Zdenko Šimić
zdenko.simic@fer.hr
Fakultet elektrotehnike i računarstva
2009.

Analiza stablom događaja i Vjerojatnosna analiza sigurnosti

Sadržaj

- Uvod
- Temeljni koraci
- Stablo događaja
- Stablo kvara
- Podaci
- Mjere važnosti
- Neodređenost

Razvoj ET & FT metoda?

- Ranih šezdesetih godina, u Bell Telephone laboratoriju u vezi s US Air Force studijom kontrolnih sistema Minuteman Missile lansera.
- Početkom sedamdesetih u studiji sigurnosti nukleranih elektrana u Americi WASH-1400.
- Osnovni motivi za primjenu ET i FT analiza mogu biti:
  - sigurnost,
  - ekonomija i
  - tzv. proizvodna odgovornost.
- Industrije poput vojne, svemirske, zrakoplovne i nuklearne imaju primarni zahtjev na sigurnost.

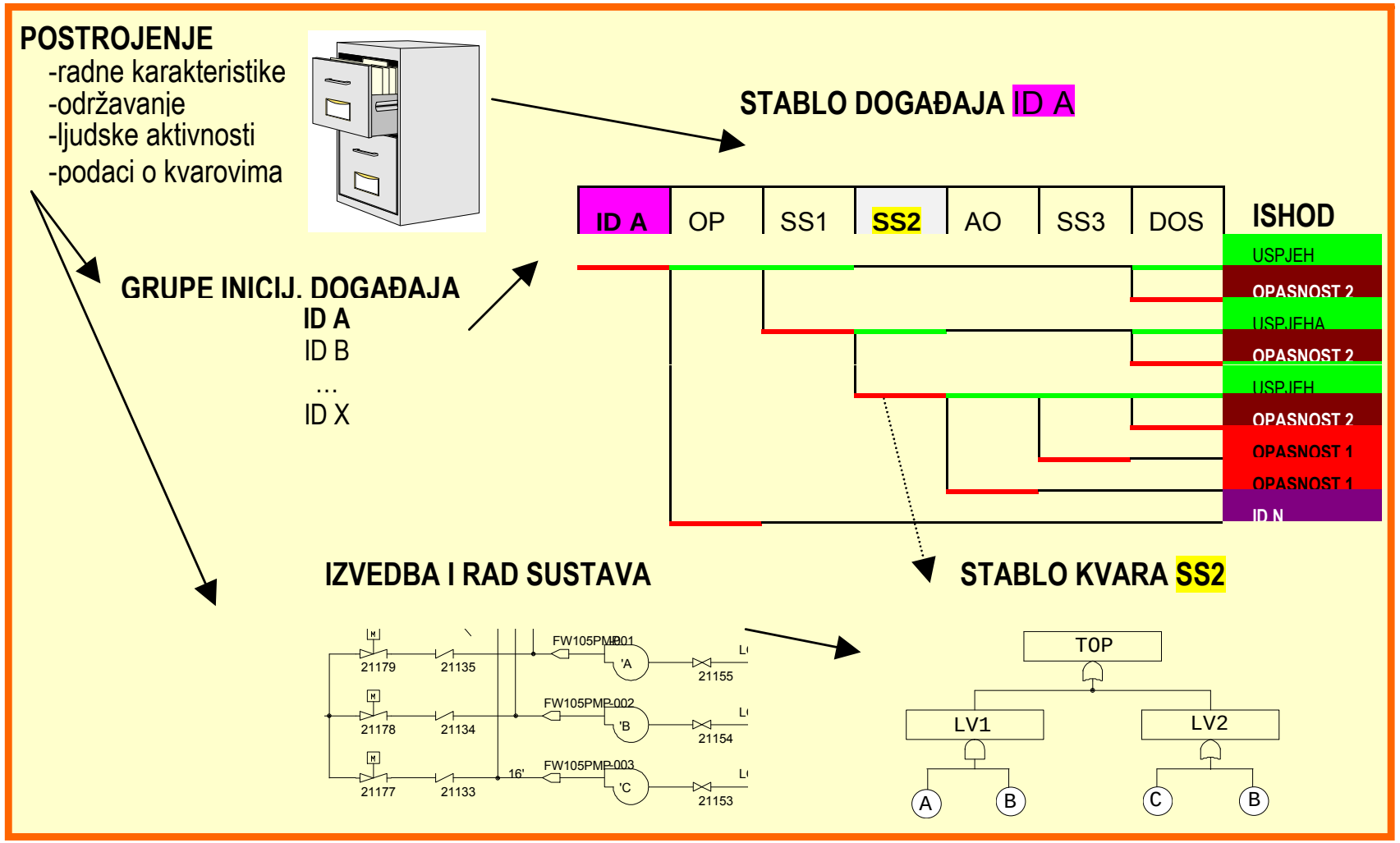
Što je to vjerojatnosna procjena rizika

- Kreiranje modela razvoja akcidenata u postrojenju.
- Posebno se analiziraju akcidenti koji rezultiraju neželjenim događajima.
- Različiti načini realiziranja akcidenta nazivaju se sekvence akcidenta.
- Jedna sekvenca akcidenta sastoji se od inicijalnog događaja i kvarova sustava koji vode do neželjene posljedice (požara, eksplozije, kontaminacije i sl.)

Pet temeljnih koraka VPR

1. Upoznavanje s radom postrojenja, shemama i podacima.
2. Identificiranje i grupiranje inicijatora akcidenata (inicijalnih događaja).
3. Modeliranje sekvenci akcidenata (stablo događaja, SD)
4. Modeliranje otpovijeda sustava (stablo kvara, SK)
5. Određivanje i kvantificiranje sekvenci akcidenata.

VPR na slici


POSTROJENJE
-radne karakteristike
-održavanje
-ljudske aktivnosti
-podaci o kvarovima
STABLO DOGAĐAJA ID A
ID A
OP
SS1
SS2
AO
SS3
DOS
ISHOD
USPJEH
OPASNOST 2
USPJEHA
OPASNOST 2
USPJEH
OPASNOST 2
OPASNOST 1
OPASNOST 1
ID N
GRUPE INICIJ. DOGAĐAJA
ID A
ID B
…
ID X
IZVEDBA I RAD SUSTAVA
21179
21135
FW105PMP-001
'A'
21155
21178
21134
FW105PMP-002
'B'
21154
21177
21133
16'
FW105PMP-003
'C'
21153
STABLO KVARA SS2
TOP
LV1
LV2
A
B
C
B

Korak 1: Upoznavanje s postrojenjem

Inicijalno se prikupljaju sve informacije o projektu, pogonu i dosadašnjem iskustvu s postrojenjem.

- Projektne informacije sačinjavaju P&I dijagrami, sheme sustava, sheme ožičenja i sva ostala dokumentacija.
- Informacije o pogonu prikupljaju se iz postupaka za pogon postrojenja u normalnim i posebnim radnim situacijama.
- Iskustveni podaci dolaze iz svih zapisa o dosadašnjem radu postrojenja (kvarovi, posebna stanja, promjene u postrojenju i sl.)

Korak 2: Identificiranje inicijalnih događaja

- Inicijalni događaji (**ID**) predstavljaju sve poremećaje u pogonu koji zahtijevaju aktiviranje sigurnosnih sustava.
- Inicijalni događaji uključuju veliki spektar poremećaja: gubitak energenta, razna popuštanja i pucanja, slučajne obustave rada postrojenja, gubitak nekog sustava i sl.
- Veliki broj inicijalnih događaja nije pogodan za nastavak analize te se oni stoga se grupiraju.
- Grupiranje IDa ide po sličnosti koja se najčešće određuje prema zahtjevima na sigurnosne sustave. Moguće je grupu lakših IDa modelirati jednim “težim".

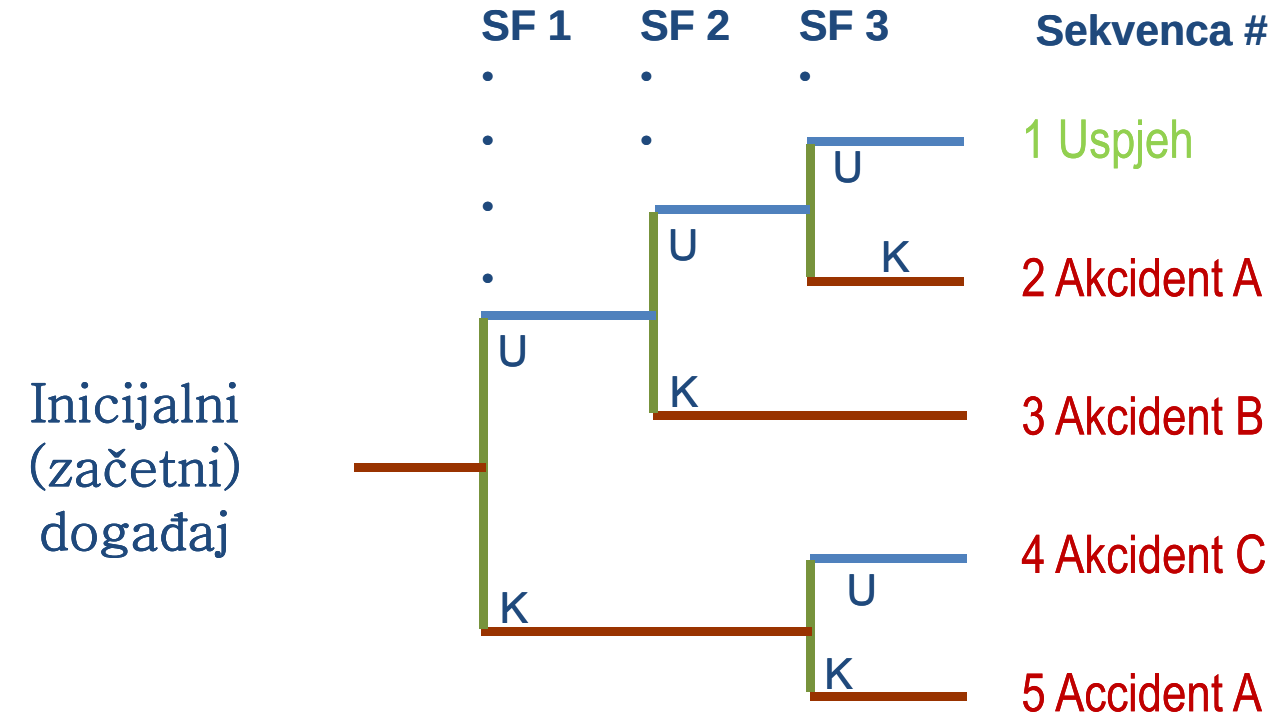
Primjer grupa ID-a:

1. Veliko pucanje voda ili spremnika (energenta, kemikalije i sl.).
2. Malo pucanje voda ili spremnika (energenta, kemikalije i sl.).
3. Prijelazne promjene koje rezultiraju promjenom moda rada procesa (i time zahtijevaju iniciranje nekih sigurnosnih funkcija i potencijal za neželjeni razvoj situacije).
4. Gubitak hlađenja primarnih komponenti u procesu.
5. Gubitak energenta za pogon sustava koji ispunjavaju sigurnosne funkcije (npr. el. energija i gorivo).
6. Gubitak sekundarnog ponora topline.
7. Aktiviranje sigurnosnog sustava bez potrebe.
8. Otkazivanje sustava za obustavu procesa.

Korak 3: Modeliranje sekvenci akcidenata

- Sekvence akcidenata razvijamo pomoću stabla događaja (SD ili *ET*) za svaki inicijalni događaj i prema radu sigurnosnih funkcija te odgovarajućih sustava.
- Stablo događaja razvija se za svaki inicijalni događaj i prikazuje različito ponašanje sigurnosnih sustava tijekom razvoja sekvence.
- Kraj sekvence u funkciji kriterija uspjeha i odaziva sigurnosnih sustava završava uspjehom ili neuspjehom.
- Posebno se razmatraju samo sekvence koje rezultiraju neuspjehom tj. akcidentom.

Stablo događaja



U = Uspjeh sigurnosne funkcije SF
K = Neuspjeh (kvar) sigurnosne funkcije SF
SF = Sigurnosna funkcija

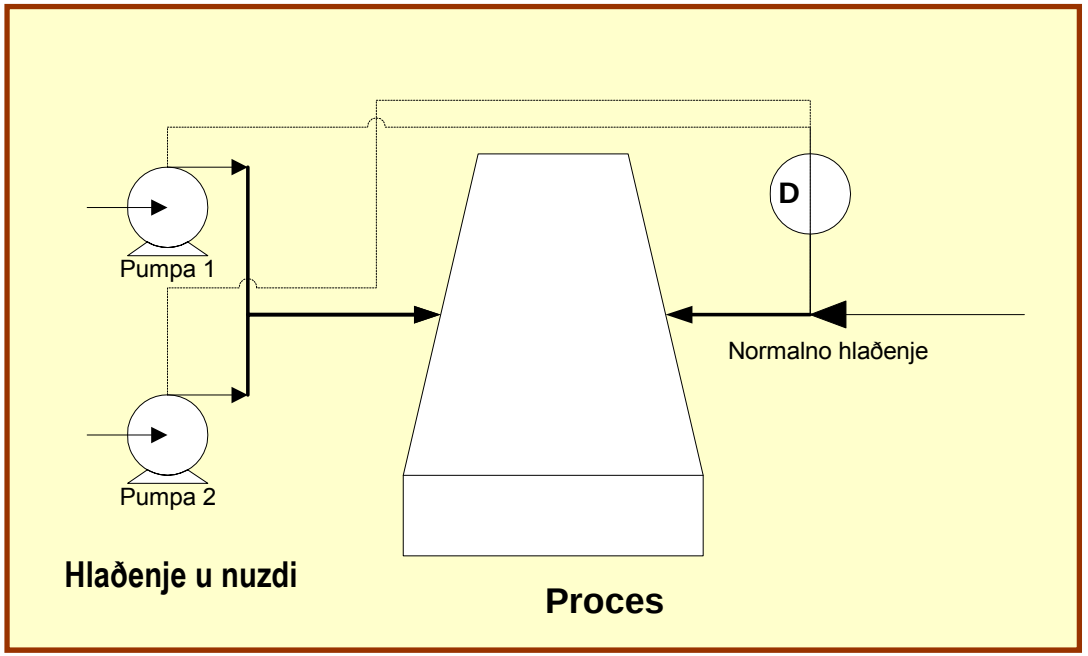
Definiranje analiziranoga sistema

- Funkcije koje obavlja sistem
- Fizičke granice
- Granice analize
- Inicijalna stanja
- “Zamrzavanje” sistema
- Identificiranje opasnosti
- Filtriranje opasnosti
- Definiranje i kategoriziranje inicijalnih (začetnih) događaja

Definiranje sigurnosnih funkcija i scenarija

- Identificiranje funkcionalnih odziva
- Identificiranje fizičkih fenomena
- Grupiranje začetnih događaja
- Određivanje scenarija - razvoja akcidenta
- Identificiranje ovisnosti sistema
- Uvažavanje uvjetnih odziva

Primjer sustava za analizu SDa i SKa

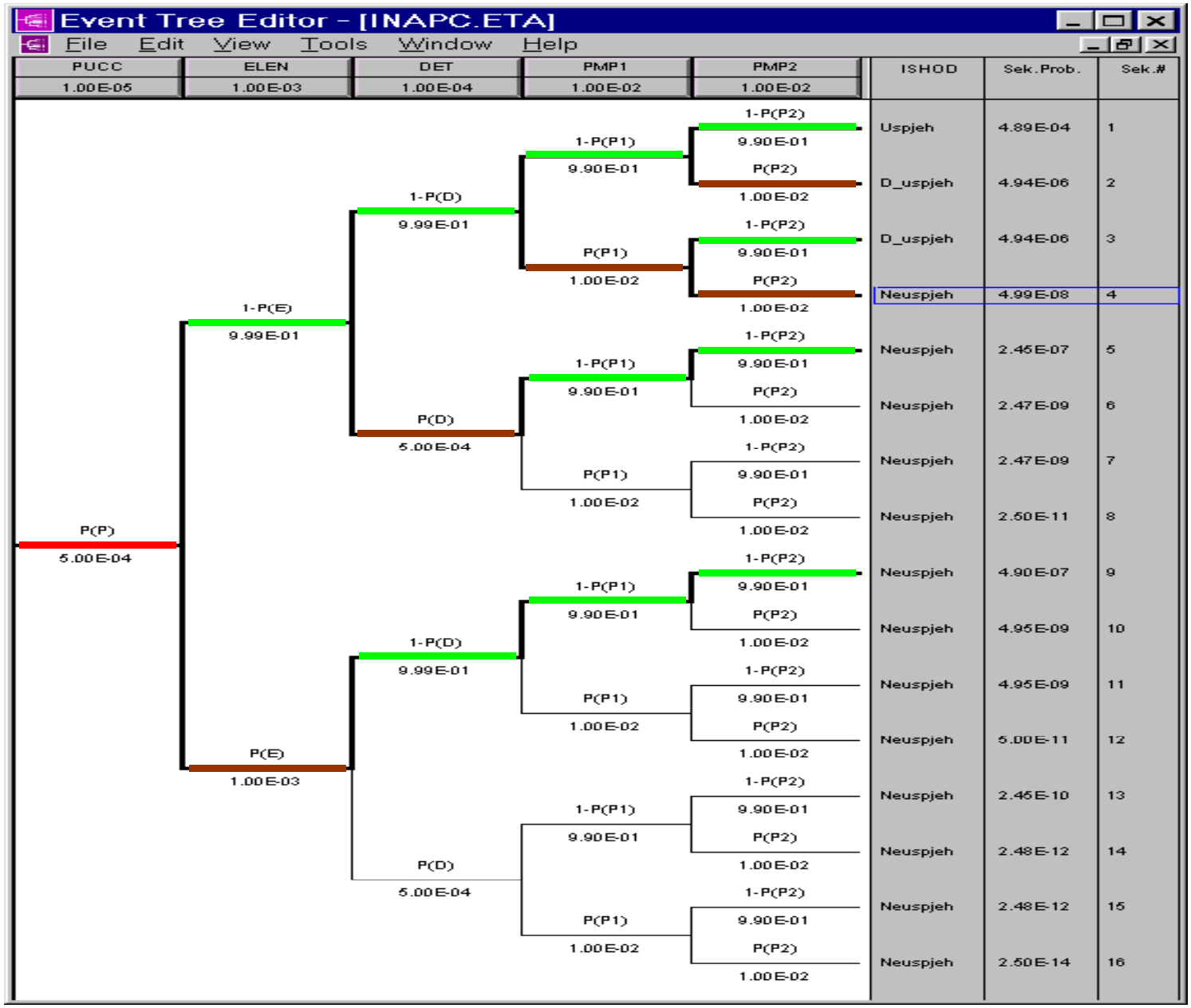


- Inicijalni događaj predstavlja **gubitak** normalnog **hlađenja** procesa.
- Sigurnosni sustav predstavljaju dvije pumpe za hlađenje u nuždi.
- Za uspjeh potrebne su obje pumpe, kontrolna logika **D** i električna energija.
- Ispravan rad samo jedne pumpe rezultira manjim akcidentom.

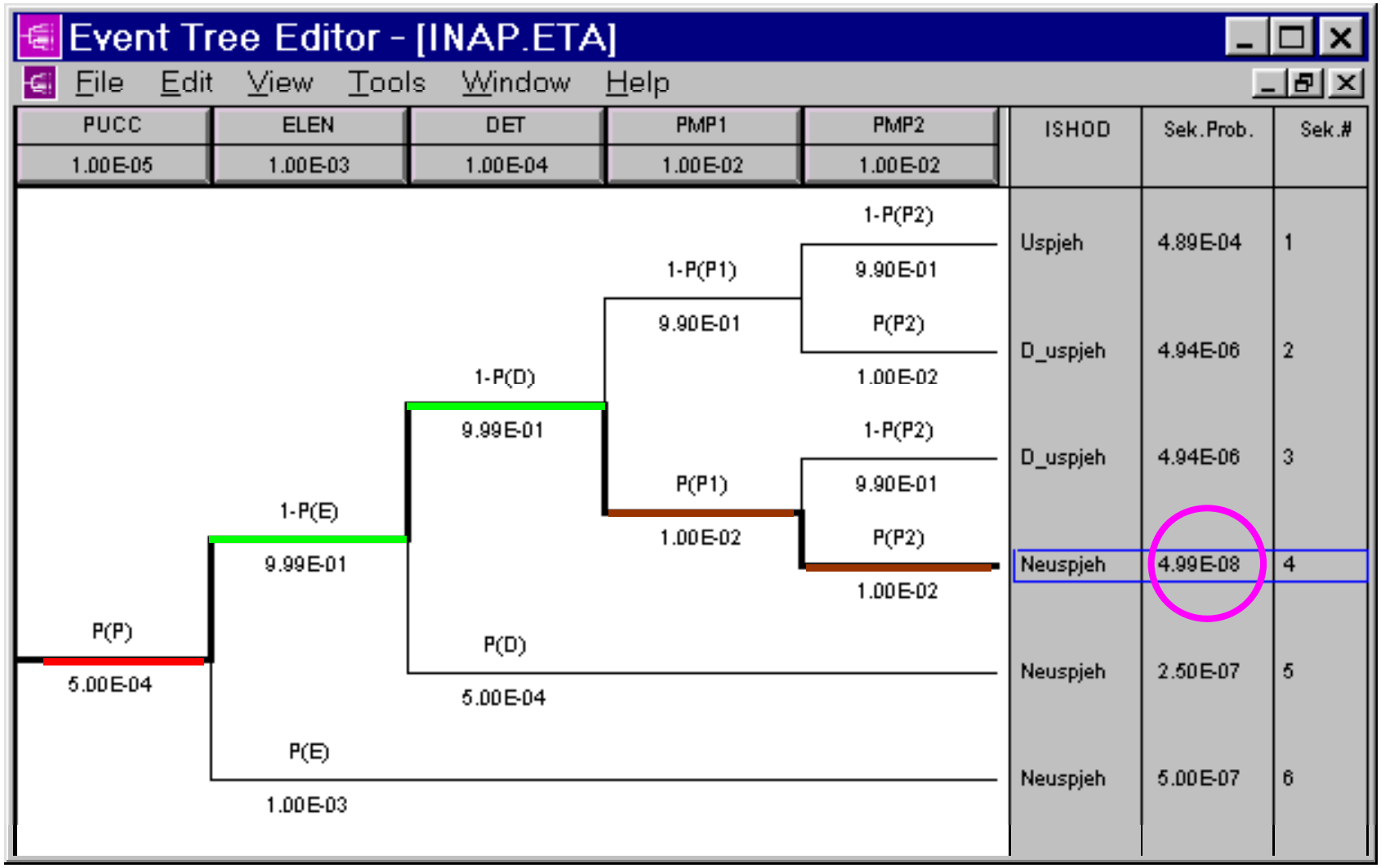
Stablo događaja, SD

- Inicijalni događaj:
  - gubitak normalnog hlađenja - PUCC
- Vršni događaji:
  - Napajanje el. energijom - ELEN
  - Detektiranje gubitka normalnog hlađenja – DET
  - Gubitak podsustava pumpe 1 – PMP1
  - Gubitak podsustava pumpe 2 – PMP2

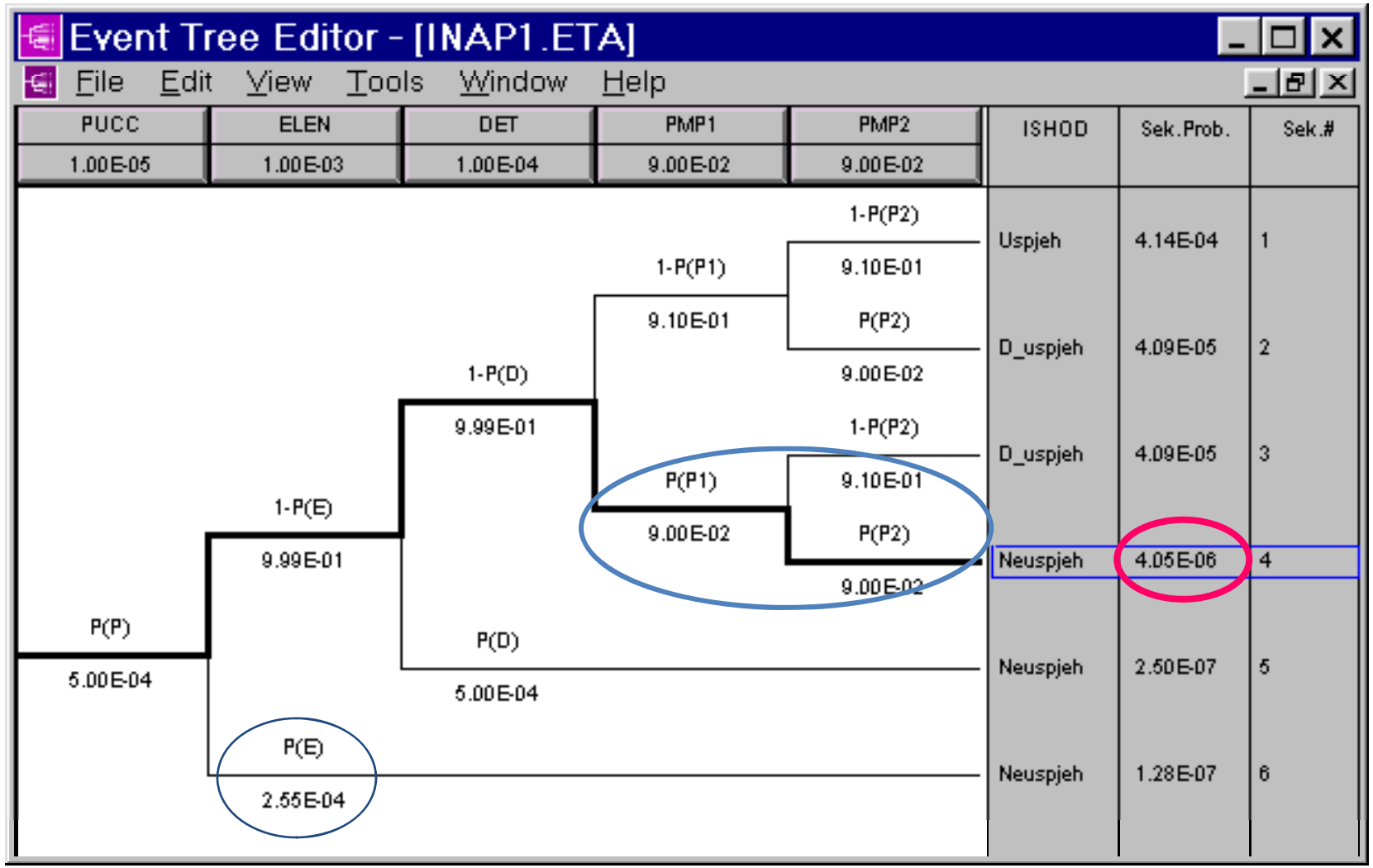
SD (ET) za zadanu situaciju



Pojednostavljeno SD za zadanu situaciju



Promjena podataka SDa



Korak 4: Modeliranje kvara sustava

- Svaki otkaz sustava u stablu događaja modeliran je u cilju iznalaženja uzroka u kvarovima komponenti.
- Relacije među elementarnim kvarovima prema kvaru sustava prikazane su logičkim dijagramom - stablom kvara.
- Stablo kvara (SK ili *FT*) omogućava kvalitativnu analizu i kvantificiranje vjerojatnosti otkaza sustava preko osnovnih događaja i njihovih vjerojatnosti.

Pretpostavke modeliranja

- Pogreške unutar segmenta uslijed kvara na **pasivnoj** komponenti "normalno" se ne razmatraju.
- Kvarovi se promatraju **binarnom** logikom: ili je kvar ili ispravno stanje.
- Kombinacija kvarova koja rezultira **povoljnim** stanjem ne modelira se.
- Ne modelira se **neodgovarajući** dizajn komponente.
- **Akcije operatera** dijele se u dvije skupine: akcija na nivou sistema i akcije na nivou dijelova sistema odnosno nivou komponenata.
- **Hlađenje** radnog prostora i komponenata ocjenjuje se od slučaja do slučaja.
- Neželjeni povratni tok **kroz dva ili više** jednosmjernih ventila u seriji ne modelira se.
- **Podmazivanje** pumpe ili kompresora modelira se samo za slučajeve kada je ovaj sistem vidno odvojen od glavne komponente.
- **Testiranje** se ne modelira za segmente i komponente koji se mogu automatski prebaciti u aktivnu ulogu za vrijeme testiranja po potrebi.

Mjere važnosti

- Kreiranje VSA (SD, SK) modela omogućava određivanje vjerojatnosti određene posljedice (rizika), ali i određivanju važnosti komponenti, podsustava, sustava i ljudskih akcija
- Važnost pojedinih događaja u modelu se određuje izračunavanjem tzv. mjera važnosti

Neodređenosti i osjetljivost

Neodređenosti i osjetljivost dodatno karakteriziraju rezultat.

Izvore neodređenosti i osjetljivosti možemo podijeliti u tri vrste:

- ***Kompletnost pristupa***.
- ***Primjerenost modela***. (ljudske akcija, kvarovi sa zajedničkim uzrokom i vremenska ovisnost nekih događaja.)
- ***Neodređenost ulaznih parametara***.

Osjetljivost

Ispitivanje osjetljivosti na promjenu ulaznih podataka ili mijenjanje dijela modela (npr. SK) radi se na odabranim podacima i dijelovima modela.

Prednosti

- Metodičan pristup: strukturirano i rigorozno
- Većim dijelom primjenjivo za računalnu podršku
- Primjenjivo na raznim nivoima složenosti
- Vizualna prezentacija odnosa uzroka i posljedica
- Relativno jednostavno za učenje
- Kompleksnost sustava se modelira postupno

Mane

- Više stabala događaja nužno za modeliranje realnih postrojenja
- Kritičan utjecaj analitičara na uključivanje svih ovisnosti i utjecaja
- Ključno poznavanje sustava za dobru analizu
- Ovisnost o deterministčkim proračunima za određivanje kriterija uspjeha
- Izostavljanje inicijalnog događaja ili vršnog događaja umanjuje kompletnost analize

Zaključno

- **Kvaliteta** metode stabla događaja i stabla kvara ogleda se u kombiniranju induktivnog i deduktivnog, primjenjivosti u vrlo složenim problemima i bogatstvu informacija koje daju rezultati.
- **Nedostaci** metoda SD i SK leže u zahtjevnosti, statičnosti i neodređenostima (ulaznih podataka). Znanost i "umjetnost".
- Za **pospješivanje efikasnosti** (pojednostavljivanje, ubrzavanje, povećavanje mogućnosti i sl.) primjene ovih metoda uputno je maksimalno koristiti sve zahtjevnije računarske tehnike.

DZ - uvodno

- Potrebno je prema zadanoj situaciji, podatcima i pretpostavkama kreirati stablo događaja i pripadajuća stabla kvara te kvalitativno i kvantitativno riješiti model.
- Svi podsustavi imaju vjerojatnost otkaza 0,001, a beta faktor za podsustave koji mogu otkazati uslijed kvarova sa zajedničkim uzrokom iznosi 0,1. Vjerojatnost inicijalnog događaja iznosi 0,01.
- Za sve redundantne podsisteme valja računati i kvar sa zajedničkim uzrokom.
- Analizirani događaj je: "Vjerojatnost sekvenca koje vode neuspjehu (akcidentu)"
- Kvantitativnu analizu treba provesti samo u prvoj aproksimaciji (suma produkata), ali tako da se najprije minimalizira rješenje.

DZ - zadatak

- Da bi neko postrojenje uspješno obavilo svoju zadaću kod određenog inicijalnog događaja potrebno je da rade sva tri sistema ***A***, ***B*** i ***C***.
  Sistem ***A*** radi ispravno kada su ispravni podsistemi ***a*** i ***b***.
  Sistem ***B*** radi ispravno kada su ispravni podsistemi ***c*** i ***d***.
  Sistem ***C*** radi ispravno kada je ispravan redundantni podsistem ***a*** ili podsistem ***c***.

DZ – rješenje

- Konvencija:

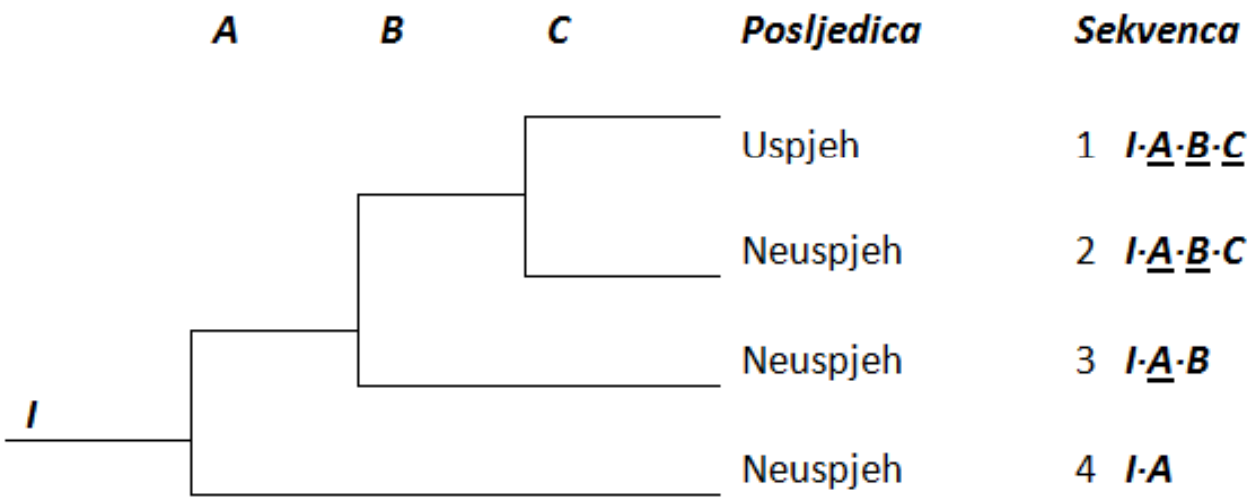
  Kvar - $\boldsymbol{A}$, $\boldsymbol{\alpha}$

  Ispravan rad - $\underline{\boldsymbol{A}}$, $\underline{\boldsymbol{\alpha}}$

  što je povezano sa kvarom - $\underline{\boldsymbol{A}}\boldsymbol{=1-A}$, $\underline{\boldsymbol{\alpha}}\boldsymbol{=1-\alpha}$

DZ – rješenje 1

Da bi neko postrojenje uspješno obavilo svoju zadaću kod određenog inicijalnog događaja potrebno je da rade sva tri sistema ***A***, ***B*** i ***C***.



DZ – rješenje 2

Sistem ***A*** radi ispravno kada su ispravni podsistemi ***a*** i ***b***.
Sistem ***B*** radi ispravno kada su ispravni podsistemi ***c*** i ***d***.
Sistem ***C*** radi ispravno kada je ispravan redundantni podsistem ***a*** ili podsistem ***c***.

Stablo kvara za sisteme:

	Podsistem A	**Podsistem B**	**Podsistem C**
Kvar	***a+b***	***c+d***	***a·c+z***
Ispravan rad	*(a+b)* = ***a·b***	*(c+d)* = ***c·d***	*(a·c+z)* = ***(a·c)·z*** = ***(a+c)·z***

z - kvar sa zajedničkim uzrokom za podsisteme ***a*** i ***c***

DZ – rješenje 3

- Vjerojatnost neuspjeha:

$$N = S1 + S2 + S3 = I \cdot \underline{A} \cdot \underline{B} \cdot C + I \cdot \underline{A} \cdot B + I \cdot A$$

$$N/I = \underline{a} \cdot \underline{b} \cdot \underline{c} \cdot \underline{d} \cdot (a \cdot c + z) + \underline{a} \cdot \underline{b} \cdot (c + d) + (a + b)$$

$$N/I = \underline{a} \cdot \underline{b} \cdot \underline{c} \cdot \underline{d} \cdot a \cdot c + \underline{a} \cdot \underline{b} \cdot \underline{c} \cdot \underline{d} \cdot z + \underline{a} \cdot \underline{b} \cdot c + \underline{a} \cdot \underline{b} \cdot d + a + b$$

$$N = I\,(\underline{a} \cdot \underline{b} \cdot \underline{c} \cdot \underline{d} \cdot z + \underline{a} \cdot \underline{b} \cdot c + \underline{a} \cdot \underline{b} \cdot d + a + b)$$

$$N = 0{,}01\,(\underline{0{,}999} \cdot \underline{0{,}999} \cdot \underline{0{,}999} \cdot \underline{0{,}999} \cdot 0{,}1 \cdot 0{,}001 + \underline{0{,}999} \cdot \underline{0{,}999} \cdot 0{,}001 + \underline{0{,}999} \cdot \underline{0{,}999} \cdot 0{,}001 + 0{,}001 + 0{,}001)$$

$$N = 4{,}10E\text{-}05$$