Kapitola 10 – Spoľahlivé systémy

Spoľahlivosť systému

- Pre mnoho počítačových systémov je najdôležitejšou vlastnosťou systému spoľahlivosť systému.
- Spoľahlivosť systému odráža mieru dôvery používateľa v tento systém. Odráža mieru dôvery používateľa, že bude fungovať tak, ako používatelia očakávajú, a že pri bežnom používaní „nezlyhá“.
- Spoľahlivosť ("systémová") pokrýva súvisiace atribúty systémov ako ("výpočtová") spoľahlivosť, dostupnosť a bezpečnosť. Všetky sú vzájomne závislé.

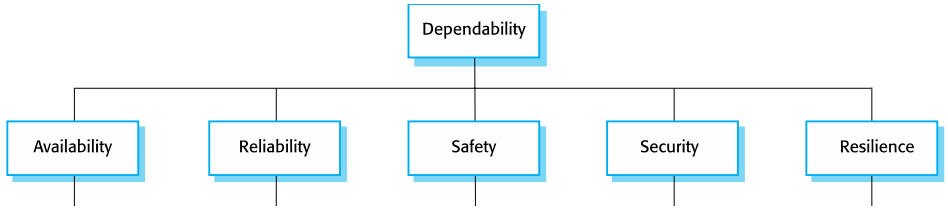
Dôležitosť spoľahlivosti

- Zlyhania systému môžu mať rozsiahle následky s veľkým počtom ľudí postihnutých zlyhaním.
- Systémy, ktoré nie sú spoľahlivé a sú nespoľahlivé, nebezpečné alebo neisté, môžu ich používatelia odmietnuť.
- Náklady na zlyhanie systému môžu byť veľmi vysoké, ak zlyhanie vedie k ekonomickým stratám alebo fyzickým škodám.
- Nespoľahlivé systémy môžu spôsobiť stratu informácií s vysokými následnými nákladmi na obnovu.

Príčiny zlyhania

- Porucha hardvéru
  - Hardvér zlyhá v dôsledku konštrukčných a výrobných chýb alebo preto, že komponenty dosiahli koniec svojej prirodzenej životnosti.
- Zlyhanie softvéru
  - Softvér zlyhá v dôsledku chýb v jeho špecifikácii, návrhu alebo implementácii.
- Prevádzková porucha
  - Ľudskí operátori robia chyby. Možno najväčšia príčina zlyhania systému v sociálno-technických systémoch.

Hlavné vlastnosti



- Dostupnosť - súčasť informačnej bezpečnosti
  - Pravdepodobnosť, že systém bude v prevádzke a bude schopný poskytovať používateľom užitočné služby.
- Výpočtová spoľahlivosť
  - Pravdepodobnosť, že systém bude správne poskytovať služby podľa očakávania používateľov.
- Ochrana zdravia, života a prostredia
  - Posúdenie toho, aká je pravdepodobnosť, že systém spôsobí škody ľuďom alebo životnému prostrediu.
- Informačná bezpečnosť
  - Posúdenie toho, aká je pravdepodobnosť, že systém dokáže odolať náhodným alebo úmyselným prienikom. C-I-A: dôvernosť, integrita, dostupnosť.
- Odolnosť
  - Posúdenie toho, ako dobre môže systém zachovať kontinuitu svojich kritických služieb v prítomnosti rušivých udalostí, ako je zlyhanie zariadenia a kybernetické útoky.

Ďalšie vlastnosti spoľahlivosti

- Opraviteľnosť
  - Odráža mieru, do akej je možné systém opraviť v prípade poruchy
- Udržiavateľnosť
  - Odráža mieru, do akej je možné systém prispôsobiť novým požiadavkám;
- Tolerancia chýb
  - Odráža mieru, do akej sa možno vyhnúť chybám pri zadávaní údajov a tolerovať ich.

Závislosti atribútov spoľahlivosti

- Bezpečná prevádzka systému závisí od dostupnosti a spoľahlivosti systému.
- Systém môže byť nespoľahlivý, pretože jeho údaje boli poškodené vonkajším útokom.
- Útoky odmietnutia služby na systém sú určené na to, aby bol nedostupný.
- Ak je systém infikovaný vírusom, nemôžete si byť istí jeho spoľahlivosťou alebo bezpečnosťou.

Typy kritických systémov

- Systémy kritické z hľadiska bezpečnosti
  - Porucha má za následok stratu života, zranenie alebo poškodenie životného prostredia
  - *Chemický systém ochrany rastlín*
- Systémy kritické pre danú úlohu alebo cieľ
  - Zlyhanie má za následok zlyhanie nejakej cieľovo orientovanej činnosti
  - *Navigačný systém kozmickej lode*
- Systémy kritické pre podnikanie
  - Zlyhanie má za následok vysoké ekonomické straty
  - *Účtovný systém zákazníkov v banke*

Dosiahnutie spoľahlivosti

- ✧ Vyhnite sa náhodným chybám pri vývoji systému.
- ✧ Navrhnite V & V procesy, ktoré sú efektívne pri odhaľovaní zvyškových chýb v systéme.
- ✧ Navrhnite systémy tak, aby bol tolerantný: aby systém mohol pokračovať v prevádzke, keď sa vyskytnú poruchy
- ✧ Navrhnite ochranné mechanizmy, ktoré chránia pred vonkajšími útokmi.

Dosiahnutie spoľahlivosti (2)

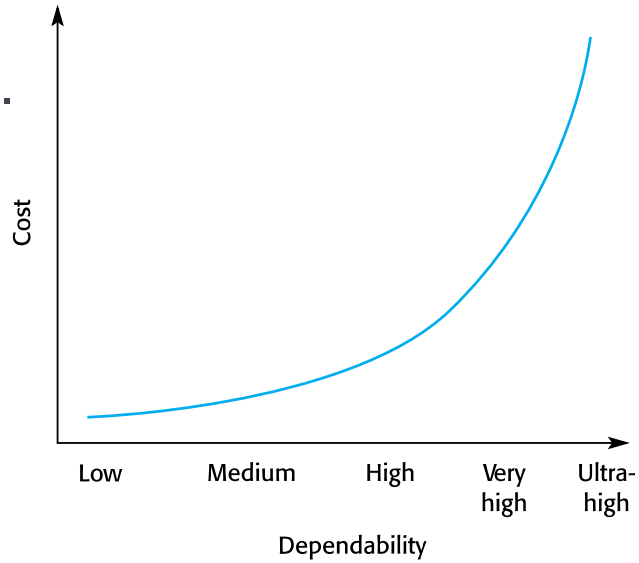
- Správne nakonfigurujte systém pre jeho operačné prostredie .
- Zahrňte systémové schopnosti na rozpoznanie a odolanie kybernetickým útokom.
- Zahrňte mechanizmy obnovy, ktoré pomôžu obnoviť normálnu systémovú službu po zlyhaní.

Ekonomika spoľahlivosti

- Kvôli veľmi vysokým nákladom na dosiahnutie spoľahlivosti môže byť nákladovo efektívnejšie akceptovať nedôveryhodné systémy a zaplatiť náklady na zlyhanie
- To však závisí od sociálnych a politických faktorov. Povesť produktov, ktorým nemožno dôverovať, môže viesť ku strate budúceho podnikania
- Závisí od typu systému – najmä pre obchodné systémy môže byť primeraná mierna úroveň spoľahlivosti

Náklady na spoľahlivosť

- Náklady na spoľahlivosť majú tendenciu exponenciálne rásť, pretože je potrebná vyššia úroveň spoľahlivosti .
- Sú na to dva dôvody
  - Použitie drahších vývojových techník a hardvéru, ktoré sú potrebné na dosiahnutie vyššej úrovne spoľahlivosti.
  - Zvýšené testovanie a overovanie systému je potrebné na presvedčenie klienta systému a regulátorov, že boli dosiahnuté požadované úrovne spoľahlivosti .



Spoľahlivé procesy

- Na zabezpečenie minimálneho počtu softvérových chýb je dôležité mať dobre definovaný a opakovateľný softvérový proces.
- Dobre definovaný a opakovateľný proces je taký, ktorý nezávisí úplne od individuálnych zručností; skôr môžu byť uzákonené rôznymi ľuďmi.
- Regulačné orgány používajú informácie o procese na kontrolu, či bola použitá správna prax softvérového inžinierstva.
- Pre detekciu chýb je jasné, že aktivity procesu by mali zahŕňať značné úsilie venované overovaniu a validácii.

Spoľahlivé charakteristiky procesu

- Explicitne definované
  - Proces, ktorý má definovaný procesný model, ktorý sa používa na riadenie procesu výroby softvéru. Počas procesu sa musia zbierať údaje, ktoré dokazujú, že vývojový tím dodržal proces, ako je definovaný v modeli procesu.
- Opakovateľné
  - Proces, ktorý sa nespolieha na individuálny výklad a úsudok. Proces sa môže opakovať v rámci projektov a s rôznymi členmi tímu, bez ohľadu na to, kto sa podieľa na vývoji.

Vlastnosti spoľahlivých procesov

Charakteristika procesu	Popis
Auditovateľný	Proces by mal byť zrozumiteľný pre ľudí okrem účastníkov procesu, ktorí môžu kontrolovať dodržiavanie procesných štandardov a podávať návrhy na zlepšenie procesov.
Rozmanitý	Proces by mal zahŕňať nadbytočné a rôznorodé overovacie a validačné činnosti.
Dokumentovateľný	Proces by mal mať definovaný procesný model, ktorý stanovuje činnosti v procese a dokumentáciu, ktorá sa má pri týchto činnostiach vytvárať.
Robustný	Proces by mal byť schopný zotaviť sa z porúch jednotlivých činností procesu.
Štandardizovaný	K dispozícii by mal byť komplexný súbor štandardov vývoja softvéru pokrývajúcich výrobu softvéru a dokumentáciu.

Činnosti pre dosiahnutie spoľahlivosti

- Recenzie požiadaviek: skontrolovať, či sú požiadavky, pokiaľ je to možné, úplné a konzistentné.
- Správa požiadaviek: aby sa zabezpečilo, že zmeny požiadaviek sú kontrolované a že je pochopený vplyv navrhovaných zmien požiadaviek.
- Formálna špecifikácia: kde sa vytvorí a analyzuje matematický model softvéru.
- Systémové modelovanie: kde je návrh softvéru explicitne zdokumentovaný ako súbor grafických modelov a sú zdokumentované prepojenia medzi požiadavkami a týmito modelmi .

Činnosti pre dosiahnutie spoľahlivosti (2)

- Kontroly dizajnu a programu: kde sa rôzne popisy systému kontrolujú a kontrolujú ich rôzni ľudia.
- Statická analýza: kde sa vykonávajú automatizované kontroly zdrojového kódu programu.
- Plánovanie a správa testov: kde je navrhnutý komplexný súbor testov systému.
  - testovania musí byť starostlivo riadené, aby sa preukázalo, že tieto testy pokrývajú systémové požiadavky a boli správne aplikované v procese testovania.