejít (např. problémy s instalací, nebo selhání klíčové funkcionality)
- S3 Major – ovlivňuje důležitou funkcionalitu nebo data, lze složitě obejít (např. nejde založit uživatele, lze ručně v DB), ale zbytek aplikace je použitelný
- S4 Minor – ovlivňuje vedlejší funkcionalitu nebo méně důležitá data, může způsobit neočekávané chování, lze snadno obejít (např. v jedné obrazovce nejde změnit přezdívka)
- S5 Low/Trivial – neovlivňuje funkcionalitu ani data, není třeba obcházet (např. překlep, nezarovnané popisky)

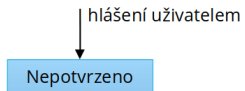
<https://www.qamadness.com/bug-severity-vs-priority/>

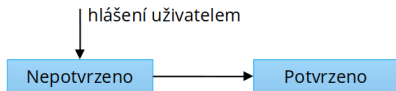
Hlášení chyby (požadavku) by mělo obsahovat maximum relevantních informací:

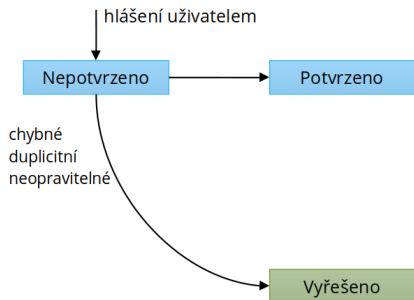
- název požadavku
- stručný popis
- verze SW
- verze operačního systému, knihoven, platforma, . . .
- postup, jak chybu reprodukovat (video?)
- popis očekávaného chování
- popis skutečného chování
- kontaktní údaje

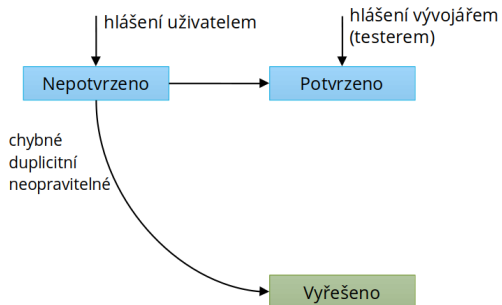
Hlášení chyby (požadavku) by mělo obsahovat maximum relevantních informací:

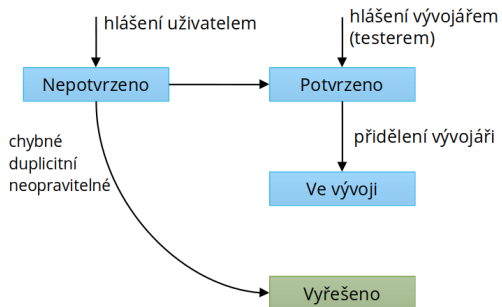
- Nicneřikající popis
 - „CHYBA!“
 - „Systém nefunguje“
 - „Nízký výkon aplikace“
- Shlukování více chyb do jedné – pro každou zvláštní ticket
- Neuvádí se, na jakém prostředí se chyba projevuje
- Nedostatek relevantních informací
- Špatně nastavená závažnost/priorita (barva menu je jistě kritická)

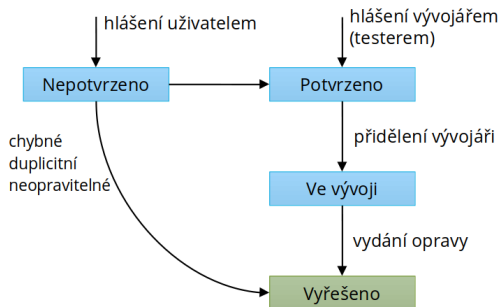


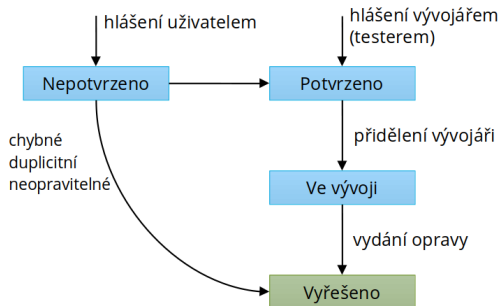






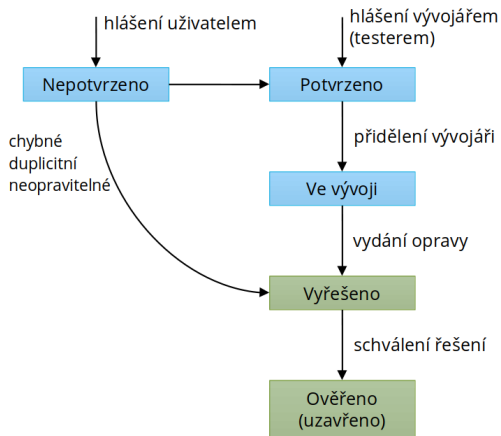






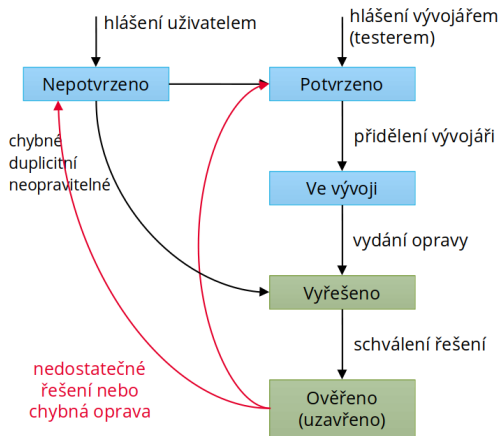
Možná řešení:

- chybné
- opraveno
- duplicitní
- neopravitelné (won't fix)
- rozpracováno
- později



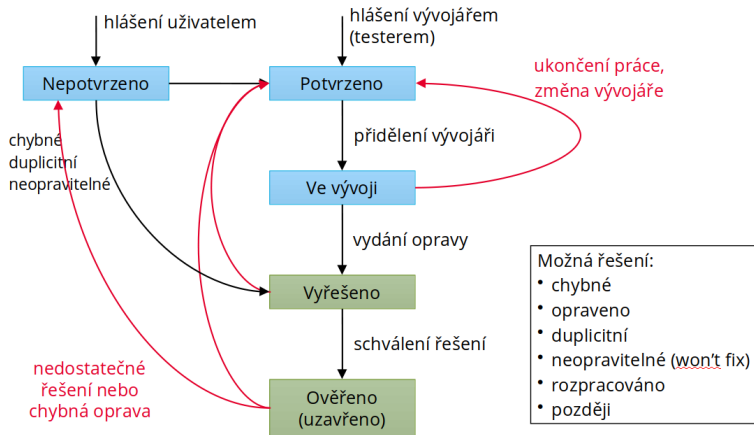
Možná řešení:

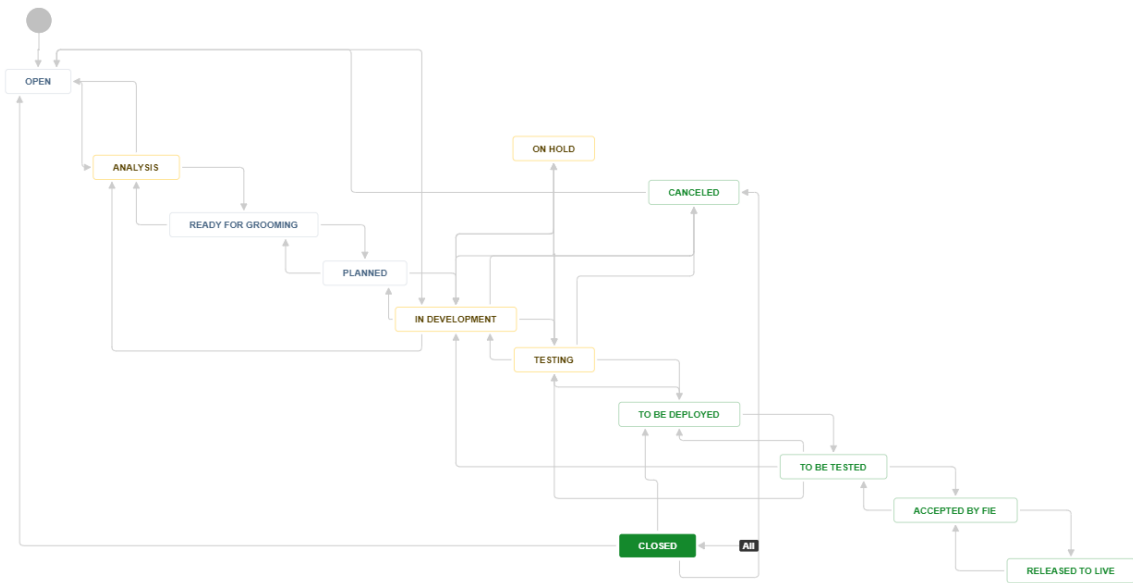
- chybné
- opraveno
- duplicitní
- neopravitelné (won't fix)
- rozpracováno
- později



Možná řešení:

- chybné
- opraveno
- duplicitní
- neopravitelné (won't fix)
- rozpracováno
- později







Marker / MAR-131

[Pricing] - Update the price to \$29

[Edit](#) [Comment](#) [Assign](#) [To Do](#) [In Progress](#) [Workflow](#) [Admin](#)

Details

Type: **Bug** Status: **TO DO** [\(View workflow\)](#)
Priority: **High** Resolution: **Unresolved**
Labels: **None**
Environment: **> — Browser Chrome 54.0.2840.71 Screen Size 1920 x 1200 Viewport Size 1607 x 920 Zoom L...**

Description

Summary:

The price mentioned on the pricing page is not correct

Steps to Reproduce:

Go to the pricing page

Expected Results

The price for the basic plan should be \$29

Actual Results:

The price for the basic plan is currently \$25

Source URL: <https://www.shopify.com/pricing>

Attachments

Drop files to attach, or browse.



People

Assignee: [gary](#)
[Assign to me](#)
Reporter: [Christophe Han](#)
Votes: 0
Watchers: [Stop watching th](#)

Dates

Created: 1 minute ago
Updated: 1 minute ago

Agile

[View on Board](#)

HipChat discussions

Do you want to discuss this issue? Connect

[Connect](#) [Dismiss](#)

Jak to bude s kachničkou? #3

[New issue](#)

Redak37 opened this issue 14 days ago · 1 comment



Redak37 commented 14 days ago



Jak to bude tento semestr, je nějaký plán, od kdy bude zase normálně fungovat bar a tak podobně?



2



Toaster192 commented 2 days ago

Member



Potřebujeme zlepšit evidenci pohybu věcí na baru

proto pracujeme na novem systemu který potřebujeme prve dodelat

viz.:

Jsi frontend vývojář? Otravuje tě, že Kachna je otevířeva v provizorním režimu a chceš pomoci?

Hledáme pomoc s implementací webové aplikace pro informační systém postavený na REST API (zdokumentovaném pomocí OpenAPI 3). Pivní odměna jistá (případně dle domluvy v rámci možnosti). V případě zájmu nás neváhej kontaktovat (xbudis02@stud.fit.vutbr.cz nebo prostřednictvím Discordu SU).

Jde na poměry SU o velký projekt, který byl dlouho odkládán, a proto jsme se do toho rozhodli "hodit vidle" aby se konečně realizoval.



michkot added **question** **SU / Kachna** labels 20 hours ago



Write

Preview

AA B i ☰ ☹ ↺ ↻ ⋮ ☰ ☹ @ 📌 ↶

Leave a comment

Attach files by dragging & dropping, selecting or pasting them.

Styling with Markdown is supported

Comment

Assignees

No one assigned

Labels

SU / Kachna

question

Projects

None yet

Milestone

No milestone

Notifications

Subscribe

You're not receiving notifications from this thread.

3 participants



Debugging

You can't keep doing the same
thing and expect different results

LET ME INTRODUCE YOU



TO DEBUGGING

Postup v případě řešení nalezeného problému:

- 1 nalezení chyby (vývojář, tester, uživatel)
- 2 reprodukce chyby, napsání testu
- 3 zjednodušení problému na to důležité (jednodušší testování)
- 4 vytipování možných příčin
- 5 zaměření se na pravděpodobné příčiny (většinou bývá příčina zřejmá)
- 6 identifikace příčin
- 7 oprava chyby
- 8 testování (nejen opravy chyby, nesmíme zapomenout na **regresní testy** – co když jsme při opravě chyby pokazili něco dalšího?)
- 9 změna dokumentace

Např. `ptrace`

Umožňuje

- krokování programu
- sledování hodnot proměnných (registrů CPU, RAM, ...)
- změnu hodnot proměnných
- zastavení programu na určeném místě (breakpoint)
 - nepodmíněně
 - podmíněně
 - při změně hodnoty proměnné (watchpoint)

Při překladau je nutno přidat ladící informace

- jména proměnných, mapování instrukcí na místo ve zdrojovém kódu, ...
- u gcc parametr `-g`

GDB – The GNU Project Debugger

- Konzolové rozhraní, standard pro UNIX-like systémy
- Ada, C, C++, Objective-C, Pascal, ...
- příkaz `tui enable` (Text User Interface)

DDD – Data Display Debugger

- grafická nadstavba nad konzolovými debugery (GDB, DBX, WDB, Ladebug, ...)
- umí zobrazit grafy na základě dat programu

Prakticky každé IDE obsahuje debugger

- třeba i jako nadstavbu nad GDB

- textové rozhraní, velké množství funkcí
- HW i SW debugování
- podporuje řadu procesorů a jazyků
- vzdálené ladění (po síti, rs232) – embedded systémy
- simulátor různých procesorů (bez periférií)
- breakpointy, watchpointy, krokování (i zpět)
- podporuje programy s vlákny
- existují nadstavby (DDD, Eclipse)

<https://www.sourceware.org/gdb/documentation/>

<https://www.root.cz/clanky/trasovani-a-ladeni-nativnich-aplikaci-v-linuxu-pouziti-gdb-a-jeho-nadstaveb/>

```
$ gcc ./segfault.c -o segfault -g  
$ gdb ./segfault
```

```
GNU gdb (GDB) 7.12
```

```
...
```

```
Reading symbols from ./segfault...done.  
(gdb)
```

```
$ gcc ./segfault.c -o segfault -g
$ gdb ./segfault
```

```
GNU gdb (GDB) 7.12
```

```
...
```

```
Reading symbols from ./segfault...done.
```

```
(gdb) run
```

```
Starting program: ~/segfault
```

```
Program received signal SIGSEGV, Segmentation fault.
```

```
0x00007ffff7aca301 in __strlen_sse2 () from /lib64/libc.so.6
```

```
(gdb)
```

```
$ gcc ./segfault.c -o segfault -g
$ gdb ./segfault
```

```
GNU gdb (GDB) 7.12
```

```
...
```

```
Reading symbols from ./segfault...done.
```

```
(gdb) run
```

```
Starting program: ~/segfault
```

```
Program received signal SIGSEGV, Segmentation fault.
```

```
0x00007ffff7aca301 in __strlen_sse2() from /lib64/libc.so.6
```

```
(gdb) backtrace
```

```
#0 0x00007ffff7aca301 in __strlen_sse2() from /lib64/libc.so.6
```

```
#1 0x00007ffff7ab199b in puts () from /lib64/libc.so.6
```

```
#2 0x0000000000400544 in main () at ./segfault.c:6
```

Základní příkazy GDB:

- **help (command)**
- **run** – spuštění programu
- **backtrace** – výpis obsahu zásobníku (call stack)
- **step** – postup o jeden krok (step into v CodeBlocks)
- **next** – krok, ale nevstoupí do cyklů a funkcí (step over)
- **break funkce** – breakpoint při zavolání funkce
- **break main.c:6** – breakpoint na konkrétním řádku
- **break main.c:6 if i>=10** – podmíněný breakpoint
- **watch myvar** – zastavení při změně hodnoty `myvar`
- **print myvar** – výpis hodnoty `myvar`
- **quit**

Funguje doplňování tabulátorem, šipky a zkratky (`bt` = backtrace)

- grafická nadstavba nad různými debuggery

DDO: /home/tester/xxx/factorial.c

```

17 (
18     long n1 = 0;
19     long n2 = 10;
20     long n;
21     for (n=n1; n<n2; n++)
22     (
23         printf("1!d = %ld\n", n, factorial(n));
24     )
25
26     return 0;

```

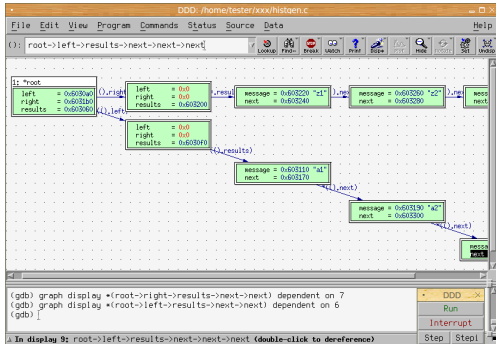
Assembly view (gdb):

```

0:000000000040956c <+16>: movq $0xa, %0x8(%rip)
0:0000000000409576 <+24>: mov  %rax,%0x10(%rip),%rax
0:000000000040957a <+28>: mov  %rax,%0x10(%rip)
0:000000000040957e <+32>: jmp  0x40958a (main+76)
0:0000000000409580 <+34>: mov  %rax,%0x10(%rip),%rax
0:0000000000409584 <+38>: mov  %rax,%rdi
0:0000000000409587 <+41>: callq 0x40952d (factorial)
0:000000000040958c <+46>: mov  %rax,%rdx
0:0000000000409591 <+49>: mov  %0x10(%rip),%rax
0:0000000000409593 <+53>: mov  %rax,%rsi
0:0000000000409596 <+56>: mov  %0x409544,%edi
0:0000000000409599 <+61>: mov  %0x0,%eax
0:00000000004095a0 <+66>: callq 0x409418 (printf@plt)
0:00000000004095a5 <+71>: addq $0x1,%0x10(%rip)
0:00000000004095aa <+76>: mov  %0x10(%rip),%rax
0:00000000004095ae <+80>: cmp  %0x10(%rip),%rax
0:00000000004095b2 <+84>: jle  0x40958a (main+34)
0:00000000004095b4 <+86>: mov  %0x0,%eax

```

(gdb) break 1d
Function '1d' not defined.
(gdb) break factorial.c:26
Breakpoint 2 at 0x40958a: file factorial.c, line 26.
(gdb) |
Function '1d' not defined.



<https://www.gnu.org/software/ddd/manual/>

<https://mojefedora.cz/debuggery-a-jejich-nadstavby-v-linuxu-2-cast/>

...je nejvíc po ruce

The screenshot shows a code editor with a JavaScript file named `app.js`. The code defines an Express.js application with a REST API for tweets. A breakpoint is set at line 22, which is highlighted in red. The debugger is active, showing the current state of variables in the `scope` window. The `newTweet` object is visible, with `sentiment` set to `'Amanda Silver'`. The `level` property is an object with `percentage` set to `NaN` and `faceImage` set to `"/a"`. The `sentimentWithLevel` array is also visible, containing the current tweet object. The `CALL STACK` on the left shows the execution path from the `anonymous function` to `init inspector_async...`, `emitInitNative async...`, `handle layer.js 95:5`, `next route.js 137:13`, and `dispatch route.js`. The `DEBUG CONSOLE` at the bottom shows the message `app listening on port: 3000`. The status bar at the bottom indicates the current position is `Ln 24, Col 33` in `app.js:37`.

„printf debugging“

- výpis „jsem zde“, hodnoty proměnných, všeho zajímavého (pozor na ... ne úplně slušná slova ...)
- pomocí mohou i makra `__FILE__`, `__LINE__`, výpis stack trace, ...
- může se hodit takticky umístěný `if`, `assert`, `break`, `exit`, ...

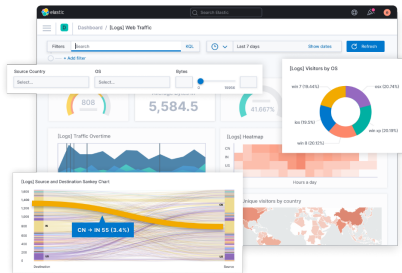
```
$time = $xml->location[0]->time[0];

$phase = $time->moonphase[0]['desc'];
dump($phase);
dump($time);
dump($time->moonphase[0]);
dump($time->moonphase[0]['desc']);
if (preg_match('#\\(([^)]+)\\)#', $phase, $m)) {
    dump('matched');
    $phase = $m[1];
}
dump($phase);
```



Logování

- chybu lze najít i zpětně (když se nikdo neřídíval)
- log lze odeslat technické podpoře (i automaticky)
- logování může ovlivnit chování programu
 - pravděpodobnost vzniku race condition
 - zpomalení
 - může snadno dojít místo na disku, hlavně u vestavěných systémů (logrotate, logger)
- uživatel se zobrazí stručné chybové hlášení
- vygeneruje se log a odešle se vývojáři (e-mailem, přes logovací službu)



Agregace v nástrojích – např. Kibana

Je třeba hledání chyb co nejvíce usnadnit:

- jasné názvy proměnných
- dodržování konvence pojmenování – Coding Standards¹!
- přehledné a konzistentní formátování
- dostatečně komentovaný kód
- seskupování kódu do skupin
- neduplikovat kód (Don't repeat yourself = DRY)
- nemít příliš hluboké zanoření (if, for, while)
- dodržovat best practices pro daný jazyk
 - Google Style Guide, PEP-8 pro Python, PSR-12 pro PHP, ...
- mít zapnutá varování překladače

¹<https://google.github.io/styleguide/>

- hledá problémy v kódu bez jeho spuštění
- může detekovat více chyb než překladač
- také jako plugin do editoru či IDE

Lze použít na:

- typová kontrola, neinicializovaná data
- kontrola indexování polí
- přenositelnost konstrukcí
- pravidla pro časté chyby `if (confirmation = "yes") format_hdd();`
- nedodržení stylu formátování
- vlastní pravidla

Pro C např.: Lint, cppcheck, mygcc, codan, ...

- **-g**: vytváří ladící informace pro debugger
- **-ggdb**: rozšíření pro GDB
- **-Wall**: zapnutí všech varování
- **-Wextra**: zapnutí dalších varování
- **-pedantic**: striktně vyžaduje doržování normy (-std=xxx, -ansi)

<https://gcc.gnu.org/onlinedocs/gcc/Debugging-Options.html>

<https://gcc.gnu.org/onlinedocs/gcc/Warning-Options.html>

Chyby mohou mít i exotické příčiny

- chyba v překladači
- dokonce i chyba v procesoru <https://blog.cloudflare.com/however-improbable-the-story-of-a-processor-bug/>

Chyba se nemusí projevit během ladění (race condition nevznikne, protože kód běží pomaleji, lze odhalit pomocí `strace`).

Pozor na optimalizace (je nutné důkladně testovat, jestli něco nerozbijí).

Důležité je opravovat příčinu a ne následek, **nejlepší je chybám předcházet.**

Valgrind



- Valgrind = Posvátná brána do Valhally
 - Palác boha Ódina, který sem svolává padlé bojovníky, aby zde trénovali na poslední bitvu Ragnarök
- Původní název Heimdall
 - Strážce nordických bohů, který vidí stovky mil daleko ve dne i v noci, slyší růst trávu i vlnu na hřbetech ovcí
 - ... ale již existoval balíček s tímto názvem
- Sada nástrojů pro ladění a profilování programů

- pouze pro unixové systémy (Windows – WSL)
- v podstatě virtuální stroj
 - analyzovaný program je oddělený od procesoru
 - podstatně pomalejší běh programu (4-5krát)
- Umožňuje připojení GDB k běžícímu programu

Skládá se z několika nástrojů:

- Memcheck – správa paměti, nejpoužívanější, používali jste v IZP
- Callgrind – profilování
- Helgrind – detekce race conditions
- Cachegrind – profilování cache CPU

Existují i externě vyvíjené nástroje.

Memcheck detekuje:

- použití neinicializované paměti
- čtení/zápis do uvolněné paměti
- čtení/zápis mimo alokovaný blok
- čtení/zápis nad vrchol zásobníku
- úniky paměti (memory leaks)
- neshody v použití malloc / new vs. free /delete
- špatné použití POSIX knihovny pthreads
- překrytí ukazatelů v memcpy



A TODO buys you time.

Čtení z neplatné adresy:

```
Invalid read of size 4
at 0x40F6BBCC: (within /usr/lib/libpng.so.2.1.0.9)
by 0x40F6B804: (within /usr/lib/libpng.so.2.1.0.9)
by 0x40B07FF4: read_png_image(QImageIO *)
(kernel/qpngio.cpp:326)
by 0x40AC751B: QImageIO::read() (kernel/qimage.cpp:3621)
Address 0xBFFFF0E0 is is 0 bytes after
a block of size 40 alloc'd
```

Zároveň se snaží zjistit, kde se neplatná adresa vzala:

- již uvolněná paměť – hlásí, kde se volalo free
- adresa těsně za alokovaným blokem (chyba o jedničku?)

Použití neinicializované paměti:

```
Conditional jump or move depends on uninitialised value(s)
at 0x402DFA94: _IO_vfprintf (_itoa.h:49)
by 0x402E8476: _IO_printf (printf.c:36)
by 0x8048472: main (tests/manuell.c:8)
```

Nehlásí kopírování neinicializovaných dat, ale až jejich použití, které může mít vliv na funkci programu.

Úniky paměti:

LEAK SUMMARY:

```
definitely lost: 48 bytes in 3 blocks.  
indirectly lost: 32 bytes in 2 blocks.  
possibly lost: 96 bytes in 6 blocks.  
still reachable: 64 bytes in 4 blocks.  
suppressed: 0 bytes in 0 blocks.
```

S parametrem **--leak-check=full** je výpis podrobnější:

```
8 bytes in 1 blocks are definitely lost in loss record 1 of 14
at 0x.....: malloc (vg_replace_malloc.c:...)
by 0x.....: mk (leak-tree.c:11)
by 0x.....: main (leak-tree.c:39)
```

```
88 (8 direct, 80 indirect) bytes in 1 blocks are definitely lost
in loss record 13 of 14
at 0x.....: malloc (vg_replace_malloc.c:...)
by 0x.....: mk (leak-tree.c:11)
by 0x.....: main (leak-tree.c:25)
```

Pro zobrazení čísel řádků je potřeba překládat s ladícími informacemi (**-g**).

- je dobré chyby opravovat shora dolů
 - chyby níže ve výpisu mohou být jen důsledkem předchozích
- některé chyby jsou v systémových knihovnách
 - není třeba se jimi trápit
 - Valgrind je umí skrýt
- Memcheck není stoprocentní!
 - Například chyba o jedničku v poli alokovaném na zásobníku může přepsat jinou lokální proměnou
 - Ale z pohledu Valgrindu jde o korektní přístup do paměti – neví, že program pracuje s polem
 - Je vhodný pro programy, ve kterých alokujete paměť na hromadě.
- ulimit², stress³ – další možnosti, jak testovat

²<https://man7.org/linux/man-pages/man3/ulimit.3.html>

³<https://linux.die.net/man/1/stress>

Profiling

Using a profiler



Using the time command



Using a stopwatch



Counting the seconds



Using an hourglass



- program funguje **správně**, ale **pomalu**
- malé urychlení jedné malé smyčky může způsobit velké urychlení celého programu
- pravidlo 80/20 (80 % strojového času se stráví nad 20 % kódu)
- profiler pomáhá identifikovat místa v programu, kde se spotřebuje nejvíce strojového času

Postup:

① Měření

- získání údajů o běžícím programu
- počet vyvolání funkcí, počet iterací cyklů, čas strávený v jednotlivých částech kódu, čekání na I/O, ...

② Analýza

- statistické vyhodnocení naměřených dat
- vizualizace pomocí tabulek a grafů

③ Optimalizace

Sampling (statistický přístup)

- periodické přerušení, ve kterém se zaznamená aktuální poloha v programu
- nepřesné, ale nezpomaluje tolik běh programu
- např. AMD CodeAnalyst, Apple Shark, Intel Vtune

Instrumentace programu

- do programu se vloží volání speciální funkce
- více ovlivňuje rychlost programu
- některé chyby se nemusí projevit, jiné se naopak začnou projevovat

Flat profile

- čas strávený v jednotlivých funkcích
- počet volání

Graf volání (Call graph)

- pro každou funkci: odkud byla volána, jaké funkce volala
- jak dlouho každé volání funkce trvalo

Anotovaný kód (Annotated source)

- ke každému řádku kódu je přidán počet vykonání

- kombinuje statistický přístup s instrumentací
- čas strávený v jednotlivých funkcích pomocí periodického sledování
 - čas běhu programu by měl být výrazně vyšší než perioda vzorkování (1×10^{-2} s)
- počet volání funkcí pomocí instrumentace
- výstup: flat profile, graf volání

```
$ gcc -Wall -Wextra -O2 -g -pg ./program.c -o program
$ ./program
$ ls
program gmon.out
$ gprof program gmon.out > gprof-report.txt
```

- soubor `gmon.out` vznikne v pracovním adresáři
- každý modul je třeba přeložit pro profilování (`-pg`)

Pro zvýšení přesnosti lze zkombinovat více běhů:

```
gcc -Wall -Wextra -O2 -g -pg ./program.c -o program
```

```
# první běh
```

```
$ ./program
```

```
$ mv gmon.out gmon.sum
```

```
# opakuj n-krát
```

```
$ ./program
```

```
$ gprof -s program gmon.out gmon.sum
```

```
# souhrnné výsledky
```

```
$ gprof program gmon.sum > gprof-report.txt
```

Each sample counts as 0.01 seconds.

% cumulative		self		self	total	
time	seconds	seconds	calls	s/call	s/call	name
31.75	9.90	9.90	1	9.90	9.90	new_func1
31.62	19.76	9.86	1	9.86	9.86	func2
22.17	26.68	6.91	1	6.91	16.82	func1
0.23	26.75	0.07				main

Časy které nejsou o moc větší než vzorkovací perioda **nejsou příliš věrohodné**.

granularity: each sample hit covers 2 byte(s) for 0.04% of 26.75 seconds

index	% time	self	children	called	name
					<spontaneous>
[1]	100.0	0.07	26.68		main [1]
		6.91	9.90	1/1	func1 [2]
		9.86	0.00	1/1	func2 [4]

		6.91	9.90	1/1	main [1]
[2]	62.9	6.91	9.90	1	func1 [2]
		9.90	0.00	1/1	new_func1 [3]

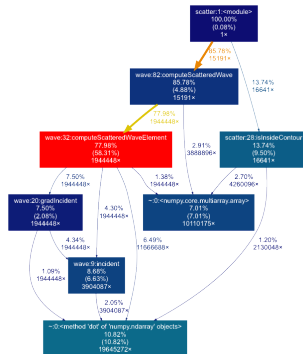
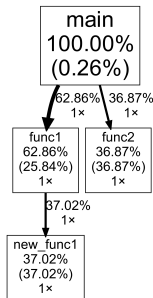
		9.90	0.00	1/1	func1 [2]
[3]	37.0	9.90	0.00	1	new_func1 [3]

		9.86	0.00	1/1	main [1]
[4]	36.9	9.86	0.00	1	func2 [4]

- <https://github.com/jrfonseca/gprof2dot>
- převodník do formátu pro GraphViz
- umí i jiné vstupní formáty než gprof

```
$ gprof2dot gprof-report.txt > gprof-report.dot
$ dot -Tpng -ogprof-report.png gprof-report.dot
$ dot -Tsvg -ogprof-report.svg gprof-report.dot
```

```
gprof2dot -c print
```





- součást Valgrindu
- výrazně pomalejší běh programu, ale **není** třeba speciální překlad
- analýza např. pomocí KCachegrind

```
$ valgrind --tool=callgrind ./program
```

```
$ ls
```

```
program program.out.pid
```

```
$ ./gprof2dot.py -f callgrind program.out.pid > vis.dot
```

Soubor Pohléd Přejít Nastavení Nápořádě

Otevřít Reload Force Dump Nahoru Zpět Vpřed % Show Relative Costs Percentage Relative to Parent Skip Cycle Detection Instruction Fetch

Flat Profile

Hledat: ELF Object

Self ELF Object

- 123 941 |libc-2.8.90.so
- 98 329 |ld-2.8.90.so
- 22 912 |proj3

Incl.	Self	Callee	Funkce	Umístění
149 099	11	1	0x0000000004008C0	proj3
146 898	31	1	main	proj3: proj3.c
145 609	36	1	doOperation	proj3: proj3.c
122 368	37	1	readMatrix	proj3: proj3matrix.c
58 009	2 000	1	_readMatrix	proj3: proj3matrix.c
21 516	21	1	doSudoku	proj3: proj3.c
20 025	252	1	isSudokuSolved	proj3: proj3sudoku.c
9 153	4 698	9	isBlockSolved	proj3: proj3sudoku.c
5 310	4 257	9	isRowSolved	proj3: proj3sudoku.c
5 310	4 257	9	isColSolved	proj3: proj3sudoku.c
3 159	3 159	243	isBadNumber	proj3: proj3sudoku.c
2 683	236	1	allocMatrix	proj3: proj3matrix.c
1 782	1 782	81	bToR	proj3: proj3sudoku.c
1 689	144	1	freeMatrix	proj3: proj3matrix.c
1 620	1 620	81	bToC	proj3: proj3sudoku.c
1 470	11	1	writeValidation	proj3: proj3.c
1 258	284	1	doParams	proj3: proj3.c
54	25	1	_libc_csu_init	proj3
29	6	1	0x0000000004007A8	proj3: crt1.S, crtn.S
22	4	1	0x000000000404988	proj3: crt1.S, crtn.S
18	18	1	0x000000000400910	proj3
11	11	1	0x000000000404950	proj3
6	6	1	0x000000000400980	proj3
6	6	1	0x0000000004008E8	proj3: crt1.S

isSudokuSolved

Typy Callers All Callers Source Code Callee Map

isBlockSolved	9 153	isRowSolved	5 310	isColSolved	5 310
bToR	1 782	bToC	1 620	isBadNumber	1 053
				isBadNumber	1 053
				isBadNumber	1 053

```

graph TD
    doSudoku[doSudoku 20 025] --> isSudokuSolved[isSudokuSolved 20 025]
    isSudokuSolved --> isBlockSolved[isBlockSolved 9 153]
    isSudokuSolved --> isRowSolved[isRowSolved 5 310]
    isSudokuSolved --> isColSolved[isColSolved 5 310]
    isBlockSolved --> bToR[bToR 1 782]
    isBlockSolved --> bToC[bToC 1 620]
    isBlockSolved --> isBadNumber1[isBadNumber 3 159]
    isRowSolved --> isBadNumber2[isBadNumber 3 159]
    isColSolved --> isBadNumber3[isBadNumber 3 159]
    
```

Caller Map Části Call Graph Callees All Callees Assembly Code

callgrind.out.12582 [1] - Total Instruction Fetch Cost: 245 182

- profiler napoví, kde se vyplatí optimalizovat
- je zbytečné optimalizovat funkci, které se zavolá jednou a neběží dlouho
- výstup profileru může být zatížen statistickou chybou
- vhodné pro rozsáhlejší programy
- může pomoci odhalit chyby
 - více/méně volání funkce, než se očekává
- spuštění s profilerem ovlivňuje běh programu
 - rychlost, heisenbugs (bugy, které zmizí, nebo změní svoje chování, když je začneme zkoumat)
- optimalizace kódu může zhoršit čitelnost
 - mnohdy je lepší optimalizovat algoritmus než implementaci
 - opravit návrh je mnohem levnější, než opravovat kód na produkci – viz IUS

Protokol z profilování je součástí **druhého projektu**.

- profiling je **měření**
- v protokolu o měření je nutné vždy uvést minimálně
 - pomocí čeho bylo měření prováděno (včetně parametrů a verzí použitých nástrojů, ...)
 - na čem je měření prováděno (použitý HW, SW včetně verzí, ...)
- na základě protokolu by mělo být možné **vaše měření zopakovat**

**QUALITY MEANS DOING IT RIGHT
WHEN NO ONE IS LOOKING.**

-HENRY FORD

- https://en.wikipedia.org/wiki/Boeing_737_MAX
- <https://medium.com/nowports-tech/introduction-to-software-quality-assurance-a2f1b4e7fec7>
- <https://westworld.fandom.com/wiki/File:Bernard.basement.jpg>
- <https://xkcd.com/371/>
- <https://www.express.co.uk/news/uk/754664/Buckingham-Palace-Changing-Guard-security-terror-threat-fixed-times>
- <https://www.qamadness.com/bug-severity-vs-priority/>
- <https://marker.io/blog/bug-report-template/>
- <https://docs.microsoft.com/cs-cz/dotnet/core/tutorials/debugging-with-visual-studio>
- <https://en.wikipedia.org/wiki/Valgrind>

- <https://preview.redd.it/rtw113wht1311.png?width=640&crop=smart&auto=webp&s=9148e2ea9924f61c08a847a73ad9fe93643f0d43>
- <https://9gag.com/gag/aQ3MAow>
- https://en.wikipedia.org/wiki/1986_Black_Sea_incident
- <https://www.sfgate.com/chris-mcginnis/article/United-transcontinental-dreamliner-787-13270374.php>
- <https://www.facebook.com/photo/?fbid=156602703665118>
- <https://twitter.com/ProgrammersMeme/status/1141238273089658882>