L1

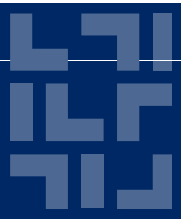
University of Ljubljana
Faculty of
Computer and
Information Science

1. Uvod – riziki digitaliziranih sistemov

Prosojnice za predavanja 4.UNI/RS

Avtor: izr.prof.dr.Miha Mraz

Šol.leto 2009/10



Slide 1

L1 LRSS; 14.2.2009

Motivacija za področje zanesljivosti računalniških sistemov

- Vsesplošna digitalizacija, vse večja kompleksnost sistemov
- Upravljanje s svojim okoljem prepuščamo avtomatiziranim sistemom
- Določene aktivnosti smo že prepustili avtomatiziranim sistemom (informiranje, komuniciranje, ogrevanje, promet, itd.)
- V prihodnosti se bo naša odvisnost od avtomatiziranih sistemov samo še povečevala (npr. bela tehnika, popoln nadzor ambientalnega okolja, itd.)
- Kaj če avtomatizirani sistemi odpovedo?

“Space Shuttle” Columbia (2003)?

Prve predpostavke za vzrok nesreče (kasneje zanikane): računalniški sistem

Figure: http://upload.wikimedia.org/wikipedia/commons/e/e1/STS-107-Debris_KSC_Hangar.jpg

Strmoglavljenje letala Airbus A-320 (1988)?

Prve predpostavke za vzrok nesreče (kasneje zanikane): računalniški sistem

Figure: http://pagesperso-orange.fr/crashdehabsheim/Galerie%20photos.htm

Therac 25 (1985-1987)?

- Računalniško krmiljeni medicinski radiacijski sistem (Atomic Energy of Canada Ltd.).
- 6 smrtnih 100 kratnih preobsevanj v 2 letih
- Analiza nesreč: N.G. Leveson (FDA, USA):
  - SW brez tehnične dokumentacije
  - Neznan vir programske opreme
  - SW gre v eksploatacijo brez testiranja
  - Vzrok: primitivna SW napaka

Patriot missiles (1991)?

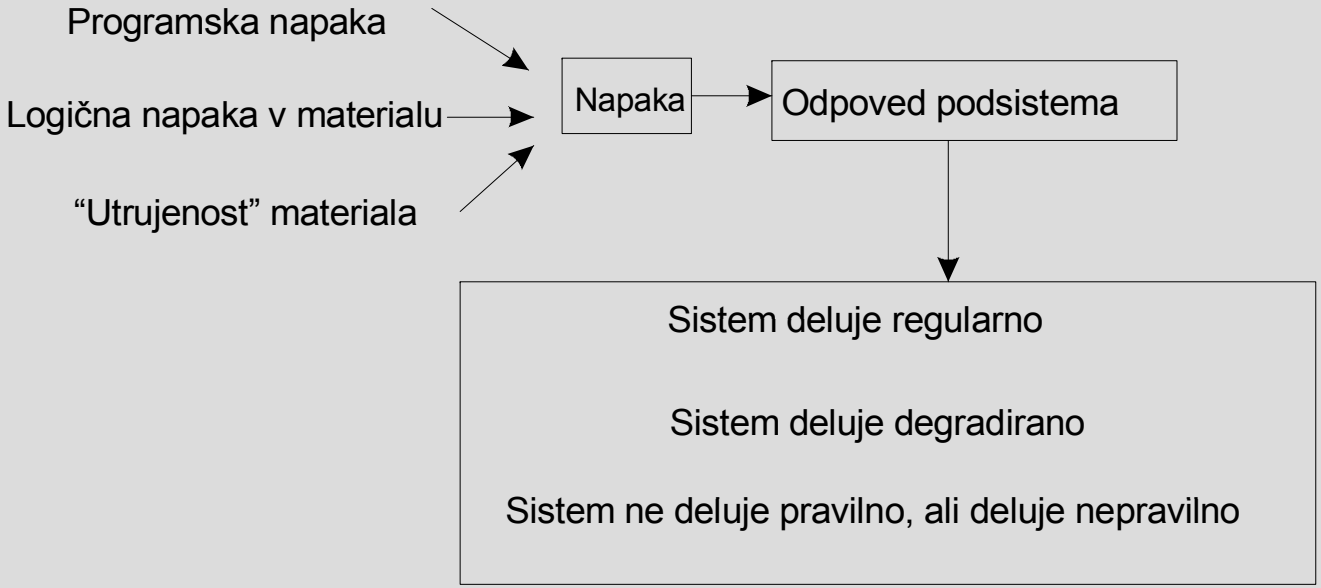
- Puščavski vihar: izstrelki za sledenje in uničevanje sovjetskih izstrelkov Skud
- Zaradi slabe sinhronizacije izstrelka z sistemom vodenja so rezultati zadetkov pod predvidenim odstotkom;

Tehnični, sociološki in gospodarski vidiki kot vplivni faktorji potencialne nezanesljivosti

- Tehnične rešitve so vse bolj kompleksne – težka logična verifikacija
- Ljudje zaupajo računalniškim sistemom (HAL fenomen je pozabljen)
- Globani trgi zahtevajo vse hitrejše pojavljanje na trgu (čas za razvoj produkta se drastično krajša)
- Pojavljanje novih storitev (sistemov) z neverificiranimi algoritmi
- Pojavljanje novih razvojnih okolij

Hierarhija napaka - odpoved

- Tehnični pogled na zanesljivost rač.sistema:



Ostali vplivi na odpovedovanje rač.sistemov

- Človeški faktor:
  - Znanje uporabe
  - Zlonamerna uporaba
- Fizična izpostavljenost sistema (vreme, naravne nesreče, itd.)
- Energetska odvisnost

Napake uporabnikov rač. sistemov

Uporabniki so premalo zahtevni do izvajalcev rešitev

Tipična vprašanja, na katera si uporabnik ne odgovarja:

- Ali sistem vrši samo željene funkcije, ali lahko ob določenih neželjenih pogojih vrši tudi neželjene?
- Ali lahko sistem ob odpovedi vodi do delovanja, ki je za uporabnika nesprejemljivo?
- Kakšne garancije za pravilno delovanje sistema nam nudi prodajalec?
- Kakšne materialne škodne posledice je pripravljen nase prevzeti proizvajalec?

Napake ponudnikov rešitev in sistemov

Vprašanja postavljena ponudnikom:

1. Ali ste izvedli FMEA analizo za vaš produkt?
2. Ali ste izvedli FTA analizo za vaš produkt?
3. Kakšen je povprečni čas med dvema odpovedima vašega sistema (MTBF)?
4. Kakšna je pričakovana življenska doba vašega sistema (MTTF)?
5. Kakšna je dosegljivost vašega sistema?
6. Kako in koliko časa je potekalo testiranje sistema?
7. Kolikšen je čas popravila sistema (MTTR)?

In odgovori?

1. ?
2. ?
3. ?
4. ?
5. ?
6. ?
7. Odvisno od vzdrževalne pogodbe!