Међузависност и безбедност

Перица Трајков
1023/2012

Циљеви

- Разумети важност међузависности и безебедности
- Схватити поделу међузависности на 4 подкатегорије
- Научити на који начин креирати софтвер који је безбедан и међузависан

Увод

- значај проблема који настају услед неодговарајућег рада софтвера
- Термин “међузависност” (dependability) – Лаприе (1995)
- Међузависност је значајнија од функционалности:
  - софтверски пропусти утичу на велики број људи
  - корисници избегавају системе који су несигурни
  - трошкови софтверских грешака могу бити огромни
- Софтвер је увек део већег система (хардвер и корисници)
- Критични системи

Дефиниција и подела

- Међузависност је својство система које означава степен поверења и поузданости у њега

Подела:

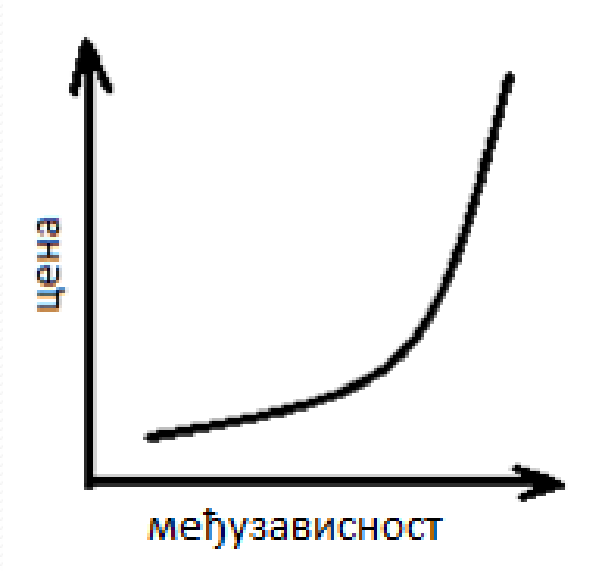
- **Доступност**: способност система да пружа услуге кад год су потребне
- **Поузданост**: способност система да пружа тражене услуге
- **Сигурност**: Способност система да ради без изазивања штете
- **Безбедност**: Способност система да се заштити од спољашњих напада

Додатна подела

- **Поправљивост**: могућност система да се лако уоче и поправе грешке
- **Одрживост**: Способност система да одржи корисност у складу са променама захтева
- **Способност преживљавања**: омогућавање пружања сервиса и током напада, или приликом пада дела система
- **Толеранција на грешку**: Способност система да игнорише или поправља сам грешке

Цена међузависности

- Да би софтвер или целокупни систем био међузависан морају се правити уступци
- Укључивање редундатног кода
- Повећање цене развоја



Доступност и поузданост

- Изражавање преко нумеричке вероватноће
- **Доступност** – вероватноћа да ће систем бити покренут и спреман да пружи услуге када се од њега траже
- **Поузданост** – вероватноћа да ће пружене услуге бити онакве какве су спецификоване документацијом
- Уска повезаност – али, некада је једна особина битнија од друге

Доступност и поузданост

Прецизније дефиниције:

- **Поузданост:** вероватноћа да операција буде без грешке у неком спецификованом интервалу времена у задатом окружењу, за одређену намену
- **Доступност:** Вероватноћа да систем, у тренутку времена, буде оперативан и способан да испоручи захтеване услуге
- Пример: поузданост апликације за текст у зависности од окружења и корисника

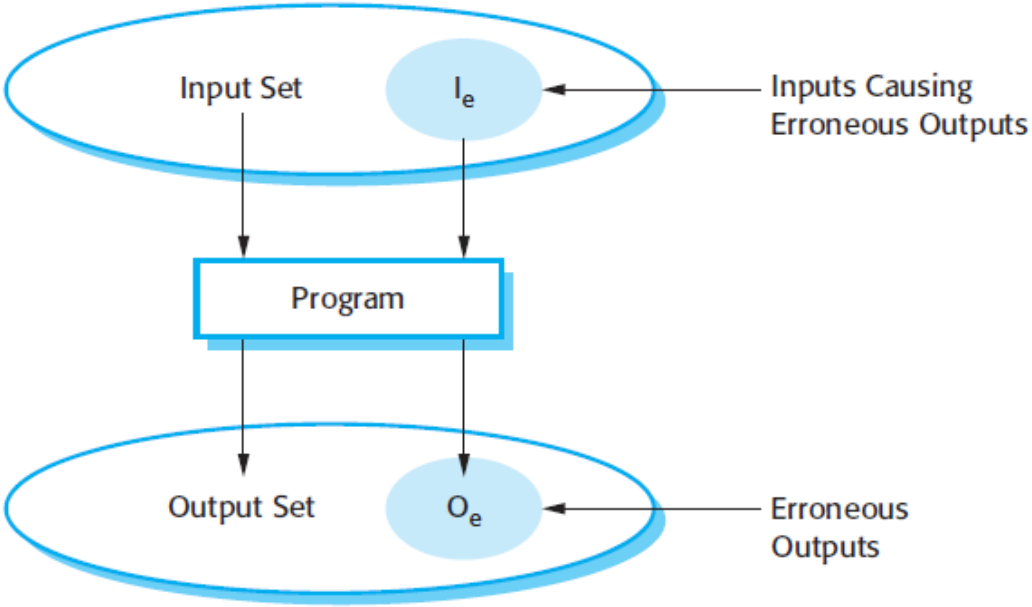
Доступност и поузданост

- Дефиниције не узимају у обзир озбиљност грешки и последице недоступности
- Пример: грешке које као последицу имају коруптиране податке су опасније него оне које замрзну машину
- Систем се понаша поуздано ако се понаша у складу са спецификацијом (која може бити лоша и непоуздана)
- Доступност не зависи само од броја падова система, већ и од времена које је потребно да се систем подигне
- Време када је систем пао је такође од пресудног значаја

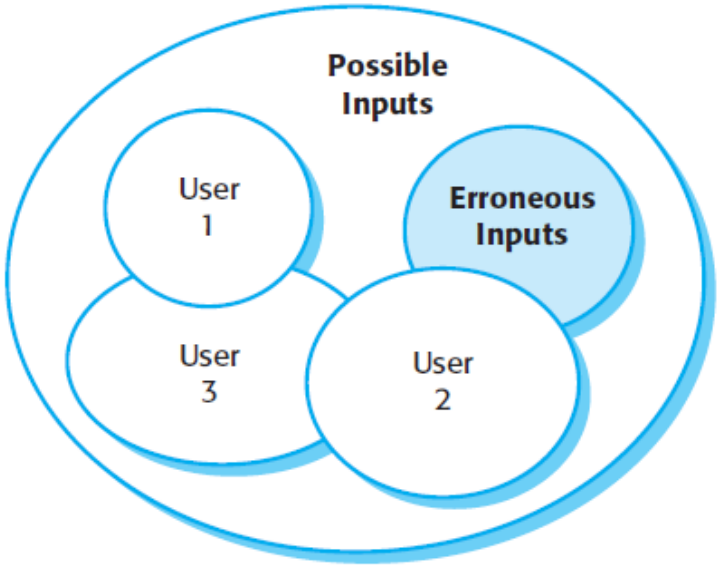
Доступност и поузданост - терминологија

- **Људска грешка (Human error):** Понашање човека које доводи до “уласка” грешке у систем
- **Системска “мана” (System fault):** Карактеристика софтверског система која може довести до системске грешке
- **Системска грешка (System error):** Погрешно стање система које може довести до понашања које је неочекивано
- **Пад система (System failure):** Догађај који се јавља у неком тренутку када систем не пружа услугу која је очекивана

Доступност и поузданост



Слика 1: Систем као мапирање улаза и излаза



Слика 2: Шаблони коришћења софтвера

Доступност и поузданост - наставак

- Отклањање софтверских грешака не мора значајно да смањи укупну поузданост система
- Неке грешке се испољавају након месеци и месеци употребе
- Системске “мане” не доводе увек до системских грешака, а системске грешке не доводе увек до пада система

  разлози:

  - сав код се не извршава
  - неке софтверске мане се у међувремену “поправе”
  - детекција грешке и њено исправљање
  - сами корисници “избегавају” сумњиве улазе

Доступност и поузданост - приступи

- Три приступа за унапређење поузданости:

- Избегавање грешака
- Препознавање грешака и отклањање
- Игнорисање грешака

Сигурност

- Сигурносно-критични системи

  - хардвесрка контрола је једноставнија него софтверска

  - примарни (контролер) и секундарни (индиректни) сигурносно-критични софтвер

- Поузданост и сигурност су повезани
- Поуздан систем може бити несигуран, и обрнуто:

  непотпуна документација, хардверски проблеми, улази који генерално гледано не воде до проблема али понекад то чине (подизање точкова у авиону)

Сигурност - терминологија

- Незгода (Accident)
- Опасност (Hazard)
- Оштећење (Damage)
- Озбиљност опасности (Hazard severity)
- Вероватноћа опасности (Hazard probability)
- Ризик (Risk)

Сигурност

- Обезбеђивање сигурности: обезбеђивање да се незгоде не појављују, или да су последице њих минималне. Три начина:

  - избегавање опасности

  - детекција опасности и отклањање

  - ограничавање оштећења
- Незгоде као последица вишеструких догађаја
- Прављење баланса – немогуће је направити 100% сигуран систем

Безбедност

- Способност система да се одбрани од екстерних напада, намерних или случајних
- Умреженост рачунара
- За неке системе (војни, електронско пословање, системи са поверљивим подацима) безбедност је кључна

Безбедност - терминологија

- Податак (Asset)
- Последица изложености (Exposure)
- Рањивост (Vulnerability)
- Напад (Attack)
- Претња (Threat)
- Контрола (Control)

Безбедност

- Три типа безбедносних претњи

  - претње поверљивости података

  - претње интегритету система и података

  - претње доступности система и података
- Међусобна повезаност претњи
- Главни разлог рањивости је грешка човека

Безбедност

- Повећање безбедности:

  - избегавање рањивости

  - детекција напада и неутрализација

  - ограничавање изложености и опоравак

- Без безбедности нема доступности, поузданости ни сигурности

- ПИТАЊА?!?