1. Mjere važnosti, osjetljivost i neodređenost

- razne vrste analize osjetljivosti (jednostruka, dvostruka, tornado dijagrami, mjera diferencijalne važnosti)
- analiza neodređenosti (Monte Carlo, globalna anliza osjetljivosti)
- analiza osjetljivosti:
    - provjera ispravnosti i robusnosti modela
    - naglašava kritičnu ovisnost ishoda o parametrima modela
    - proučavanje promjene rezultata (izlaz) modela u ovisnosti o promjenama vrijednosti parametara (ulaz) modela
    - prednosti – jednostavno numerički provesti, rezultati su odmah razumljivi
    - mane – istovremeno se mogu mijenjati samo jedan ili dva parametra, raspon ulaznih vrijednosti parametara ne razmatra se zajedno s rasponom izlaznih parametara (nije iskoristivo za određivanje važnosti parametara)
    - koncept važnosti parametara nije formaliziran, ali se široko primjenjuje za donošenje odluka prema riziku i optimiranje resursa
    - model : $U = f(x_1, x_2, ... , x_n)$
    - lokalna a.o. : određuje relevantnost parametara sa fiksnim vrijednostima ostalih parametara
    - globala a.o. : određuje relevantnost parametara s njegovom ukupnom neodređenošću
    - diferencijalna mjera važnosti
        - nominalni rezultat – nema neodređenosti parametara; vrijednosti parametara su nominalne
        - lokalna dekompozicija (parcijalna derivacija od f po svim parametrima)
        - aditivnost – $I(x_i, x_j) = I(x_i) + I(x_j)$; DMV uvijek aditivna
- analiza neodređenosti:
    - aleatorna neodređenost – odnosi se na realizaciju događaja (pr. ostvarivanje kvara pumpe)
    - epistemička neodređenost – neodređenost uslijed nedostatka znanja u prikazivanju stvarnosti odabranim modelom (vjerojatnosti kvara itd.)
    - neodređenost rezultata u ovisnosti o funkciji neodređenosti parametara; ponavljanjem za sve ostale parametre dobije se ukupna neodređenost rezultata
    - Monte Carlo metoda
        - generator slučajnih brojeva „u“ između 0 i 1
        - brojevi se generiraju prema uniformnoj distribuciji
        - lambda = $F^{-1}(u)$
        - vrijednosti za lambda se sempliraju preko vrijednosti „u“ i tako imaju distribuciju vjerojatnosti iz koje smo ih kreirali
        - za svaki parametar modela treba kreirati statističku distribuciju
        - postupak: generirati broj između 0 i 1 -> odrediti vrijednost inverzijom iz pripadajuće distribucije -> korištenjem tih vrijednosti izračunati rezultate modela -> zabilježiti dobiveni rezultat – N puta (N = broj varijabli)
- izvore neodređenosti i osjetljivosti možemo podijeliti u tri vrste:
    - kompletnost pristupa
    - primjerenost modela (ljudske akcije, KZU, vremenska ovisnost nekih događaja)
    - neodređenost ulaznih parametara
- ispitivanje osjetljivosti na promjenu ulaznih podataka ili mijenjanje dijela modela (npr. SK)

radi se na odabranim podacima i dijelovima modela
- analiza važnosti omogućuje:
    - rangiranje komponenata i sustava važih za sigurnost postrojenja
    - rangiranje po utjecaju na nepouzdanost (neraspoloživost) postrojenja
    - rangiranje po utjecaju na održavanje postignute razine sigurnosti postrojenja
- mjera smanjenja rizika, mjera povećanja rizika

2. Funkcionalna sigurnost

- funkcionalna sigurnost čini dio ukupne sigurnosti ovisne o ispravnom radu sustava u interakciji s okolinom
- analiza opasnosti:
    - identificiranje značajnih opasnosti vezano za korištenje određenog sustava
    - opasnosti identificira korisnik i to odobrava sigurnosni autoritet
    - određuje potrebu za sigurnosnim funkcijama sustava kao zaštitu od posljedica opasnosti
- f.s. predstavlja jedan pristup smanjivanju rizika
- rješenja inherentne sigurnosti i uklanjanje mogućnosti pojavljivanja opasnosti – preferirane alternative
- sigurnosni zahtjevi sustava:
    - sigurnosna funkcija – što sustav treba raditi; definiraju se na temelju analize opasnosti
    - sigurnosni integritet – s kojom vjerojatnosti će sustav obaviti zadanu funkciju; definiraju se na temelju analize rizika
- sigurnosni sustav – složena mehanička, električna, elektronička i programabilna rješenja
- postizanje sigurnosnog integriteta:
    - dobra i kompletna specifikacija zahtjeva sustava
    - smanjivanje slučajnih ili sustavnih kvarova (utjecaj pomoćnih sustava, predviđanje vanjskih utjecaja, oprema, KZU, ljudska greška...)
- uloga standarda:
    - uskladiti mogućnosti novih tehnoloških rješenja i povećanih sigurnosnih zahtjeva
    - definirati tehnički konzistentan okvir za određivanje sigurnosnih zahtjeva na bazi rizika
    - jasnoća zahtjeva, efikasnost komunikacije, razvoj tehnika analiza potrebe i usklađenosti
    - određivanje zahtjeva integriteta sigurnosti na temelju rizika uz obrazlaganje općeg pristupa i primjene
    - pristup vezan za ukupni životni ciklus sustava i nužnih aktivnosti za osiguravanje postizanja funkcionalne sigurnosti
    - zajedničko djelovanje prevencije opasnosti i kontrole rizika
    - propisivanje tehnika i mjera nužnih za postizanje i demonstriranje zahtijevanog integriteta sigurnosti
- životni ciklus sustava:
    - koncept i izvedivost – sve aktivnosti koje prethode specificiranju zahtjeva sustava i sve pripadajuće opreme
    - definiranje zahtjeva – definiranje sustava i uvjeti primjene; analiza rizika; zahtjevi sustava
    - dizajn – raspodjeljivanje zahtjeva sustava; konstrukcija i primjena

    - implementacija – konstrukcija i primjena; proizvodnja
    - instaliranje i predaja – instalacija; validacija sustava; prihvaćanje sustava
    - pogon i održavanje – praćenje performansi; modifikacije i unapređenja
    - stavljanje izvan pogona i razgradnja
- određivanje TIO (tolerantni intenzitet opasnosti):
    - održavanje postojećeg nivoa sigurnosti (GAMAB ili GAME – minimum)
    - malo koliko je razumno provedivo (ALARP – as low as reasonable practicable)
    - ograničenje prema relativnom riziku (MEM – minimum endogenous mortality)
- plan sigurnosti – uvod, pozadina i zahtjevi, aktivnosti upravljanja sigurnosti, kontrole sigurnosti, dokumentiranje sigurnosti, sigurnosno inženjerstvo, validacija i verifikacija vanjskih elemenata
- dokumentacija i kontrola konfiguracije
    - plan upravljanja konfiguracijom
    - dnevnik opasnosti – uvod, dnevnik, imenik, podaci o opasnostima, podaci o incidentima, podaci o akcidentima
- nužno je analizom pouzdanosti sustava demonstrirati zadovoljenje zahtjeva sigurnosnog integriteta i dizajna (metoda stabla kvara, analiza kvarova i posljedica)
- neovisna ocjena usklađenosti sa standardima – kontrolni sigurnosni pregledi, ocjena sigurnosti, nalazi pregleda i ocjene
- sigurnosni integritet softvera
    - definiran na osnovi uloge u sustavu
    - definiranje životnog ciklusa softvera
- specifikacija softvera
    - specifikacija i testiranje zahtjeva na osnovi dokumentacije sustava i plana osiguranja kvalitete softvera
    - preporučene metode – JSD, MASCOT, SADT, SDL, SSADM, Yourdon (strukturirane)
    - za NIS3 i NIS4 preporučene:
        - formalne – CCS, CSP, HOL, LOTS, OBJ, Temporal Logic
        - poluformalne – dijagrami slijedova, logički blok dijagrami, tablice odluka, dijagrami promjene stanja, vremenske petrijeve mreže
- kvantitativna i kvalitativna dimenzija zahtjeva
- plan i izvještaj moraju postojati za sve faze životnog ciklusa sustava
- kompletan pristup inženjerskom upravljanju ima čitav niz formalnih šustinskih pretpostavki i zahtjeva
- serija CENELEC standarda predstavlja cjelovito i složeno definiranje zahtjeva u procesu konstrukcije i korištenja sigurnosnih uređaja

3. Odlučivanje i upravljanje rizikom

- odlučivanje u uvjetima:
    - izvjesnosti – sigurni smo u ishode odluka
    - rizika – nismo sigurni, ali znamo kakve su nam šanse (vjerojatnosti i posljedice)
    - neizvjesnosti – ne znamo vjerojatnosti ni ishode
- odlučivanje u uvjetima izvjesnosti
    - vjerojatnost svakog ishoda je 1
    - bira se alternativa čiji je „I“ najpovoljniji
- odlučivanje u uvjetima rizika
    - vjerojatnost može biti objektivna (zasnovana na podacima iz prošlosti ili na iskustvu odlučivanja u sličnim situacijama) ili subjektivna (individualno uvjerenje donosioca odluke o ostvarenju nekog događaja na bazi informacija koje posjeduje)
    - metode donošenja odluka:
        - najveća vjerodostojnost – zasniva se na pretpostavci da će se u budućnosti ostvariti događaj s najvećom vjerojatnošću
        - maksimalna očekivana vrijednost – očekivana vrijednost = suma umnoška iznosa očekivanih ishoda i vjerojatnosti njihovog nastajanja
        - minimalno očekivano kajanje – svodi se na minimiziranje propuštenog dobitka
- odlučivanje u uvjetima neizvjesnosti
    - moguće odrediti ishode, ali nije moguće odrediti vjerojatnost njihovog nastajanja
    - metode donošenja odluka:
        - optimistička – maximax
        - pesimistička – maximin
        - optimizam-pesimizam – najbolji rezultat množi se sa indeksom optimizma, a najlošiji s indeksom pesimizma
        - minimax kajanje – minimiziranje maksimalnog iznosa kajanja
        - laplas – pretpostavka da su sve alternative podjednako vjerojatne
    - dva pristupa u konačnom izboru alternative:
        - primjeniti sve metode odlučivanja i odabrati onu alternativu koja je najbolja po većini metoda
        - analizirati sve metode i ispitati konzistentnost njihovih rješenja, a zatim donijeti odluku na temelju „najbolje“ metode
- korisnost – kada se kriterij odluke mora bazirati ne samo na očekivanoj novčanoj vrijednosti; mjera totalne vrijednosti određenog ishoda reflektirajući određeni pristup; posebno primjerena u situacijama gdje su pretpostavljene vrlo velike ili vrlo male vrijednosti dobitka
- za sve scenarije (alternativa i okolnosti) odredi se umnožak korisnosti i vjerojatnosti ostvarivanja scenarija → suma umnožaka za svaku alternativu (svi scenariji) predstavlja njenu očekivanu korisnost → odabrana alternativa ima najveću očekivanu korisnost
- ekvivalent sigurnosti – iznos novca koji odgovara iznosu novca koji uključuje rizik
- očekivana novčana vrijednost(ONV) – očekivana vrijednost rizične situacije
- premija rizika: PR = ONV – Ekvivalent sigurnosti
- očekivana korisnost rizične situacije – očekivana vrijednost rizika u korisnosti
    - OK(rizik) = Korisnost(Ekvivalent sigurnosti)
- **uzimamo očekivanu vrijednost korisnosti, a ne korisnost očekivane vrijednosti**
- svaki ishod može imati mjeru koja određuje njegovu korisnost
- funkcija korisnosti – povezuje ishode i korisnosti – $U(I_i)$
- odabir najbolje alternative moguće napraviti nakon što se odredi max. očekivana korisnost

- odlučivanje o najboljem pristupu nije jednoznačno bez obzira uključuje li se vjerojatnost ili ne
- određivanje rizika nužna je pretpostavka, ali ne i dovoljna podloga za donošenje odluka o tome koja alternativa predstavlja optimalni izbor