Využitie statickej analýzy kódu pri vývoji softvéru

Metódy inžinierskej práce 2020/2021

Lukáš Častven

Fakulta informatiky a informačných technológií
Slovenská technická univerzita v Bratislave

28. november 2021

Motivácia

- Spôsob udržania kvality kódu
- Zautomatizované hľadanie chýb a defektov
- *„Hoci čo, čo zautomatizuje nudnú prácu je skvelé."* [1]

[1] B. Johnson, Why don't software developers use staticanalysis tools to find bugs?," IEEE, may 2013.

Prehľad

Principy statickej analýzy

- Analyzovanie kódu bez spúšťania
- Informovanie o chybách a defektoch
- Príklad chybného kódu [2]

```
public String founType() {
        return this.foundType();
}
```

[2] N. Ayewah, Using static analysis to find bugs

Využitie pri vyvoji softveru

Benefity	*Nedostatky*
Automatické hľadanie chýb	Falošné pozitíva
Urdžanie kvality kódu	Prerušenie pracovného priebehu
Predintegrácia	Nejasnosť
Urdžanie tímových praktík	Nedostatočná podpora tímovej práce
Nastaviteľnosť	Netriviálnosť

Implementácia nástrojov statickej analýzy

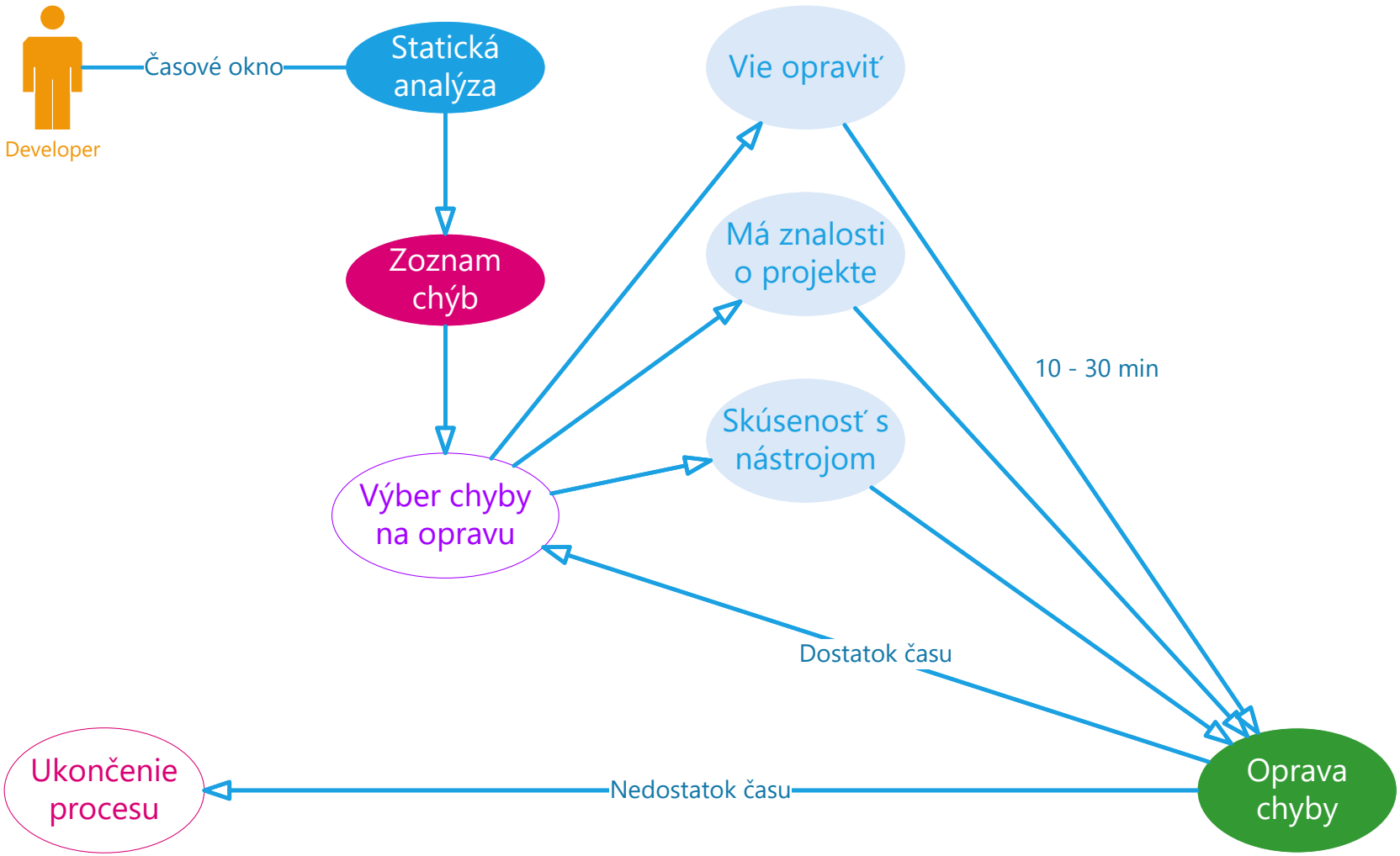
- Integrované v IDE
- Integrované v kompilátoroch [3]

```
$ gcc -c -fanalyzer double-free-1.c
double-free-1.c: In function ‘test’:
double-free-1.c:6:3: warning: double-‘free’ of ‘ptr’ [CWE-415] [-Wanalyzer-double-free]
    6 |   free(ptr);
      |   ^~~~~~~~~
  ‘test’: events 1-2
    |
    |    5 |   free(ptr);
    |      |   ^~~~~~~~~
    |      |   |
    |      |   (1) first ‘free’ here
    |    6 |   free(ptr);
    |      |   ~~~~~~~~~
    |      |   |
    |      |   (2) second ‘free’ here; first ‘free’ was at (1)
    |
```

- Rigorózne analyzátory

[3] https://developers.redhat.com/blog/2020/03/26/static-analysis-in-gcc-10#diagnostic_paths

Využitie v praxi



Záver

- Statická analýza má skvelé benefity
- Implementácie majú aj nedostatky
- Celkovo sa ale nástroje zlepšujú, vďaka spätnej väzbe od užívateľov

Ďakujem za pozornosť!