Wstrzykiwanie błędów
cele, metody, ochrona

Notatki do wykładu

Piotr Nazimek, Instutut Informatyki, Politechnika Warszawska

1.1

Spis treści

1.2

1 Wiarygodność systemów

Wiarygodność systemów

- ang. *dependability*
- dziedzina będąca wynikiem rozwoju problematyki testowania, diagnostyki, detekcji, tolerowania błędów, niezawodności, bezpieczeństwa itp. systemów komputerowych
- wiarygodność:
  - zagrożenia (błędy)
  - środki (projektowanie, walidacja, analiza)
  - atrybuty (niezawodność, dostępność, bezpieczeństwo, odporność, wydajność, . . .)

1.3

Ocena wiarygodności

- wiele technik i modeli zależnych od m. in. klasy aplikacji/sprzętu
- oszacowania ilościowe: analiza logów, niezależne testy
- istotna dla klas aplikacji dla których błędy są krytyczne

1.4

Podwyższanie wiarygodności

- bez redundancji: unikanie błędów i ich wykrywanie
- z redundancją:
  - maskowanie błędów
  - tolerowanie błędów

1.5

Błędy

- trwałość:
  - trwałe
  - przemijające
  - migoczące
- efekt propagacji:
  - błąd fizyczny
  - błąd logiczny
  - niewłaściwe zachowanie

1.6

2 Wstrzykiwanie błędów

Wstrzykiwanie błędów

- brak dokładnej definicji – zakłócenie działania programu
  - modyfikacja instrukcji
  - modyfikacja danych
  - podanie złośliwych danych
- poziom funkcjonalny, poziom strukturalny
- przypadkowe
- celowe

1.7

2.1 Cele

Cele

- badanie wiarygodności systemów poprzez analizę skutków błędów
  - niezawodność
  - bezpieczeństwo
  - łatwość serwisowania
  - diagnostyka
  - tolerowanie błędów
  - ...

1.8

2.2 Metody

Metody

- wstrzykiwanie sprzętowe
  - bardzo kosztowne ze względu na skomplikowaną technologię (dedykowany układ lub dedykowany sprzęt wstrzykujący)
  - różne techniki
    - zakłócanie sygnałów na końcówkach układu
    - zakłócanie zasilania
    - zakłócanie wiązką laserową
    - zakłócanie ciężkimi jonami
  - ograniczenia w klasach generowanych błędów

1.9

Metody

- wstrzykiwanie programowe
  - symulacja sprzętowych błędów np. sklejenia z zerem, inwersji stanu, zwarcia
  - wyniki porównywane z poprawnym przebiegiem (*golden run*) oraz trybem zakończenia programu (poprawne, niepoprawne, wyjątek systemowy, przekroczenie czasu oczekiwania, wykrycie przez użytkownika)
  - możliwość wstrzykiwania błędów o dowolnych klasach
  - powtarzalność testów

1.10

2.3 Ochrona

Ochrona

- jest trudna w realizacji
- ochrona sprzętowa
- ochrona programowa

1.11

2.4 Unikanie skutków

Unikanie skutków

- wykrycie zakłócenia
- ochrona sprzętowa
- ochrona programowa
  - obsługa wyjątków
  - redundancja programowa – duplikacja kodu źródłowego, zmiennych, detekcja błędów
  - kompilator i optymalizacja
  - język wysokiego poziomu a kod maszynowy

1.12

Redundancja

- problem wykrycia błędu
- podniesienie wiarygodności poprzez redundancję, a
  - rozmiar aplikacji/układu
  - szybkość aplikacji/układu
- kwalifikacja części programu do duplikacji

1.13

3 Podsumowanie

Podsumowanie

- wstrzykiwanie błędów jest przydatną techniką wykorzystywaną przy ocenie odporności aplikacji na błędy
- celowe sprzętowe wstrzykiwanie określonych błędów jest trudne w realizacji i kosztowne
- zabezpieczenia – co uodparniać

1.14