DOI:10.33179/BSV.99.SVI.11.CMC.19.4.6

Brane Bertoncelj

ZANESLJIVOST POSAMEZNIKA PRI DELOVANJU KRITIČNE INFRASTRUKTURE SODOBNE DRŽAVE

RELIABILITY OF INDIVIDUALS IN THE OPERATION OF A MODERN STATE CRITICAL INFRASTRUCTURE

Povzetek Vpliv posameznika na delovanje kritične infrastrukture je eden najbolj nezanesljivih in nepredvidljivih dejavnikov, zato pomeni zanjo stalno nevarnost, ki je ne smemo podcenjevati. Postavlja se vprašanje, koliko si prizadevati za še večji tehnološki napredek, da bi bile tehnološke in fizične sestavine kritične infrastrukture varnejše, po drugi strani pa, kako obravnavati posameznika pri upravljanju teh kompleksnih sistemov, saj ta postaja vse pomembnejši referent za njeno zanesljivo delovanje. Avtor predstavlja okvir modela vpliva posameznikove zanesljivosti na delovanje kritične infrastrukture sodobne države. Ugotavlja, da je zanesljivost posameznika v neobičajnih razmerah najbolj odvisna od stopnje njegove motiviranosti, usposobljenosti in pripadnosti organizaciji. Samovarovalne dejavnosti in preprečevanje možnosti za neobičajne razmere so pretežno prostovoljna dejanja, pri katerih sta najpomembnejša pojma pripravljenost in volja nekaj koristnega delati za organizacijo. Za zanesljivo delovanje posameznika moramo imeti vizijo in cilje.

Ključne besede ***Posameznikova zanesljivost, kritična infrastruktura, tveganja, neobičajne razmere, odločanje.***

Abstract The influence of individuals on the operation of critical infrastructure is one of the most unreliable and unpredictable factors, and as such represents a constant threat that should not be underestimated. The question arises as to how much effort to invest in the technological progress in order to make technological and physical components of critical infrastructure safer, and, on the other hand, how to deal with individuals in the management of these complex systems, as individuals are becoming an increasingly important reference point to insure its reliable operation. The author presents the framework of the model of the influence individuals' reliability has on the operation of a modern state critical infrastructure. He notes that the reliability of an individual in unusual circumstances mostly depends on the level of their motivation, competence and affiliation to the organization. Self-protective activities and the prevention of possible

abnormal circumstances are predominantly voluntary acts, where the most important concepts are willingness and the will to do something useful for the organization. A reliable performance of an individual requires a vision and goals.

Key words ***Reliability of individuals, critical infrastructure, risks, abnormal situation, decision making.***

Uvod

Živimo v družbenem obdobju, v katerem sta posameznik in družba izpostavljena številnim virom ogrožanja ter tveganjem. Ti so posledica procesov, ki potekajo v družbi in so odsev njenega političnega, ekonomskega, socialnega in tehnično tehnološkega razvoja. Izzivi okolja so drugačni, kot so bili nekoč, označujejo pa jih predvsem velike spremembe v načinu poslovanja, terorizem, globalizacija in mednarodna soodvisnost. Družbene spremembe so hitre, kompleksne, nestabilne in težko predvidljive. Potrjuje se teza, da smo vstopili v občutljivo obdobje tveganj, ki so sama po sebi vključena v koncept razvoja socialne, pravne in gospodarske rasti družbe (Broder, 2006). Za današnjo družbo je značilno, da postajajo varnostni izzivi, ogrožanja in tveganja vse bolj osebni.

Obravnavanje posameznikove zanesljivosti pri delovanju kritične infrastrukture ni novo, v zadnjem času pa se je zaradi terorističnih napadov, groženj in škodnih dogodkov zanimanje za to področje močno povečalo. Posameznik do zdaj ni še nikoli imel toliko intelektualnih in tehničnih zmogljivosti za oblikovanje svoje prihodnosti, kot jih ima danes. Nikoli do zdaj še ni bilo pred eno generacijo toliko pomembnih odločitev, čeprav je družba zelo omejujoča.

Pomembnost posameznikove vloge kaže podatek, da naravni kapital danes sestavlja le še 20 odstotkov, fizični 16 in človeški kapital kar 64 odstotkov poslovnih procesov (Svetličič, 2005). Ob predpostavki, da razpolagamo s tehnološko dovršeno kritično infrastrukturo in da lahko na učinke iz zunanjega okolja vplivamo le delno, je posameznik eden najpomembnejših dejavnikov tudi pri zagotavljanju neprekinjenosti njenega delovanja. Če se je ta v preteklosti nanašala pretežno na tehnične rešitve, se je danes treba osredotočiti tudi na družbeno socialne in korporativno varnostne vidike ter poudariti pomen odločanja posameznika pri tem. Posameznik je konkurenčna prednost kritične infrastrukture in tudi največji dejavnik tveganja.

Sistematično opredeljevanje ukrepov in postopkov, kar je v splošnem značilno za upravljanje kritične infrastrukture, je pomembno z vidika preventive, saj ta prispeva k zmanjševanju, preprečevanju in izogibanju varnostnim izzivom ter grožnjam, ki so povezane s tako občutljivim družbenim področjem delovanja.

Poznamo vsaj dva vidika razmerja posameznik – sistem na področju kritične infrastrukture:

– kognitivni inženiring, ki se nanaša na nenehno strokovno usposabljanje in motiviranje posameznika za uspešno delovanje kritične infrastrukture;

– posameznikovo zanesljivost, ki pomeni povečevanje njegove učinkovitosti, ustvarjalnosti, pripadnosti organizaciji, odpornosti na napake, osebne trdnosti ipd.

Posameznikovo odločanje je zapleteno in pogosto je racionalno omejeno. Postavlja se vprašanje, koliko si prizadevati za še večji tehnološki napredek, da bi bile fizične sestavine kritične infrastrukture varnejše, po drugi strani pa, kako obravnavati posameznikovo nezanesljivost. Prevladujoče mnenje je, da morajo biti za ocenjevanje zanesljivosti posameznika organizacija dela, vodenje poslovanja, računalniška programska oprema in delovni postopki dovolj vzdržljivi, da se lahko poleg naravnih nesreč uprejo neprimernim posameznikovim posegom, ki so naključni ali zlonamerni.

1 METODOLOŠKI OKVIR

Zanesljivost bom obravnaval kot psihosocialno kategorijo posameznika v družbenem sistemu sodobne države. Analiziral bom teoretična izhodišča in ugotovitve iz drugih raziskav o vplivu zanesljivosti posameznika na upravljanje kritične infrastrukture, predstavljena pa bodo temeljna spoznanja obravnavane tematike. V tem okviru si postavljamo raziskovalni vprašanji, kako sodobne države opredeljujejo zanesljivost posameznika pri delovanju kritične infrastrukture in katere so metode ugotavljanja zanesljivosti posameznika. Na podlagi pregleda metodologij in praks bom oblikoval okvir modela za ocenjevanje posameznikove zanesljivosti pri delovanju kritične infrastrukture.

2 ZAGOTAVLJANJE POSAMEZNIKOVE ZANESLJIVOSTI PRI DELOVANJU KRITIČNE INFRASTRUKTURE SODOBNE DRŽAVE

Grožnje kritične infrastrukture po eni strani izhajajo iz mogočega vpliva na posameznika kot uporabnika njenih storitev, po drugi strani pa je kljub visoki stopnji avtomatizacije delovanja posameznik pri upravljanju teh kompleksnih sistemov eden najpomembnejših referentov za njeno varno delovanje. Ta vpliv je lahko neposreden ali posreden. Tehnologija je dosegla točko, ko bo izboljšano varnost mogoče doseči le na podlagi boljšega razumevanja tveganj in možnosti za posameznikovo napako. V okviru verjetnostnih varnostnih analiz se ugotavlja, kateri scenariji groženj kritične infrastrukture se lahko zgodijo, kako verjetno je, da se zgodijo, kako hude so lahko njihove posledice in kakšna je pri tem posameznikova zanesljivost.

Zagotavljanje delovanja kritične infrastrukture je zahtevna naloga sodobne države, ki vključuje več ukrepov in dejavnosti, kot so načrtovanje, razvoj in ocenjevanje tveganj varnostnih izzivov ter groženj in sprejemanje preventivnih ter kurativnih ukrepov in postopkov glede na razpoložljive finančne, tehnične in kadrovske zmogljivosti. Morebitno namerno ali nenamerno ogrožanje narave ali posameznika vpliva na zanesljivo poslovanje kritične infrastrukture. Pomembnost kritične infrastrukture za sodobno družbo je bila v različnih raziskavah navedenega kompleksnega področja

korporativne varnosti z uporabo multidisciplinarnih pristopov v Sloveniji že večkrat utemeljena (na primer avtorji Vršec, Čaleta, Podbregar, Prezelj), tuje raziskave pa bodo predstavljene v nadaljevanju. Kritična infrastruktura ima ekonomski pomen (vpliv na gospodarstvo), politični pomen (stabilnost družbenega sistema in nacionalne varnosti) ter funkcionalni pomen (storitve infrastrukture vplivajo na delovanje gospodarskih in družbenih dejavnosti, ohranjajo tradicionalni način življenja ter družbeno blaginjo).

Pregled številnih opredelitev in dejavnikov kritične infrastrukture kaže, da avtorji posebej ne opredeljujejo posameznikove zanesljivosti kot bistvenega pogoja za njeno neprekinjeno delovanje. Pojem zanesljivosti se obravnava predvsem glede na dostopnost storitve kritične infrastrukture (Johnson, 2006). Pri zagotavljanju zanesljivosti delovanja kritične infrastrukture so se raziskovalci ukvarjali zlasti z organizacijskimi, tehničnimi in fizičnimi vidiki. V zadnjem obdobju se sicer povečuje vloga družboslovnih pristopov (Dunn, 2005), podcenjena pa je vloga posameznika v tem sistemu.

Analizirali smo opredelitev zanesljivosti posameznika pri delovanju kritične infrastrukture v strateških dokumentih o kritične infrastrukture izbranih držav in skupnosti, in sicer Evropske unije, ZDA, Nemčije in Slovenije.

Evropska unija (Direktiva Sveta Evropske unije o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite, 2008), Nemčija (Nacionalna strategija varovanja kritične infrastrukture, 2004) in Slovenija (Uredba o evropski kritični infrastrukturi, 2011, Osnovni in sektorski kriteriji kritičnosti za določanje kritične infrastrukture državnega pomena v Republiki Sloveniji, 2014), v javno dostopnem gradivu nimajo opredeljene posameznikove zanesljivosti pri delovanju kritične infrastrukture, niti ni znana metodologija ocenjevanja tveganj s tega področja.

Pomembnost zaščite kritične infrastrukture, preglednost obravnave in sistematičen pristop na tem področju se kaže v varnostni politiki ZDA. Sprejet je bil Nacionalni načrt zaščite infrastrukture (NIPP, 2013), ki predstavlja celostni izbor programov, ukrepov in dejavnosti, ki potekajo med različnimi sektorji, pa tudi nove in razvijajoče se zaščite kritične infrastrukture. Analiza tveganja se nanaša na fizične, računalniške in človeške elemente. Podrobno obravnava cilje zaščite, identificira področja kritične infrastrukture, prepoznava in ocenjuje tveganja, načrtuje dejavnosti in jih implementira z zmanjšanjem varnostnih izzivov in groženj ter minimaliziranjem posledic škodljivih učinkov delovanja narave ali posameznika. Posebna pozornost je namenjena pretoku informacij in usposabljanju udeležencev na vseh ravneh delovanja. Načrt omogoča integracijo strategij, zmogljivosti in struktur upravljanja kritične infrastrukture ter tudi medsebojno obveščenost o kritičnih tveganjih. Pristop k upravljanju tveganj kritično dopolnjuje in podpira Program za prepoznavanje nevarnosti in oceno tveganj (FEMA, 2013).

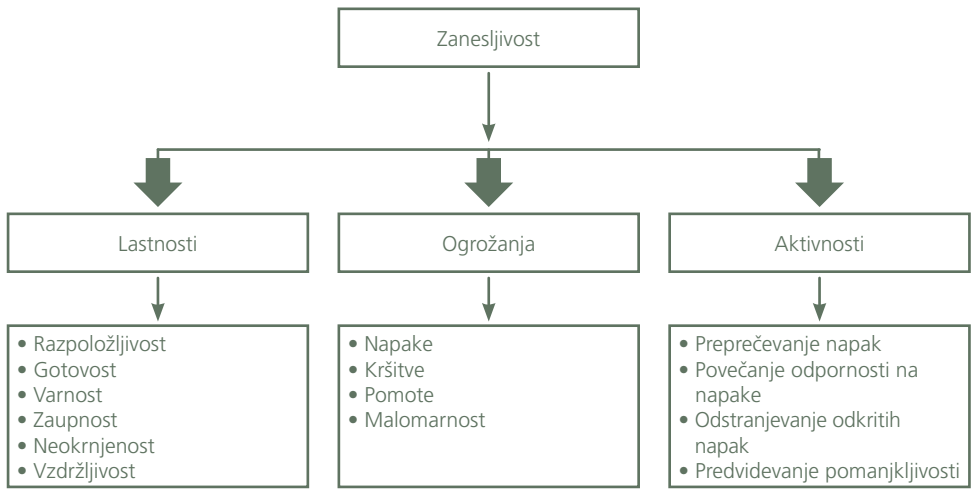
3 POSAMEZNIKOVA NEZANESLJIVOST

Tradicionalno pojmovanje zanesljivosti vključuje razpoložljivost in interval razpoložljivosti. Zanesljivost je verjetnost (ponovljivost, doslednost), da sestavni del ali sistem kot celota pod določenimi pogoji in po vnaprej določenem časovnem intervalu opravlja svojo nalogo brez odpovedi (Rausand, 2004, Condra, 2001)[1]. V vsakem sistemu, ki je podvržen entropiji in homeostazi, je prednostna naloga sistemskega inženiringa določiti zahteve glede zanesljivosti in razpoložljivosti.

Zanesljivost je sposobnost kritične infrastrukture, da ohrani svoje delovne parametre. Ti se nanašajo na zaupanje v sposobnost kritične infrastrukture, da opravi kakovostno storitev na določenem območju in v določenem času. Zanesljivost se kot skupni izraz uporablja za opis razpoložljivosti in njenih vplivnih dejavnikov, kot so uspešnost, zmogljivost vzdrževanja in uspešnost strokovne podpore. Dobra praksa delovanja na tem področju je osredotočena na ekstrapolacijo sedanjih tehnoloških, gospodarskih ali družbenih gibanj in poskuša predvideti prihodnja gibanja, z upoštevanjem delovanja socialnih ter tehničnih sistemov v razmerah negotovosti in nestabilnosti.

Pojem zanesljivost kritične infrastrukture lahko obravnavamo s treh povezanih vidikov, in sicer lastnosti, ogrožanja in aktivnosti (kazalniki so prikazani na sliki 1). Lastnosti se nanašajo na razpoložljivost, gotovost, varnost, zaupnost, neokrnjenost in vzdržljivost. Pri ogrožanju je lahko kritična infrastruktura izpostavljena napakam v poslovnih procesih, kršitvam, pomotam in/ali malomarnosti. Zanesljivost kritične infrastrukture je mogoče zagotavljati s preprečevanjem napak, povečanjem odpornosti na napake, z odstranjevanjem odkritih napak in predvidevanjem pomanjkljivosti (Avizienis idr., 2001).

Slika 1: Kazalniki zanesljivosti (prirejeno po Avizienis idr., 2001)



[1] *Razprava o teorijah zanesljivosti in verjetnosti presega obseg članka.*

Vpliv posameznika na kritično infrastrukturo je eden najbolj nezanesljivih in nepredvidljivih dejavnikov, zato pomeni zanjo stalno nevarnost, ki je ne smemo podcenjevati. Posameznik z vsemi svojimi pristojnostmi, potrebami, motivi, stališči in notranjimi osebnostnimi dejavniki pomeni pomemben ter kritični člen kritične infrastrukture, ker vstopa v interakcije z njo, zaznava in nadzira nevarnosti ter dela napake in jih popravlja. Zlonamerna napaka je posameznikova odločitev in je iz delovanja kritične infrastrukture ne moremo izločiti, lahko pa s preventivnimi ukrepi in postopki zmanjšamo njen škodljivi učinek. Posameznikova vloga je negativna, kadar povzroča naključne ali zlonamerne napake, in pozitivna, kadar jih odpravlja (Polič idr., 1998). Posameznikova napaka je univerzalna in tudi neizogibna. Organizacija si lahko prizadeva, da bi jo preprečila, vendar je nikoli ni mogoče popolnoma odpraviti. Napaka sama po sebi ni slaba, saj uspeh in neuspeh izhajata iz istih temeljev. Brez uspeha in neuspeha se ne moremo naučiti in tudi ne pridobiti znanja ter spretnosti, ki so bistveni za varno in učinkovito delovanje kritične infrastrukture.

Na posameznika pri delovanju kritične infrastrukture vpliva več dejavnikov, na primer družbeni, socialni, okoljski, fiziološki, organizacijski, fizični ipd. Osnovna domneva sistemskega pristopa je, da je posameznik zmotljiv in napako lahko pričakujemo tudi pri delovanju kritične infrastrukture. Napaka se pojavlja kot posledica in ne kot vzrok, ki ima svoj izvor v posameznikovi naravi, ali kot tehnični dejavnik. Protiukrepi temeljijo na domnevi, da če ne moremo spreminjati posameznikovega stanja, lahko spremenimo razmere, v katerih ta opravlja poslovne procese. Kritična infrastruktura je s tehnološkega vidika varna, zaščititi pa jo je treba pred nezanesljivim posameznikom.

Posameznikova napaka pomeni opravljanje dejavnosti, ki v poslovnem procesu niso zaželene, na primer kršitev delovnih navodil, malomarnost, upravljanje sistema zunaj sprejemljivih meja ipd. To je odklon od namere, pričakovanj ali zaželenosti. Izraz posameznikova napaka ima negativno konotacijo, ki nastane kot vrhunec kontekstualnih in situacijskih dejavnikov. Pri tem se moramo zavedati, da so posameznikova napaka, njegova delovna zmogljivost in pristojnost sestavni deli običajnega spektra posameznikovega odločanja in vedenja na delovnem mestu.

Posameznikova napaka je bila navedena kot glavni vzrok ali pomemben dejavnik pri nesrečah v kritični infrastrukturi, na primer v jedrski industriji (nesreče v jedrskih centralah Three Mile Island leta 1979, v Černobilu leta 1986 in Fukušimi Daiči leta 2011), v letalstvu (padec letala Air France 447 sredi Atlantskega oceana leta 2009, padec letala v Franciji zaradi samomora kopilota leta 2014), pri raziskovanju vesolja (nesreči vesoljskih plovil Challenger in Shuttle Columbia), medicini[2], kemiji (kemični nesreči v Bophalu leta 1984 in Exxonu leta 1989), pri nafti (izliv nafte v Mehiškem zalivu leta 2010), v prometu (železniški nesreči v Nemčiji in Italiji

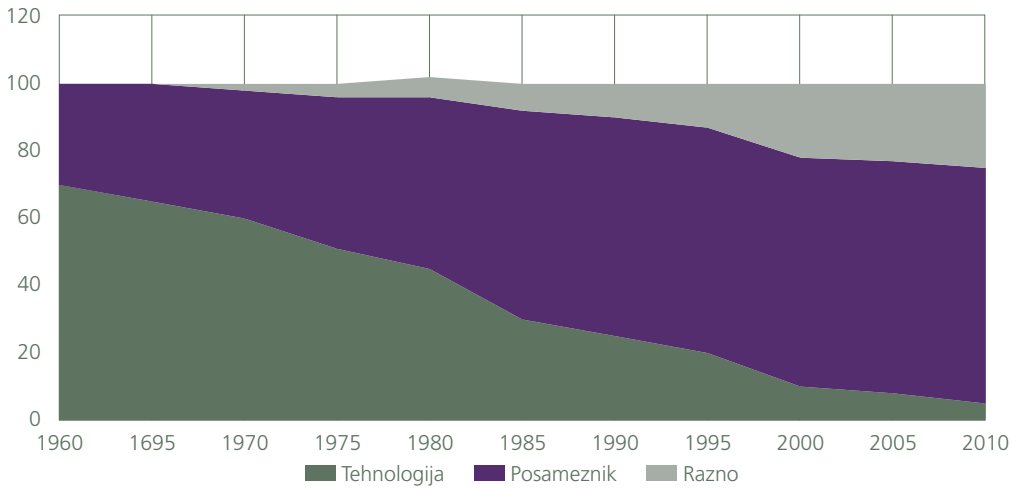
[2] *Z raziskavo Inštituta za medicino ZDA (2000) so ugotovili, da je bilo zaradi zdravniških napak od 44.000 do 100.000 naključnih smrti vsako leto in približno 1.000.000 naključnih poškodb.*

leta 2016), energetiki (incident v TEŠ 6 v Sloveniji leta 2016) in informacijski tehnologiji[3]. Težava je, da je treba pogosto oblikovati sisteme z zelo visoko zanesljivostjo, velikokrat s splošno odpovedjo velikostnega reda manj kot en primer na milijon dogodkov.

Statistični podatki kažejo, da je posameznikova napaka vključena v:
- več kot 90 odstotkov napak v jedrski industriji (Reason, 1990, United States NCR 2004);
- več kot 80 odstotkov napak kemične in petrokemične industrije (Kariuki idr., 2007);
- več kot 75 odstotkov pomorskih nesreč (Ren idr., 2008.);
- več kot 70 odstotkov letalskih nesreč (Helmreich, 2000);
- več kot 75 odstotkov napak pri distribuciji pitne vode in higiene (Wu idr., 2009).

Rast storitvenih dejavnosti z novimi poslovnimi modeli nakazuje še večjo odvisnost organizacij in gospodarstva od zanesljivega posameznikovega poslovanja[4].

Slika 2: Neobičajne razmere zaradi posameznikove napake ali tehnologije v letih (Hollnagel, 2010)



S slike 2 je razvidno, da se delež posameznikove napake od leta 1960 do 2010 močno povečuje in se potrjuje tako imenovani mit o 70 odstotkih napak zaradi nezanesljivega delovanja posameznika.

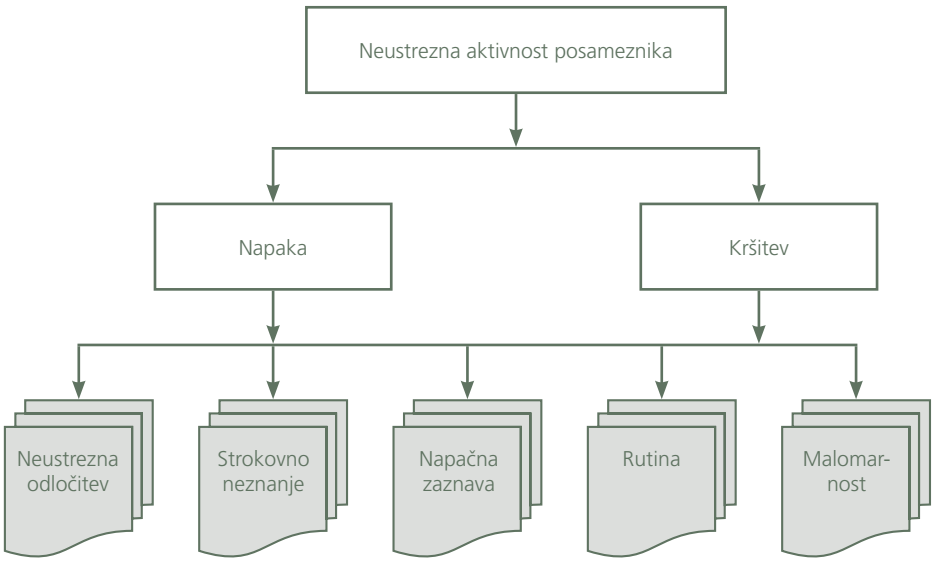
Dekker (2005) je opozoril, da je pojem posameznikova napaka lahko zavajajoč. Stari pogled na posameznikovo napako, imenovan tudi teorija gnilih jabolk, izhaja

[3] *IBM (2014) meni, da 95 odstotkov vseh napak povzroči posameznik.*

[4] *Banka Société Générale iz Francije (2008) je na primer »spregledala« dvomljivo investicijsko vedenje tržnika, kar je povzročilo izgubo 4,9 milijarde evrov in je imelo velike gospodarske ter finančne posledice tudi zunaj banke.*

iz predpostavke, da je posameznik nezanesljiv, posameznikova napaka pa lahko povzroči neobičajne razmere in škodni dogodek ter da so take razmere neprijetna presenečenja. Novi pogled obravnava posameznikovo napako kot učinek ali simptom globljih težav, posameznikova napaka pa je sistematično povezana z delovnimi orodji, poslovnimi procesi, delovnim okoljem ipd. Posameznikova napaka ne pomeni konec preiskave, temveč njeno izhodišče. Za razumevanje napake moramo proučiti odzive organizacije na napako.

Slika 3: Mogoče posameznikove neustrezne dejavnosti (lastni vir)



Na sliki 3 so predstavljene nekatere posameznikove neustrezne dejavnosti, ki lahko povzročijo neobičajne razmere. Neustrezne dejavnosti lahko delimo na namerne ali nenamerne oziroma naključne, ki se zgodijo zaradi napak ob neustrezni odločitvi, strokovnem neznanju ali napačni zaznavi ali zaradi kršitev.

Poleg navedenega so vzroki za posameznikovo napako brez posebnega vrstnega reda z vidika pomembnosti še pomanjkljiva zakonska ureditev kritične infrastrukture, ocena tveganj ne obravnava resničnega stanja, neustrezno organiziranje in vodenje dela, slab vodstveni nadzor, neupoštevanje zakonov in predpisov, neustrezna navodila, nejasne pristojnosti in odgovornosti, pomanjkljivo usklajevanje dela, premajhna usposobljenost zaposlenih, slaba organizacijska in varnostna kultura, nelojalnost do delodajalca, neetično delo, pomanjkljiv varnostni sistem, neupoštevanje zahtev notranje in zunanje revizije, navzkrižje interesov, neustrezni odzivi na prejšnje neobičajne razmere, nasilje na delovnem mestu, neučinkoviti usposabljanje in komuniciranje, neustrezni dejavniki dela, na primer nelogično oblikovanje strojev, opreme in instrumentov, stalne motnje in napake, slabo vzdrževana oprema, visoka

delovna obremenitev, neustrezne delovne razmere, slabo upravljanje zdravja in varnosti pri delu ipd. Vzroki za posameznikovo napako so tudi zahteve po delovni zmogljivosti, ki presega njegove zmožnosti, težke delovne naloge, nevarne ali neprijetne naloge, ponavljajoče se ali dolgočasne naloge, utrujenost, stres, delovna izgorelost, mobing, spolno nasilje, pomanjkanje spanja, poškodbe, zdravstvene težave ipd. Posledice neobičajnih razmer zaradi izgube življenja zaposlenega ali strank oziroma ugleda, nedelovanja kritične infrastrukture ali škode na premoženju so za družbo in organizacijo drage in jih je težko vnaprej predvideti ter materialno oceniti (finančno škodo).

Po drugi strani pa je posameznik na splošno pozitivno bitje, njegovo vedenje pri delu je opredeljeno kot zavzeto, predano in vpeto (Scaufeli idr., 2002). Delovna zavzetost kaže, kako posameznik doživlja svoje delo, ali mu torej pomeni nekaj stimulativnega, čemur rad namenja svoj čas in trud. Je tudi pokazatelj predanosti, torej kako pomembno se posamezniku zdi delo, in vpetosti, torej ali je delo nekaj, čemur namenja veliko pozornosti (Bakker idr., 2008).

Posameznik z veliko delovno zavzetostjo je učinkovitejši. Izraža več pozitivnega odnosa in višjo raven dejavnosti, zaradi česar doživlja več pozitivnih odzivov, kot so spoštovanje, prepoznavnost in uspeh. Delovno zelo zavzet posameznik opisuje svojo utrujenost po delovnem dnevu precej pozitivno, saj se zaveda vseh delovnih dosežkov (Gorigievski idr., 2010).

Bakker idr. (2003) so v povezavi z delovno zavzetostjo opredelili model JO – R (angl.: Job Demands – Resources), ki temelji na predpostavki, da na vsako delovno mesto delujejo določeni dejavniki tveganja, ki jih lahko označimo kot delovne vire in delovne zahteve. Med delovne vire štejemo pozitivne vidike zaposlitve, ki skupaj z zahtevami vplivajo na raven delovne zavzetosti, pripomorejo k doseganju delovnih ciljev in zmanjšujejo delovno obremenitev. Delovne zahteve se nanašajo na fizične, psihološke, socialne, varnostne in organizacijske dejavnike delovnega mesta, ki lahko povzročijo psihosocialno škodo (Bakker idr., 2008). Delovni viri so lahko tudi vir notranje motivacije, saj posameznik prek njih izpolnjuje svoje potrebe po avtonomiji, pripadnosti in kompetentnosti (Van Der Broeck idr., 2008). Delovne vire lahko opredelimo tudi kot dejavnike zunanje motivacije, saj je v takih delovnih okoljih večja verjetnost, da bo postavljen cilj dosežen (Meijman idr., 1998, v: Bakker idr., 2008). Luthans idr. (2007; v: Bakker idr., 2008) so vire definirali kot:
– prizadevati si in imeti pozitiven pristop za optimalno doseganje cilja;
– pripravljenost na spremembe za doseganje cilja;
– znati se spoprijemati s težavami poslovanja.

Na podlagi motivacijske funkcije delovnih virov številne študije potrjujejo pozitivno povezanost delovnih virov z delovno zavzetostjo. Vpliv delovnega mesta oziroma delo kot vir se kaže predvsem takrat, ko se posameznik spoprijema z visokimi delovnimi zahtevami, kar pomeni, da je motiviran za pridobivanje novega znanja in razvijanje svojih sposobnosti (Bakker idr., 2007).

4 RAZISKAVE POSAMEZNIKOVE ZANESLJIVOSTI

Raziskave posameznikove zanesljivosti (angl.: The Human Reliability Analysis) so v tuji strokovni javnosti že dalj časa znana orodja za napovedovanje posameznikovih zmogljivosti. Uporabljajo se za analizo, kje lahko v kritični infrastrukturi nastanejo neobičajne razmere kot posledica posameznikove nezanesljivosti. Pri proučevanju ogrožanja in ranljivosti kritične infrastrukture gre torej za razumevanje, kaj, zakaj, kako in kdaj lahko nastanejo neobičajne razmere. Ta pristop spodbuja analitično razmišljanje, ki temelji na analizah, simulacijah in dobri praksi, žal pa tudi na analizah po škodnem dogodku.

Razvoj raziskav na navedenem področju sovpada z razvojem družbe, zlasti na tehničnem področju. Začetki raziskav posameznikove zanesljivosti so bili v ocenah verjetnostnega tveganja, ocene so bile opravljene v okviru jedrskega programa razvoja energije ZDA leta 1960 (Bedford idr., 2001). Prva dokumentirana metoda teh raziskav je bila prikazana leta 1980 po nesreči v jedrski elektrarni Three Mile Island v ZDA kot tehnika za napovedovanje posameznikove napake (Technique for Human Error Rate Prediction – THERP), (Swain idr., 1983)[5]. Bila je zelo podobna metodam na drugih področjih analize zanesljivosti. Verjetnost posameznikove napake se namreč oceni z metodo drevo napak. S to metodo obravnavamo sistemske napake, ki so posledica posameznikove dejavnosti, in nato določimo vrsto poslovnih dejavnosti za preprečevanje neobičajnih razmer. V navedenih zgodnjih modelih je posameznik obravnavan kot druga sestavina v sistemu. Velik del razprav je osredotočen na vprašanja, kako sistem modelirati brez neprimernih posameznikovih dejavnosti. V zadnjem času je ta dvojnost bogatejša za kakovostno razumevanje posameznika s spoznavanjem njegove motivacije, pristojnosti in odločanja, vključno z učinki stresa, izgorelosti, čustev, usposabljanja, interakcije v skupini, organizacijske kulture, družbene kulture ipd. (Bazerman, 2006; Kahneman idr., 2000).

Raziskava posameznikove zanesljivosti ima dve glavni sestavini:
– razumevanje neobičajnih razmer in delovanje naprav ter opreme;
– razumevanje posameznikove zmogljivosti glede na razmere, ki so odvisne od vmesnika človek – stroj.

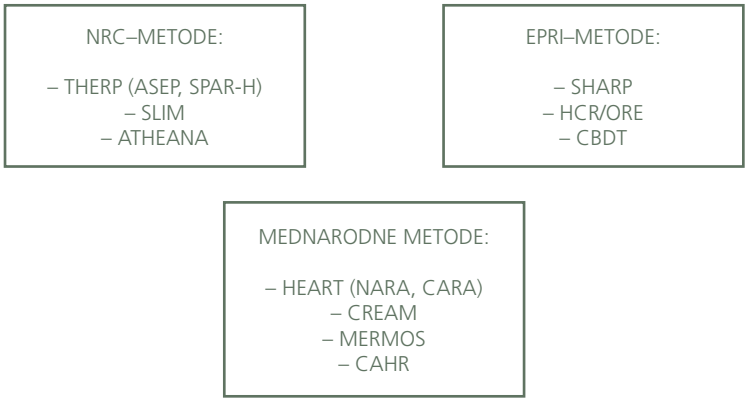
Raziskava posameznikove zanesljivosti je pogosto sestavljena iz treh ločenih faz (Boring, 2009):
– modeliranje in opredelitev mogočih posameznikovih napak. Ta faza navadno obsega različne mogoče scenarije ogrožanja kritične infrastrukture zaradi posameznikove napake. V navedeni dejavnosti ni splošno sprejetega standarda, kar lahko vodi do različnih pristopov;
– identifikacija mogočih ogrožanj neprekinjenega poslovanja kritične infrastrukture. Pristopi in metode raziskave posameznikove zanesljivosti so zelo različni. V zadnjem času so vzpostavljeni standardi dobre prakse (Kolaczkowski idr., 2005);

[5] *U. S. Nuclear Regulatory Commision ima na primer 77 modelov, ki se nanašajo na 104 reaktorje v ZDA.*

– količinska analiza posameznikovih napak, pri čemer je verjetnost posameznikove napake tudi izračunana. Vsaka metoda raziskovanja posameznikove zanesljivosti ima nekoliko drugačen pristop h kvantifikaciji, vključno s strokovno oceno, uporabo multiplikatorjev in simulacij. Količinsko se določa verjetnost za nastanek neobičajnih razmer. Napaka verjetnosti od enega primera na 100.000 dogodkov pomeni visoko zanesljivost sistema, srednje vrednosti pa se gibljejo od približno enega primera na 1000 do enega primera na 100 dogodkov. Sistem pod temi vrednostmi je nezanesljiv.

Analiza različnih metod raziskovanja posameznikove zanesljivosti (Bell idr., 2009) se do zdaj nanaša na kar 39 pristopov. Različne metode so prikazane v French idr. (2009), Adhikari idr. (2008), Čepin (2008), Lois idr. (2008), Forester idr. (2006). Pomembno je, da v praksi veliko metod raziskovanja posameznikove zanesljivosti v novejših različicah izhaja iz skupnega nabora funkcij raziskovanja posameznikove zanesljivosti.

Slika 4: Različne metode raziskovanja posameznikove zanesljivosti (lastni vir)



Legenda:
- NCR (U. S. Nuclear Regulatory Commision), komisija za jedrsko regulacijo, ZDA,
- EPRI (The Electric Power Research Institute), Elektro raziskovalni inštitut, ZDA,
- ATHEANA (A Technique for Human Error Analysis), analiza človeških napak,
- ASEP (Accident Sequence Evaluation Program), program za vrednotenje nesreč,
- CAHR (Connectionist Assessment of Human Reliability), ocena človeške zanesljivosti,
- CARA (Controller Action Reliability Assessment), kontrolne aktivnosti za oceno zanesljivosti,
- CBDT (Cause Based Decision Tree), odločitveno drevo,
- CREAM (Cognitive Reliability Error Analysis Method), kognitivna metoda zanesljivosti napak,
- HCR/ORE (Human Cognitive Reliability/Operator Reliability Experiments), kognitivna človeška zanesljivost oziroma poskus zanesljivosti,
- HEART (Human Error Assessment and Reduction Technique), ocena človeških napak in tehnik za njihovo zmanjšanje,
- MERMOS (Method d'Evaluation de la Realisation des Missions Operateur pour la Surete), metoda za evalvacijo dejavnosti operaterja,
- NARA (Nuclear Action Reliability Assessment), ocena jedrske zanesljivosti,
- SHARP (Systematic Human Action Reliability Procedure), sistematični postopek za oceno človeške zanesljivosti,
- SLIM (Success Likelihood Index Method), verjetnostna indeksna metoda,
- SPAR-H (Standardized Plant Analysis Risk-human), standardizirana analiza človekovega tveganja,
- THERP (Technique for Human Error Rate Prediction), tehnika za napovedovanje človeške napake.

Na sliki 4 je poenostavljen pregled nekaterih metod raziskovanja posameznikove zanesljivosti glede na njihov pristop. Predstavljene so v treh skupinah, in sicer metode, ki jih priporoča ameriška komisija za jedrsko regulacijo (NCR), metode Elektro raziskovalnega inštituta ZDA (EPRI) in druge mednarodne metode.

Med bolj uporabljenimi metodami je tehnika za napovedovanje človeške napake (THERP), ki je povezana s programom za vrednotenje nesreč (ASEP). Razvil jo je Swan (1987), pozneje pa so jo dopolnili Gertman idr. (2005) kot standardizirano analizo človekovega tveganja (SPAR-H). Eden izmed načinov za analizo posameznikove zanesljivosti je tudi razširitev verjetnostne ocene tveganja (Probabilistic Risk Assessment – PRA, 2004). Večina metod je podprta z računalniškim programskim orodjem.

Različne metode raziskovanja posameznikove zanesljivosti v zadnjem času postajajo vse bolj uporabne tudi na drugih področjih kritične infrastrukture. Do zdaj je večina metod raziskovanja posameznikove zanesljivosti analizirala posameznikov vpliv na področju jedrske energije, v zadnjem času pa se te metode uporabljajo tudi v transportnem sektorju (Sträter, 2000), naftni industriji (Aven idr., 2007), zračnem prometu (Kirwan idr., 2007) ipd.

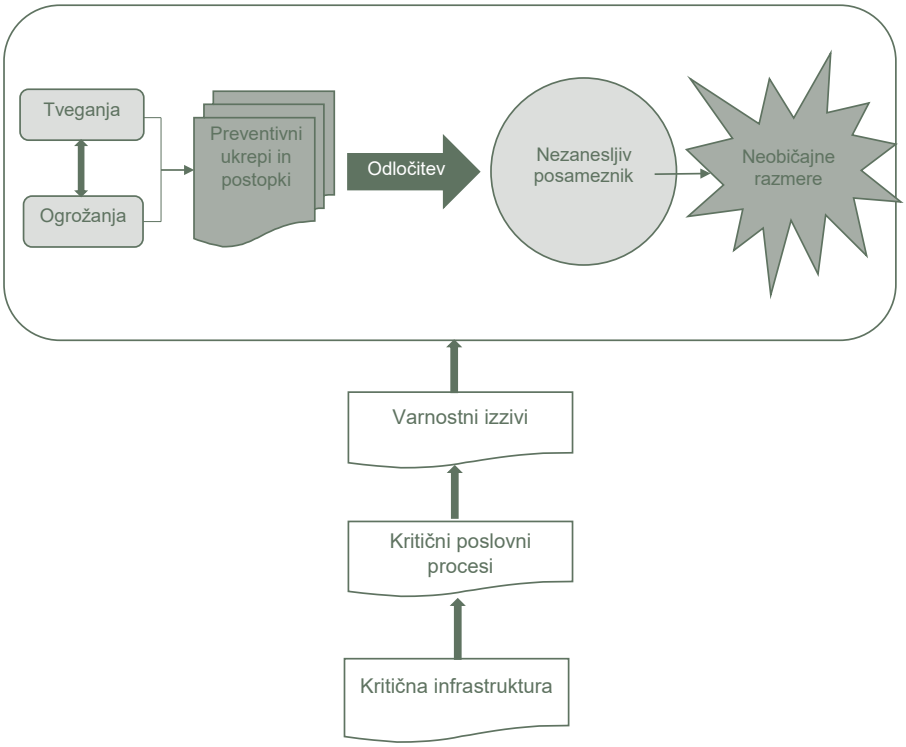
5 OKVIR MODELA POSAMEZNIKOVE ZANESLJIVOSTI PRI DELOVANJU KRITIČNE INFRASTRUKTURE

Obravnavanje posameznikove zanesljivosti pri delovanju kritične infrastrukture zahteva interdisciplinarni pristop, saj so za obravnavanje tega vprašanja potrebni tehnično, sociološko, družboslovno in psihološko znanje ter izkušnje oziroma dobra praksa.

Verjetnostne varnostne analize so eno izmed mogočih orodij za proučevanje zanesljivosti poslovanja kritične infrastrukture. V tem okviru se ugotavlja, katere neobičajne razmere oziroma scenariji lahko nastanejo pri delovanju, kako verjetno je, da nastanejo, in v kakšnem časovnem intervalu ter kako težke so lahko njihove posledice, na primer izguba zaposlenih in drugih ter neposredna in posredna materialna škoda. Kot prispevek k obravnavi navedenega področja je prikazan okvir za vzpostavitev modela posameznikove zanesljivosti pri delovanju kritične infrastrukture.

Na sliki 5 je predstavljena možnost nastanka neobičajnih razmer v kritični infrastrukturi. Poudarek je na kritičnih poslovnih procesih, varnostnih izzivih, ogrožanju in tveganju ter preventivnih ukrepih in postopkih. Pred ugotavljanjem tveganj je treba analizirati kritičnost poslovnih procesov, in sicer tako, da se upošteva njihov najslabši mogoč scenarij. Ta metodološki okvir tveganj zagotavlja, da so prepoznani vsi pomembni viri negotovosti, določeni vzroki za tveganja in opisane mogoče posledice tveganj v smislu vplivov na neprekinjeno delovanje.

Slika 5:
Okvir modela posameznikove zanesljivosti pri delovanju kritične infrastrukture (lastni vir)



Za preventivne ukrepe je priporočljiva uporaba tako imenovane metode švicarskega sira (Reason, 1990)[6].

Posamezni deli modela vsebujejo naslednje kazalnike:

- *Kritična infrastruktura:* navedeni pojem je bil v članku predhodno že obravnavan.

- *Kritični poslovni procesi:* za analizo kritičnih poslovnih procesov se upošteva najslabši mogoč scenariji. V okviru scenarija je treba pri vsakem poslovnem procesu predvideti in upoštevati vplive na poslovne cilje, finančna sredstva in ugled organizacije kritične infrastrukture, če odpovedo notranje kontrole. Posamezen poslovni proces se oceni s stališča integritete, zaupnosti in razpoložljivosti. Merila za prepoznavo so vzroki in posledice tveganj ter mogoče vrste neobičajnih razmer, verjetnosti pojavljanja tveganja in mogočega vpliva realizacije tveganja na poslovanje.

[6] *Metoda švicarskega sira je hevristični pojasnjevalni pripomoček za sporočanje interakcij med latentnim ogrožanjem, tveganjem in neobičajnimi razmerami. Reason (1990) meni, da luknje v obrambi nastanejo zaradi dveh vzrokov, in sicer aktivne posameznikove pomanjkljivosti in latentnih razmer. Sistem ne odpove zaradi ene napake, temveč je potrebnih več dejavnikov. Razprava o tem modelu presega obseg članka.*

- *Varnostni izzivi:* pomenijo ogrožanje varnosti kritične infrastrukture in tveganje, povezano z njenim delovanjem.

- *Ogrožanje kritične infrastrukture:* nastaja zaradi neustreznosti ali nepravilnega izvajanja poslovnih procesov, nepravilnega ravnanja zaposlenih, neustreznosti ali nepravilnega delovanja sistema in zunanjih dogodkov ali dejanj.

- *Tveganje:* metodološki okvir za identifikacijo tveganja zagotavlja, da so prepoznani vsi pomembni viri za negotovost in ogrožanje, določeni najpomembnejši vzroki za tveganje in opisane vse mogoče posledice tveganja v smislu vplivov na poslovanje. Proces upravljanja tveganja obsega med seboj povezane procese, in sicer identifikacijo, ocenjevanje in obvladovanje tveganja ter spremljanje in poročanje o tveganjih.

- *Preventivni ukrepi in postopki:* nanašajo se na organiziranje in vodenje dela, motiviranje zaposlenih, organizacijsko kulturo, usposabljanje in obveščanje, organizacijske, kadrovske in tehnične ukrepe ter postopke, vključno z varnostnim načrtom, načrtom za neprekinjeno poslovanje in s kriznim komunikacijskim načrtom, nadzorom nad dostopom do najpomembnejših področij poslovanja in z notranjim kontrolnim ter nadzornim sistemom.

- *Odločanje:* lahko ga opredelimo tudi kot proces izbiranja ustrezne alternative iz množice mogočih. Ob tem se pojavljajo vprašanja iz teorije odločanja:
  - kako posameznik presoja mogoče neobičajne razmere;
  - kako verjetnost in posledice neobičajnih razmer vplivajo na njegovo odločanje;
  - kako razložiti dejstvo, da se posameznik v enakem položaju pogosto različno odloča.

- *Neobičajne razmere:* povzroči jih nepričakovan dogodek ali sosledje dogodkov, v katerem se lahko pojavijo žrtve in/ali škoda. Škoda nastane, ko zahteve neobičajnih razmer presegajo zmožnosti posameznika, organizacije in družbe za njihovo obvladovanje. V resnici je ocena neobičajnih razmer zelo zapleten miselni proces, zasnovan bolj na teoretičnih analizah, simulacijah in operativnih vajah kot pa na neposredni izkušnji.

V nadaljevanju bom pojasnil glavni del okvira modela, in sicer odločanje, obravnava drugih elementov pa presega obseg članka.

6 ODLOČANJE

Sprejemanje odločitev je eden temeljnih posameznikovih kognitivnih procesov, ki jih uporablja pri racionalnih, hevurističnih in intuitivnih odločitvah v različnih primerih. Odločanje je mentalni proces, ki se zavestno ali nezavedno zgodi vsakih nekaj sekund. V tem procesu prihaja do izbire med različnimi možnostmi prepričanj, prepoznave ali dejavnosti, kar vpliva na končno izbiro. Sprejemanje odločitev je nerazdružljivo povezano z zadovoljevanjem posameznikovih potreb.

Nekateri menijo, da se bodo posamezniki, če so pri odločanju racionalna in svobodna bitja, vedli skladno s teorijo racionalnega odločanja. Ta trdi, da posamezniki sprejemajo odločitve z določanjem verjetnosti in vrednosti mogočega izida.

Najboljše mogoče odločanje otežuje pretirana prepričanost o pravilnosti svoje sodbe. Posameznik preveč zaupa svojim, tudi napačnim, predpostavkam in sodbam. Podlaga za to je verjetno neobčutljivost za pomanjkljivost domnev in predpostavk, na katerih temeljijo njegove ocene. Najbrž noben dejavnik slabe odločitve ni bolj odločujoč kot pretirana samozavest. Narava nerešenega vprašanja in sodbe določa tudi raven samozavesti. Splošno strokovno znanje povzroča visoko stopnjo pretirane samozavesti, velja pa tudi nasprotna trditev.

Na sprejemanje odločitve vpliva več dejavnikov, in sicer strokovno znanje in izkušnje (Juliusson idr., 2005), kognitivne pristranskosti (Stanovich idr., 2008), starost in individualne razlike (Bruin idr., 2007) ter samozaupanje (Acevedo idr., 2004).

Zaradi nepopolnih informacij posameznik sprejema pogojno dobre odločitve. Nekatere odločitve so preproste in pri njih lahko najdemo neposredno povezavo med nekim dejanjem in posledicami, druge pa so večplastne, s številnimi spremenljivkami. Pri odločanju imajo največjo vlogo narava nerešenega vprašanja in situacijski dejavniki, zato lahko predvidevamo, da se posamezniki med seboj razlikujejo v pogostosti uporabe posameznih načinov odločanja, ne glede na nerešeno vprašanje. Kognitivne pristranskosti, ki temeljijo na opazovanju, in posplošitve lahko vodijo do napak, netočnih sodb in napačne logike (West idr., 2008).

V raziskavah načinov odločanja so bile izpostavljene predvsem medosebne razlike med posamezniki, ki morajo odločitev sprejeti (Thunholm, 2004). Scott in Bruce (1995) sta načine odločanja opredelila kot naučen odziv oziroma vedenjski vzorec posameznika, ki se spoprijema z odločitvijo. Definirala sta pet načinov odločanja, in sicer racionalni, intuitivni, odvisni, izogibajoči se in spontani. Racionalni način je značilen za posameznika, ki podrobno išče in logično ovrednoti vse možnosti. Osredotoča se predvsem na logiko, red in sistematično analizo informacij. Intuitivni način je značilen za tiste, ki namenjajo veliko pozornosti podrobnostim in upoštevajo svoje občutke o tem, ali je neka odločitev pravilna, odvisni način pa je značilen za tiste, ki iščejo nasvete in vodenje pri drugih. Izogibajoči se način je značilen za posameznika, ki se želi izogniti sprejemanju odločitve, spontani pa za tistega, ki ima občutek, da je v časovni stiski in želi odločitev čim hitreje sprejeti. Poznamo še druge načine odločanja, na primer naključno, rutinsko in sistematično. Posameznik ne uporablja le enega načina odločanja, temveč njihovo kombinacijo, pri čemer eden ali dva načina prevladujeta.

Kognicija je lahko intuitivna ali analitična, pri čemer je prva nezavedna, druga pa se nanaša na zavestno delovanje. Intuicija temelji na prejšnjem znanju in izkušnjah in ni posledica nekaterih prirojenih dejavnikov, na primer nagona ali refleksa. Obe vrsti kognicije navadno delujeta hkrati in skupaj oblikujeta mišljenje ter delovanje. Betch (2008) meni, da razmišljanja v čisti obliki ni.

Po Kleinovi teoriji (2009) odločevalci presojajo razmere na podlagi primerjav s podobnim, že doživetim dogodkom oziroma podobno, že doživeto izkušnjo. Zanimiv je njegov model za prepoznavo odločitev na spodnji sliki.

Slika 6: Model za prepoznavo odločitev (Klein, 2009)

Model se shematsko nanaša na razmere in njihove značilnosti. Za razmere so odločilni znaki, ki jih izkušen odločevalec oblikuje v vzorec, torej prepozna različne možnosti, ki potem vplivajo na odločitev oziroma najustreznejšo dejavnost. Kdaj posameznik poskuša analizirati vse možnosti? Ko bi moral uporabiti svojo intuicijo ali ko bi se moral zanašati na logiko in navodila? Klein (2009) meni, da mora posameznik pri pomembnih odločitvah upoštevati nekatere smernice, na primer zbrati čim več informacij, primerjati možnosti in natančno določiti cilje, preden se odloči. Izkušnje iz prakse kažejo, da se lahko učinkovito odločamo na podlagi prilagajanja okoliščinam, ne pa le po navodilih. Dosledno upoštevanje navodil je dobro, ko je položaj jasen, toda odločitve v neobičajnih razmerah vključujejo tudi kompleksnost in dvoumnost.

Učinkovito odločanje otežuje več dejavnikov, in sicer močno omejen razpoložljivi čas za odločanje, dopustnost napačne odločitve je minimalna, nepričakovano pojavljanje novih elementov za odločanje, odločanje v razmerah, ki so presenetile ali celo šokirale, ne poznamo vseh dejavnikov razmer, kar vpliva na odločitev, veliko različic, vsi podatki niso dosegljivi ipd. Posebna težava so nepoznavanje nerešenega vprašanja in ciljev odločitve, omejena sredstva, kot so čas, denar, strokovnjaki ipd., ter morebitna nesoglasja med posamezniki, ki sodelujejo pri odločanju.

7 PREDLOGI NADALJNJIH DEJAVNOSTI

7.1 Pripravljenost na morebitne neobičajne razmere

Posameznikovo odločanje in njegove dejavnosti ter delovanje kritične infrastrukture so odvisni od njegove individualne in skupinske pripravljenosti na neobičajne razmere. Posameznikova pripravljenost je odvisna tudi od prejšnjih izkušenj z neobičajnimi razmerami in tudi od njegovih predstav o tem, kaj bi se lahko zgodilo. Stopnja posameznikove zanesljivosti pri delovanju kritične infrastrukture je najbolj odvisna od stopnje njegove motiviranosti, usposobljenosti in pripadnosti organizaciji (Bertoncelj, 2000).

7.2 Obveščati in opozarjati zaposlene

Obveščeni posamezniki se bodo učinkovito spoprijemali z neobičajnimi razmerami, saj zaradi pripravljenosti nanje nastanejo prilagoditveni procesi. Pri opozarjanju na morebitne neobičajne razmere moramo izhajati predvsem iz najbolj neugodnega scenarija ogrožanja. Obvestila morajo potekati k tistim posameznikom, ki bi lahko bili bolj ogroženi, in od njih nazaj, da bi zagotovili ustrezne povratne zveze in želene odzive (Bass idr., 2006). Obveščanje torej deluje kot čustveno »cepljenje«, ki omogoča povečanje stresne tolerance.

7.3 Motivirati zaposlene

Pomemben dejavnik, od katerega je odvisna ustrezna pripravljenost na neobičajne razmere, je motivacija. To pomeni, da mora biti posameznik pozitivno motiviran in želeti, da se pripravi na morebitne neobičajne razmere. Posameznikovi ravnanje, prepričanja, nazori, mnenja in stališča so pod vplivom notranjih motivov in ciljev (Musek, 2000). Vse pomembnejši parameter pri tem postaja varnostna kultura kot del organizacijske kulture organizacije.

7.4 Usposobiti zaposlene

Za ustrezno pripravljenost na morebitne neobičajne razmere je pomembna tudi usposobljenost. Ta vključuje znanje in veščine, ki imajo predvsem dva cilja, in sicer omogočajo posamezniku samovarovalno dejavnost, kar predstavlja temeljni element individualne in kolektivne zaščite ter so psihološke narave, saj bo posameznik, ki se zaveda svojega strokovnega znanja in pozna ukrepe ter postopke tudi v najtežjih razmerah, lažje obvladal strah in psihološki pritisk ter bo bolj samozavesten in zanesljiv. Ustrezno pripravljen posameznik se bo lahko uspešno spoprijel z zahtevami neobičajnih razmer (Wiesner idr., 2003).

Sklep Zagotavljanje posameznikove zanesljivosti pri delovanju kritične infrastrukture v sodobni državi je v današnjem globalnem svetu dinamičen interdisciplinarni proces.

Na vprašanje, kako sodobne države opredeljujejo zanesljivost posameznika pri delovanju svoje kritične infrastrukture, analiza literature kaže, da izbrane države, razen ZDA, v strateških dokumentih ne omenjajo posameznikove vloge pri

delovanju kritične infrastrukture. Pomembnost zaščite kritične infrastrukture, preglednost obravnave in sistematičen pristop na tem področju se najbolje kažejo v varnostni politiki ZDA. Navedene nadaljnje dejavnosti bodo predlagane za smiselno vključitev v osnutek Zakona o kritični infrastrukturi Republike Slovenije, ki je v postopku obravnave v Državnem zboru Republike Slovenije.

Raziskave posameznikove zanesljivosti so v strokovni javnosti že dalj časa znana orodja in metodologije za napovedovanje posameznikovih zmogljivosti. Analiza različnih metod se do zdaj nanaša na kar 39 pristopov. Med bolj uporabljenimi metodami je tehnika za napovedovanje človeške napake, ki je povezana s programom za vrednotenje nesreč. Različne metode po posameznih sektorjih kritične infrastrukture v zadnjem času postajajo vse bolj univerzalne.

Menim, da je za posameznikovo zanesljivost v neobičajnih razmerah pomembna ustrezna konstruktivna strategija spoprijemanja z ogrožanjem in tveganji. Uspešnost ali neuspešnost spoprijemanja je tesno povezana s posameznikovimi osebnostnimi lastnostmi, pristojnostjo in odzivom, ki se nanaša na strokovno znanje, realno oceno neobičajnih razmer, zavestno razčlenjevanje razmer, pozitivno stališče do sebe in drugih, torej osebno trdnost, vključno z zaupanjem v svoje sposobnosti in preventivne dejavnosti kritične infrastrukture ter državnih organov, aktiven odnos do stvarnosti namesto togosti in bega iz stvarnosti, prilagodljivo iskanje rešitev, konstruktivno sodelovanje z drugimi namesto pasivnega pričakovanja pomoči ter sprejemanje in prenašanje čustvene obremenitve namesto neorganiziranosti in panike.

Posameznikove dejavnosti v neobičajnih razmerah so pretežno prostovoljna dejanja, pri katerih sta najpomembnejša pojma pripravljenost in volja nekaj koristnega delati za organizacijo, da ne bi nastale nezaželene posledice škodnega dogodka. Na splošno velja, da se bo posameznik toliko učinkoviteje spoprijel z neobičajnimi razmerami in njihovimi posledicami, kolikor bolj bo nanje pripravljen.

Literatura

1. *Aven, T. in Vinnem J. E., 2007. Risk Management: With Applications from the Offshore Petroleum Industry. Springer–Verlag, London.*
2. *Acevedo, M. in Krueger, J. I., 2004. Two egocentric sources of the decision to vote: The voter's illusion and the belief in personal relevance. Political Psychology, 25 (1), 115–134.*
3. *Adhikari, S., Bayley, C., Bedford, T., Busby, J., Cliffe, A., Devgun, G., Eid, M., French, S., Keshvala, R., Pollard, S., Soane, E., Tracy, D. in Wu, S., 2008. Human reliability analysis: A review and critique. Final Report for EP/E017800/1. UK Engineering and Physical Sciences Research Council.*
4. *Avizienis, A., Laprie, J. C. in Randell, B., 2001. Fundamental Concepts of Dependability (Research Report No 1145), LAAS–CNR.*
5. *Bakker, A. B., Schaufeli, W. B., Leiter, M. P. in Taris, T. W., 2008. Work engagement: An emerging concept in occupational health psychology. Work and Stress, 22, 187–200.*
6. *Bakker, A. B. in Demerouti, E., 2007. The Job Demands-Resources model: State of the art. Journal of Managerial Psychology, 22, 309–328.*

7. *Bakker, A. B., Demerouti, E., De Boer, E. in Schaufeli, W. B., 2003. Job demands and job resources as predictors of absence duration and frequency. Journal of Vacational Behaviour, 62, 341–356.*
8. *Bass, B. M. in Ronald, E. R., 2006. Transformational leadership. London, Lawrence Erlbaum associates, Publishers.*
9. *Bazerman, M., 2006. Managerial Decision Making, 6th ed. John Wiley and Sons, New York.*
10. *Betch, T., 2008. The Nature of Intuition and Its Neglect in Research on Judgment and Decision Making. V Plessner H., Betsch, C. in Betsch, T., (ur.): Intuition in Judgment and Decision Making. LEA, New York, 3–22.*
11. *Bedford, T. in Cooke, R., 2001. Probabilistic Risk Analysis: Foundations and Methods. Cambridge University.*
12. *Bell, J. in Holroyd, J., 2009. Review of human reliability assessment methods Health and Safety Laboratory, Harpur Hill, http://www.hse.gov.uk/research/rrpdf/rr679.pdf, 16.1.2017.*
13. *Bertoncelj, B., 2000. Psihosocialni vidiki zagotavljanja varnosti računalniško podprtega informacijskega sistema: doktorska disertacija. FDV, Ljubljana.*
14. *Boring, R. L., 2009. Human reliability analysis in cognitive engineering. Frontiers of Engineering: Reports on Leading–Edge Engineering from the 2008 Symposium (103–110). Washington, DC: National Academy of Engineering.*
15. *Bruine de Bruin, W. B., Parker, A. M. in Fischhoff, B., 2007. Individual differences in adult decision–making competence. Journal of Personality and Social Psychology, 92 (5), 938–956.*
16. *Broder, J. F., 2006. Risk Analysis and the Security Survey. Boston/Oxford, Butterworth–Heinemann.*
17. *Condra, L. W., 2001. Reliability Improvement with Design of Experiments, Marcel Dekker Inc.*
18. *Čepin, M., 2008. DEPEND–HRA–A method for consideration of dependency in human reliability analysis, Reliability Engineering and System Safety, vol. 93 (10), 1452–1460.*
19. *Dekker, S. W. A., 2005. Ten Questions About Human Error: a new view of human factors and systems safety, Lawrence Erlbaum Associates.*
20. *Direktiva Sveta Evropske unije o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite (ES), št. 114/2008.*
21. *Dunn, M., 2005. The Socio–political Dimensions of Critical Information Infrastructure Protection. International Journal of Critical Infrastructures, vol. 1, no. 2/3.*
22. *Federal Emergency Management Agency (FEMA), Threat and Hazard Identification and Risk Assessment Guide Comprehensive Preparedness Guide (CPG) 201, Second Edition, THIRA, 2013, https://www.fema.gov/media-library data/8ca0a9e54dc8b037a55b402b2a269e94/CPG201_htirag_2nd_edition.pdf,12.1.2017.*
23. *Forester, J., Kolaczkowski, A., Lois, E. in Kelly, D., 2006. Evaluation of human reliability analysis methods against good practices. NUREG–1842 Final Report, U. S. Nuclear Regulatory Commission.*
24. *French, S., Maule, A. J. in Papamichail, K. N., 2009. Decision Behaviour, Analysis and Support. Cambridge University Press, Cambridge.*
25. *Gertman, D., Blackman, H., Marble, J., Byers, J. in Smith, C., 2005. The SPAR-H human reliability analysis method. NUREG/CR–6883. Idaho National Laboratory, prepared for U. S. Nuclear Regulatory Commission.*
26. *Gorgievski, M., Bakker, A. B. in Schaufeli, W. B., 2010. Work engagement and workaholism: Comparing the selfemployed and salaried employees. Journal of Positive Psychology, 5, 83–96.*
27. *Helmreich, R. L., Sexton, J. B. in Thomas, E. J., 2000. Error, stress, and teamwork in medicine and aviation: cross sectional surveys, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC27316/, 12.1.2017.*

28. *Hollnagel, E., 2010. The diminishing relevance of human–computer interaction. V Boy, G. (ur.), Handbook of Human–Machine Interaction. Farnham, UK: Ashgate.*
29. *Jullisson, E. A., Karlsson, N. in Garling, T., 2005. Weighing the past and the future in decision–making. European Journal of Cognitive Psychology, 17(4), 561–575.*
30. *Johnson, C., 2006. Understanding the Interaction between Public Policy, Managerial Decision–Making and the Engineering of Critical Infrastructures. Research paper, Reliability Engineering and System Safety.*
31. *Kahneman, D. in Tversky, A. ur., 2000. Choices, Values and Frames. Cambridge University Press, Cambridge.*
32. *Kariuki, S. G. in Lowe, K., 2007. Integrating human factors into process analysis. Reliability Engineering and System Safety 92 1764–1773.*
33. *Kirwan, B. in Gibson, H., 2007. CARA: A human reliability assessment tool for air traffic safety management–Technical basis and preliminary architecture. V Redmill, F. in Anderson, T. (ur.), The Safety of Systems: Proceedings of the Fifteenth Safety-Critical Systems Symposium (197–214). London: Springer Verlag.*
34. *Klein, G., 2009. Streetlights and Shadows: Searching for the Keys to Adaptive Decision Making. Cambridge, MA: MIT Press.*
35. *Kolaczkowski, A., Forester J., Lois, E. in Cooper, S., 2005. Good Practice for Implementing Human Reliability Analysis (HRA). NUREG–1792, U.S. Nuclear Regulatory Commission.*
36. *Lois, E., et al., 2008. International HRA Empirical Study Pilot Phase Report. OCED Halden Reactor Project, HWR–844.*
37. *Musek, J., 2000. Temeljni vidiki samopodobe. Ljubljana, Psihološka obzorja, letnik 9, številka 2, 131–132.*
38. *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), http://www.bmi.bund.de/cae/servlet/contentblob/544770/publicationFile/27031/kritis.pdf, 12.1.2017.*
39. *NIPP, 2013. Partnering for Critical Infrastructure Security and Resilience, https://www.dhs.gov/, 12.1.2017.*
40. *Prezelj, I., 2010. Kritična infrastruktura in sodobna varnost. V: Prezelj, I. (ur.): Kritična infrastruktura v Sloveniji. Ljubljana: FDV.*
41. *Polič, M. idr., 1998. Javnost in nesreče: obveščanje, opozarjanje, vplivanje. Ljubljana, Znanstveni inštitut Filozofske fakultete.*
42. *Rausand, A. M., 2004. System reliability theory: Models, statistical methods, and applications. John Wiley & Sons, Inc.*
43. *Reason, J., 1990. Human error. Cambridge University Press.*
44. *Ren, J., Jenkinson, I., Wang, J., Xu, D. L. in Yang, J. B., 2008. A methodology to model causal relationships in offshore safety assessment focusing on human and organisational factors. Journal of Safety Research 39 87–100.*
45. *Schaufeli, W. B., Salanova, M., Gonzalez - Roma, V. in Bakker, A. B., 2002. The measurement of engagement and burnout: A two sample confirmatory factor analytic approach. Journal of Happiness Studies, 3, 71–92.*
46. *Scott, S. G. in Bruce R. A., 1995. »Decision–making style: The development and assessment of a new measure«. V: Educational and Psychological Measurement, V/55, Thousand Oaks, CA: Sage Publications, Inc., str. 818–831.*
47. *Sklep Vlade RS, 2015. Osnovne in sektorske kriterije kritičnosti za določanje kritične infrastrukture državnega pomena v Republiki Sloveniji.*
48. *Stanovich, K. E. in West, R. F., 2008. On the relative independence of thinking biases and cognitive ability. Journal of Personality and Social Psychology, 94 (4), 672–695.*
49. *Svetličič, M., 2005. Kako se uspešno pogajati. Ljubljana, Ekonomska fakulteta, Cisef, 2.*

50. *Swain, A. D. in Guttman, H. E., 1983. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR–1278, U.S. Nuclear Regulatory Commission.*
51. *Thunholm, P., 2004. Decision–making style: habit, style or both? Personality and Individual Differences, 36 (4), 931–944.*
52. *Van den Broeck, A., Vansteenkiste, M., de Witte, H. in Lens, W., 2008. Explaining the relationships between job characteristics, burnout and engagement the role of basic psychological need satisfaction. Work and Stress, 22, 277–294.*
53. *U. S. Nuclear Regulatory Commission, 2004. An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk–Informed Activities. Regulatory Guide 1.200, U.S Nuclear Regulatory Commission.*
54. *West, R. F., Toplak, M. E. in Stanovich, K. E., 2008. Heuristics and biases as measures of critical thinking: Associations with cognitive ability and thinking dispositions. Journal of Educational Psychology, 100 (4), 930–941.*
55. *Wiesner, R. in Millet, B., 2003. HRM: Challenges and Future Directions. John Wiley and Sons Australia, Ltd.*
56. *Wu, S., Hrudey, S., French, S., Bedford, T., Soane, E., Pollard, S. Grabowski, M. in Roberts, K. H., 2009. A role for human reliability analysis (HRA) in preventing drinking water incidents and securing safe drinking water, Water Research, Volume 43, No. 13, 2009, 3227–3238.*