Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

1. Uvod v zanesljivost računalniških sistemov

(2019/2020)

prof.dr.Miha Mraz

24. februar 2020

Motivacija za področje zanesljivosti

- **Vsesplošna digitalizacija** - upravljanje s svojim okoljem vse bolj prepuščamo avtomatiziranim sistemom (npr. komuniciranje, nadzor objektov, nadzor prometa, itd.)
- **Eksplozija števila računalniških sistemov** (tako kompleksnejših, kot tudi enostavnejših)
- **Rast kompleksnosti** funkcij računalniških sistemov in njihovih realizacij (sistemi vršijo vse bolj kompleksne funkcije in vse bolj kompleksna je tudi njihova arhitektura)

- Dejstva, s katerimi se soočamo snovalci sistemov:
  - Število rač.sistemov v eksploataciji narašča
  - Kompleksnost narašča hitreje kot metode logične verifikacije pravilnosti delovanja
  - Uporabniki vse bolj **zaupajo** digitaliziranim sistemom in so od njih vse bolj **odvisni** (HAL fenomen je pozabljen)
  - Globalnost trga: zahteve po vse manjših časih od idejne zasnove produkta do njegove pojavitve na trgu
  - Nove paradigme razvoja programske opreme in nova razvojna okolja
  - Pomanjkanje regulatornih normativov (standardi, priporočila, certificiranje, nacionalne smernice in omejitve, itd.)
- Problem odgovornosti - zavedanja rizikov in posledic nepravilnega delovanja digitaliziranih sistemov

Odnos kupec - ponudnik

- Nedozorel odnos (hiter razvoj, nereguliranost, globalni trg)
- Ponudnik: razvijalec ali integrator
- Kupci so premalo zahtevni do ponudnika rešitev - tipična vprašanja, na katera si kupec ne odgovarja:
  - Ali sistem vrši samo željene funkcije, ali lahko ob določenih robnih 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 ponudnik?
  - Kakšne materialne škodne posledice je pripravljen nase prevzeti ponudnik ob neustreznem delovanju sistema?

- Vprašanja, ki jih naročnik običajno ne zastavi ponudniku ali pa odgovori nanje niso pogodbeno urejeni:
  - Kakšne zanesljivostne analize je ponudnik izvedel za sistem, ki ga trži?
  - Kakšen je pričakovani čas do odpovedi ponudnikovega sistema?
  - Kakšna je pričakovana življenska doba sistema?
  - Kakšna je dosegljivost sistema (99,999%)?
  - Kako in koliko časa je potekalo testiranje sistema?
  - Kolikšen je čas za popravilo sistema in kdo ter pod kakšnimi pogoji ga bo izvajal?

Ostali vplivi na zanesljivost sistema

- Človeški faktor:
  - Nezlonamerna napačna uporaba (usposobljenost za rokovanje, utrujenost, starost, koncentracija, zmožnost, slab vid, funkcionalna pismenost, itd.)
  - Zlonamerna napačna uporaba
- Fizična ranljivost sistema: vreme, naravne nesreče, ostali dogodki (l.2001 - NewYork, primer žleda v februarju 2014 v Sloveniji)
- Energetska odvisnost in avtonomnost sistemske rešitve

Klasifikacija sistemov z vidika zanesljivosti

Računalniške sisteme z vidika namena eksploatacije (misije) delimo na naslednje skupine:

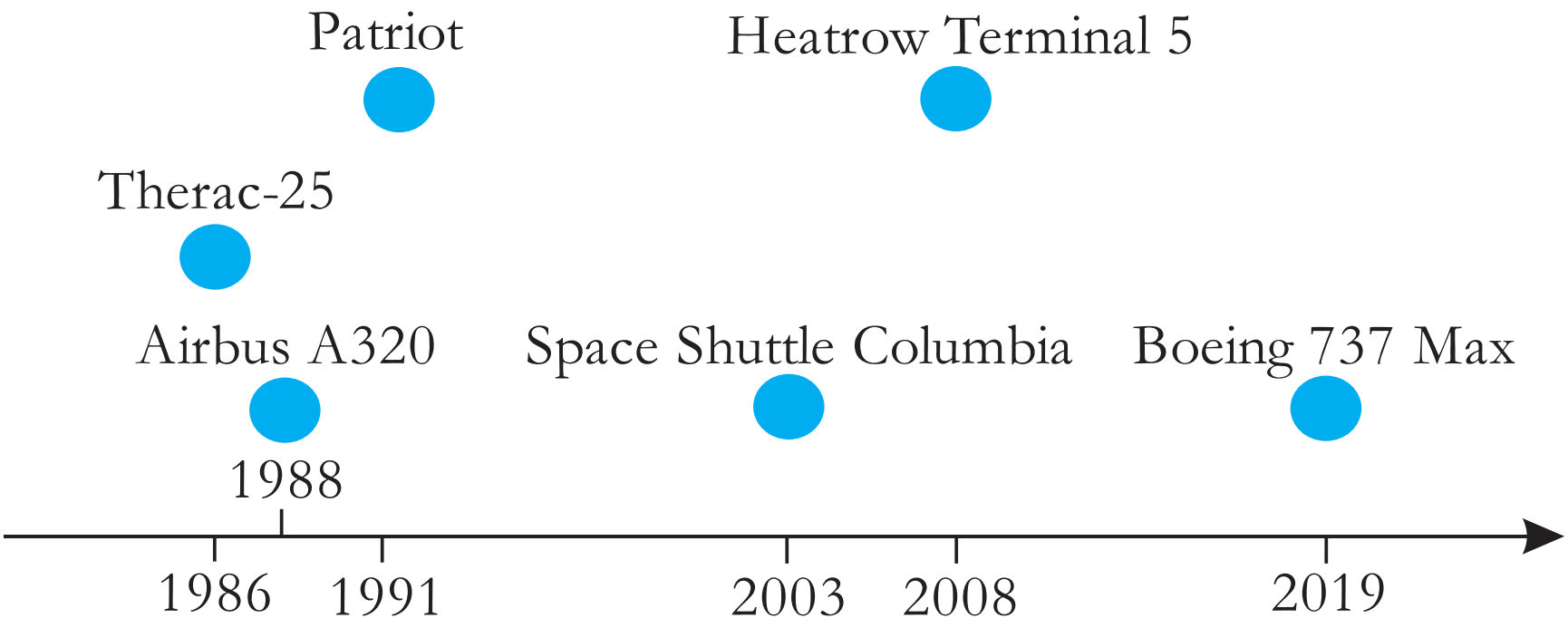
1. Splošno namenski računalniški sistemi (angl. *gadget equipment, general purpose computers*)
2. OLTP sistemi (angl. *on line transaction systems*): visoko dosegljiva osrčja distribuiranih računalniških sistemov (na končnih točkah splošno namenski sistemi)
3. Sistemi z dolgimi misijami (angl. *long mission systems, long life systems*): sistemi so v eksploatacijski (produkcijski) fazi praktično nedosegljivi
4. Misijsko kritični sistemi (angl. *critical mission systems*): sistemi, ki pri uporabi lahko povzročijo veliko škodo (npr. medicinske naprave, krmiljenje jedrskih elektrarn, navigacijski sistemi, itd.)

- Zanesljivost po naštetih skupinah narašča od zgoraj navzdol; temu primerno narašča (eksponentno) tudi cena sistemskih rešitev;
- Cena izvedbe razvojno – življenskega cikla sistemov se okvirno giblje v razmerju 1:10:100:1000

Primeri odmevnih računalniških incidentov in nesreč

- Zgodovinsko dejstvo: Za povzročitelje večjih incidentov in nesreč v zadnjih štirih desetletjih so na začetku preiskav praviloma proglašeni računalniški sistemi;
- **Incident**: nepričakovan dogodek, ki prekine normalno delovanje sistema in rezultira v gospodarsko škod, ne rezultira pa v poškodbe ali bolezni ljudi;
- **Nesreča**: nepričakovan dogodek, ki prekine normalno delovanje sistema in rezultira v poškodbe ali bolezni ljudi, lahko pa poleg tega rezultira tudi v gospodarsko škodo;

- Vzorčne nesreče in incidenti:



Therac 25 (1985-1987)

- Član produktne družine računalniško vodenih obsevalnih radiološko terapevtskih aparatov (Atomic Energy of Canada Limited (AECL), danes Theratronics Ltd.)
- Medicinski linearni pospeševalnik visoko energetskih žarkov za uničevanje tumorjev z minimalnim vplivom na okoliško tkivo
- Prvi primer računalniško vodene obsevalne naprave (predhodno vodenje realizirano mehansko): mikroračunalnik, 20.000 vrstic izvorne kode (angl. *lines of code* – LOC)
- 6 dokazanih primerov 100 kratnega predoziranja pacientov (4 mrtvi pacienti): 1985-1986

- Vzrok: ko 6 bitni programski števec doseže vrednost 0 odpovedo kontrole nadzora nastavitve naprave (krivda pomanjkljive programske opreme (PO) in mehanske realizacije naprave)
- Posredne ugotovitve (N.G.Leveson, FDA, ZDA): PO ni bila pregledana s strani nedovisne institucije, slaba dokumentacija, neznan vir PO, pomanjkljivo testiranje, itd.
- Posledica – vpeljava standarda IEC 62304 (definira življenski cikel PO za medicinske naprave)

Airbus A320 (1988)

- Airbus A320 – prvo civilno letalsko plovilo s konceptom „fly by wire“
- Strmoglavljenje na letalskem mitingu
- Prve predpostavke za vzrok nesreče (kasneje zanikane): računalniški sistem

Vir: Google - photos

Patriot (1991)

- Puščavski vihar: izstrelki za sledenje in uničevanje sovjetskih izstrelkov Skud
- Zaradi nespoštovanja napotkov za doseganje sinhronizacije krmilnega sistema izstrelka s sistemom vodenja so bili rezultati zadetkov pod predvidenim odstotkom;

Vir: Wikipedia

Space Shuttle Columbia (2003)

- Razpad plovila v fazi vstopanja v zemljino atmosfero (ZDA, Texas)
- Prve predpostavke za vzrok nesreče (kasneje zanikane): računalniški sistem je nepravilno vodil proceduro nagibanja plovila ob vstopu v zemeljsko atmosfero

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


AIRPORT CENTER
DIRECTV
NASA
United States
oneworld
AA

Heathrow terminal 5 (2008)

Boeing 737 max (2018,2019)

Literatura

[1]http://www.docstoc.com/docs/85190213/%E2%80%9CAn-Investigation-of-the-Therac-25-Accidents%E2%80%9D-by-Nancy-G-Leveson

[2] P.G.Neumann: Computer related risks, Addison – Wesley, 1995 (knjigo lahko dobite pri prof.dr.Mrazu)

[3] I.Peterson: Fatal defect – Chasing killer computer bugs, Vintage Books, 1996 (knjigo lahko dobite pri prof.dr.Mrazu)