Jure Marn
Matjaž Fras
Jurij Iljaž

Varnost in zanesljivost v okoljski tehniki

Univerzitetna založba
Univerze v Mariboru

Univerza v Mariboru

Fakulteta za strojništvo

VARNOST IN ZANESLJIVOST V OKOLJSKI TEHNIKI

Avtorji

Jure Marn

Matjaž Fras

Jurij Iljaž

Junij 2021

Naslov *Title* **Varnost in zanesljivost v okoljski tehniki**
Safety and Reliability in Environmental Engineeering

Avtorji *Authors* Jure Marn (Univerza v Mariboru, Fakulteta za strojništvo)
Matjaž Fras (Univerza v Mariboru, Fakulteta za strojništvo)
Jurij Iljaž (Univerza v Mariboru, Fakulteta za strojništvo)

Recenzija *Review* Mitja Robert Kožuh (Univerza v Ljubljani, Fakulteta za kemijo in kemijsko tehnologijo)
Jure Ravnik (Univerza v Mariboru, Fakulteta za strojništvo)

Jezikovni pregled *Language edeting* Nataša Belšak

Tehnični urednik *Technical editor* Jan Perša (Univerza v Mariboru, Univerzitetna založba)

Oblikovanje ovitka *Cover designer* Jan Perša (Univerza v Mariboru, Univerzitetna založba)

Grafike na ovitku *Cover graphics* Grafika Web Avtor: geralt (Pixabay)
Grafične priloge *Graphic material* Avtorji

Založnik *Published by* **Univerza v Mariboru**
Univerzitetna založba
Slomškov trg 15, 2000 Maribor, Slovenija
https://press.um.si, zalozba@um.si

Izdajatelj *Co-published by* **Univerza v Mariboru**
Fakulteta za strojništvo
Smetanova ulica 17, 2000 Maribor, Slovenija
https://www.fgpa.um.si, fgpa@um.si

Izdaja *Edition* Prva izdaja
Izdano *Published at* Maribor, junij 2021

Vrsta publikacije *Publication type* E-knjiga
Dostopno na *Available at* https://press.um.si/index.php/ump/catalog/book/576

CIP - Kataložni zapis o publikaciji
Univerzitetna knjižnica Maribor

62:502/504

MARN, Jure
Varnost in zanesljivost v okoljski tehniki [Elektronski vir] / Jure Marn, Matjaž Fras, Jurij Iljaž. - 1. izd. - E-knjiga. - Maribor : Univerza v Mariboru, Univerzitetna založba, 2021

Način dostopa (URL):
https://press.um.si/index.php/ump/catalog/book/576
ISBN 978-961-286-477-4 (brezplačni izvod)
doi: 10.18690/978-961-286-477-4
COBISS.SI-ID 66710787

ISBN 978-961-286-477-4 (pdf)
DOI https://doi.org/10.18690/978-961-286-477-4

Cena *Price* Brezplačni izvod
Odgovorna oseba založnika *For publisher* prof. dr. Zdravko Kačič, rektor Univerze v Mariboru

Citiranje *Attribution* Marn, J., Fras, M. in Iljaž, J. (2021). *Varnost in zanesljivost v okoljski tehniki.* Maribor: Univerzitetna založba. doi: 10.18690/978-961-286-477-4

ZAHVALA

Avtorji se zahvaljujemo družinam za podporo in skrb, zlasti pa recenzentoma

doc. dr. Mitji Kožuhu

in

red. prof. dr. Juretu Ravniku

za nasvete in pomoč pri izdelavi tega dela.

Univerzitetna založba
Univerze v Mariboru

Kazalo

Univerzitetna založba
Univerze v Mariboru

Najpogosteje uporabljeni simboli in kratice

p	–	verjetnost [/]
R	–	tveganje [/]
f	–	frekvenca [1/s]
q	–	nerazpoložljivost
c	–	posledica (1/dogodek)
λ	–	pogostost odpovedi [1/s]
t	–	čas misije [s]
Ø	–	premer cevi [mm]
l	–	dolžina cevi [m]
FTA	–	analiza drevesa odpovedi (angl. *FTA – Fault Tree Analysis*)
HRA	–	analiza človeške zanesljivosti (angl. *Human Reliability Analysis*)
RM	–	upravljanje s tveganji (angl. *Risk Management*)
HCR	–	zanesljivost človeške kognitivnosti (angl. *Human Cognitive Reliability*)
CREAM	–	postopek kognitivne (spoznavne) zanesljivosti in analize odpovedi (angl. *Cognitive Reliability and Error Analysis Method*)

Osnovni

CREAM	–	osnovni postopek kognitivne (spoznavne) zanesljivosti in analize odpovedi (angl. *Basic-CREAM – Cognitive Reliability and Error Analysis Method*)

Razširjeni

CREAM	–	razširjeni postopek kognitivne (spoznavne) zanesljivosti in analize odpovedi (angl. *Extended-CREAM – Cognitive Reliability and Error Analysis Method*)
CPC	–	Splošni pogoji dela (angl. *Common Performance Conditions*)
COCOM	–	funkcija kontrolnega modela (angl. *Cognitive Control Model Function*)

UF	–	uravnalna funkcija (angl. *WF – Weighting Factor*)
SUF	–	skupni uravnalni faktor (angl. *CWF – Common Weighting Factor*)

Univerzitetna založba
Univerze v Mariboru

1 Uvod

Skripta so namenjena študentom okoljskega inženirstva. Zasnovana so na večletnih izkušnjah, pridobljenih s predavanji, in zlasti na predlogih študentov, da bi bilo smiselno pripraviti literaturo v slovenskem jeziku.

Besedilo predpostavlja osnovno znanje fizike in matematike ter poznavanje statističnih metod. Namenjeno je bodočim inženirjem, zato se bolj posveča delovanju in manj namenom, ki izhajajo iz varstva okolja.

Najprej se moramo vprašati, čemu se ukvarjati z vprašanji varnosti in zanesljivosti tudi na področju okoljske varnosti.

Povsem okoljsko varnih tehnologij ni, zato se moramo inženirji pogosto odločati glede potencialno okoljsko nevarnih tehnologij. Primer: Ali je smiselno zgraditi lakirnico na najboljših kmetijskih zemljiščih? Na eni strani tehtamo ekonomske koristi, kot so delovna mesta, razvoj znanosti in stroke, na drugi strani pa so morebitni izpusti, ki lahko škodijo okolju.

Če bomo znali in razumeli ocenjevati tveganja zaradi tovrstnih gradenj, bomo lažje odločali v upravnih postopkih. Pri tem gre bolj za primerjavo med posameznimi tveganji. Tipično takšno tveganje je npr. rentgensko slikanje. Res je, vsako ionizirajoče sevanje je lahko potencialno nevarno, po drugi strani pa lahko odkrije bolezen, od katere bi človek

skoraj gotovo umrl (npr. pljučni tumor). Prav tako smo ionizirajočega sevanja deležni, če se vozimo z letalom, saj nas visoko nad tlemi zračni ovoj manj ščiti kot pri tleh.

Na osnovi razvoja modelov in hipotez bomo lahko modelirali vpliv nevarnih tehnologij na okolje. Ne le to, lahko bomo modelirali vpliv na okolje tehnologij, ki so same namenjene ščitenju okolja, kot so npr. čistilne naprave.

Strokovnjaki[1] predlagajo, da osnove zdravja, varnosti in okolja (kratica HSE) vgradimo v vsak projekt, ki se ga lotevamo. Predvsem se moramo potruditi, da ne bomo le slepo sledili zakonskim varnostnim zahtevam, ampak (in morda), da bomo upravnim organom in drugim deležnikom predložili razloge za svoje odločitve, ki jih bodo lahko primerjali z drugimi, podobnimi projekti.

Potencialne tokove odpadkov moramo npr. zaznati zgodaj v procesu konstruiranja in izbire tehnologije. Tako bomo lahko od samega začetka načrtovali njihovo varno odstranitev, vključno z učinkom NIMBY[2]. Družba je sposobna razumeti, da je sama odgovorna za odpadke, ki jih proizvaja, in da je strošek odpadkov čim višji, tem več jih je in čim dlje jih je treba odvažati.

Podobno velja za vprašanje hrupa. Pri načrtovanju vozne poti se moramo vprašati, kako bomo škodovali okolici. Kakšne bodo posledice zanemarjanja poškodb zaradi povišanega hrupa v obratih?

Kaj pa požari? Požari so lahko velik vir emisij in imisij, zlasti kadar gre za zgorevanje plastičnih snovi, so posledice lahko posebej hude. A kaj so posledice? Kaj je tveganje? Kaj je verjetnost odpovedi?

Na ta in druga vprašanja bomo poskusili odgovoriti v nadaljevanju.

[1] Edwards, V.H., English, A., Ellis, R., Chosnek, J., Geaslin, E., Jones, S.F., Integrate Health, Safety, and Environment into Engineering Projects, American Institute of Chemical Engineers (AIChE), 2013, https://www.aiche.org/sites/default/files/cep/20130450_1.pdf
[2] Not In My Back Yard (Samo ne pri meni, drugod mi je vseeno).

1.1 Definicije

Takoj na začetku bomo postavili nekaj definicij[3] [31], ki so pomembne za razumevanje gradiva. V nadaljevanju bomo o njih povedali nekaj več.

Pri določitvi posameznih elementov se bomo naslonili zlasti na dokument Fault Tree Handbook (NUREG-0492)[4] in na Pojmovnik jedrske tehnike in varstva pred sevanji[3].

Varnost (angl. *safety*)[5] je z vidika okoljskega inženirstva značilnost posameznega sistema, da je brez primerov nesreč (nezgod ali okvar), torej neželenih dogodkov, ki vodijo do katastrofalnih posledic. Med take katastrofalne posledice spadajo npr. izlivi strupenih snovi v okolje, vplivi sevanja in radioaktivne kontaminacije na zdravje in okolje in podobno. Varnost dosežemo z uporabo zanesljivih struktur, komponent, sistemov in postopkov.

Zanesljivost (angl. *reliability*) je verjetnost, da bo sistem ali komponenta predvideno funkcijo opravljal predpisani čas in v predpisanih okoljskih pogojih.

Posledica (angl. *consequence*) je vpliv na okolje. Če se določeni dogodek zgodi, gre za običajno za neprijetno posledico dogodka, ki je lahko tudi merljiva, pogosto v denarnih zneskih.

Tveganje (angl. *risk*) je zmnožek verjetnosti in posledice. Tveganje bodočega dogodka ne more biti enako nič.

Verjetnost (angl. *probability*) je matematični koncept, izhajajoč iz statistike; ima različne definicije, v odvisnosti od opazovanega sistema. Izbrali bomo verjetnost po von Misesu, ki je razmerje med številom uresničitev izbranega dogodka in celotnim številom poizkusov, v limiti, ko število poizkusov teži proti neskončnosti, a takoj je treba pojasniti, da obstaja še mnogo več definicij. Za dogodke z izjemo začetnih dogodkov uporabljamo verjetnosti.

---

[3] Igor Jenčič, Pojmovnik jedrske tehnike in varstva pred sevanji, Društvo jedrskih strokovnjakov Slovenije, Ljubljana, junij 2012, vir: https://www.djs.si/upload/files/PojmovnikDJS.pdf

[4] Vesely, W.E., Goldberg, F. F., Roberts, H. H., Haasl, D. F., Fault Tree Handbook (NUREG-0492), U.S. Nuclear Regulatory Commission, January 1981, vir: https://www.nrc.gov/docs/ML1007/ML100780465.pdf

[5] Courtois, P. J., Safety, Reliability and Software Based System Requirements, PJC/13/06/1997, AVN-97/007, vir: https://dvikan.no/ntnu-studentserver/reports/Safety%20and%20Reliability.pdf

Frekvenca (angl. *frequency*) je število uresničitev nekega dogodka v časnovni enoti. Uporabljamo jo za začetne dogodke.

Razpoložljivost (angl. *availability*) je razmerje med časom obratovanja nekega elementa v določenem času in tem določenim časom.

Pogostost odpovedi (angl. *failure rate*) je število odpovedi v časovni enoti.
Čas misije (angl. *mission time*) bo v tej skripti čas, znotraj katerega opazujemo sistem. To je lahko čas delovanja elementa ali čas, ko mora biti element na razpolago, možne so tudi drugačne definicije.

Nerazpoložljivost (angl. *unavailability*) je nezmožnost nekega sistema, da bi opravljal svojo funkcijo.

Osnovni dogodek (angl. *basic event*) je dogodek, ki je na dnu drevesa odpovedi.

Glavni dogodek (angl. *top event*) je tisti dogodek, ki je na vrhu drevesa odpovedi.

Vmesni dogodek (angl. *intermediate event*) je vmesni dogodek med osnovnim in glavnim dogodkom v drevesu odpovedi.

Začetni dogodek (angl. *initiating event*) je dogodek ali človeško ravnanje, ki sproži zaporedje dogodkov do škodljivih posledic.

Odpoved (angl. *failure*) je prenehanje obratovanja obravnavanega sistema ali stanje opreme, zaradi katerega ne opravlja več svoje predvidene funkcije. Gre za prenehanje delovanja določenega sistema.

Napaka (angl. *error*) je z neskladje z določenim pravilom, določeno normo, neskladje z resničnostjo, dejstvi ali neskladje z zahtevanimi lastnostmi oz. zahtevano kakovostjo, tehnično pa tudi razlika med dejansko, zaželeno in izmerjeno, dobljeno vrednostjo količine. Odpoved je praviloma posledica napake, vendar vsaka napaka ne povzroči odpovedi.

Človeška napaka (angl. *human error*) je napaka, ki jo je povzročil človek.

Enojna odpoved (angl. *single failure*) je odpoved, zaradi katere celotni sistem ali komponenta izgubi zmožnost za opravljanje svoje funkcije. Tudi odpovedi s skupnim vzrokom in večkratne neidentificirane odpovedi spadajo med enojne odpovedi.

Odpoved s skupnim vzrokom (angl. *common cause failure*) je odpoved, ki nastane zaradi dogodka, ki sočasno prizadene tudi druge sisteme. Zapisali bi lahko, da gre za večkratne odpovedi, ki jih lahko pripišemo skupnemu vzroku (npr. napaka na različni opremi, ki je bila kalibrirana z istim, okvarjenim instrumentom).

Popolna odpoved (angl. *breakdown*) je odpoved, pri kateri je oprema v celoti izgubila sposobnost opravljanja svoje funkcije.

Naključna odpoved (angl. *random failure*) je odpoved, katerega nastanka ni bilo mogoče napovedati.

Osnovni vzrok (angl. *root cause*) je osnovni vzrok za opaženo okvarjeno stanje, če ga odpravimo, se naprava ne bo več kvarila.

Pot odpovedi (angl. *cut set*) je pot, ki vodi od osnovnega dogodka do vrhnjega dogodka.

1.1.1 Varnost ali zanesljivost?

Ali je lahko zanesljiv sistem nevaren? Da, seveda. Vodeni izstrelek je lahko in v primeru vojaškega spopada mora biti izjemno zanesljiv in je seveda izjemno nevaren.

Ali je lahko varen sistem nezanesljiv? To vprašanje je mnogo težje, saj je del določitve varnosti predpostavka, da bo sistem opravljal svojo nalogo določen čas v določenem okolju, vendar sta obseg in dolžina uporabe odvisna od naše lastne določitve meja delovanja. Sistem, ki deluje, je lahko varen, vendar njegova visoka nezanesljivost pomeni, da ga nimamo, ko ga bi potrebovali. Je torej nezanesljiv sistem v takem primeru varen ali nevaren?

Smiselno je razmišljati ločeno, se posebej ukvarjati z varnostjo in posebej z zanesljivostjo. Za nas je pomembnejša varnost kot je zanesljivost, zanesljivost je eden od parametrov, ki jih moramo pri analizi upoštevati, gre pa še vedno za varnostne analize.

1.2 Primer procesnega postroja

Da bomo lažje razumeli koncepte ocene varnosti in zanesljivosti, bomo najprej izbrali procesno enoto, na kateri bomo preizkušali svoje znanje. Uporabili bomo bazo podatkov raziskovalnih reaktorjev, ki pa za tak namen ni najbolj primerna. V resničnih primerih bo bralec moral najti bazo podatkov, ki izvira iz zakladnice znanja v povezavi s konkretnimi vprašanji.

V procesnem inženirstvu obstaja kopica rešitev, ki so namenjene doseganju določenih rezultatov. Najdemo jih v kemijskem inženirstvu, strojništvu, pa tudi drugih inženirski vejah. Običajno so sestavljeni iz rezervoarjev, zasunov, loput, ventilov, črpalk, cevi, elektromotorjev, aktuatorjev in drugih elementov. Lahko so izjemno zapleteni in zelo natančni, lahko so enostavni. Skupno vsem pa je, da se lahko, kot vsak drug človeški izdelek, pokvarijo oziroma, kot bomo to imenovali, odpovedo ali porušijo.

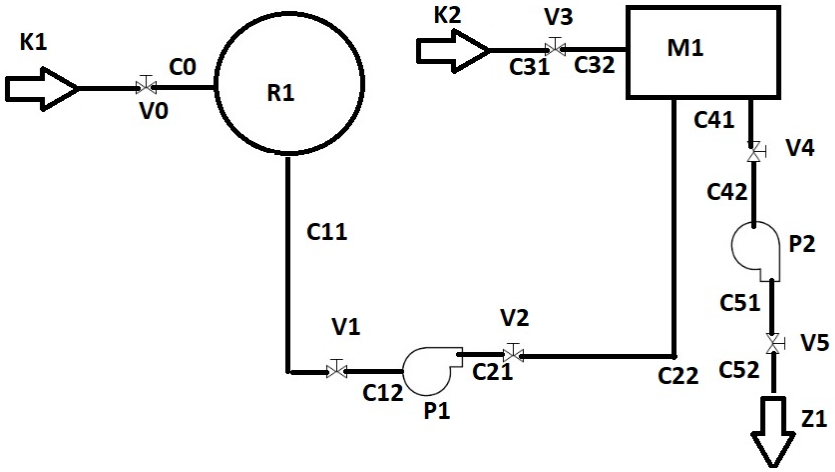
V našem primeru si bomo izmislili procesno napravo za mešanje dveh kapljevin. V strojništvu uporabljamo izraz kapljevine za tiste tekočine, ki tvorijo gladino. Mešali bomo dve tekočini – kapljevino 1 in kapljevino 2.

Kapljevina 1, ki jo bomo označili s K1, bo vstopala v rezervoar R1, nato bo tekla skozi cev C11 do ventila V1 in v cev C12 do črpalke P1. Nato bo tekla skozi črpalko P1 in cev C21 do ventila V2 in skozi cev C22 do mešalne komore M1.

V mešalno komoro M1 vstopa druga kapljevina K2 skozi ventil V3 in cev C32 ter se v mešalni komori M1 meša s kapljevino K1, ki vstopa skozi cev C22. Po opravljenem mešanju se tvori mešanica (zmes) Z1, ki izstopa skozi cev C41 do ventila V4 in nato skozi črpalko P2 in cev C51 ter ventil V5 do cevi C52, kjer mešanica Z1 izstopa.

Dogajanje pred R1 nas ne zanima, zato smo označili predhodno ocevje s C0, pripadajoč ventil pa z V0. To lahko npr. storimo, če vnašamo kapljevino R1 v šaržah, recimo s cisternami, kjer ima vsaka cisterna svoj sistem, ki je lahko predmet svoje analize, ali pa je za delovanje odgovoren nekdo tretji.

Slika te procesne naprave je na sliki 1



Slika 1: Procesna naprava za mešanje dveh kapljevin.

Naša naloga je oceniti, kolikšno je tveganje (torej zmnožek verjetnosti in posledice), da naprava svojega dela ne bo opravila, in to vrednost bomo znali bolje določiti ob koncu.

Smiselno je nemudoma razčistiti z nekaterimi napačnimi predpostavkami[6] [31]. Kot inženirje (o tem več v nadaljevanju) nas zanimajo številke, vendar so številke brez pojasnil lahko precej nevarne. Tako je netočna trditev, da lahko številska analiza (kvantitativna analiza, kot bomo pisali v nadaljevanju) dokaže, da je neki postroj varen ali nevaren. Pokaže lahko samo na primerjavo med tem, kar že poznamo, in tem, kar še moramo spoznati. Kvantitativna analiza nam lahko pomagamo, da tveganje zmanjšamo, izogniti pa se mu ne moremo. Čeprav utegne biti kvantitativna analiza naporna, pa je strošek sprejemljiv, če nam pomaga znižati tveganje, npr. elektrarna 1000 MW(e) (tj. megavatov električne energije) na dan ustvari 24.000 MW(e). Cena megavatne ure na tržišču niha, lahko pa predpostavimo, da je vredna okoli 50 EUR (leta 2015 je stala okoli 135 EUR, v letu 2020 pa med 44,50 in 61,50 EUR). Dan, ko takšna elektrarna stoji, stane (najmanj!) 1,2 milijona evrov. Kvantitativna analiza, ki nam pomaga, da se izognemo nenačrtovanim zaustavitvam, ne bo stala toliko.

Pri vsakem izračunavanju tveganja je treba biti zelo previden. Napake v predpostavkah nimajo posledic le v računskem rezultatu, temveč tudi (ali predvsem) v morebitno napačnem razumevanju posledic odpovedi. V izračun prihajajo številke z večjo ali manjšo

[6] Flage, R., Askeland, T, Assumptions in quantitative risk assessments: When explicit and when tacit?, Reliability Engineering & System Safety, Volume 197, May 2020.

negotovostjo in s tem je izračun obremenjen[7] [31]. Kako naj npr. določimo tveganje, da se nam bo investicija v jedrsko elektrarno povrnila, če cene elektrike nihajo tudi do 100 % na osnovno vrednost? Lahko primerjamo različne opcije in se med njimi, na isti osnovi, odločimo za eno.

Prav ta faza odločitve je najpomembnejša. Tveganje nam pomaga pri primerjavi med posameznimi potmi odločitve. Če se pojavi bistvena razlika v tveganju (in tu mislimo na več redov velikosti), je odločitev seveda lažja. Če bomo npr. obravnavali tveganje, da bomo umrli od črnih koz (30 %, WHO) s tveganjem smrti po cepljenju (4 na milijon cepljenih), bi morala biti odločitev lahka, vendar so v tehniki tovrstne primerjave sistemov in tehnologij, ki dajejo podobne rezultate redke (a se dogajajo, npr. azbest, freon ipd.).

Med zablode spada tudi predpostavka, da bomo analizirali vse možne nezgode. Tudi če bi to znali (pa tega ne znamo), bi bilo to nesmiselno.

In kaj storiti, če nimamo zadosti podatkov, da bi izvedli kvantitativno analizo? Potem je smiselno poiskati podobne podatke, in to natančno pojasniti. Takim podatkom običajno pravimo generični podatki; na voljo so v različnih publikacijah. Tovrstne podatke je potem treba dopolniti z našimi lastnimi raziskavami, če pa le-teh ni, lahko ostanejo le generični, pri čemer moramo posebej poudariti, da so vidne meje naše raziskave.

Podobno zmotno bi bilo, če bi se kvantitativne analize ne lotili zato, ker razpolagamo z zadosti podatki iz preteklih let. Ta zmota izhaja iz napačnega razumevanja verjetnosti. Verjetnost predpostavlja razpolaganje z neskončno zalogo eksperimentov, poleg navedenega pa se iz kvantitativne analize naučimo razvrstiti prioritete.

Seveda kvantitativna analiza ni povsem objektiven način razumevanja tveganja, saj je objektivnost odvisna od predpostavk, s katerimi smo analizo začeli. Prav tako bi težko zatrdili, da je kvantitativna analiza znanost v ožjem pomenu besede, če seveda pod izrazom znanost razumemo kopičenje resnic. Je pa kvantitativna analiza veda, ki ima, kot vsaka veda, svoje omejitve, in jo je varno in smiselno uporabiti znotraj lastnih omejitev.

[7] Nordgård, D.E., Exploring uncertainty in quantitative risk assessment used for decision support in electricity distribution system asset management, Reliability, risk and safety: Theory and applications, Proceedings of the European Safety and Reliability Conference (ESREL 2009), Prague, Czech Republic, vir: https://www.sintef.no/globalassets/project/riskdsam/esrel09-exploring.pdf

Za začetek se moramo najprej dogovoriti za način označevanja naše naprave. Napravo razdelimo na pet odsekov. Začne se z rezervoarjem R1. V realni procesni napravi seveda pogrešamo vstopni ventil, vendar se v tem besedilu ne ukvarjamo s procesnimi napravami, temveč procesno napravo uporabljamo le kot primer. Torej, prvi mejnik je rezervoar R1, nato črpalka P1, nato mešalna komora M1, nato črpalka P2 in področje za črpalko P2. Ventilov tipično ne uporabljamo kot mejnike, ker običajno služijo dvojemu – nadzoru pretoka kapljevine in osamitvi posameznih elementov procesnih naprav, če jih moramo menjati (torej en ventil pred posameznim elementom in en ventil za njim).

Da bi lahko ocenili verjetnost, da naprava svojega dela ne bo opravila, moramo najprej določiti nevarnosti, ki nam bi preprečile, da bi dobili mešanico Z1 v želenem razmerju.

1.3 Nevarnosti

Naša procesna naprava je podvržena celi kopici morebitnih nevarnosti. Prav identifikacija nevarnosti je prvi korak v analizi tveganja in je kvalitativen postopek[8] [31]. Predpostavimo, da ima kakšna od cevi razpoko (recimo, zaradi korozije), vendar cev še ne pušča. Nevarnost je potencial, ko se nevarnost realizira, nastane tveganje. Tveganje se realizira z verjetnostjo in ima velikost zmnožka verjetnosti in posledice. Posledica nevarnosti je npr. če poči katerakoli od cevi. Posledica nevarnosti je, če se rezervoar R1 ne napolni do želene višine ali se napolni prek želene višine. Posledica nevarnosti je, če začne katerakoli črpalka puščati.

Nevarnosti se uspešno izognemo, kadar naprava ali njen element normalno deluje ali je v normalnem stanju. Normalno delovanje pomeni delovanje skladno s procesnimi parametri, za katere je bila naprava ali njen element projektiran, normalno stanje pa je tisto, ki ne odstopa od pričakovanega (projektnega) stanja.

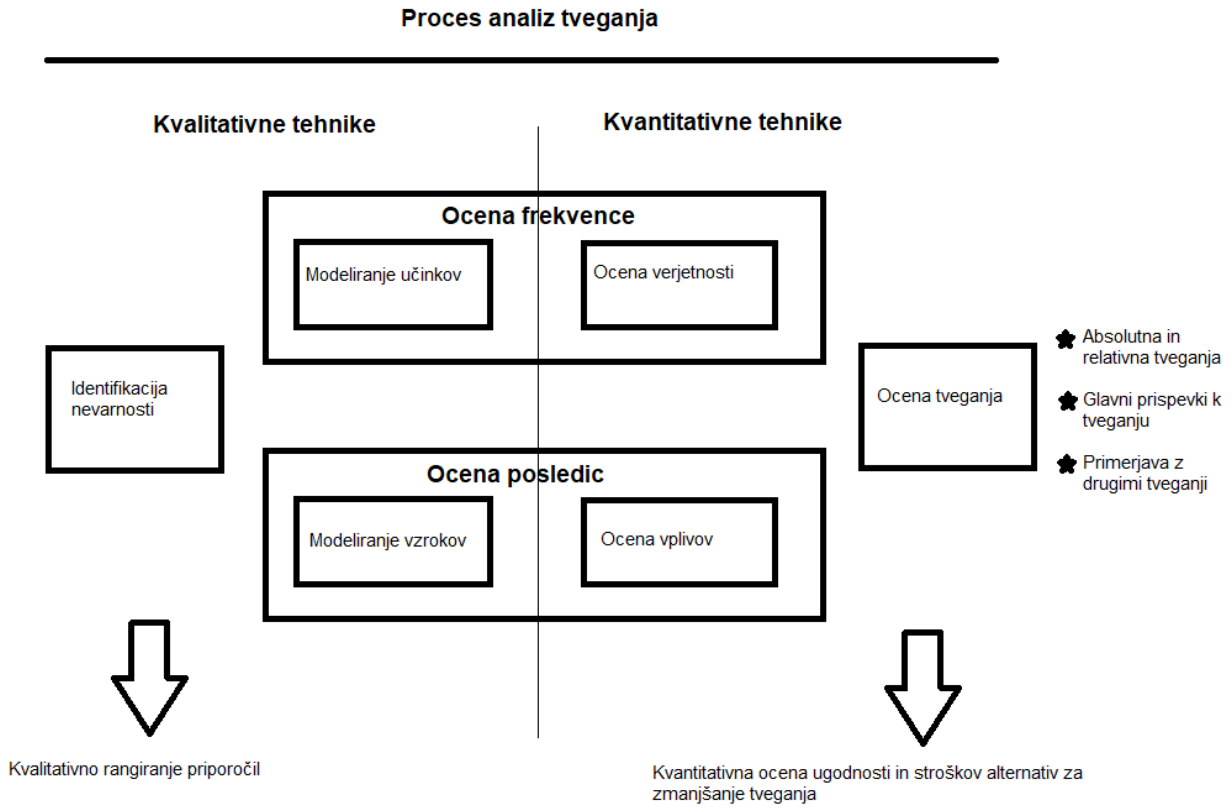
V tem delu se bomo posvetili vsakemu od elementov procesa in kvalitativno ugotovili, kaj se lahko zgodi.

Morda beseda ali dve o tem, kaj mislimo z izrazom kvalitativno in kaj mislimo z izrazom kvantitativno. Lord Kelvin je zapisal: »Če zmerim in izrazim v številkah, potem o tem nekaj vem«[9] [31]. Dober pregled obravnavanega je na sliki 2.

---

[8] Recommended Practices for Safety and Helath Programs: Hazard Identification and Assessment, United states department of labor, prispevek, vir: https://www.osha.gov/shpguidelines/hazard-Identification.html

[9] In praise of Lord Kelvin, Stars and solar physics, 2017, prispevek na spletni strani https://physicsworld.com, vir: https://physicsworld.com/a/in-praise-of-lord-kelvin/



Slika 2: Primerjava kvalitativnih in kvantitativnih tehnik določitve tveganja[10], prevod [31]

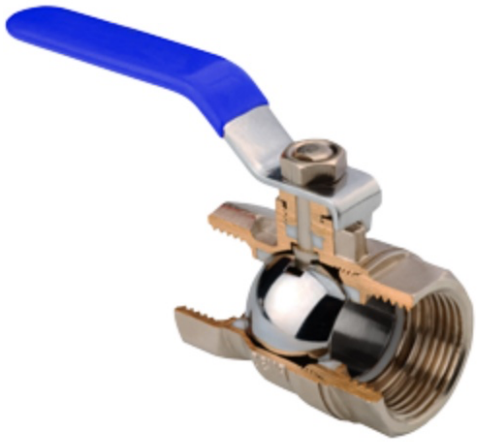
Zapisali smo že, da v tehniki računamo. Osnova tehnike je primerjava med napravami, postopki ali stanji. Temu pravimo kvantitativna ocena naprave, postopka ali stanja. Vendar potrebujemo za vsako kvantitativno oceno najprej postopek, s katerim takšno oceno dobimo. Takemu postopku pravimo kvalitativna ocena. Primer: Če želimo 50-odstotno utežno raztopino NaCl v vodi, moramo najprej stehtati obe sestavini (NaCl in H_2O) in ju nato zmešati. Na kvalitativni ravni bomo pojasnili, da vmešamo NaCl v H_2O ob sočasnem mešanju, dobili bomo raztopino, ne bomo pa (točno) vedeli, ali ustreza zahtevi po 50-odstotni utežni raztopini. Nato bomo postopek dopolnili z meritvijo, stehtali bomo vsak element, npr. po 10 N vsake od sestavin. V praksi seveda raje uporabljamo maso (recimo po 1 kg od vsake od sestavin), vendar uporaba mase ni rigorozna. Mase namreč ne moremo določiti s tehtanjem, s tehtanjem določimo težo. Če tehtamo maso na isti geografski lokaciji v istem času, je približek mase in teže med tehtanjem zadosten za inženirske aplikacije.

[10] Povzeto po Arendt, J.S., Lorenzo, D.K., Evaluating Process Safety in the Chemical Industry: A User's Guide to Quantitative Risk Analysis, EQE International, Wily, 2000.

V našem primeru bomo morali najprej kvalitativno določiti vsa stanja, ki jih označimo kot neuspeh. Naj bo takoj zapisano, da brez dobre kvalitativne ocene ne moremo dobiti dobre kvantitativne ocene.

Pojdimo po vrsti.

Ventil V1 lahko odpove. Da bi lahko določili načine odpovedi ventilov, moramo ventile poznati. V našem primeru bomo uporabili krogelne ventile, kot je prikazano na naslednji sliki:



Slika 3: Krogelni ventil [11].

V tem primeru gre za ročni ventil, to je ventil, ki ga odpiramo in zapiramo z ročko.

Kaj gre lahko narobe? Lahko se pojavi puščanje kapljevine K1 ob vstopu ali izstopu iz ventila, to se pojavi, kadar so cevi slabo uvijačene. Lahko se pojavijo notranje poškodbe krogle, in sicer zaradi dolgotrajne uporabe (obraba), zaradi slabega materiala, zaradi neprimernega vzdrževanja, zaradi nekompatibilnosti med kapljevino K1 in materialom krogle ali cevi. Lahko se pojavijo poškodbe mehanizma zapiranja in odpiranja. Lahko se zlomi ročica, lahko se zlomi vijak, s katerim je ročica pritrjena. Lahko se ventil zatakne v položaju odprto ali v položaju zaprto.

Vsaka odpoved pa ne pomeni nujno kriterija neuspeha. Če se ventil zatakne npr. v položaju odprto, lahko še vedno tok krmili izhodni ventil. Zato bo del kvalititativne analize tudi medsebojna odvisnost posameznih elementov.

[11] Vir slike: https://magneetventielshop.nl/kogelkraan-introductie.html

A mnogo lažje je, če se osredotočimo samo na kriterij uspeha posameznega elementa. Takemu pogledu pravimo konzervativen pristop. Konzervativen pristop je vsak pristop, ki v najslabšem primeru ohrani trenutno stanje, ga »konzervira«. Pristop glede trditve, da je kriterij neuspeha vsak odklon od normalnega delovanja, je konzervativen, ker lahko zagotovimo, da normalno stanje zagotavlja kriterij uspeha.

V bazah podatkov najdemo vrednosti za različne načine odpovedi ali pa tudi za vse možne skupaj. Katero uporabimo, se moramo odločiti glede na naš primer, in to tudi ustrezno utemeljiti. Rešitve ne moremo prepisati in iti naprej. Podatke, ki jih uporabljamo, moramo ustrezno dokumentirati in napisati, od kod in na kakšen način smo jih dobili ali izračunali[12] [31].

Ampak, ali je to res? Ali res normalno stanje ali normalno delovanje zagotavlja kriterij uspeha? V realnem življenju temu ni nujno tako. Vendar pa je delovanje, ki ni uspešno, a so pogoji za normalno delovanje ali normalno stanje izpolnjeni, posledica napačnega projektiranja. S tem se ne bomo ukvarjali, to je predmet drugih ved. Za nas je projekt uspešen, kadar ga potrdi ustrezna organizacija. O tem se bomo več pogovarjali kasneje.

Za nas bo v vsakem primeru naprava (ali njen element) izpolnila kriterij uspeha, ko bo delovala normalno ali bo v svojem normalnem stanju.

V procesni tehniki je koristno, če so vsi podobni elementi med seboj enaki. To je koristno z več vidikov. Vsak nov element procesne naprave, ki se loči od drugih, s seboj prinese morebitne težave. Treba ga je skladiščiti za primer menjave, če gre za enostaven element (kot recimo krogelni ventil), ali skladiščiti dele zanj (če gre npr. za črpalko). Kasneje se bomo naučili, kako oceniti pogostost odpovedi posameznega elementa ali naprave. Če je pogostost odpovedi zadosti nizka, potem lahko skladiščimo manj rezervnih delov na posamezno napravo ali elementov naprave, če imamo več istovrstnih naprav ali elementov. Prav tako vzdrževanje vsake naprave zahteva usposobljene vzdrževalce, tudi če gre za podobnovrstne naprave.

Seveda se bodo naprave ali elementi morali ločiti med seboj, če bodo delovali v različnih razmerah. Vendar v našem konkretnem primeru ni tako. Vsi ventili, z izjemo vhodnih ventilov za kapljevine, so na istem cevovodu (ki je seveda prekinjen z različnimi napravami ali elementi le-teh). Tudi vhodni ventili morajo biti sposobni enakih pretokov kot drugi –

[12] What's the Difference Between Qualitative and Quantitative Risk Analysis?, prispevek na spletni strani https://www.safran.com, vir: https://www.safran.com/blog/whats-the-difference-between-qualitative-and-quantitative-risk-analysis

lahko se namreč zgodi, da moramo hitro dodati samo eno od kapljevin, in tedaj bo za kratek čas pretok skozi vhodni ventil skoraj enak pretoku skozi izhodni ventil. Tudi če je to le za kratek čas, mora ventil prenesti takšno obremenitev.

Iz navedenega sledi, da bodo v našem primeru vsi ventili, od V1 do V5, enaki. Vsi naj bodo ročni krogelni ventili istega proizvajalca.

In kolikšna je pogostost odpovedi?

Verjetnost smo na kratko že definirali. Več o tem bomo zapisali kasneje, definicija verjetnosti pa je, skladno s Slovarjem slovenskega knjižnega jezika (od tu naprej SSKJ): »vrednost, ki izraža število ponovitev slučajnega dogodka pri sorazmerno velikem številu istovrstnih poskusov: ugotoviti verjetnost dogodka; razpredelnica verjetnosti po Bernoulliju vrednost, izražena z razmerjem med vsemi ponovitvami poskusa in ponovitvami, pri katerih določeni dogodek nastopi: verjetnost je dve proti ena« oziroma »v povedni rabi izraža prepričanost o možnosti obstajanja, nastopa česa: ni verjetnosti, da bo kaj drugače; majhna verjetnost je, da se bosta pobotala; precejšnja verjetnost je, da do spopada ne bo prišlo«.

Kot zapisano, obstaja več definicij verjetnosti. Poleg že zapisane velja tudi izraz za verjetnost, kjer pogostost odpovedi pomnožimo s časom misije. Pri tem je pogostost odpovedi N/T, kjer je N število odpovedi in T čas, v katerem so nastale te odpovedi. Izračun pojasni, koliko časa bo v povprečju minilo med dvema zaporednima odpovedima, lahko pa tudi, koliko časa bo poteklo med začetkom obratovanja in odpovedjo.

Pogostost odpovedi ima torej dva pomena – prepričanost o možnosti nastopa dogodka in nadalje številska vrednost.

Pri tem je treba pojasniti, da nas ne zanima obratovanje zunaj predpisanih parametrov. Povsem logično je, da bo pri porastu tlaka v sistemu prek vseh meja prav vsak element prej ali slej odpovedal.

1.4 Odpovedi opreme[13]

Bistven korak varnostne analize je pridobitev mernih podatkov o odpovedih in vzdrževanju opreme, ki je uporabljena. Podatki o odpovedi opreme se v osnovi razlikujejo od podatkov drugih inženirskih in znanstvenih ved, kajti na tem področju se vedno pojavljajo naključni in nepredvidljivi dogodki. Naključnost je izraz, ki temelji na velikem številu spremenljivk, ki vplivajo na zanesljivost nekega predmeta (opreme).

Prvi korak pri oblikovanju podatkovne baze zanesljivosti opreme je identifikacija načinov odpovedi opreme oz. ugotovitev poti, po katerih lahko oprema odpove. Čeprav ta faza na prvi pogled deluje jasno in enostavno, lahko hitro pride do nepravilnega razumevanja, tudi med izkušenimi inženirji.

Eden izmed praktičnih problemov pri podatkovnih bazah zanesljivosti, tudi če so bili osnovni podatki pridobljeni od proizvajalca, je nezadostna oz. ne dovolj podrobno opisana oprema.

Odpoved opreme lahko razdelimo v naslednje tri kategorije:

1. primarna odpoved → pojavi se pod normalnimi pogoji delovanja neke opreme in je razlog za odpoved v njej;
2. sekundarna odpoved → odpoved opreme, ki je povzročena zaradi vpliva zunanjih pogojev, in ne zaradi svoje odpovedi;
3. izsiljena odpoved (napaka pri uporavljanju)[14] → poseben tip sekundarne odpovedi, pojavi se zaradi odpovedi sistema, ki nadzira opremo [9].

1.4.1 Podatki o odpovedi

Kakovost vsake varnostne analize temelji na posedovanju kvalitetnih in verodostojnih podatkov vsake posamezne komponente oz. opreme. Na žalost ti podatki v veliki večini niso na razpolago ali pa so dokaj neverodostojni.

[13] Zanesljivost opreme (angl. *equipment reliability*)
[14] Izsiljena odpoved (angl. *command failure*)

Razlogi pomanjkanja kvalitetnih podatkov:

- Podatki o zanesljivosti niso nikoli konstantni oz. enaki, kajti pogoji delovanja in vzdrževanja se vedno spreminjajo.
- Nikoli niso znani vsi možni načini odpovedi.
- Mnogo komponent opreme (npr. tlačna posoda) ni moč opredeliti s podatki merljivosti pogostosti pojava odpovedi, zaradi česar je vzpostavitev podatkovne baze izjemno težka.
- Podjetja nerada posredujejo svoje podatke, saj se bojijo svoje konkurence.
- Pogoji obratovanja se za enako komponento opreme lahko spreminjajo od sistema do sistema in od časa do časa.
- Vir podatkov je lahko prirejen s strani proizvajalca, saj ta želi predstaviti svoj izdelek v najboljši luči [23, 24].
- In kaj, ko imamo različne proizvajalce podobne opreme?

1.4.2 Viri podatkov zanesljivosti opreme

Poznamo tri različne vire podatkov zanesljivosti opreme. To so:

- realni podatki našega obravnavanega sistema[15],
- strokovno mnenje,
- splošne (generične) podatkovne baze.

Od teh treh navedenih virov podatkov so realni podatki našega obravnavanega sistema najboljši vir podatkov, saj se vsak proces sistema redno analizira in se vodi evidenca (protokoli, kontrolni listi, video in glasovni posnetki itd.). Ti podatki ponavadi pokrivajo zelo kratko časovno obdobje (to pomeni, da smo jih spremljali kratek čas), zato jih običajno združimo z generičnimi podatki, ki obstajajo za daljše obdobje (to pomeni, da so njihov temelj različne komponente iz različnih virov, ki so bili opazovani dlje ali so se opazovanja ponavljala). Pri tem si pomagamo z Bayesovo metodo[16] [31]

[15] Posnetki sistema (angl. *plant records*)
[16] Aven, T., Bayesian analysis: Critical issues related to its scope and boundaries in a risk context, Reliability Engineering & System Safety, Volume 204, December 2020.

Strokovno mnenje pridobimo z intervjuvanjem ljudi, ki so dalj časa delali na nekem sistemu in imajo občutek o zanesljivosti delovanja sistema, čeprav nimajo ustreznih znanj za to. Takšna informacija je lahko neprecenljive vrednosti [23], pri čemer se uporablja postopek Delfi [17] [31].

Če posnetki sistema in strokovno mnenje niso na voljo, se moramo poslužiti splošnih podatkov, pridobljenih iz različnih virov, pri čemer pa osnovo predstavljajo podatki, ki jih je pridobil proizvajalec, vendar so ti izjemno težko pridobljivi zaradi varovanja poslovnih skrivnosti.

V večini primerov se zato poslužujemo splošno dosegljivih podatkov iz razpoložljivih zgodovinskih baz podatkov, ki zajemajo primerjalne vrednosti več področij (jedrska, letalska, avtomobilska, procesna industrija itd.), vrednosti izvedenih raziskovalnih študij, obravnavanih primerov ipd. ter se periodično posodabljajo. Ob pravilni primerjavi karakteristik npr. opreme analiziranega primera z razpoložljivimi viri baz podatkov, nam slednje omogočajo dobro osnovo za primerno izvedbo varnostne analize in zanesljivosti nekega sistema [19].

Strokovno mnenje mnogokrat predstavlja najlažji postopek pridobitve podatkov, ki so lahko izredno zanesljivi, če je bila analiza sistema opravljena korektno [24]. Treba pa je pojasniti, da ljudje zelo slabo ocenjujejo verjetnost[18].

Kot inženirje nas seveda zanima številska vrednost. Te številske vrednosti dobimo na različne načine, tudi o tem več kasneje, na tem mestu bomo citirali bazo podatkov, ki je bila aktivna ob času pisanja[19], za potrebe okoljskega inženirstva pa se lahko zanašamo tudi na bolj specializirano bazo podatkov[20].

To bazo podatkov vzdržuje Mednarodna agencija za jedrsko energijo (IAEA), saj je jedrska industrija ena od dveh industrij, kjer so številski podatki postopkovno in dolgoletno obravnavani; druga industrija je letalstvo.

---

[17] Program Management: Delphi Technique, prispevek na spletni strani https://acqnotes.com,
vir: https://acqnotes.com/acqnote/careerfields/delphi-technique

[18] Slovic, P, Fischhoff, B., Lichtenstein, S. Facts and Fears: Understanding Perceived Risk, objavljeno v Schwing, R.C., Albers, W.A. (eds) Societal Risk Assessment. General Motors Research Laboratories. Springer, Boston, vir: https://link.springer.com/chapter/10.1007/978-1-4899-0445-4_9 , tudi [31]

[19] Generic component reliability data for research reactor PSA, IAEA-TECDOC-930, IAEA – International Atomic Energy Agency, 1997, vir: https://www-pub.iaea.org/MTCD/Publications/PDF/te_0930_scr.pdf

[20] Goble, W., Getting Realistic Failure Rate Data – Part 3, prispevek na strani https://www.exida .com, 2015,
vir: https://www.exida.com/Blog/getting-realistic-failure-rate-data-part-3

V citirani bazi podatkov najdemo pogostost odpovedi ventila, in sicer je označena z izrazom VX in oznako posamezne naprave, torej prvi dve črki sta vedno VX, in tako jih tudi prepoznamo. V bazi podatkov je najti več rezultatov, ki so odvisni od posameznega reaktorja, in so zapisani z vrednostjo 1E-6/h , torej v številu dogodkov na milijon obratovalnih ur (ali 114 let).

Za potrebe tega besedila bomo uporabljali izraz X,XXE-YY, kar pomeni X,XX x 10^{-YY}. Zapis, ki smo ga izbrali, je dovoljen inženirski zapis in uporaben pri računalniških izračunih, zato se ga bomo držali tudi pri računanju »peš«.

Zapis v urah je pogosto zavajajoč. Težko si predstavljamo, kaj pomeni, če posamezni element obratuje milijon ur. Lažje, je, če si predstavljamo čas v letih. Milijon ur je 114 let, in to številko bomo obravnavali v nadaljevanju.

Najvišja vrednost za odpoved ventila na straneh 66 in 67 je 13,5 na 114 obratovalnih let ali 0,118/a. Najnižja vrednost je 0,3 na 114 obratovalnih let ali 2,63E-3/a[21]. Vendar je ob tem treba pogledati še številne dogodke – obe, najvišja in najnižja številka, sta bili izračunani na osnovi le nekaj dogodkov. Na isti strani je najti še dve srednji vrednosti na osnovi nekaj deset dogodkov, in ti sta okoli 5 na 114 obratovalnih let ali 4,38E-2/a. Že ta bežen vpogled pojasni pomembnost podatkov. Najdemo še dve številki – pri 5-odstotnem intervalu zanesljivosti in pri 95-odstotnem intervalu zaupanja (te pojme ste spoznali pri statistiki, na kratko pa jih bomo tudi pojasnili v nadaljevanju). Pri 95-odstotnem intervalu zaupanja je pogostost odpovedi ventila v enem od primerov 6,2 na 114 obratovalnih let ali 5,43E-2/a, in to bo naša izbrana vrednost. Pri vsakem takšnem izboru moramo pojasniti, zakaj smo se tako odločili. V konkretnem primeru predpostavimo, da poznamo osnovno napravo, na kateri so beležili odpovedi, in ocenimo, da je naša naprava podobna tisti napravi. Najprej npr. na strani 67 ugotovimo, da so dobili raziskovalci podatke iz naprave, označene s kodo PRC-H, in sicer so zaznali kar 76 dogodkov. To pomeni, da imajo precej dober vpogled v delovanje ventila. Nato v dokumentu na strani 28 ugotovimo, da je šlo za napravo HWRR v kitajskem jedrskem inštitutu. Če je ta naprava podobna tisti, ki jo obravnavamo, lahko podatke uporabimo neposredno, v nasprotnem pa se moramo poučiti o morebitnih razlikah. Večina naprav na področju jedrske tehnike je dodobra raziskanih (če gre za civilne naprave) in je zato uporaba teh podatkov smiselna.

[21] Merska enota verjetnosti odpovedi je 1/leto, ali 1/a (*per annum*, latinska beseda, ki pomeni *na leto*.).

Pri ventilih bomo zlahka našli več podatkov na osnovi industrijskih standardov, saj gre za bolj ali manj standardne elemente. Pri specializiranih elementih bo to težje. Odgovornost za iskanje pravih podatkov je seveda pri tistih, ki oceno dajejo.

In kako je s črpalkami? Črpalke, ki so gnane z elektromotorji, so označene s PMA. Iz baze podatkov ugotovimo rezultate od 7,1 na 114 let do 192 na 114 obratovalnih let. Po številu dogodkov odstopa številka 14,2 na 114 let ali 0,125/a. Pri 95-odstotnem intervalu zaupanja je pogostost odpovedi z motorjem gnane črpalke 19,8 na 114 let ali 0,174/a in to bo naša izbrana vrednost. Vrednost je nekako v sredini obravnavanih vrednosti. Lahko bi se odločali konzervativno in izbrali najslabšo vrednost ali optimistično in izbrali najboljšo vrednost, najbolje pa je, da izberemo vrednost za napravo, ki je naši najbolj podobna.

Kaj te številke pomenijo?

Pogostost odpovedi označujemo s številom let, ko lahko pričakujemo, da se bo dogodek zgodil. V našem primeru torej pričakujemo, da bo z intervalom zaupanja 95 % (kar je v inženirski praksi sprejemljivo) ventil odpovedal nekako 5-krat v 100 obratovalnih letih.

Naslednji element, ki ga obravnavamo, je rezervoar. V našem primeru je označen z R1 (sorodni element je mešalna posoda, ki pa ni zgolj rezervoar). V bazi podatkov odpovedi je označen z GT. Pri pregledu ugotovimo, da gre za več rezervoarjev; še najbolj podoben je GTE (raztezna posoda). Vendar pri GTE ni najti rezultatov, več je na voljo pri GTA. GTA za nas ni neposredno uporaben, treba bi bilo najti boljše informacije. Ne glede na to pa moramo za obravnavo našega sistema uporabiti neko vrednost in uporabili bomo GTA-vrednost 4,4 na 114 let obratovanja ali 3,85E-2/a.

Naslednji element, s katerim se soočamo, so cevni odseki. Cevne odseke smo s prvo številko oštevilčili s številkami odsekov, od 1 do 5. Z drugo številko smo označili številko cevi znotraj istega cevnega odseka. Konkretno: pri cevnem odseku 1 najdemo dve cevi, eno pred ventilom in eno za ventilom.

Cevi so sicer dobro znani procesni elementi. Pri ceveh se odpoved lahko pojavi zaradi različnih vzrokov. Pri varjenih ceveh je lahko zvar nepravilno izveden. Lahko nastane korozija. Odpoved se lahko pojavi zaradi vključkov v cevni steni. Med delovanjem se lahko pojavijo napake zaradi vibracij.

V »naši« bazi podatkov so ravni cevni odseki označeni s FS, sledi oznaka posamezne naprave. S 95-odstotnim intervalom zaupanja najdemo za manjše cevi številki od 0,3 do 10 na 114 let delovanja. Predpostavimo konzervativno vrednost 8,77E-2/a. Ob tem je pri ceveh treba pojasniti še to, da lahko najdemo baze podatkov, kjer bo pogostost odpovedi cevi temeljila tudi na dolžini posamezne cevi. A za naš izračun bo taka številka zadostna.

1.5 Kaj je tveganje?

Tveganje je zmnožek verjetnosti in posledice istega dogodka. Pogosto govorimo tudi o stopnji tveganja (npr. varstvo pri delu, vendar nas zanima samo številska vrednost kot metrika varnostne stroke, pri čemer velja opozoriti, da stopnje tveganja med različnimi poklici ni možno povsem primerjati[22] [31]).

Verjetnost izračunamo na različne načine, v odvisnosti od vrste dogodka oziroma načina obratovanja. V splošnem poznamo vsaj dva načina obratovanja: obratovanje je lahko stalno, ali pa naprava začne obratovati, kadar jo potrebujemo (obratovanje na zahtevo).

Kadar poznamo pogostost odpovedi in kadar poznamo podatke o času obratovanja (čas misije, t), lahko izračunamo verjetnost odpovedi tako, da pogostost odpovedi pomnožimo s časom obratovanja.

Kadar poznamo podatke o verjetnosti, da bo naprava odpovedala, ko bomo zahtevali njeno obratovanje, potem je že to verjetnost odpovedi na zahtevo. Vendar bo naprava tudi obratovala. Naprava mora delovati toliko časa, da opravi svojo funkcijo, zato pomnožimo pogostost odpovedi s časom misije in rezultat prištejemo k verjetnosti, da bo naprava začela delovati na zahtevo.

Pogostnost letalskih nesreč je zelo nizka. Po podatkih International Civil Aviation Organization (ICAO), ki je specializirana agencija Združenih narodov, je bilo v letu 2019 3,02 nesreč (pod nazivom nesreča pomeni dogodek, ki ima za posledico lom trupa) na 1.000.000 vzletov komercialnih letal nad 5,7 tone nosilnosti[23]. Na dan sicer vzleti okoli 100.000 letal [24]. Vsa seveda niso komercialna. Predpostavimo, da vzleti na dan 10.000

[22] Hill, T., Kusev, P., van Schaik, P., Choice Under Risk: How occupation Influences Preferences, Front. Psychol., 2019, vir: https://www.frontiersin.org/articles/10.3389/fpsyg.2019.02003/full
[23] Accident Statistics, ICAO SAFETY, vir: https://www.icao.int/safety/iStars/Pages/Accident-Statistics.aspx
[24] July 25, 2019, Aviation's busiest day in history, prispevek na spletni strani https://www.flight-delayed.com, vir: https://www.flight-delayed.com/news/2019/07/30/july-25-2019-aviations-busiest-day-in-history

komercialnih letov, to pomeni, da je potrebnih 100 dni za 1.000.000 vzletov, kar pomeni približno 9 nesreč na leto.

Na leto na vsem svetu v posledici letalskih nesreč komercialnih letal (nad 5,7 tone nosilnosti) umre približno 400 ljudi. To je seveda grozen rezultat, vendar je ta rezultat treba primerjati z drugimi vrstami transporta.

V ZDA[25] je verjetnost smrti v motornem vozilu približno 1 : 7.700, v vlaku 1 : 306.000 in letalu 1 : 2.067.000. Ne more biti dvoma: z letali je daleč najbolj varno potovati, in sicer okoli 200-krat bolj varno kot z motornimi vozili.

Vendar človeška percepcija letalskih nesreč ne jemlje zlahka. Letalske nesreče so prikazane kot nekaj velikega. Čeprav se zgodijo redko, so predmet medijske pozornosti. Poleg tega ljudje, ki so udeleženi v letalskih nesrečah, nimajo prav nobene kontrole nad tem, kaj se jim je zgodilo. Vse to pripomore k temu, da ljudje dojemamo letalske nesreče kot tveganje, ki je pomembno. Ljudi, ki potujejo z letali, pogosto prežema strah. Včasih do te mere, da ne bodo leteli, čeprav podatki nesporno dokazujejo, da je letalski prevoz najvarnejši.

Ali ste že kdaj doživeli trenutek, ko ste si rekli: »Skoraj bi se mi zgodila nesreča.«? Ti trenutki niso tako redki. Pogosto lahko npr. koreliramo tveganje z verjetnostjo[26] .

Dogodek, ki se zgodi 1-krat v 10 primerih, označujemo kot zelo visoko verjeten. Dogodek, ki se zgodi 1-krat v 100 primerih, je visoko verjeten. Dogodek, ki se zgodi 1-krat v 1000 primerih, je srednje verjeten in dogodek, ki se zgodi manj kot 1-krat v 1000 primerih, je redek.

Kaj pa posledice? Vir[26], ki se ukvarja z zdravljenjem, določa posledice kot majhne (tiste, ki nimajo vpliva na zdravje ali imajo zanemarljiv ekonomski učinek), srednje (brez neposrednega vpliva na zdravje ali povračljiv ekonomski učinek), resne (takšne, ki poslabšajo zdravje ali imajo večji nepovračljiv ekonomski učinek) ter katastrofalne (smrt ali trajna prizadetost, velik nepovračljiv ekonomski učinek).

Strogo matematično gledano seveda ne moremo množiti kvalitativnih pokazateljev. Zmnožek redkega dogodka z majhno posledico nima prave enote.

[25] How Risky is Flying? vir: https://www.pbs.org/wgbh/nova/planecrash/risk-01.html
[26] Vir: https://ehealthresearch.no/files/documents/Appendix-Definitions.pdf

Znana je kvalitativna matrika tveganja:

Posledica Verjetnost dogodka?	majhna	srednja	resna	katastrofalna
redka				
srednja				
visoka				
zelo visoka				

Slika 4: Matrika tveganja – prazna

To matriko lahko zdaj napolnimo s kvalitativno oceno tveganja

Posledica Verjetnost dogodka?	majhna	srednja	resna	katastrofalna
redka				
srednja				
visoka				
zelo visoka				

Slika 5: Matrika tveganja – izpolnjena

Z zeleno smo označili nizko stopnjo tveganja, z oranžno srednjo stopnjo in z rdečo visoko stopnjo tveganja.

Pojasniti velja, da je ta matrika lahko bistveno drugačna. Predpostavimo, da gre za vprašanje dobrobiti našega otroka. Ali bo mati dveletnika ocenila, da je stopnja tveganja visoka, če se na igrišču otroku približa kašljajoči odrasli (Covid-19?)? Verjetnost prenosa okužbe v odprtem prostoru je nizka, vendar mati tega ne bo obravnavala kot nizko tvegan dogodek.

Z vidika matere dveletnika je svet okoli njenega otroka videti takole:

Posledica Verjetnost dogodka?	majhna	srednja	resna	katastrofalna
redka				
srednja				
visoka				
zelo visoka				

Slika 6: Matrika tveganja za osebo, nenaklonjeno tveganju

Kaj pa vidik poklicnega avtomobilskega dirkača? Realistično gre za izzivanje usode v vozilih, ki so sicer zavarovana z različnimi varnostnimi mehanizmi, ki pa so predmet raziskav.

Z vidika poklicnega avtomobilskega dirkača bo tabela bržkone takšna:

Posledica Verjetnost dogodka?	majhna	srednja	resna	katastrofalna
redka				
srednja				
visoka				
zelo visoka				

Slika 7: Matrika tveganja za osebo, naklonjeno tveganju

Šele odpoved zavor pri visoki hitrosti bo dirkača resno zaskrbela.

Takšen način obravnave tveganja nas ne more zadovoljiti. Vsak ocenjevalec bi podal svoj lastni pogled in z vidika odločevalcev ravnanja ne bi bila vnaprej predvidljiva. Zato je treba postaviti številski standard.

Čeprav je slišati precej morbidno, je najenostavnejši standard denarni strošek. Človeško življenje je moč postaviti v okvir odškodnine, prav tako zdravje. Ti zneski so javni, splošni in razmeroma enostavno dostopni.

Vendar včasih pripeljejo do neželenih rezultatov.

V ZDA so do vprašanj tveganj zelo pragmatični. Začeli so leta 1982, ko so izračunali, da je vrednost človeškega življenja okoli 300.000 dolarjev[27]. Ta znesek je bil tako nizek, da se proizvajalcem barve ni izplačalo tiskati nalepk, da so barve nevarne. Zato so vrednost zviševali, vse do trenutne vrednosti, ki je okoli 9 milijonov dolarjev. V Avstraliji je vrednost življenja okoli 4,2 milijona avstralskih dolarjev, na Novi Zelandiji 2 milijona leta 1991 in 4,14 milijona leta 2016, na Švedskem okoli 3,7 milijona evrov itd.[28].

[27] Lives Vs. The Economy, 15 April 2020, prispevek na spletni strani https://npr.org, vir: https://www.npr.org/transcripts/835571843
[28] Value of life, prispevek na spletni strani https://en.wikipedia.org, vir: https://en.wikipedia.org/wiki/Value_of_life

Strinjamo se lahko, da je vrednost življenja v Evropi okoli 4 milijone evrov. Iz tega zneska je mogoče izračunati druge vrednosti posledice. Slovenska sodišča za enostavne poškodbe določijo okoli 10.000 evrov odškodnine. V spodaj obrazloženi zadevi je sodišče za bolečine določilo EUR 12.500. Ugotovilo je, da je bila »tožnica ob nesreči stara 48 let in je utrpela težji pretres možganov z blago oteklino možganovine, udarnino glave, zvin vratne hrbtenice in odrgnino desnega kolena. K zavesti je prišla četrti dan po nesreči in bila nato v bolnišnici 10 dni. Tožnica je seveda morala prestati več preiskav (rentgensko slikanje, MRI-preiskave, zdravljenje v zdravilišču, avdiogram itd.), ves čas pa je dobivala tudi zdravila za lajšanje bolečin. Izvedenec je ocenil, da je tožnica trpela bolečine srednje stopnje v trajanju dveh mesecev, da je blage bolečine trpela pri ukrepih v zvezi z vratno hrbtenico, skupno v trajanju enega meseca, da pa ima občasne glavobole tudi še zdaj. Sodišče prve stopnje je ugotovilo, da je imela tožnica že pred nesrečo težave z hrbtenico in da je nihajna poškodba v prometni nesreči prispevala 30 % težav«[29].

Vidimo, da percepcija raste logaritemsko. Če štejemo, da je zvin vratne hrbtenice poškodba, a ne posebej huda, gre za srednjo posledico. Tako lahko, v evrih, izdelamo naslednjo tabelo

Tabela 1: Tveganje = verjetnost x posledica.

Posledica / Verjetnost	majhna 1.000 EUR	srednja 10.000 EUR	resna 100.000 EUR	katastrofalna 1.000.000 EUR
redka – 1 v 10.000 primerih	0,1	1	10	100
srednja – 1 v 1.000 primerih	1	10	100	1.000
visoka – 1 v 100 primerih	10	100	1.000	10.000
zelo visoka – 1 v 10 primerih	100	1.000	10.000	100.000

Zdaj so zadeve jasne. Rezultat je številski, v enoti EUR/primer. S podobnimi preračunavanji se ukvarjajo tisti, ki v zavarovalnicah izračunavajo premije. Imenujemo jih aktuatorji. Seveda so njihovi modeli bistveno bolj zapleteni.

[29] Vrhovno sodišče republike Slovenije, Evidenčna številka: VS0017830, datum odločbe: 14. 08. 2015, vir: http://www.sodnapraksa.si/?q=od%C5%A1kodnina%20zvin%20vratne%20hrbtenice&database[SOVS]=SOVS&_submit=i%C5%A1%C4%8Di&order=date&direction=desc&rowsPerPage=20&page=0&id=2015081111389278

1.6 Zgodovina varnostnih analiz

Analize varnosti in zanesljivosti so se začele pojavljati in izvajati v prejšnjem stoletju zaradi izrazitega tehnološkega napredka. Sprva se je obravnava zanesljivosti začela na področju jedrske in letalske industrije, sčasoma pa se je preselila tudi na preostala industrijska področja (kemična industrija, industrija elektronike, procesna industrija ipd).

Izredno hiter razvoj delovnih okolij, vezanih na kompleksne tehnologije, je namreč omogočil nove izzive, vendar s tem tudi povečanje števila delovnih nesreč in zastojev sistemskih (proizvodnih) procesov oz. sistemov. Pri tem je izjemno pomembno preučevanje in preprečevanje faktorja človeških napak in tehnoloških odpovedi [5].

Avtorji [6] pojasnjujejo, da so Atenci pred več kot 2.400 leti poskušali oceniti tveganje pred sprejetjem odločitev. Vendar je sistematski pristop k oceni tveganja in upravljanju tveganja mnogo mlajši, sega v osemdeseta leta prejšnjega stoletja. A od tedaj se je to področje bistveno razvilo.

Z namenom zagotavljanja zanesljivosti in varnosti sistemov so se v šestdesetih letih prejšnjega stoletja začeli razvijati in vse bolj uporabljati postopki varnosti in zanesljivosti v tehnoloških sistemih. Večji preskok razvoja in uporabe teh metod (analiz) je bil sredi osemdesetih let, na kar sta vplivala izredno hiter tehnološki razvoj in pojav večjega števila nezgod, z večjim poudarkom na človeške napake.

Od vseh industrijskih področij prav procesna industrija najbolj izstopa, saj vsebuje največ možnih in različnih načinov obratovanja in s tem povezano največje število tako tehničnih napak (okvar) kot človeških napak (nezgode zaradi človeške nezanesljivosti). Ker dandanes človeške napake v povprečju predstavljajo kar 80 % vseh nesreč, se njim posveča še posebna pozornost [16].

Zaradi vsega navedenega je bilo v zadnjih desetletjih razvitih nemalo metod analiziranja tako tehnične kot človeške napake.

Polje tveganja ima dvoje glavnih nalog [6], in sicer:

(I) uporabo ocen tveganja in obvladovanje tveganj za preučevanje in obravnavanje tveganja določenih dejavnosti (npr. obratovanje obalnih naprav ali naložba) in

(II) razvoj, povezan s koncepti, teorijami, okviri, pristopi, načeli, postopki in modeli za razumevanje, ocenjevanje, karakterizacijo, komuniciranje in (v širšem smislu) upravljanje/upravljanje.

Drugi del del (II) vsebuje koncepte in orodja za ocenjevanje in upravljanje, ki se uporabljajo pri posebnih problemih ocenjevanja in upravljanja v (I). Poenostavljeno lahko rečemo, da gre pri področju tveganja za razumevanje sveta (v zvezi s tveganjem) in kako lahko in moramo razumeti, oceniti in upravljati ta svet.

V tem besedilu je prikazan način, kako lahko izvedemo ugotavljanje vpliva tehnične odpovedi in človeške nezanesljivosti na delovanje čistilne naprave. Slednje predstavlja kvantitativno določevanje verjetnosti zanesljivosti čistilne naprave (tehnična odpoved) in s poudarkom predvsem na ugotavljanju verjetnosti nastanka človeške odpovedi/napake (človeške nezanesljivosti). Verjetnost tehnične in človeške odpovedi je analizirana na podlagi naslednjih dveh spektrov nezaželenih dogodkov: trenutne odpovedi čistilne naprave (celotna/popolna odpoved) in kontinuirane odpovedi (delna odpoved/omejeno delovanje). Posledice obeh spektrov nezaželenih dogodkov predstavlja izpust medija, tj. neprečiščene ali nezadostno prečiščene odpadne vode v okolico (ponikanje v tla ali vodotok), kar lahko povzroči resnejše in trajnejše onesnaženje okolja.

Ta problematika kljub večletnim izkušnjam obravnavanja področja čistilnih naprav predstavlja izziv v okviru raziskovanja področja te veje Procesne tehnike. Po eni strani zaradi dejstva, da je razpoložljive svetovne literature in virov s tega področja zelo malo, po drugi strani pa, ker je vpliv potenciala človeške napake v analizah zanesljivosti sistemov prečiščevanja odpadnih voda (čistilnih naprav) izjemno slabo raziskan.

V tem besedilu je prikazana metodologija (in/ali orodje), ki bo uporabna za bralca, in, konkretno, s katero bo sorazmerno hitro in učinkovito mogoče ugotovili verjetnosti nastanka napak in na osnovi slednjih pripraviti ukrepe za njihovo preprečevanje.

V primeru obsežnih sistemov je smiselno in potrebno uporabljati ustrezne računalniške programe, ki omogočajo rigorozno in konkretno spremljanje sprememb v delovanju sistema. Taki računalniški programi so na voljo in omogočajo zelo natančne izračune. Spregledati pa ne smemo, da je kvaliteta rezultata odvisna od vhodnih pogojev.

Univerzitetna založba
Univerze v Mariboru

2 Delovanje sistemov in človeška zanesljivost

2.1 Postopki ugotavljanja verjetnosti odpovedi in človeških napak

Tveganje, zanesljivost in odpovedi oziroma napake so pojmi, ki so pogosto v sopomenski spregi. Zanesljiva naprava je manj podvržena odpovedim in obratno: nezanesljiva naprava je tista, na katero se ne moremo zanesti. Vendar sta pojma drug od drugega ločena. Prav lahko se zgodi, da se zanesljiva naprava pokvari večkrat kot nezanesljiva, kot se lahko zgodi, da pri dvojnem metu kock večkrat vržemo 2 kot 7, kljub bistveno višji verjetnosti slednjega.

Oba izraza sta povezana z zaupanjem – torej s tem, s kakšnim zaupanjem verjamemo v rezultate analize. Pri tem se pogosto naslonimo na interval zaupanja. Interval zaupanja je ocena, narejena na osnovi opazovanih podatkov. Določa obseg (interval), v katerem je z želeno stopnjo tveganj izračunani parameter (npr. povprečna vrednost neke meritve). Interval zaupanja je neposredno povezan z zanesljivostjo izbranega postopka ocenjevanja. Interval zaupanja pa ne pomeni, da bo npr. (ob upoštevanju 95-odstotne gotovosti) 95 % podatkov znotraj želenega intervala, niti da bo želena vrednost s 95-odstotno verjetnostjo znotraj intervala. A v splošnem lahko zaključimo, da je analiza, katere rezultat je znotraj intervala zaupanja, bolj zanesljiva kot tista, pri kateri je rezultat zunaj intervala zaupanja.

Pri varnostni analizi moramo upoštevati še, da podatki, ki jih vstavljamo, ne predstavljajo točkovnih vrednosti, temveč so to porazdelitve, ki bolj ali manj vplivajo na končni rezultat. Po analizi občutljivosti posamezne komponente ugotovimo, da imajo nekatere komponente na končni rezultat višji vpliv kot druge[30,31].[31] Komponente torej lahko rangiramo.

Zakaj se ukvarjamo z verjetnostjo napak?

Izredno hiter razvoj delovnih okolij, vezanih na kompleksne tehnologije, je omogočil nove izzive, s tem pa tudi povečanje števila delovnih nesreč in zastojev sistemskih (proizvodnih) procesov sistemov. Kljub temu da kakovosten sistem organizacije in sistemskega vodenja v delovnem okolju igra pomembno vlogo pri preprečevanju teh nesreč in zastojev, je treba opozoriti tudi na izjemno pomembnost preučevanja in preprečevanja faktorja človeških napak in tehnoloških odpovedi [5].

Z namenom zagotavljanja zanesljivosti in varnosti sistemov so se v šestdesetih letih prejšnjega stoletja začeli razvijati in vse bolj uporabljati postopki varnosti in zanesljivosti v tehnoloških sistemih. Večji preskok pri razvoju teh metod (analiz) in njihove uporabe je bil sredi osemdesetih let, na kar je vplival izredno hiter tehnološki razvoj in pojav večjega števila nezgod, z večjim poudarkom na človeških napakah.

Korenine obravnavanja zanesljivosti so nastajale v različnih industrijah, in sicer v kemični, jedrski, letalski in procesni industriji. Od vseh naštetih najbolj odstopa procesna industrija, ki vsebuje največ možnih in različnih načinov obratovanja. Zaradi raznolikosti opravil v procesni industriji je zato posebej pomemben poudarek na človeški zanesljivosti. Vendar pa procesna industrija ni tako podrobno in natančno regulirana kot jedrska industrija, kajti posledice nesreče v slednji so lahko katastrofalne za širši življenjski prostor [11].

Postopki analize varnosti in zanesljivosti se dandanes uporabljajo v zelo širokem spektru, in sicer za različne dejavnosti, postopke, postrojenja ipd., pri katerih sta varnost in zanesljivost delovanja posebno pomembni. Izkušnje iz prakse kažejo, da delovanje raznih sistemov, ki bi v primeru nezaželenega dogodka imeli večje posledice, ne sme biti prepušeno naključju, ampak je tveganje treba venomer nadzorovati [10].

---

[30] Mariarosa, G., Castiglia, F., Tomarchio, E. A. G., Risk assessment of component failure modes and human errors using a new FMECA approach: Appllication in the safety analysis of HDR brachytherapy, Journal of Radological Protection, 34(4), 891-914, 2014,vir: https://www.researchgate.net/publication/267930872_Risk_assessment_of_component_failure_modes_and_human_errors_using_a_new_FMECA_approach_Application_in_the_safety_analysis_of_HDR_brachytherapy

[31] Mike W. Schmidt, The Use and Misuse of FMEA in Risk Analysis, 1. marec 2004, prispevek na spletni strani https://www.mddionline.com, vir: https://www.mddionline.com/testing/use-and-misuse-fmea-risk-analysis

Kot že pojasnjeno, tveganje neželenega dogodka pri tem predstavlja produkt med verjetnostjo za nastanek dogodka in oceno posledic tega dogodka [23].

Izjemno pomembna je naslednja definicija: Varnost in zanesljivost nekega sistema je v veliki meri odvisna od ravnanja ljudi, ki vodijo neki tehnološki postopek, od organizacije in zanesljivosti tehnike [10]. S povečanjem zanesljivosti se povečuje tudi varnost sistema, z izjemami določenih primerov.

Bistvena težava, s katero se pri načrtovanju sistemov soočamo, je pomanjkanje podatkov o lastnih napakah iz preteklosti. Zapise ali zaznave o takih preteklih napakah označimo s pojmom zgodovinski spomin. Pri odpovedi naprav, o katerih bomo govorili v nadaljevanju, je zgodovinski spomin zagotovljen z vodenjem dnevnikov, spremljanjem odpovedi, z načrtovanjem vzdrževanja. Ta zgodovinski spomin je zagotovljen v bazah podatkov, od koder ga je mogoče enostavno pridobiti. Tam, kjer gre za skupen interes, kot je npr. pri združenjih proizvajalcev, takšne informacije vzdržuje organizacija, v dobro vseh njenih članov.

Pri človeških napakah pa smo z zgodovinskim spominom omejeni. Izkušnje lahko zapišemo v učbenikih, člankih ali knjigah, vendar moramo pri tem upoštevati stigmo, ki se pojavlja pri tistih, ki so takšne napake zagrešili, ali tudi tistih, ki so jih odkrili. Zato je zgodovinski spomin omejen na tiste, ki so bili udeleženi v postopkih. Pogosto je vire najti tudi v sodnih spisih. Človeške napake je zato mnogo težje proučevati, jih pregledovati in se na njih učiti.

Verjetnosti neželenih dogodkov poskušajo zadolžene osebe oceniti in določiti z modeli, različnimi postopki, analizami, tehnikami in predpostavkami. Njihova temeljna naloga je oceniti, ali so posledice neželenega dogodka ali odstopanje od načrtovanega poteka na sprejemljivi ravni, ter ugotoviti, kako takšne dogodke vnaprej preprečiti. Izhodišče za analizo predstavljajo vrednosti pogostosti pojava takšnih dogodkov v preteklosti [18].

Iz statističnih podatkov izhaja, da je verjetnost človeške napake glede na verjetnost tehnične napake manj raziskana in da človeške napake predstavljajo v poprečju kar 80 % vseh nesreč [16]. K že zapisanemu gre dodati, da je verjetnost človeške napake tudi težje kvantitativno določiti kot verjetnost tehnične napake. Človeški organizem je namreč zelo zapleten sistem in zaradi tega je človeške napake mnogo težje predvideti, ocene napak pa so bolj subjektivne.

Pri oceni vplivov človeške napake je treba upoštevati, da na reakcijo operaterja vplivajo njegove lastnosti, usposobljenost in delovne izkušnje, trenutno fizično in psihično stanje, pogoji dela itd., skratka, številni dejavniki, katerih vpliva ni mogoče kvantitativno oceniti na osnovi kemijskih, fizikalnih in matematičnih zakonitosti, kot to lahko storimo pri tehničnih napakah [28].

Pri analizi verjetnosti tehnične napake lahko upoštevamo morebitne posledice različnih nepravilnih dejavnikov, ki so lahko vključeni že v zasnovi (projektiranju) ali konstrukciji, operativnem izvajanju procesa, vzdrževanju itd. Izbira slednjih je prepuščena presojevalcu oz. izvajalcu analize varnosti in zanesljivosti nekega sistema [9].

Univerzitetna založba
Univerze v Mariboru

3 Varnostna analiza sistemov – tehnična odpoved

3.1 Zanesljivost v procesni industriji

Procesna industrija je odvisna od zanesljivosti delovanja naprav. Postavimo se v čevlje tistega, ki odloča o nakupu neke naprave, pomembno za okoljsko varnost, npr. čistilne naprave. Posledice nedelovanja čistilne naprave so lahko hude: od resnih posledic v okolju do širjenja epidemij. Tveganje (ki je, kot že vemo, zmnožek verjetnosti in posledice) je tako veliko.

Strokovnjaki različnih profilov so sestavili več priročnikov za obravnavanje verjetnosti odpovedi posameznih sistemov. Ena od takih knjig je tudi Rdeča knjiga[32]. Avtorji so jo na pot pospremili z naslednjim pojasnilom:

»Delovanje (petro)kemijskih objektov, proizvodnje nafte in plina ter jedrskih elektrarn ni mogoče brez sprejetja določenega tveganja. Tveganje zaradi določene dejavnosti lahko opredelimo kot merilo neželenega dogodka tako glede verjetnosti dogodka kot tudi glede na velikost neželene posledice. Pri ocenjevanju tveganja se opravi ocena velikosti oz. resnosti neželene posledice in verjetnosti nastopa te posledice.

[32] Schüller, J.C.H., Brinkman, J.L., van Gestel, P.J., van Otterloo, R.W., Methods for determining and processing probabilities – »Red book«, The Hague, 1997, vir: https://content.publicatiereeksgevaarlijkestoffen.nl/documents/PGS4/PGS4-1997-v0.1-probabilities.pdf

V preteklosti so bile za oceno tveganja razvite različne vrste analiznih tehnik. Pomembno je razlikovati med tehnikami kvalitativne in kvantitativne varnostne analize. Kvalitativna tehnika temelji na izkušnjah, pridobljenih na določenem področju uporabe. Na podlagi teh izkušenj se lahko oceni sprejemljivost tveganj, povezanih z obratovanjem določenega obrata. Pri kvantitativni oceni tveganja se poizkusi oceniti tveganje v številskih vrednostih, to je velikosti posledice, npr. število žrtev in verjetnost pojava.«

Da bi bilo to mogoče, je treba natančno voditi dnevnike odpovedi in jih (zlasti) deliti, kar je pogosto težko doseči. V Rdeči knjigi tako avtorji prikažejo primere transformacije podatkov v takšne, ki jih je mogoče med seboj primerjati. Gre za podatke odpovedi dizelskih generatorjev v termoelektrarnah.

Tabela 6.6: Rezultati zbirk podatkov za določene elektrarne

Elektrarna	Moč dizel generatorjev (kVA)	Število zahtev	Število neuspehov
A	600	520	1
B	1000	653	2
C	200	408	1
D	200	408	9
E	2500	199	2
F	100	943	16

Slika 8: Primer podatkov iz Rdeče knjige

Tabela 6.7: Povprečje, spodnja meja, zgornja meja

Elektr.	Število zahtev	Število neuspehov	Povprečje (1/d)	Spodnja meja (5%)	Zgornja meja (95%)	Faktor napake
A	520	1	1.9E-03	9.9E-05	9.1E-03	9.6
B	653	2	3.1E-03	5.41E-04	9.61E-03	4.2
C	408	1	2.5E-03	1.3E-04	1.2E-02	9.6
D	408	9	2.2E-02	1.2E-02	3.8E-02	1.8
E	199	2	1.0E-02	1.8E-03	3.1E-02	4.2
F	943	16	1.7E-02	1.1E-02	2.6E-02	1.6

Slika 9: Primer obdelanih podatkov iz Rdeče knjige

Na sliki 9 je povprečje aritmetično povprečje dostopnih podatkov, (1/d) pomeni pogostost odpovedi na dan, za razliko od podatkov na sliki 8, kjer so bili podani podatki o verjetnosti odpovedi v enem letu.

Kljub temu da rezultati iz prve tabele na prvi pogled precej nihajo, pa so v drugi tabeli rezultati razporejeni v dve ločeni skupini, ena za elektrarne A, B in C, in druga za D, E in F. V resnici je videti, kot da prihajajo generatorji iz dveh povsem različnih virov. Pri tem je faktor napake v zgornji tabeli razmerje med zgornjo mejo in povprečjem ali povprečjem in spodnjo mejo.

Čistilne naprave so drage. Tisti, ki bo odločal o nakupu, bo odgovoren tako za učinkovitost kot tudi za zanesljivost delovanja. Čistilna naprava je le ena od naprav, ki jih najdemo v okoljski tehniki, prav vse pa morajo zagotavljati zadostno mero donosnosti tistemu, ki vanje vlaga.

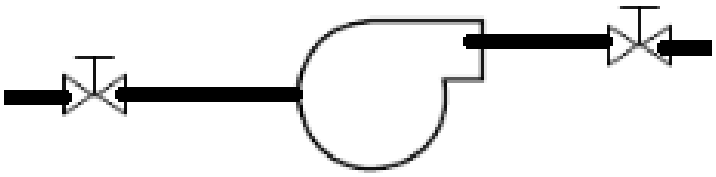
Najučinkovitejši način zagotavljanja donosnosti kateregakoli industrijskega sistema dosežemo z zmanjšanjem števila odpovedi njegovega delovanja, z zmanjševanjem števila neplaniranih motenj ali pa z zmanjševanjem potrebnega časa nekega načrtovanega (npr. proizvodnega) ciklusa. Dandanes je v uporabi kar nekaj metod upravljanja s tveganji (RM[33]), ki poleg izboljšanja varnosti pripomorejo k izboljšanju zanesljivosti delovanja nekega sistema [9].

Zmanjšano število odpovedi sistema generalno vpliva na:

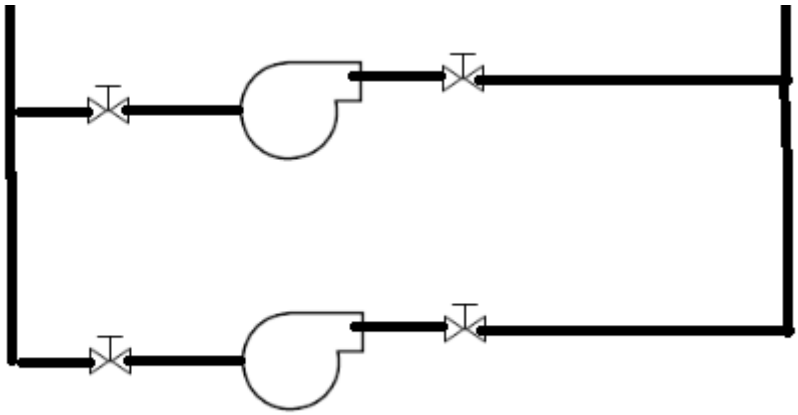
- povečanje produkcije,
- povečanje delovne storilnosti,
- zmanjšanje števila odpovedi delovanja (zmanjšanje stroškov vzdrževanja),
- redno spremljanje delovanja (baza morebitnih napak),
- izboljšano varnost,
- zmanjševanje nevarnosti vpliva na okolje.

Posamezne vplive bomo pojasnili na osnovi črpalke na sliki 1.

[33] RM – upravljanje s tveganji (angl. *Risk Management*)



Slika 10: Črpalka



Slika 11: Redundanca črpalk

Takšne črpalke najdemo seveda tudi v čistilnih napravah. Predpostavimo, da gre za črpalko, namenjeno črpanju vode, obremenjene z odpadnimi snovmi.

Povečanje neželene posledice je direktna posledica odpovedi. Pogosto okvarjena črpalka ne bo opravljala svoje funkcije. Kljub redundanci se bodo lahko pojavljali izpadi delovanja čistilne naprave, če se bo okvarila tudi druga črpalka. Hkrati pa drži, da se bo verjetnost odpovedi z redundanco bistveno zmanjšala, in to na kvadrat verjetnosti odpovedi ene same črpalke.

Uvedli smo nov izraz: redundanca. Redundanca je poslovenjen izraz, gre za podvojenost ali večkratnost. Uporabimo ga, kadar se težavam pri izpadu procesa ali dela procesa izognemo tako, da ta proces ali del procesa podvojimo. Namesto ene črpalke bi lahko npr. na sliki 10 izvedli dve, vzporedni (slika 11). Eno uporabimo, ko druga odpove, ko moramo drugo popraviti, če jo zamenjamo z novo, zmogljivejšo, ipd. Namesto dveh naprav lahko uporabimo tri, pri čemer dve delujeta, ena pa je v rezervi. Tako ravnamo, kadar imamo opravka bodisi z visoko verjetnostjo odpovedi bodisi z velikimi posledicami. V nuklearnih elektrarnah so npr. v primeru nezgod nujno potrebni viri električne energije. To so lahko

akumulatorji ali generatorji. Generatorji so običajno gnani z dizelskimi motorji, ki pa lahko odpovedo – ker ni zadosti goriva ali ker kateri od sistemov ne deluje. Zato jih običajno postavimo več, odvisno od stopnje varnosti, ki jo želimo doseči. Ne gre prezreti, da je bila ena od najhujših nesreč (Fukushima Daiichi) prav posledica nepravilne postavitve sicer redundantnih generatorjev.

Pred začetkom izvedbe varnostne analize je treba ponoviti izraze, kot sta zanesljivost in razpoložljivost, ter morda dodati še učinkovitost in sposobnost vzdrževanja [23]:

- učinkovitost (angl. *effectiveness*) → stopnja (merilo) doseganja, npr. število proizvedenih produktov v daljšem časovnem obdobju (npr. v 1. letu);
- sposobnost vzdrževanja (angl. *maintainability*) → stopnja delovanja sistema brez prekinitev oz. napak v daljšem časovnem obdobju.

S temi izrazi se tudi sicer pogosto srečujemo. V letu 2020 smo se npr. soočali z izrazom »učinkovitost cepiva«. Pri tem moramo pojasniti, da gre v vseh teh primerih za stopnje, ki so lahko izražene kvalitativno ali bolje, kvantitativno. V tehniki težimo h kvantitativnim vrednostim, ker je tako primerjava olajšana.

Kvantitativne vrednosti so včasih zavajajoče. V tehniki smo navajeni delovati v okviru štirih relevantnih števk, tj. štirih števk neupoštevaje leve ničle, npr. 0,01234 ali 12,34. Tak sistem je za ocenjevanje tveganja neprimeren. Zadošča ena ali morda dve števki.

Mogoče je, da se pri ocenjevanju tveganja lahko zgodi lažen občutek natančnosti. Ne smemo pozabiti, da so naše številke točne toliko, kolikor so zanesljive, zanesljive pa so toliko, kolikor so zasnovane na zanesljivih podatkih. Če je v ozadju podatkov groba ocena, potem tudi po še tako zapleteni računski operaciji rezultat ne bo bolj natančen od vira, čeprav ga bomo zapisali s štirimi relevantnimi števkami.

Varnost sistemov je v neposredni povezavi s področjem upravljanja s tveganji (angl. *Risk Management, RM*). Tveganje v tem primeru predstavlja kakršnokoli izgubo [23].

Določitev tveganja je običajno proces, sestavljen iz naslednjih štirih delov:

1. identifikacija nevarnosti kot najpomembnejši korak,
2. identifikacija verjetnosti pojava (nevarnosti) in vzrokov,
3. določitev posledic pojava (če bi se ta pojavila),
4. izračun tveganja.

Področje upravljanja s tveganji je široko zastopano v procesni industriji z namenom izboljševanja varnosti sistemov. Z rahlo modifikacijo trifaznega procesa določitve tveganja to področje vpliva tudi na izboljšanje varnosti. Največja razlika med področjem varnosti in področjem upravljanja s tveganji je v tem, da se prvo ne nanaša na obravnavo malo verjetnih napak, ampak daje večji poudarek merljivosti in optimizaciji nekega sistema [24].

3.2 Identificiranje sistemskih nevarnosti

Prvi korak v varnostni analizi predstavlja identificiranje tveganj, pri čemer se izraz tveganje nanaša na kakršnokoli izgubo [21]. Izdelava drevesa odpovedi praviloma poteka od ponora do izvora[34]. V našem obravnavanem primeru, prikazanem na sliki 1, to pomeni, da se bomo najprej vprašali, ali smo dobili zmes Z1. Če zmesi Z1 ne dobimo, moramo slediti poti nezgode navzgor, do izvira.

Pri tem obstajata naslednja dva načina identificiranja tveganj:

1. uporaba kontrolnih listov, znanih kriterijev in predpisov (standardov),
2. bolj ustvarjalen postopek: identificiranje izredne napake pri pregledu sistema.

Tehnike identificiranja tveganj so običajno kvalitativne narave.

Uporaba kontrolnih listov je povezana z rutinskimi pregledi. Gotovo smo kdaj opazili pilote, ki se s podlago v roki gibajo okoli letala in potrjujejo kontrolne točke pregleda. Ne gre zato, da piloti ali mehaniki ne bi vedeli na pamet, kaj je treba pregledati, gre za to, da se tako izognejo temu, da bi katero od kontrolnih točk pozabili pregledati. Ti pregledi so posledica številnih nesreč v preteklosti in jih je treba tako tudi obravnavati. Podobno je v nuklearnih elektrarnah. Operaterji nuklearnih elektrarn sledijo točno določenim protokolom za vsako spremembo in nadzor v delovanju le-teh, vsemu pa sledijo na osnovi pisnih (ali računališko zapisanih) diagramov.

Ko imamo pripravljene kontrolne liste, ob upoštevanju kriterijev in standardov, sledi naslednji korak identifikacije tveganj, tj. razvoj scenarija, ki privede do sistemske napake (odpovedi) [9].

[34] »sink to source«, Nicholay Melly, Module 1: Internal Event, At-Power Probabilistic Risk Assessment Model for SNPP, NUREG/CR-6850 FIRE PRA Methodology, FIRE PRA Workshop, 24. junij 2019–28. junij 2019, Rockviller, vir: https://www.nrc.gov/docs/ML1916/ML19162A415.pdf, tudi [31].

Poznanih je mnogo metod identifikacije tveganj, pri čemer navajamo le nekatere, bolj znane [23, 24]:

Postopek tveganja in obratovanja (HAZOP)

Izraz HAZOP[35] izhaja iz skovanke štirih angleških besed – Hazard and Operability Study. Enak izraz se široko uporablja tudi v slovenskem jeziku in ga zato nima smisla prevajati. Ni vezan le na tehnična vprašanja, še pogosteje ga je najti v analizah varne priprave hrane ali v medicinskih aplikacijah.

Postopek izhaja iz sedemdesetih let prejšnjega stoletja. Postopek HAZOP se lahko izvede tako v fazi pred gradnjo sistema kot tudi, ko sistem že obratuje. Postopek izvaja skupina strokovnjakov, ki dobro poznajo sistem in ki podrobno pregledajo vsak vod in vsak del opreme s tehniko ključnih besed (angl. *guidewords*) in odstopanja od le-teh. Delno izhaja iz kratice OP, to pomeni, da lahko ta postopek uporabimo tudi za izboljšanje obratovanja sistema.

Postopek na področju tehnike poteka tako, da skupina strokovnjakov postopek najprej razčleni na posamezne elemente, da torej pripravi tokovni diagram postopka. V tokovnem diagramu postopka, ki je predmet analize, so seveda označene tudi naprave, ki so lahko vir odpovedi. Skupina strokovnjakov nato sledi tokovnemu diagramu in ob vsakem elementu odgovori na vprašanje glede kriterijev uspeha. Razčlenitvi sledi določitev parametra uspeha, temu sledijo pregled s ključno besedo, odstopanje od le-te, ugotovitev morebitnih vzrokov in morebitnih posledic ter določitev potrebnega ravnanja in odgovornega za izvedbo ravnanja.

V našem primeru (slika 1) bi tako skupina strokovnjakov postavila tokovni diagram, ki sledi sliki 1. Ko bi skupina npr. obravnavala črpalko, bi si postavila vprašanje glede obratovanja ventila V1, črpalke P1 in ventila V2. Oba ventila sta sicer povsem ločena (tehnično, pa tudi v kontekstu varnosti in zanesljivosti) od P1, a P1 brez njiju ni mogoče obravnavati, saj je njun obstoj (tehnično) nujen za varno obratovanje P1. Če kateri od ventilov ne deluje, P1 ni mogoče zamenjati. Torej, skupina strokovnjakov bi pregledala V1, P1 in V2 glede na vnaprej znane kriterije zunanjega (ali tudi bolj podrobnega) pregleda – ali elementi obratujejo, ali se zatikajo, kakšne so znane pretekle odpovedi in na osnovi

[35] Kletz, T.A., Hazop—past and future, Reliability Engineering & System Safety, Volume 55, Issue 3, March 1997, Pages 263–266.

tega bi skupina odgovorila na vprašanje, ali po njenem mnenju V1, P1 in V2 ustrezajo standardom in kriterijem za varno delovanje sistema.

Tako bi skupina strokovnjakov nadaljevala po posameznih elementih, dokler ne bi obravnavala celotnega sistema, skladno s ključnimi besedami. Kadar skupina naleti na odstopanje, se mora opredeliti do vzrokov in posledic ter v primeru zadostnega vpliva na varnost tudi opraviti posamezno varnostno analizo novega stanja. Takšne ključne besede so npr. »NE« (če sistem ne ustreza projektnim pogojem), »TAKO DOBRO KOT«, »OBRATNO«, »PREJ«, »POTEM« in podobno.

Kot vidimo, se postopek lahko uporablja pri sistemih, kjer je na voljo zadosti informacij in so kriteriji uspeha zadosti dobro določeni. Prav tako so sistemi, ki so predmet HAZOP, takšni, ki se sčasoma ne spreminjajo bistveno. Po zaključku postopka HAZOP je sistem utrjen v delujoči različici in ga je ob spremembi te različice treba znova pregledati.

Za obravnavani sistem je značilno, da v njem ni prav veliko kreativnosti in razmišljanja, pač pa obilo potrebe po zelo dobrem poznavanju delovanja procesa, ki je predmet analize HAZOP.

Postopek analize slojev zaščite (LOPA)

LOPA[36] je metodologija ocene tveganja, ki uporablja poenostavljena, konzervativna pravila za opredelitev tveganja kot pogostosti in resnosti posledic. LOPA je opredeljena kot poenostavljena ocena tveganja v smislu en vzrok – ena posledica.

Konceptualno se LOPA uporablja za razumevanje, kako lahko odstopanje procesa vodi do nevarnih posledic, če ga ne prekine uspešno delovanje zaščitnega sredstva, imenovanega neodvisna zaščitna plast (IPL). IPL je zaščitni ukrep, ki lahko prepreči, da bi se scenarij razširil do zaskrbljujoče posledice, ne da bi nanj negativno vplival bodisi začetni dogodek bodisi dejanje (ali neukrepanje) katere koli druge zaščitne plasti v istem scenariju.

LOPA obsega osem slojev; to so:

1. sloj: načrtovanje postopka, npr. po naravi varnejši modeli,
2. sloj: osnovni nadzor, alarmi procesov in nadzor operaterja,

[36] Willey, R.J., Layer of Protection Analysis, December 2014, Procedia Engineering 84, vir: https://www.researchgate.net/publication/268527070_Layer_of_Protection_Analysis

3. sloj: kritični alarmi, nadzor operaterja in ročni poseg,
4. sloj : samodejno delovanje, npr. SIS – varnostni instrumentiran sistem (angl. *Safety Instrumented System*) ali ESD – zasilna zaustavitev (angl. *Emergency Shut Down*),
5. sloj: fizična zaščita, npr. naprave za razbremenitev,
6. sloj: fizična zaščita, npr. nasipi,
7. sloj: odziv na nujne primere v obratu,
8. sloj: odziv skupnosti na izredne razmere.

Postopek LOPA je moč predstaviti tudi matematično, in sicer se frekvenca začetnega dogodka pomnoži z verjetnostmi, da bo vsak neodvisni sloj zaščite prenehal izvajati svojo funkcijo.

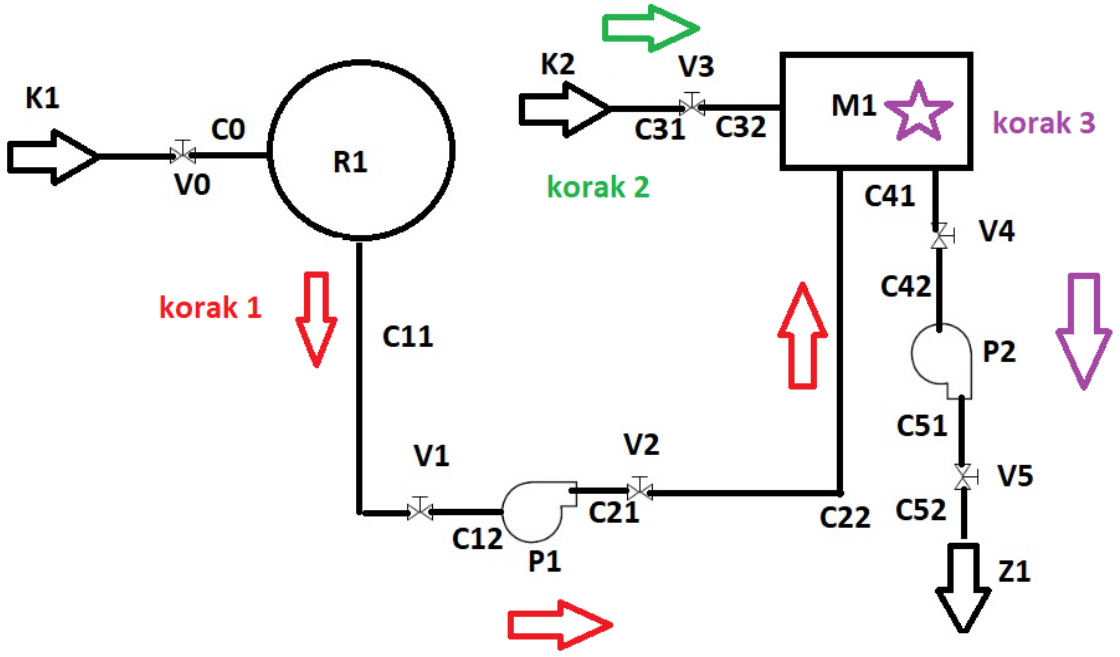
Postopek korak za korakom

Postopek korak za korakom (angl. *step-by-step*) se uporablja v sistemih, pri delovnih operacijah, kjer se pogoji s časom spreminjajo. Te operacije predstavljajo kritični element pri izboljševanju varnosti. Postopek je podoben postopku HAZOP in se uporablja pri večjih sistemih.

Pomembno je razumeti, da tu ne gre za različna stanja kot posledico odpovedi, temveč za različna stanja znotraj normalnega obratovanja.

Kot pri postopku HAZOP tudi pri tem postopku pregled opravlja skupina strokovnjakov. Sledi podobnemu vzorcu kot pri sistemu HAZOP, le da je treba obravnavati različne scenarije, saj lahko časovno spremenljiv proces vedno znova spremeni procesne parametre.

Pri zgoraj opisanem procesu, na sliki 1, bi tako lahko analizo korak za korakom opravili, če bi šlo za šaržni, in ne kontinuirani proces. Kontinuirani proces namreč predpostavlja eno, bolj ali manj statično konfiguracijo – kapljevina 1 teče iz rezervoarja skozi ocevje v mešalno posodo, kjer se meša s kapljevino 2, in nato zmes zapusti sistem.



Slika 12: Prikaz treh korakov šaržnega postopka

Šaržni postopek bi lahko potekal takole: kapljevina 1 najprej napolni R1, nato izteka skozi ocevje v M1. Nato sledi drugi korak: kapljevina 2 napolni M1. V tretjem koraku se v M1 kapljevini 1 in 2 zmešata in nato zmes odteče.

Naprave so torej enake kot pri kontinuiranem postopku, vendar imajo naprave (ali z eno besedo: postrojenje) tri ločena stanja, gre za tri ločene korake.

V koraku 1 je npr. vseeno, ali ventil V5 deluje ali ne. V koraku 3 je stanje R1 nepomembno.

Treba je torej opraviti tri ločene analize HAZOP, in to sledeč posameznemu koraku. Vsak predhodni korak lahko ima posledice za kasnejši korak in tudi to je treba obravnavati v kontekstu ključnih besed HAZOP.

Vprašanje časovne spremembe postopkov je seveda lahko zavajajoče. Ko je korak utrjen, se sistem ne sme bistveno spreminjati. Če bi uporabili izrazoslovje, poznano iz prenosa toplote, bi lahko rekli, da je sistem »kvazistacionaren«, torej, da gre za sosledje sicer stacionarnih stanj, ki pa se skozi čas spreminja.

Tehnika »Kaj, če«

Tehnika »Kaj, če« (angl. *What if*) je uporabna pri zelo majhnih sistemih ali pri delih sistemov. Z njo se hitreje identificira tveganje kot npr. s postopkom HAZOP.

Tehnika »Kaj, če« od ocenjevalca zahteva precejšno mero domišljije za razliko od postopka HAZOP, ki zahteva rigorozno sledenje morebitnim točkam obratovanja in odgovor, ali je kriterij uspeha izpolnjen ali ne in če ni, zakaj ni in kakšna bo posledica. Ta tehnika zato predpostavlja, da pozna ocenjevalec sistem do te mere, da je zmožen predvideti odziv kompleksnega stanja.

V splošnem analiza »Kaj, če« identificira nevarnost ali položaje, ki bi utegnili voditi v neželena stanja. Rezultat teh stanj so neželene posledice, bodisi za sistem bodisi za rezultat postopka bodisi za okolico. Ocenjevalec kot rezultat prepozna stanja, ki vodijo v neželene posledice kot tudi nabor teh neželenih posledic. Če je zadosti izkušen, bo ocenjevalec lahko predstavil tudi ravnanja, ki bodo škodljive posledice preprečile ali odpravile posledice, pa tudi ravnanja, ki bodo preprečila, da bi postopek zašel v stanje nevarnosti ali položaj, ki bi utegnil voditi v nevarnost.

Ocenjevalec postavi vprašanje, kaj bi se zgodilo ob morebitni odpovedi posameznega elementa, z vidika končnega rezultata postopka, npr. kaj če R1 odpove npr. tako, da je stena porušena. V takem primeru bo seveda rezultat ta, da ne bo zmesi Z1, prav tako pa bo tudi posledica za okolje. Kaj pa, če odpove elektromotor črpalke P1? V tem primeru sicer ne bo (nujno) posledic za okolje, ne bo pa zmesi Z1, torej kriterij uspeha ostane neizpolnjen.

Seveda je tudi v teh primerih mogoče postaviti formalno strukturo, ki jo ocenjevalec upošteva, da identificira nevarnost.

Najprej ocenjevalec identificira postopek ali stanje ter določi zahteve, ki so potrebne za ocenjevanje (kriterij uspeha, neželena stanja). Najbolje je, če tudi v tem primeru ocenjevalec takšno identifikacijo opravi na osnovi tokovnega diagrama, saj ta identificira tako postopek kot tudi posamezne naprave, potrebne za delovanje. Nato ocenjevalec prouči stanja postopka, ki so neželena ali bi utegnila postati neželena. Zatem ocenjevalec na osnovi vprašanj »Kaj, če« razvije analizo nevarnosti, pri čemer lahko opravi tudi rangiranje neželenih stanj. Ne gre prezreti, da gre tu za enostavnejše načine ocenjevanja in za iskanje hitrih rezultatov, kot posledica tega pa bo ocenjevalec zanemaril nekatera od

stanj. Iz nabora tako dobljenih rangiranih stanj lahko ocenjevalec izbere nekaj stanj, ki bi jih veljalo posebej ovrednotiti.

Ta izbrana stanja za posebno ovrednotenje nato ocenjevalec oceni glede na nevarnosti. Lahko se odloči, da bo ostal pri kvalitativni analizi. Lahko se odloči za katero od dosegljivih kvantitativnih analiz.

V vsakem primeru ocenjevalec analizo »Kaj, če« zaključi s predlogi, kako preprečiti neželena stanja ali stanja, ki lahko postanejo neželena, in kako omejiti ali odpraviti posledice teh stanj.

Analiza načinov odpovedi in posledic (FMEA[37])

FMEA je postopek, ki se deli v dva ločena podpostopka:

- ugotovitev načina odpovedi in
- analiza posledic odpovedi.

Postopek se je razvil v letalski industriji, zlasti kot odziv na vojaške potrebe. Pri načinih odpovedi je treba analizirati načine, ki vodijo v odpoved posameznega sistema. Pri našem obravnavanem primeru je želeni rezultat dobava zmesi Z1. Ocenjevalec se mora zato vprašati, kateri so načini, ki bi vodili v preprečitev tega želenega stanja.

Postopek FMEA sledi, podobno kot drugi postopki, formalnim korakom, ki jih je mogoče zapisovati oziroma spremljati tudi po opravljeni analizi, pri čemer so zlasti vidne korenine postopka v letalski industriji.

Postopek se začne s sestavo skupine strokovnjakov, ki ima zadostno znanje o postopku, predmetu analize. Pri tem je treba poskrbeti za prekrivanje poznavanja ali pa za komplementarno poznavanje postopka, kar pomeni, da vsak od članov skupine pozna del postopka, pri čemer se morajo ekspertize vsaj deloma prekrivati, da je mogoča navzkrižna kontrola. Nato je treba identificirati obseg analize FMEA, zlasti globino oziroma nivoje rezultatov. Gre za vprašanje, ali se bomo zadovoljili z ugotovitvijo načina odpovedi in analize ali pa bomo te načine tudi obdelali z vidika ranljivosti ali možnosti odprave napak.

[37] FMEA (angl. *Failure modes and effects analysis*), vir: https://asq.org/quality-resources/fmea

Ko določimo obseg, je treba začeti izpolnjevati protokol FMEA, narejen za posamezni postopek. Primer protokola je v spodnji tabeli, pri čemer smo uporabili šaržni način, obravnavamo pa korak 3.

Tabela 2: Primer protokola FMEA

Opis sistema: mešalna komora, korak 3
Način delovanja: šaržni

Oznaka	Opis naprave	Funkcija	Št.	Način odpovedi	Učinek	Posledični učinek	Končni učinek	Stopnja posledice	Način detekcije	Odprava
P1	črpalka 1	zagotovitev toka v koraku 1	1	ne deluje	ni toka	ni učinka	ni učinka	IV	ni detekcije	popravilo
			2	deluje brez signala	zviša tlak v sistemu	porušitev tesnila v črpalki	razlitje v okolico	I	porast tlaka v črpalki	prenehanje obratovanja
V1	ventil 1	preprečitev vtoka v črpalko 1	1	zataknjen – zaprt	ne omogoča pretoka	ni učinka	ni učinka	IV	ni zaznan	remont ventila
			2	zataknjen – odprt	omogoča zvišanje tlaka	omogoča porušitev tesnila	razlitje v okolico	I	porast tlaka, če P1 odpove	remont ventila

Pri tem smo stopnjo posledice razdelili od I – izjemno pomembno prek II – pomembno, III – vredno opazke do IV – zaenkrat nepomembno.

Ugotovili smo, da v koraku 3 delovanje črpalke 1 ni pomembno, zato njeno nedelovanje (način odpovedi 1) ni pomembno. Lahko pa se zaradi neželenega delovanja ob sicer zaprtem ventilu V2 pojavita porast tlaka v sistemu črpalke in posledično obremenitev tesnila črpalke. Le-ta lahko (ker ni padca tlaka oziroma je padec tlaka prek tesnila) zaide v situacijo, da popusti. V tem primeru bo se kapljevine 1 izlila v okolico, kar želimo preprečiti. Drug način odpovedi je odpoved ventila 1. Tu sta možna dva načina odpovedi – ventil se lahko zatakne v položaju odprto ali v položaju zaprto. Če se zatakne v položaju odprto, potem bo kapljevina 1 imela prost vtok v črpalko 1 in če se bo pokvarila tako, da bo delovala navkljub signalu, da naj ne deluje, bodo posledice lahko podobne kot v primeru neželenega delovanja črpalke 1. Če bo ventil zataknjen v položaju zaprto, pa posebne posledice ne bo.

Detekcija posameznega stanja je zelo pomemben element. Ob tem gre spomniti na nezgodo v nuklearni elektrarni na Otoku treh milj, kjer operaterji niso zaznali praznjenja primarnega sistema prav zaradi nezadostne opremljenosti sistema oziroma nesposobnosti detekcije puščanja skozi prelivni vod.

V konkretnem primeru bo mogoča detekcija posameznega stanja samo, če bo šlo za delovanje in zvišanje tlaka v sistemu, torej, da bo črpalka 1 delovala, čeprav ne bi smela, oziroma da bo hkrati odprt ventil 1. V obeh primerih bo viden porast tlaka v ocevju pred ventilom V2.

Postopek predvideva tudi ravnanja, ki bodo vodila v preprečevanje posledic oziroma odpravo le-teh, v konkretnem primeru zamenjavo tesnila črpalke in remont ventila oziroma odpravo napake, zaradi katere je ventil ostal zataknjen v odprtem položaju.

Postopek torej raziskuje način odpovedi posameznega glavnega dela sistema in ugotavlja posledice le-tega – kako bo ta odpoved učinkovala glede na celoten sistem.

Kvalitativno drevo odpovedi (QFT[38])

Kvalitativno drevo odpovedi je eno od dreves odpovedi. Drevo odpovedi je logični diagram poteka, ki pokaže kombinacije dogodkov pred nastopom nesreče oz. napake v sistemu. Drevo odpovedi je zlasti namenjeno odločanju (angl. *decisionmaking*)[39].

Drevo odpovedi obravnava neželeno stanje. V spodnjem primeru je neželeno stanje, da kapljevina K1 ne teče. Takemu neželenemu stanju pravimo tudi glavni dogodek.

Podobno kot v prejšnjih primerih je tudi tu osnova za analizo poteka tokovni diagram, ki pojasnjuje redosled posameznih postopkov. Pogosto se namreč zgodi, da je fizična upodobitev poteka postopka podobna ali celo enaka logičnemu postopku.

To seveda ni nujno res. Kot primer postavimo fizično in logično zaporedje toka vode skozi kotel. V kotlu je logično zaporedje dogodkov gretje vode, nato uparjanje in nato pregretje, pri čemer je z vidika termodinamike najbolj logično, da dimni plini sevalno pregrejejo paro, nato ohlajeni dimni plini konvektivno uparijo kapljevino in nato še bolj ohlajeni dimni plini ogrejejo vodo. Vendar fizični potek ne sledi temu logičnemu poteku, saj bi se zaradi visoke temperature dimnih plinov lahko pojavil prežig stene kotlovskih cevi, v posledici česar dimni plini najprej sevalno uparjajo, nato konvektivno pregrevajo in končno grejejo vodo.

[38] QFT – Qualitatie fault tree: Lundteigen M.A., Rausand M, Chapter 5. Fault Tree Analysis (FTA), RAMS Group, NTNU – Trondheim, vir: https://www.ntnu.edu/documents/624876/1277046207/SIS+book+-+chapter+05+-+Introduction+to+fault+trees/fa8ba01a-3baf-4bb8-94ed-116bf5bc6b44

[39] Vesely, W.E., *et al.* Fault Tree Handbook, NUREG-0492, U.S. Nuclear Rgeulatory Commission, 1981, vir: https://www.nrc.gov/docs/ML1007/ML100780465.pdf

Za postavitev drevesa odpovedi je tako potrebna fizična, in ne logična razporeditev postopkov. Drevo odpovedi sledi od vrhnjega dogodka do osnovnega dogodka. Pri tem je treba definirati naslednje pojme:

- glavni dogodek je opis nezgode v sistemu (recimo odpoved dizelskega generatorja),
- osnovni dogodki so dogodki, ki so najnižje na hierarhiji identificiranih vzrokov,
- logična vrata, kot so vrata ALI in IN, ki postavijo logično sosledje med glavnim dogodkom in osnovnimi dogodki.

Drevo odpovedi je mogoče analizirati kvalitativno ali kvantitativno, v tem delu se bomo pogovorili o kvalitativni analizi.

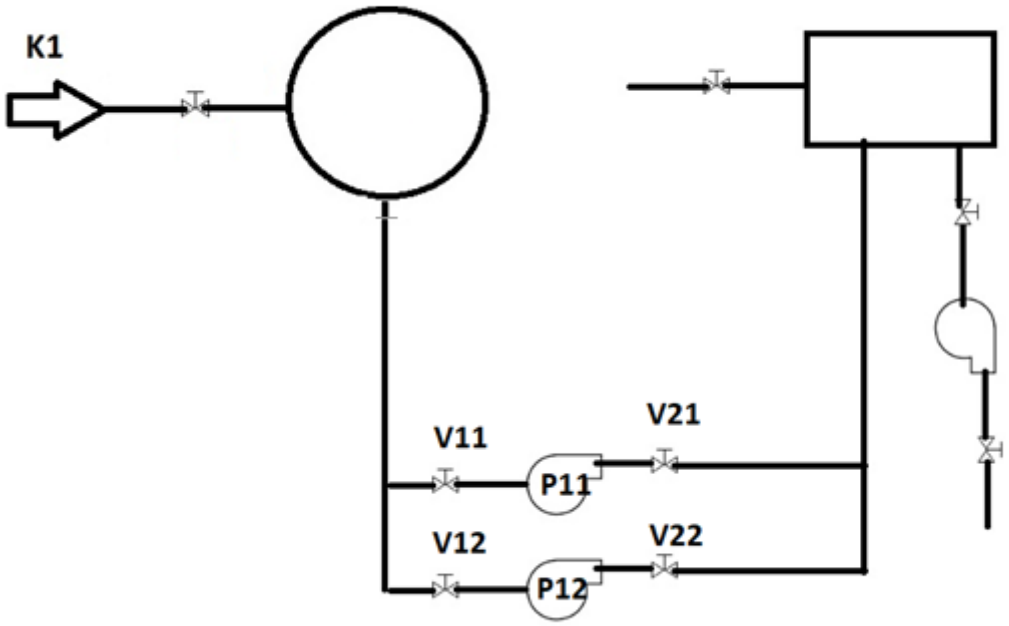
Drevo odpovedi je pogosto izpeljano z naslednjimi koraki:

- določitev problema, sistema in robnih pogojev analize,
- izdelava drevesa odpovedi,
- identifikacija minimalne poti odpovedi (angl. *cut set*);
- kvalitativna analiza drevesa odpovedi,
- kvantitativna analiza drevesa odpovedi.

Nezgodna množica je množica osnovnih dogodkov, ki so potrebni, da se pojavi vrhnji dogodek. Načeloma so v drevesu odpovedi v množici osnovnih dogodkov vsi osnovni dogodki. Minimalna pot odpovedi pa je tista množica, ki še pripelje do vrhnjega dogodka; posledica znižanja števila osnovnih dogodkov bi bila, da se vrhnji dogodek sploh ne bi pojavil.

V konkretnem primeru želimo ugotoviti pojavnost vrhnjega dogodka, tj. dogodka, pri katerem kapljevina K1 ne bo tekla. Pot odpovedi v tem primeru je nedelovanje ventila V11, nedelovanje črpalke P11, nedelovanje ventila V12 in nedelovanje črpalke P12. Kot bo vidno v nadaljevanju, je minimalna pot odpovedi bodisi nedelovanje črpalke P11 in nedelovanje ventila V11 bodisi nedelovanje črpalke P11 in nedelovanje ventila V12. Obstajata torej dve minimalni poti odpovedi.

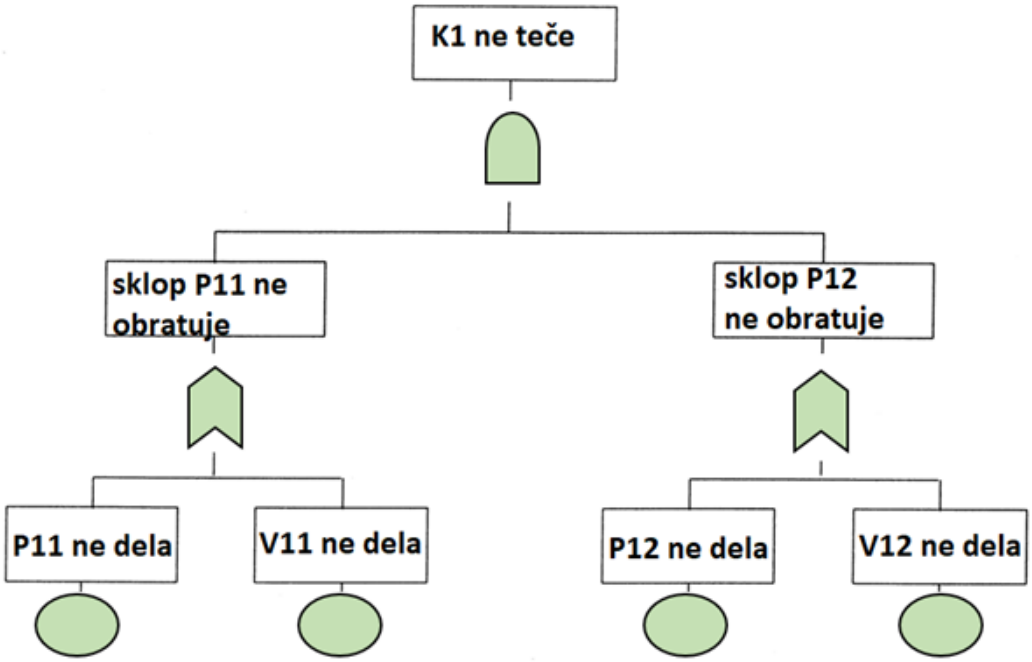
Na sliki 13 je prikazana različica sistema, ki ga analiziramo.



Slika 13: Sistem z redundantnimi črpalkami

Ko je logična kombinacija razvita, lahko drevo uporabimo za kalkulacijo verjetnosti odpovedi sistema. Razvoj drevesa odpovedi je sestavljen iz dve korakov: (1) razvoj logike sistema in (2) merljivosti (kvantifikacije). Celotni postopek drevesa odpovedi je podrobneje opisan v nadaljevanju. QFT-postopek se razlikuje od postopka »line-by-line« v tem, da se sistem analizira gleda na funkcije. Uporablja se predvsem pri manjših sistemih, ki nimajo točno definiranih procesnih poti delovanja.

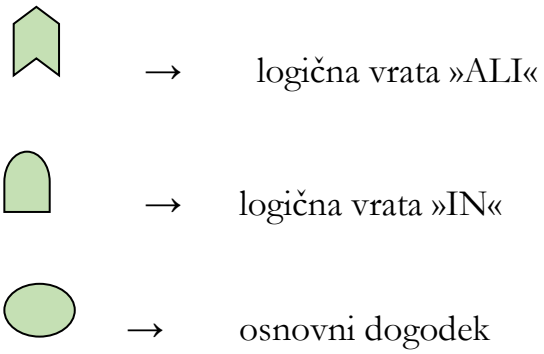
Na sliki 14 je prikazano kvalitativno drevo odpovedi za sliko 13:



Slika 14: Prikaz QFT

Več o drevesu odpovedi bo prikazano v delu, ki se nanaša na kvantitativno analizo dreves odpovedi, zaenkrat pa prikažemo le kvalitativno drevo odpovedi.

V tem drevesu so prikazana naslednja logična vrata



Na sliki 13 smo uvedli redundantni črpalki.

QFT slike 13 deluje na naslednji način: glavni dogodek je prenehanje toka kapljevine 1 (K1). To se seveda lahko zgodi na več načinov, prikazan pa je način, pri katerem preneha tok v eni ali obeh sklopih redundantnih črpalk (P11, P12). O sklopu govorimo zato, ker je za delovanje potrebno delovanje tako črpalke kot ventilov. Kljub temu da je potrebno delovanje obeh ventilov, za prikaz prikažemo le enega od obeh.

Kapljevina K1 ne bo tekla, če ne deluje sklop črpalke P11 in hkrati sklop črpalke P12. Če bo katerikoli od sklopov deloval, bo kapljevina K1 tekla, saj gre za redundantne sisteme. Posamezni sklop ne bo deloval, če ne bo delovala bodisi črpalka bodisi ventil. Delovanje obojega, črpalke in ventila v posameznem sklopu, je potrebno za delovanje sistema.

Za zagotavljanje varnosti je ta korak identifikacije tveganj običajno dovolj (ni treba kvantitativno določevati rezultata). Ravno nasprotno pa je pri analizi tveganja, saj je tam običajno treba kvantitativno določevati rezultat [23].

Prav bi bilo, če bi se nekoliko posvetili tudi odpovedim s skupnim vzrokom. Drevo odpovedi bo delovalo samo, če gre za neodvisne odpovedi. Odpoved s skupnim vzrokom pa je odvisna od skupnega vzroka. Kot primer lahko navedemo istega vzdrževalca, ki vzdržuje sicer več neodvisnih sistemov, vendar med vzdrževanjem npr. ni zbran in postane to skupni vzrok. Druga možnost je uporaba sistemov, ki jih izdeluje isti proizvajalec in imajo vgrajene enake komponente.

3.3 Merljivost (kvantifikacija)

Za analizo sistemov so kvalitativni postopki pogosto zadovoljivi. Vendar pa imamo v tehniki radi primerjave, te pa so mogoče samo na osnovi enakovrstnih dogodkov oziroma kriterija, ki ga je mogoče primerjati. Tak kriterij smo že vpeljali, gre za verjetnost posameznega dogodka, merimo ga jo v številu na leto.

Kvantifikacijo lahko dosežemo z bolj ali manj kompleksnimi postopki. Najprej bomo pregledali bolj enostavne, tem bodo sledili kompleksnejši.

Med enostavnejše, a uporabne postopke kvantifikacije tveganj spadajo:

- Paretovo pravilo (angl. *Pareto Principle*),
- resničnostne tabele (angl. *truth tables*),
- tabele učinkovitosti (angl. *effectiveness tables*).

Uporaba teh enostavnih postopkov je primerna takrat, kadar potrebujemo grobo oceno razmerja napak ali kadar imamo pomanjkanje zanesljivih podatkov. S temi postopki na hiter način ugotovimo vrednost sistemskega tveganja, služijo nam kot osnova za bolj prefinjene tehnike, kot sta drevo odpovedi in analiza Monte Carlo [23, 25].

Merljivost tveganja zahteva osnovno razumevanje teorije verjetnosti in Booleove algebre, ki je podrobneje predstavljena v nadaljevanju.

Pojem HAZAN[40], ki je mnogokrat uporabljen, predstavlja fazo kvantifikacije.

Nekateri strokovnjaki so pri uporabi kvantifikacije na področju upravljanja s tveganji zelo previdni, in sicer zaradi naslednjih pomislekov [23, 24]:

- Verodostojni podatki o napakah na opremi so redko dosegljivi.
- Človeška napaka je glavni faktor tveganja.
- Kvantifikacija lahko zahteva ogromno časa.
- Rezultati analize povedo osebju sistema to, kar so že vedeli.
- Pogostost, s katero se izjemni dogodki (kot npr. eksplozija) pripetijo, je tako majhna, da številčna primerjava mnogokrat ni mogoča.

Tem pomislekom velja prisluhniti. Vendar pa bo primerjava med posameznimi sistemi brez kvantifikacije nemogoča.

Če smo npr. soočeni z omejenim proračunom, katerega namen je izboljšati varnost delovanja, kateremu strokovnjaku bomo prisluhnili? Predpostaviti velja, da bo vsak strokovnjak prav za svoj postopek predpostavil, da ima največji vpliv. Vendar, ali je to res? Četudi bomo pri vpeljavi kvantifikacije vpeljali netočnosti in predpostavke ali pristranske ocene, pa so vsaj nekateri podatki zasnovani na dolgoletnih pojavih. Pravilno bi bilo seveda upoštevati dejstvo, da vsak razumen proizvajalec skrbi, da se napake čim manj ponavljajo in jih je posledično vse manj, mi pa upoštevamo, da se ponavljajo z enako pogostostjo (zanemarimo časovno komponento kot posledica odziva na podatke o odpovedih). Vendar, dokler to delamo dosledno, pri vseh svojih analizah, bo rezultat analiz medsebojno primerljiv, tako da to ne bo imelo učinka na naše lastne analize, glede primerljivosti z drugimi pa moramo zagotoviti, da črpamo iz enakih ali enakovrednih baz podatkov.

[40] HAZAN – analiza tveganj (angl. *Hazard Analysis*)

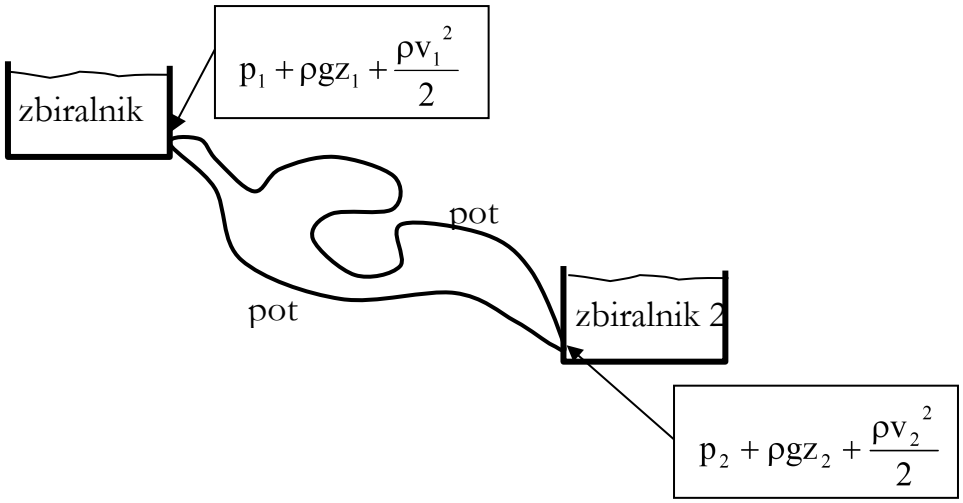
3.3.1 Paretovo pravilo

Paretovo pravilo predstavlja prvo, zelo grobo oceno merljivosti sistemskega tveganja. To pravilo je bil prvotno razvito na področju ekonomije, kjer so ga utemeljevali s predpostavko, da od 80 do 90 % svetovnega bogastva pripada od 10 do 20 % svetovnega prebivalstva. Zato je to pravilo znan0 tudi kot pravilo 80/20 ali 90/10.

V tehniki je Paretovo pravilo uporabno, če lahko dokažemo, da je velik delež procesnih sprememb pojasnjen z majhnim deležem procesnih spremenljivk[41]. Kaj bi to pomenilo v našem primeru?

Najprej se moramo vprašati, od katerih procesnih spremenljivk je naš proces odvisen? V resnici je mešanje seveda odvisno od obeh masnih tokov, kar je v skladu z energijsko in snovsko bilanco. Masni tok je odvisen od hitrosti, hitrost pa je odvisna, v idealiziranem primeru, od razlike v tlakih.

Ta soodvisnost je razvidna iz iz idealizirane enačbe za tok vzdolž tokovnice, tj. Bernoullijeve enačbe, kot prikazano na sliki 15.



Slika 15: Uporaba Bernoullijeve enačbe

Primerjava primera na sliki 15 s primerom na sliki 1 pokaže, da je primarni procesni parameter, torej tlak oziroma razlika v tlaku, na sliki 15 sicer v obliki razlike statičnega tlaka v polju težnosti, na sliki 1 pa je tlak v posledici prispevkov posameznih črpalk.

[41] *Box, George E.P. Meyer, R. Daniel, An Analysis for Unreplicated Fractional Factorials, Technometrics, 28 (1), 11–18, 2012.*

To pomeni, da je dober nadzor nad tlakom ključen. Z uporabo Paretovega pravila na sliki 1 lahko ugotovimo, da moramo biti zlasti sposobni nadzorovati tlak.

Paretovo pravilo lahko pripomore pri odločitvi vodstvenega kadra, kam naj določeno višino sredstev, časa in ljudi investira. V tem konkretnem primeru (ki je, seveda, močno poenostavljen), bomo investirali v dober nadzor tlaka v sistemu. Iz prejšnjih (kvalitativnih) analiz vemo, da lahko tlačni senzorji pomagajo pri odkrivanju napak, kot so zataknjeni ventili v odprtem ali zaprtem položaju in odpovedi pri črpalki.

Paretovo pravilo je mogoče ekstrapolirati[42]. Predpostavimo, da nam 20 % procesnih spremenljivk povzroči 80 % zaustavitev procesa. Ekstrapolacija Paretovega pravila pomeni, da 20 % od imenovanih 20 % procesnih spremeljivk pomeni 80 % od 80 % zaustavitev procesa. Z drugimi besedami: 20%*20%=4% procesnih spremenljivk pomeni 80%*80%=64% zaustavitev procesa in naprej, približno 1 % procesnih spremenljivk (0,8 %) je odgovorno za približno 50 % težav (51,2 %).

Princip je sestavljen iz naslednjih korakov:

1. identifikacija načinov (poti) oz. možnosti, v katerih lahko sistem odpove;
2. definiranje vpliva vsakega napačnega načina glede na celoten sistem;
3. rangiranje napačnih načinov;
4. izrisanje in analiziranje Paretove krivulje [23].

Paretov diagram je diagram, v katerem prikažemo tako posamezne dogodke kot skupno število pojavov.

Predpostavimo npr., da smo skozi podatke ugotovili naslednjo razporeditev odpovedi našega sistema na sliki 1.

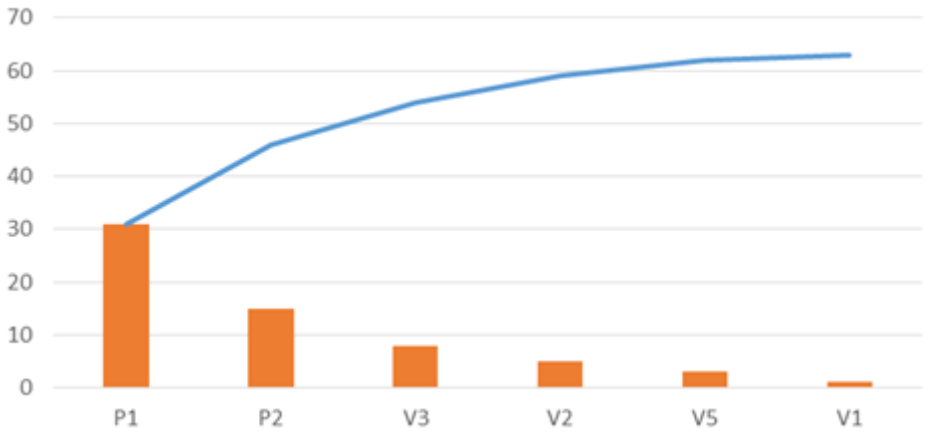
V letih od 2001 do 2020 smo npr. ugotovili 64 odpovedi. Od tega je bila P1 odgovorna za 31 odpovedi, P2 za 15, V3 za 8, V2 za 5, V5 za 3 in V1 za 1.

Zdaj lahko izdelamo Paretov diagram in Pareto krivuljo.

[42] Peter Hall, Liang Peng And Nader Tajvidi: Effect of extrapolation on coverage accuracy of prediction intervals computed from Pareto-type data, The Annals of Statistics, 2002, Vol. 30, No. 3, 875–895, https://projecteuclid.org/download/pdf_1/euclid.aos/1028674844

Najprej postavimo stolpčni diagram, ki kaže število povzročenih odpovedi za vsakega od elementov. Nato ugotovimo kumulativno distribucijo tako, da vsakemu prejšnjemu številu odpovedi dodamo novo število, torej za P2 izračunamo pogostost P1 + pogostost P2 = 31 + 15 = 46 odpovedi in to postavimo nad P2. Pri P3 bo skupno (kumulativno) število 46 + 8 = 54 itd. Dobimo Paretovo krivuljo.

Na sliki 16 je Paretova krivulja za zgornji primer, kjer oznake izhajajo s slike 1 (P1 – črpalka 1, P2 črpalka 2, V1 – ventil 1, V2 – ventil 2, V3 – ventil 3, V4 – ventil 4):



Slika 16: Paretov diagram

Glede na to, da stane remont P1 toliko kot P2 in remont V1 toliko kot V3, se lažje odločimo, v kaj bomo vložili. Pri enostavnih sistemih, kot je navedeni, bo odločitev seveda enostavna, pri bolj zapletenih, kjer imamo na eni strani odločitve, ki se tičejo okoljskih vplivov, na drugi strani pa visoke vložke, pa bo odločitev bistveno bolj zapletena.

3.3.2 Resničnostne tabele

Po identifikaciji napačnih poti in opravljenem grobem rangiranju ob uporabi Paretovega pravila sledi naslednji korak natančnejše merljivosti sistemskega tveganja. Za to obstaja več postopkov, eden od najenostavnejših postopkov je poznan kot resničnostne tabele (angl. *truth tables*). Gre za matematično orodje, ki formalizira vse možne odnose med posameznimi stanji spremenljivk[43], kot npr. v Post (1921), kot je prikazano na spodnji sliki.

[43] Post, E., Introduction to a general theory of elementary propositions, American Journal of Mathematics, 43 (3): 163–185, 1921.

For example consider the function

$$\sim (\sim (\sim p \vee q) \vee \sim (\sim q \vee p))$$

which is the ultimate definition of the function $p \equiv q$ of Principia. We have when p is $+$ and q is $+$ the following truth-values of the successive components of the function and so finally of the function:

$$p : +, \quad \sim p : -, \quad \sim p \vee q : +, \quad \sim (\sim p \vee q) : -$$

$$q : +, \quad \sim q : -, \quad \sim q \vee p : +, \quad \sim (\sim q \vee p) : -$$

$$\sim (\sim p \vee q) \vee \sim (\sim q \vee p) : -, \quad \sim (\sim (\sim p \vee q) \vee \sim (\sim q \vee p)) : +$$

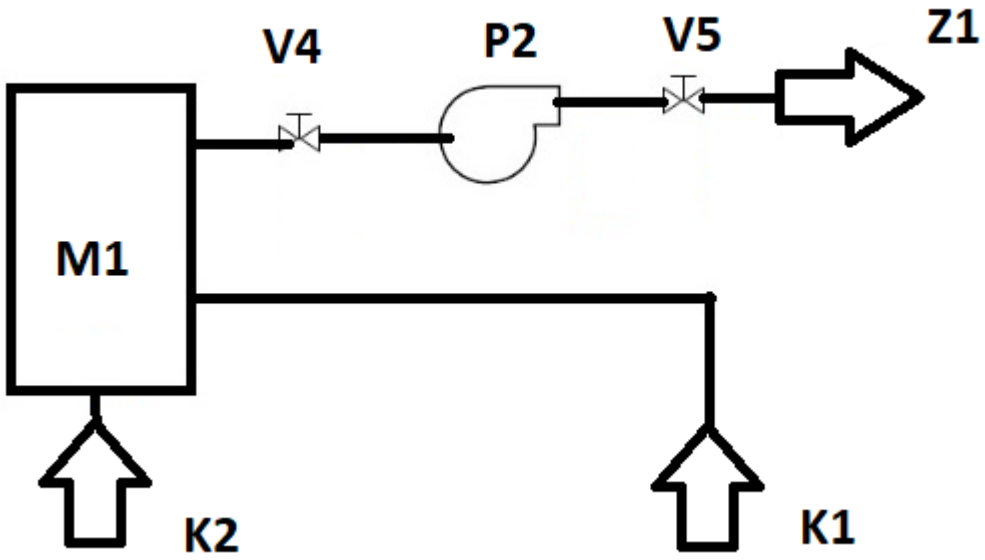
the successive truth-values being found by direct application of the primitive tables. In the same way the truth-values for $p +$, $q -$ etc. can be calculated and so we finally get the truth-table of $p \equiv q$, i.e.,

p, q	$p \equiv q$
$+ +$	$+$
$+ -$	$-$
$- +$	$-$
$- -$	$+$

It is needless to say that in actual work this amount of detail is quite unnecessary.

Slika 17: Posnetek iz izvirnega članka o resničnostnih tabelah [43]

Na podoben način lahko zgradimo vse možne logične kombinacije sistema. Tokrat obravnavajmo iztok zmesi.



Slika 18: Iztok zmesi Z1

Možna stanja, ki jih postavimo, so M1, V4, P2, V5; ta stanja delujejo ali ne delujejo, vsako zase. Končni rezultat je, ali dobimo Z1 ali ne dobimo Z1:

Tabela 3. Resničnostna tabela – kvalitativna

	V4 deluje?	P2 deluje?	V5 deluje?	Izliv Z1?
1	DA	DA	DA	DA
2	DA	DA	NE	NE
3	DA	NE	DA	NE
4	DA	NE	NE	NE
5	NE	DA	DA	NE
6	NE	DA	NE	NE
7	NE	NE	DA	NE
8	NE	NE	NE	NE

Iz zapisanega izhaja, da bo Z1 deloval, če bodo vse tri naprave delovale. Kakšna pa je verjetnost za to? Nekoliko bomo preskočili in kar zapisali, da je verjetnost delovanja gotovost z odšteto verjetnostjo nedelovanja. Zdaj je čas, da se spomnimo pogostosti odpovedi – za ventil smo privzeli 5,43E-2/a, za črpalko 0,174/a. Izračunavali bomo verjetnost za čas misije enega leta, tako bo verjetnost odpovedi za ventil postala 5,43E-2/a x 1 a = 5,43E-2, za črpalko 0,174/a x 1 a = 0,174 itd.

Verjetnost delovanja bo torej: (1-5,43E-2)x(1-0,174)x(1-5,43-2)=0,74 ali 84,5E-6/h (oziroma 84,6 na milijon obratovalnih ur).

Pogostost odpovedi bo, upoštevajoč vrata ALI, izračunana po enačbi

$p_{ALI} = p1 + p2 – (p1 \times p2)$

p_{ALI} – verjetnost dogodka, če vrata povezujejo dva dogodka, katerih verjetnost prvega je p1, verjetnost drugega pa p2.

Tako dobimo

5,43E-2+0,174+5,43E-2-(5,43E-2x0,174x5,43E-2)=0,26

oziroma 29,6E-6/h oziroma 29,6 na milijon obratovalnih ur.

Tako smo izračunali naš prvi rezultat. Je to veliko ali malo?

Regulator nuklearne energije v Kanadi[44] je postavil naslednjo primerjalno tabelo, v kateri je za mero zanesljivosti ali nezanesljivosti posameznega sistema uporabil podatke za pogostost odpovedi:

Zanesljivost	Pogostost odpovedi na milijon obratovalnih ur
izredno zanesljivo	0,01
visoko zanesljivo	0,01–0,1
dobro zanesljivo	0,1–1,0
povprečno zanesljivo	1,0–10
zelo nezanesljivo	10–100
neprimerno	nad 100

Ugotovimo, da je naš sistem zelo nezanesljiv. Treba ga je popraviti. Kako? Tako, da vpeljemo preventivno vzdrževanje in popravila, torej, da zamenjamo dele že, ko še obratujejo.

Hkrati pa tovrstne tabele niso povsem primerljive med dejavnostmi. Črpalke v kotlih npr. pogosteje odpovedo in bi bili zgornji rezultati povsem sprejemljivi, kot kaže naslednji primer.

Tabela 4: Prikaz delovanja črpalk v kotlu[45].

	Črpalni sistem A	Črpalni sistem B	Črpalni sistem C
čas delovanja , t_1 (hr)	3143	8737	8239
čas mirovanja t_2 (hr)	3509	139	404
čas okvar t_3 (hr)	2943	719	952
skupno število okvar , n	26	24	20
ocenjeno število okvar med delovanjem , m	16.7	23.8	19.5
$\mu = n/t_3$ (na uro)	0.0088	0.0286	0.0211
$\lambda_{running} = m/t_1$ (na uro)	5.39×10^{-3}	2.72×10^{-3}	2.37×10^{-3}
$\lambda_{standby} = 0.5\ \lambda_{running}$	2.65×10^{-3}	1.36×10^{-3}	1.18×10^{-3}

Pri tem z μ označimo razmerje med skupnim številom okvar in časom okvar, z λ pa razmerje med ocenjenim številom okvar med delovanjem in časom delovanja.

[44] vir: https://www.sciencedirect.com/topics/engineering/equipment-failure-rate
[45] Sudagala, N.P., Reliability Analysis And Improvement Of Turbine Side Of Lakvijaya Power Station, 2016, University of Moratuwa, Sri Lanka.

Osnovni postopek teh tabel je zelo neposreden. Analitik enostavno navede vse možne kombinacije dogodkov, zatem opravi kalkulacijo verjetnosti nastopa napake za vsako kombinacijo posebej. Verjetnost popolnega delovanja sistema izračuna na osnovi seštevka vseh posameznih verjetnosti, kjer se ne pojavijo napake. Edina težava teh tabel je, da velikost oz. dolžina teh tabel narašča eksponentno s številom operacij in lahko hitro postanejo nepregledne [9]. Na drugi strani pa je res, da obravnavamo prav vse možne kombinacije, torej je poznavanje delovanja sistema manj pomembno.

Hkrati pa se pokaže pomembnost rangiranja. Rangiranje je razvrstitev naprav po pomembnosti, od najpomembnejše do najmanj pomembne. V našem primeru tega ne moremo uporabiti, ker so vse naprave enako pomembne, če želimo doseči stanje Z1, lahko pa bi to uporabili, če bi npr. uporabili redundanco in bi črpalko P2 podvojili. Potem bi bilo morda pomembneje posvetiti se ventilu V2 kot eni od črpalk P2.

Relativno rangiranje je pozicioniranje, ki je z vsakim novim dogodkom (in odpravo letega) bliže popolni varnosti celotnega sistema. Ta tehnika predstavlja merilo, ki učinkovito prikazuje kje oz. na kateri točki naj se vloži več napora k zagotavljanju varnosti [24].

3.3.3 Tabele učinkovitosti

Tehnika resničnostnih tabel (in večino drugih postopkov kvantitativnih analiz tveganja) fokusira tako na delujočih kot tudi nedelujočih sistemih s predpostavko, da delno delujoč sistem ni uspešen. Tak pristop je seveda zahtevan v letalski in tudi jedrski industriji in ni primeren pri analiziranju tveganja, kjer lahko sistem delno (omejeno) deluje.

Efektivnost je mnogokrat analizirana z uporabo spremenjenih resničnostih tabel, imenovanih tabele učinkovitosti, ki prikazuje kapaciteto sistema v tistem trenutku ne glede na to, če sistem polno deluje ali ne [23].

3.3.4 Teorija verjetnosti in Booleova algebra

V popolnem svetu, kjer bi lahko natančno preračunali vsako ravnanje in dejanje, ne bi potrebovali koncepta verjetnosti, kajti vsi dogodki, kot npr. odpoved opreme, bi bili vnaprej predvidljivi na osnovi osnovnih fizikalnih zakonitosti. Na žalost je večina resničnih sistemov preveč kompleksnih, da bi lahko razvili enovit skupen koncept, zato uporabljamo verjetnost (angl. *probability*).

Verjetnost je definirana na nalsednje tri različne načine:

1. Klasična verjetnost (angl. *classical probability*) → Če se nek dogodek pojavi v N podobnih načinih in če se en dogodek E pojavi v n številu teh podobnih načinov, potem je verjetnost dogodka E, ki se lahko pojavi, »p(E) = n/N«.
2. Frekventna verjetnost (angl. *frequentist probability*) → Od klasične verjetnosti se razlikuje v tem, da število N podobnih načinov ni znano vnaprej ali pa se konstantno spreminja.
3. Subjektivna verjetnost (angl. *subjective probability*) → Gre za stanje zaupanja, s katerim se ukvarja Bayesova metoda. Predstavlja dragocen vir, saj je v nekaterih primerih ta verjetnost edini vir mere odpovedi opreme [23].

3.3.4.1 Vrste dogodkov

O dogodkih smo že pisali. Spoznali smo glavne dogodke in osnovne dogodke. Skupno vsem dogodkom je, da imajo vpliv na varnost in zanesljivost delovanja okoljskega postroja (z besedo postroj opišemo skupino strojev in naprav, namenjenih izvajanju postopka). Postroji pa so pogosto kompleksni, sestavljeni iz cele vrste posameznih naprav, od katerih ima vsaka svoje lastnosti.

K vsaki napravi lahko pripišemo nekatere dogodke, kot so npr. začetek obratovanja, konec obratovanja, prekinitev obratovanja, odpoved, popravilo, zamenjava. Vsak tak dogodek je lahko pomemben za varnost in zanesljivost celotnega postroja.

Ukvarjati se moramo torej ne le s posameznimi napravami in k njim pripadajočimi dogodki, ampak tudi s kombinacijami teh dogodkov. Zato moramo razdeliti dogodke na kategorije [23, 24].:

Samostojen dogodek

Dva dogodka sta samostojna, če en dogodek ne vpliva na drugega.

Kot primer poglejmo ponovno redundantni sistem črpalk P11 in P12 s slike 13. Ali je odpoved ene od črpalk samostojni dogodek? Je, če odpoved črpalke P11 ne vpliva na črpalko P12.

Večina dogodkov je samostojnih dogodkov. Naprave so običajno fizično ali logično ločene med seboj. O fizični ločenosti govorimo, kadar naprave opravljajo funkcijo na različnih krajih, četudi je funkcija enaka (vsi ventili npr. opravljajo enako funkcijo). O logični ločenosti govorimo, če so funkcije naprav različne, čeprav so naprave skupaj ali gre celo za isto napravo z več različnimi vlogami. Takšne naprave v našem primeru ni, lahko pa bi, recimo, za ventil V2 uporabili protipovratni ventil. Ta bi imel dve logični funkciji, funkcijo prepuščanja določene količine kapljevine v eni smeri in funkcijo preprečevanja vračanja kapljevine v drugi smeri. Če bi npr. funkcija preprečevanja vračanja kapljevine odpovedala, bi lahko nenadna reakcija v M1 povzročila lokalni padec tlaka v smeri R1, to pa povratni tok, če bi črpalka P1 mirovala.

Medsebojno izključujoča dogodka

Dva dogodka sta medsebojno izključujoča, če se ne moreta pojaviti ob istem času. V našem primeru take naprave nimamo, lahko pa bi, ponovno, uporabili protipovratni ventil. Protipovratni ventil, ki opravlja dve logični funkciji, prepuščanje kapljevine v eni smeri in preprečevanje gibanja kapljevine v drugi smeri, ne more hkrati prepuščati kapljevine v eni smeri in preprečevati gibanja v drugi smeri. Dogodka se med seboj izključujeta, ker kapljevina ne more teči v dve smeri hkrati – teče v eno ali v drugo smer. Odpoved ventila se lahko tako nanaša samo na gibanje kapljevine v eni smeri ali gibanje kapljevine v drugi smeri. Običajno kot primer medsebojno izključujočih se dogodkov postavljajo primer metanja kovanca, kjer je bodisi cifra bodisi mož, oboje hkrati pa ne (čeprav obstaja od nič različna možnost, da kovanec ostane na robu, kar seveda primer pokvari).

Komplementarna (dopolnilna) dogodka

Dva dogodka sta komplementarna, če se eden mora zgoditi, če se drugi ne zgodi. Pri tem gre pojasniti, da so vsi komplementarni dogodki medsebojno izključujoči, vsi medsebojno izključujoči dogodki pa niso komplementarni. Primer takega dogodka je metanje kocke – če je namen, da vržete 1 ali 2, je to medsebojno izključujoč dogodek (ker oboje hkrati ne morete vreči), ni pa to komplementarni dogodek (ker lahko poleg 1 ali 2 vržete tudi 3 ali 5).

Dogodka s skupnim vzrokom

Dva (ali več) dogodkov sta dogodka s skupnim vzrokom, če se morata zgoditi hkrati, vendar ne zaradi medsebojne soodvisnosti (formalno sta še vedno samostojna dogodka). Primer bi bili odpovedi črpalk P11 in P12, ki bi bili povzročeni npr. zaradi izgube električnega napajanja, če bi bili črpalki na istem električnem vodu.

Primer takšne napake v resničnem življenju je bila nezgoda v japonskih jedrskih elektrarnah v Fukushimi. Šlo je za šest ločenih reaktorjev, od katerih je imel vsak po dva generatorja, gnana z dizelskim motorjem. Enajst od dvanajstih dizelskih motorjev je bilo postavljenih pod gladino razlitega morja in zato so odpovedali. Skupni vzrok je bilo tedaj razlitje morja.

3.3.4.2 Boolova algebra

Boolova algrebra je imenovana po matematiku Georgeu Boolu (Matematična analiza logike, 1847) in temelji na logiki simbolov ter se navezuje na dogodke in pogoje. Poznavanje te algebre je pomembno zaradi pravilnega razumevanja, kako se izvedeta priprava in kalkulacija analize drevesa odpovedi (FTA) in analize drevesa dogodkov [23, 24].

Boolova algebra je zasnovana na osnovnih operacijah.

IN, ki je označena kot $x \wedge y$, pri čemer velja, da je $x \wedge y=1$, če je hkrati $x=1$ in $y=1$, sicer je 0.
ALI, ki je označena kot $x \vee y$, pri čemer velja, da je $x \vee y=1$, če je bodisi $x=1$ ali $y=1$ ali oba enaka 1, sicer je 0. Lahko seveda zapišemo tudi obratno, torej, da je $x \vee y=0$, če sta hkrati $x=0$ in $y=0$, sicer je 1.
NOT (ali negacija), ki je označena kot $\neg x$, pri čemer velja, da je $\neg x=0$, če je $x=1$ in obratno.

Vse osnovne operacije lahko zapišemo z resničnostnimi tabelami, o katerih smo že govorili.

Tabela 5A: Resničnostna tabela osnovnih operacij Boolove algebre

x	y	x∨y	x∧y	¬x	¬y
1	1	1	1	0	0
1	0	1	0	0	1
0	1	1	0	1	0
0	0	0	0	1	1

Iz osnovnih operacij lahko izpeljemo sestavljene operacije npr.:

IMPLIKACIJA, ki se zapiše kot x→y in pomeni, da če je x 1 in je y 0, tedaj je implikacija 0.

IZKLJUČNI ALI, ki se zapiše kot x⊕y in pomeni, da je vrednost 1, če sta x in y različna, sicer je 0.

EKVIVALENCA, ki se zapiše kot x ≡ y in pomeni, da je vrednost 1, če sta x in y enaka, sicer je 0.

Izpeljemo lahko
x→y=¬x∨y.
x⊕y=(x∨y)∧(¬x∨¬y) = (x∧¬y)∨(¬x∧y)y=¬ x≡y
x≡y=(x∧y)∨(¬x∧¬y) =¬ x⊕y

Tudi te, sestavljene, operacije lahko prikažemo v resničnostni tabeli.

Tabela 5B. Resničnostna tabela sestavljenih operacij Boolove algebre

x	y	x→y	x⊕y	x≡y
1	1	1	0	1
1	0	0	1	0
0	1	1	1	0
0	0	1	0	1

Za Boolovo algebro veljajo nekatere zakonitosti, kot sledi

Tabela 6. Zakonitosti Boolove algebre.

komplementarnost ∧	x∧¬x =0
komplementarnost ∨	x∨¬x =1
asociativnost ∧	x∧(y∧z)=(x∧y)∧z
asociativnost ∨	x∨(y∨z)=(x∨y)∨z
komutativnost ∧	x∧y=y∧x
komutativnost ∨	x∨y=y∨x
distributivnost ∧ glede na ∨	x∧(y∨z)=(x∧y)∨(x∧z)
distributivnost ∨ glede na ∧	x∨(y∧z)=(x∨y)∧(x∨z)
identiteta ∧	x∧1=x
identiteta ∨	x∨0=x
izničenje ∧	x∧0=0
izničenje ∨	x∨1=1
idempotentnost ∧	x∧x =x
idempotentnost ∨	x∨x =x
absorpcija ∧ glede na ∨	x∧(x∨y)=x
absorpcija ∨ glede na ∧	x∨(x∧y)=x
De Morganov zakon o ∧	¬x∧¬y=¬(x∨y)
De Morganov zakon o ∨	¬x∨¬y=¬(x∧y)
dvojna negacija	¬(¬x)=x

V splošnem si lahko predstavljamo operacijo IN kot presek, operacijo ALI kot unijo in NOT kot komplement množice.

3.4 Analiza drevesa odpovedi (FTA[46])

Drevo odpovedi smo na kratko že obravnavali, in sicer iz kvalitativnega vidika. V nadaljevanju se mu bomo posvetili še iz kvantitativnega vidika in bomo to imenovali analizo drevesa odpovedi.

Analizo so razvili v šestdesetih letih prejšnjega stoletja za potrebe ameriške vojske, povzeli pa so jo v agenciji ZDA, ki skrbi za letala (FAA). V procesni (in posledično okoljski) industriji se je postopek uveljavil kot posledica nezgode na Otoku treh milj konec sedemdesetih letih prejšnjega stoletja in kot logični naslednik študij na področju varnostnih analiz v ZDA[47].

[46] FTA–Analiza drevesa odpovedi (angl.Fault Tree Analysis)
[47] Poročila WASH-1400, Garrick, B.J., Gekler, W.C., Goldifisher L. Karcher, R.h.h, Shimizu, B., Wilson, J.H., Reliability Analysis Of Nuclear Power Plant Protective Systems, NSA-22-010000, 1967 (vir: https://www.osti.gov/servlets/purl/4568767/), Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants (NUREG-1150), 2020 (vir: https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1150/index.html), Vesely, W.E., Goldberg, F. F., Roberts, H. H., Haasl, D. F., Fault Tree Handbook (NUREG-0492), U.S. Nuclear Regulatory Commission, January 1981 (vir: https://www.nrc.gov/docs/ML1007/ML100780465.pdf)

Zgodovina pa kaže tudi pomanjkljivosti namernega spregleda sicer učinkovitih in uporabnih metod. Za razliko od drugih organizacij se NASA namenoma ni odločila za uporabo tega postopka pri načrtovanju programa Apollo[48], saj so rezultati kazali nesprejemljivo nizke vrednosti za možnost uspeha, namesto tega so uporabili kvalitativne postopke, o katerih smo že govorili. Šele po nesreči raketoplana Challenger se je NASA začela resneje ukvarjati s kvantitativnimi analizami.

Morda ni odveč, če na tem mestu ugotovimo, kateri so bili temeljni faktorji te kvalitativne analize:

- pregled vseh pomembnih modifikacij opreme od zadnjega pregleda dizajna in vseh še nepotrjenih modifikacij;
- identifikacija in določitev statusa kvalificiranosti katerekoli sistemske komponente, katere neposredna posledica bi lahko povzročila smrt, izgubo stopnje ali vesoljskega vozila (kriteriji enojne odpovedi, angl. *Single Failure Points*);
- pregled vseh testov vozila in posebnih sistemov;
- pregled vseh pomembnih odpovedi in posledičnih korektivnih aktivnosti;
- pregled vseh nerešenih problemov, načrtov za korektivne aktivnosti in ocenjenih datumov zaključka.
- Primer: Pri vesoljskem vozilu Challenger so odkrili, da je tesnilo slabo in zato so sprojektirali novo tesnilo, ki pa ga niso nikoli uporabili, ker so temo obravnavali kot rešeno. Od ugotovitve do nezgode je minilo 10 let[49] [31].

Seveda je iz zgodovinske distance lahko biti kritik, lahko pa zgornje točke služijo za oporo iskanja pomanjkljivosti, zlasti pri tihih predpostavkah. Tiha predpostavka v zgornjem sistemu je bila, da so sistemi, ki so delovali v prejšnjih uspešnih misijah, zadosti preizkušeni in jih ni več treba pregledovati. Prav tako so nezgode pogosto posledica več zaporednih odpovedi, ki same zase ne povzročijo nujno težav.

Primer je, ponovno, nezgoda na Otoku treh milj. Tam se je nezgoda pojavila po tem, ko so pri čiščenju filtrov po pomoti vbrizgali nekaj vode v sistem za dovod zraka za instrumente, kar je posledično povzročilo zaustavitev reaktorja in prenehanje odvoda zaostale toplote, ob tem, da so bile hkrati vse tri črpalke zunanje napajalne vode v remontu.

---

[48] Fragola, J.R., Risk Management in US Manned Spacecraft: from Apollo to Alpha and beyond, Proc. Produvct Assurance Symposium and Software Product Assurance Workshop, 19–21 March, 1996, vir: http://adsabs.harvard.edu/full/1996ESASP.377...83F

[49] Report of the PRESIDENTIAL COMMISSION on the Space Shuttle Challenger Accident, Chapter 4: An accident rooted in history, vir: https://history.nasa.gov/rogersrep/v1ch6.htm

Nobeden od teh elementov, vključno s črpalkami, ne bi sam po sebi povzročil nezgode z resnim učinkom, kombinacija vseh okoliščin pa je privedla do tega. Uporaba zgornjih principov kvalitativne ocene ne bi prispevala k prepoznanju nezgode.

Danes je drevo odpovedi eden izmed najbolj uporabniško razširjenih postopkov za analiziranje verjetnosti odpovedi. Postopek se odlikuje predvsem zaradi naslednjih razlogov:

- natančnost, sistematičnost,
- uporabnost na različnih industrijskih področjih [23],
- učinkovitost in razširljivost (praktično ni zgornje meje števila napak, ki je ne bi mogli analizirati) [24].

Z analizo ugotavljamo logične povezave med izpadi komponent ali podsistemov (nezaželenimi dogodki), katerih posledice predstavljajo odpovedi (tehnične napake) [28].

Na osnovi postopka analize drevesa odpovedi lahko analiziramo delovanje sistema ali varnost. Če je namen analizirati varnost, v drevo odpovedi vključimo tiste komponente in funkcije, ki lahko povzročijo neželena stanja [23]. Tak pristop seveda pomeni, da moramo dobro poznati analizirani sistem.

Če se ponovno osredotočimo na naš sistem na sliki 1, lahko ugotovimo, da so zaradi premočrtnosti procesa za uspeh delovanja bistveni vsi elementi. Popolna odpoved kateregakoli sistema bo povzročila, da zmes Z1 ne bo iztekala in da cilj ne bo dosežen. Prav tako lahko katastrofalna odpoved (tj. odpoved, pri kateri se pojavi porušitev ocevja ali rezervoarja) pomeni, odvisno od kapljevin K1 in K2 ter njunih zmesi Z1, resno nezgodo z okoljskimi učinki.

Drevo odpovedi predstavlja logični diagram poteka, ki nam prikaže, kako lahko neki sistem odpove oziroma nastane neželeni dogodek. Z diagramom tako določimo verjetnosti oziroma pogostosti nastanka neželenih dogodkov na osnovi logičnega modela, ki temelji na kombinacijah/kombiniranju odpovedi krovnih sistemskih komponent, odpovedi varnostnih/preventivnih sistemov in človeški (ne)zanesljivosti [20]. Postopek temelji na tem, da pri eni komponenti, podsistemu ali sistemu predpostavimo možno neželeno stanje ali dogodek ter z logičnimi povezavami prek vrat IN in ALI (možnost kombiniranja logičnih vrat), povežemo vse komponente sistema ali dogodke, ki lahko z lastno odpovedjo povzročijo predpostavljeno neželeno stanje [26]. Nato kreiramo model,

ki prikazuje odpoved nekega sistema. Verjetnost oziroma pogostost nastanka neželenega dogodka (npr. odpoved varnostnega mehanizma, eksplozija, nenadzorovana reakcija) izračunamo z uporabo razpoložljivih baz podatkov o pogostosti nastanka enostavnih nezaželenih dogodkov. Pri tem vključimo izhodiščno predpostavko postopka, ki opredeljuje, da so odpovedi sistema binarnega tipa, kar posledično pomeni delovanje ali nedelovanje komponente sistema. Sočasno s kvantitativnim vrednotenjem nekega neželenega dogodka s FTA-postopki pridobimo širšo predstavo, kako se je do neželeni dogodek zgodil.

Ugotavljanje verjetnosti odpovedi sna osnovi FTA-postopkov je dandanes še prav posebej razširjeno v procesni industriji, saj slednja zajema vedno več kompleksnih kontrolno-varnostnih mehanizmov [9, 20, 23].

Nadaljnja teoretična izhodišča smo navedli v nadaljevanju in v prilogi, in sicer ob izvedbi analize varnosti sistema čistilne naprave..

3.4.1 Programska podpora

Drevo odpovedi, kot smo ga prikazali v poglavju o kvalitativnih metodah, je kljub omejenemu obsegu predstavljalo precej informacij. Kratek pogled na analizo v dodatku nam pokaže, kako hitro lahko drevesa zrastejo in presežejo sposobnosti pregleda. Dve strani še lahko primerjamo, za kaj več nam pogosto zmanjka koncentracije.

Zato se za preračune dreves odpovedi v praksi uporablja sodobna računalniška in programska podpora, pri čemer omenjamo eno bolj uporabljenih, tj. ISOGRAPH – programski sistem integriranega inženiringa zanesljivosti (angl. *Integrated Reliability Engineering software*). Več informacij o tem sistemu je dostopnih prek spleta [15].

Omenjeni programski sistem je zelo drag in predvsem primeren kot pomoč pri analiziranju odpovedi večjih ali velikih sistemov v nuklearni, letalski, procesni industriji ipd.

Ker naš obravnavan primer čistilne naprave v dodatku ne spada med tako velike sisteme, smo se izvedbe analize lotili ročno, predvsem z namenom, da bo izvedena analiza predstavljala referenčni primer za upravljalce čistilnih naprav oz. za njihovo v praksi uporabno metodologijo analiziranja varnosti in zanesljivosti malih komunalnih čistilnih naprav.

3.4.2 Koncept analize drevesa odpovedi

Pri načrtovanju in izvedbi drevesa odpovedi bomo najprej spoznali in ponovili osnovne strokovne pojme oz. izraze, ki jih uporabimo za natančen opis dogodkov nekega procesa. Pri tem drevo odpovedi sestavljajo dogodki in vrata [23, 24].

Dogodki so procesna kategorija, z napravami so povezani ob predpostavki, da posegajo v funkcijo delovanja naprave, ki je vključena v obravnavani proces. Zato je drevo odpovedi logični diagram, ki sledi procesnim vlogam posamezne naprave.

Nekaj smo o dogodkih že zapisali, zdaj bomo to ponovili in dopolnili. Obstajajo naslednje vrste dogodkov:

Neželeni dogodek

Da bi lahko opredelili neželeni dogodek, moramo najprej opredeliti njegovo nasprotje. To je običajno delovanje in posledični želeni dogodki.

Kadar se pojavi neželen odklon od normalnega delovanja nekega sistema/komponent (odpoved nekega dela/komponente sistema), govorimo o neželenem dogodku. Pri tem je lahko tak dogodek z vidika znižanja varnosti in zanesljivosti malo pomemben, lahko pa ima resne posledice.

V našem primeru na sliki 1 bi lahko bil neželeni dogodek npr. znižanje nivoja kapljevine K1 v rezervoarju R1, kar bi lahko bila posledica neažurnega dolivanja kapljevine v R1. Tak neželeni dogodek bi bilo enostavno odpraviti tako, da se kapljevina K1 dolije ali pa, alternativno, da se ustavi delovanje naprave.

V skupini neželenih dogodkov so lahko tudi takšni, ki imajo resne posledice. Takšen dogodek je neželeni dogodek. Takšne dogodke postavimo na vrh drevesa odpovedi, če želimo ugotoviti, zakaj bi tak dogodek utegnil nastopiti. S tem postane neželeni dogodek glavni dogodek. Z uporabo logičnih vrat ga nato razvijamo do osnovnih dogodkov in analiziramo pot odpovedi, ki vodi do takšnega dogodka, kar nam omogoči kvanitifikacijo pogostosti dogodka.

V našem primeru na sliki 1 bi to lahko bilo npr. prenehanje dobave zmesi Z1.

Osnovni dogodek

Z razvojem neželenega dogodka skladno s pravili Boolove algebre pridemo do enega osnovnega dogodka ali več osnovnih dogodkov. Osnovni dogodek je tisti dogodek, ki ne omogoča ali ne potrebuje nadaljnjega razvoja.

V našem primeru bi to lahko bila npr. odpoved ventila V2.

Z osnovnimi dogodki se začne izračun verjetnosti vrhnjega (neželenega) dogodka. Zato je informacije o pogostosti nastanka takšnega dogodka treba pridobiti, bodisi iz lastnih podatkov bodisi iz razpoložljivih baz podatkov.

Vmesni dogodek

Vmesni dogodek je dogodek med glavnim (neželenim) dogodkom in osnovnim dogodkom. Vmesne dogodke dodajamo zaradi lažje in boljše razčlenitve procesa. Vmesne dogodke obravnavamo kot vrhnje dogodke neposredno vhodnim dogodkom, bodisi vmesnim bodisi osnovnim.

Gre torej za dogodek, ki označuje vmesno stopnjo/povezavo med osnovnim dogodkom in glavnim dogodkom [16, 20].

V našem primeru na sliki 1 bi lahko to bila odpoved iztočnega segmenta, ki obsega cevi C41, C42, C51 in C52, ventila V4 in V5 ter črpalko P2. Osnovni dogodki temu vmesnemu dogodku so odpovedi posameznih elementov (npr. cev C42, ventil V5 ipd.)

Nerazviti dogodek

Včasih moramo ugotoviti, da glede posameznega dogodka ne bomo mogli pridobiti zadosti informacij. Takega dogodka ne obravnavamo ali pa mu pripišemo pavšalno vrednost verjetnosti, z vedenjem, da bomo morali ta dogodek kasneje raziskati ali razumeti, da drevo odpovedi ni zadosti raziskano.

Logična vrata

Logična vrata so temeljni gradnik drevesa odpovedi. Obstajata dva osnovna tipa vrat, vrata ALI in vrata IN[50].

Med posameznimi dogodki so prikazane logične povezave, s t. i. logičnimi vrati. Logična vrata so stikala, ki pojasnjujejo tok dogodkov. Če opazujemo npr. redundančni sistem črpalk, ugotovimo, da obstaja povezava med nedobavo Z1 in nedelovanjem P11 in P12. Predvsem morata odpovedati tako P11 kot tudi P12. Če samo ena od njiju deluje, bo Z1 dobavljena kot previdenо, vrhnjega (neželenega) dogodka torej ne bo.

Logična vrata so ekvivalent operacijam Boolove algebre. Posamezna logična vrata so logična povezava med vhodnim (osnovnim, vmesnim) dogodkom ter izhodnim (vmesnim, glavnim) dogodkom [20, 23, 24].

Logična vrata IN

V tem primeru so vhodni dogodki povezani z izhodnim tako, da izhodni dogodek nastane samo, če so nastali vsi vhodni dogodki. Lahko obstaja več vhodnih odpovedi v vrata IN [49]. Če obstaja možnost obstoja dveh vhodnih dogodkov (x in y) in oba podrejena dogodka v resnici tudi nastaneta, potem bo v vsakem primeru izpolnjen pogoj za nastanek nadrejenega dogodka.

Če je torej x = 1 in je y = 1, potem je tudi x∧y = 1.

Simbol za logična vrata IN je običajno navzgor obrnjen polkrog, spodaj zaključen z ravno osnovo:

logična vrata IN

Logična vrata ALI

Vrata ALI se uporabljajo, da se izhodni dogodek (angl. *output event*) zgodi samo, če se zgodi eden ali več vhodnih dogodkov (angl. *input event*). Obstaja lahko cela vrsta vhodnih dogodkov, ki vodijo v vrata ALI. Pomembno pa je poudariti, da vzročnost (angl. *causality*) nikoli ni prehajala skozi vrata ALI, temveč izključno skozi vrata IN[51]. Kaj to pomeni? To

[50] Vesely, W.E., Goldberg, F. F., Roberts, H. H., Haasl, D. F., Fault Tree Handbook (NUREG-0492), U.S. Nuclear Regulatory Commission, January 1981, vir: https://www.nrc.gov/docs/ML1007/ML100780465.pdf

[51] Vesely, W.E., Goldberg, F. F., Roberts, H. H., Haasl, D. F., Fault Tree Handbook (NUREG-0492), U.S. Nuclear Regulatory Commission, January 1981, vir: https://www.nrc.gov/docs/ML1007/ML100780465.pdf

pomeni, da imata lahko dva vhodna dogodka v vrata ALI različna vzroka (npr. črpalka odpove zaradi puščajočega tesnila, črpalka odpove zaradi zloma gredi), izhodni dogodek pa je, da črpalka odpove. Če namreč v tem primeru zlom gredi preide v izhodni dogodek, je to znak, da so bila nekje po poti izpuščena vrata IN.

Vhodni dogodki so torej povezani z izhodnim tako, da izhodni dogodek nastane, če je nastal vsaj en vhodni dogodek. Če obstaja možnost obstoja dveh vhodnih dogodkov (x in y) in eden od vhodnih dogodkov v resnici tudi nastane, potem bo v vsakem primeru izpolnjen pogoj za nastanek nadrejenega dogodka.

Če je torej x = 1 in je y = 1 ali y = 0 in obratno, če je x = 1 ali x = 0 in je y = 1, potem je tudi x∨y = 1.

Simbol za logična vrata ALI je običajno navzgor obrnjen polkrog, spodaj zaključen s konkavno osnovo, ali stilizirana puščica:

logična vrata ALI

Obstaja še več drugačnih logičnih vrat, ki ustrezajo osnovnim ali sestavljenim operacijam Boolove algebre, a najpogosteje je najti prav oba zgoraj zapisana simbola.

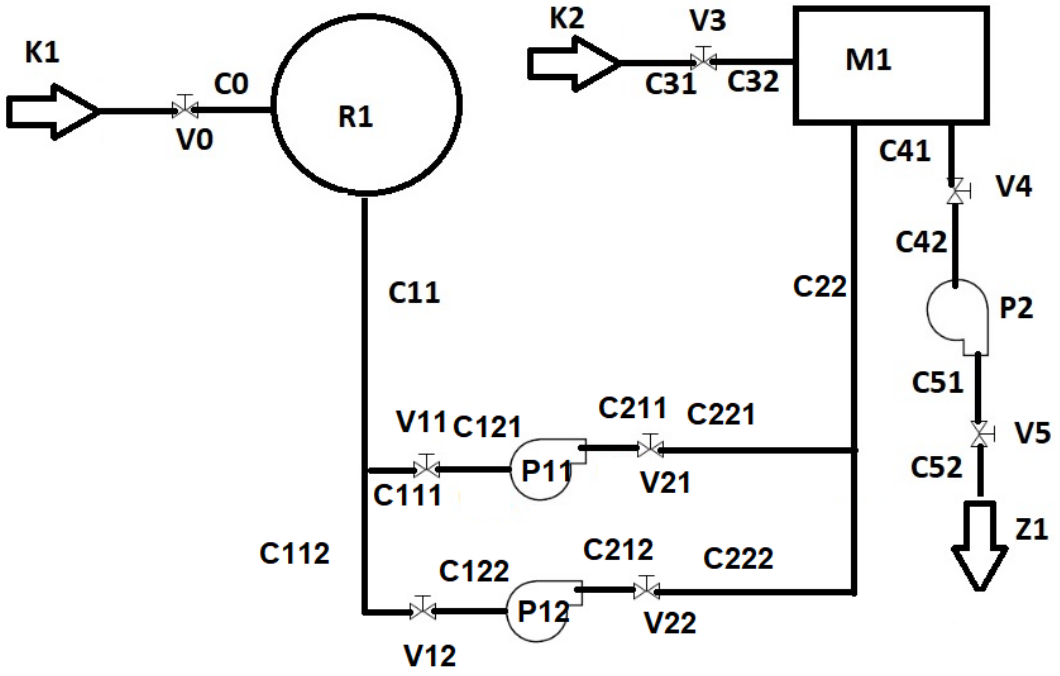
Poleg navedenih pogosto najdemo še simbol za osnovni dogodek, ki je elipsa ali krog, kot sledi:

osnovni dogodek

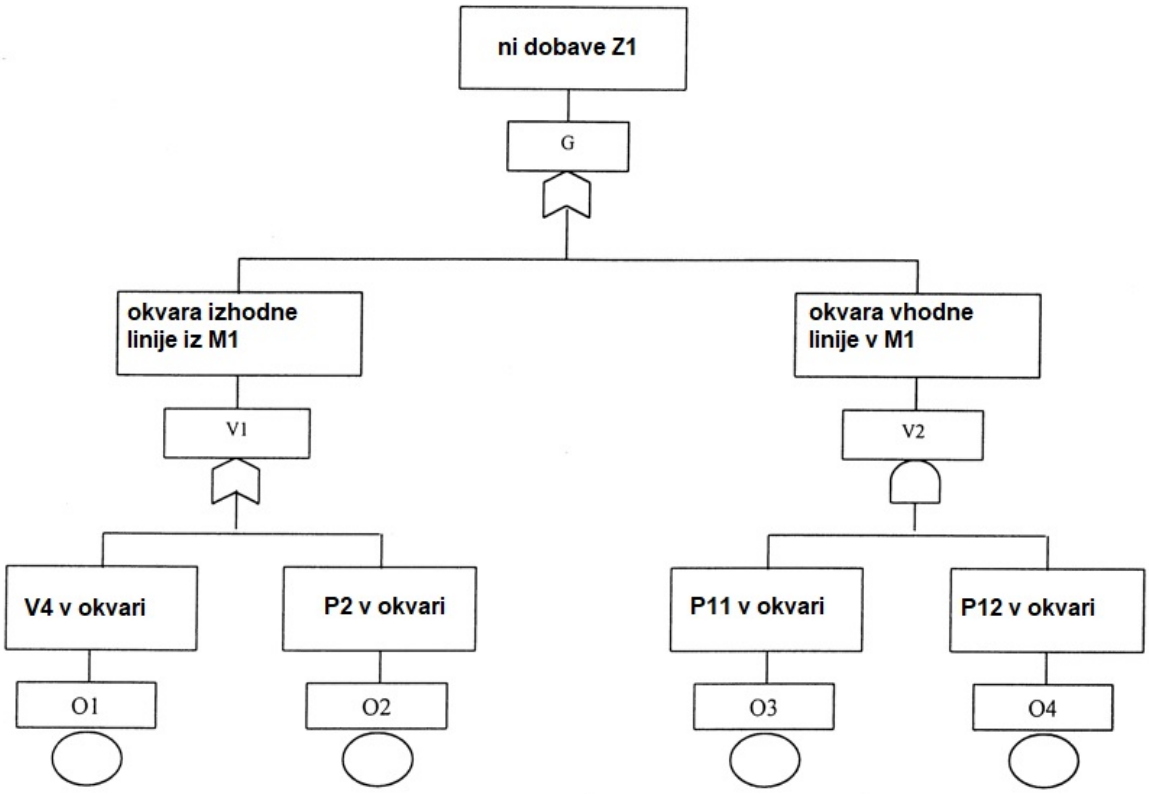
V tehniki dreves odpovedi je najti še več simbolov[52], a za naš primer bodo ti zadostovali.

Slika 19 v nadaljevanju prikazuje modificirano postrojenje slike 1 z redundanco črpalk, slika 18 pa enostavno shemo drevesa odpovedi za nekatere od morebitnih dogodkov.

[52] Fault Tree Analysis, Reliability Block Diagrams and BlokSim, prispevek na strani https://www.reliasoft.com, vir: https://www.reliasoft.com/resources/resource-center/fault-tree-analysis-reliability-block-diagrams-and-blocksim



Slika 19: Primer postrojenja z redundanco črpalk



Slika 20: Drevo odpovedi za del funkcij redundantnega postrojenja

Slika 20 prikazuje glavni dogodek, ko ni dobave Z1. Ta je z vrati ALI povezan z dvema možnostma: linija, ki vodi iz M1, ne deluje ali pa linija, ki vodi v M1, ne deluje. Linija, ki vodi v M1, ima dve neodvisni črpalki. Da ne deluje, morata obe odpovedati. Linija, ki vodi iz M1, pa ima eno črpalko in vsaj en ventil. Če katerikoli od teh elementov odpove, linija ne deluje.

Z G, V1, V2, in O1 do O4 so prikazane verjetnosti pojava posameznih dogodkov.

3.4.3 Potek in posamezni koraki FTA-analize

Potek postopka FTA-analize in opis posameznih korakov [16, 23]:

Korak 1: Opis sistema

Zapis prvega koraka je zelo pomemben del v sestavi drevesa, ker z njim na razumljiv in natančen način obrazložimo vzroke za neželene dogodke. Zato je pomembno, da dobro poznamo delovanje procesa in v tej povezavi poznamo še:

- podrobno shemo procesne regulacije in nadzorno-varnostnih sistemov,
- obratovanje in delovanje procesa (npr. redno obratovanje, vzdrževalna dela),
- strokovna izhodišča procesnih tokov (npr. mehanika tekočin, termodinamika),
- fizikalno-kemijske pojave v nekem procesu,
- nevarne lastnosti snovi,
- dejavnike okolice ipd. [20, 23].

V našem konkretnem primeru smo postavili logično povezavo vhodne in izhodne linije ter ugotovili, da Z1 ne bo dobavljena, če ne bo delovala bodisi vhodna bodisi izhodna linija.

Korak 2: Identifikacija nevarnosti

Pri identifikaciji nevarnosti se lahko uporabi npr. postopek HAZOP. Namen koraka 2 je v identifikaciji najpomembnejših neželenih dogodkov, ki bodo umeščena na vrhu drevesa odpovedi in se jih bo nadalje razvijalo. Razvoj drevesa odpovedi je v večjem obsegu zamuden, zato se priporoča od 10 do 20 neželenih dogodkov [20 ,24].

Korak 3: Razvoj drevesa odpovedi

Razvoj drevesa odpovedi je zelo kreativen korak (naloga), saj ni generalnih pravil, katera logična vrata in vmesne dogodke naj vključimo. Pravilna in kvalitativna postavitev drevesa je zatorej popolnoma odvisna od izvajalca analize. Drevo odpovedi se postavlja od vrha proti dnu. Na vrhu drevesa je vedno neželeni dogodek (npr. izpust kemikalij, eksplozija ipd), za katerega ni moč pridobiti ali oceniti verjetnosti nastanka odpovedi iz zgodovinskih virov in strokovnih baz. Za ta dogodek se nato na osnovi logičnih vrat iščejo konkretni in kvalitativni vzroki nastanka dogodka, vse dokler ne pridemo do osnovnega dogodka, za katerega lahko ocenimo verjetnost nastanka napake ali dogodka. Primeri osnovnih dogodkov v zgoraj prikazanem procesu so odpoved črpalke, odpoved ventila, zlom cevi, porušitev rezervoarja, porušitev mešalne posode itd.

Korak 4: Boolova redukcija ali iskanje minimalnih poti v drevesu odpovedi [31]

Po razvoju drevesa odpovedi se natančno analizira njegova struktura z namenom čim boljšega razumevanja, kako odpoved nastane. Naknadno je potrebno in pomembno raziskati tudi odpovedi, ki lahko nastanejo na osnovi skupnega vzroka (npr. odpoved ene od črpalk, pri čemer jih je npr. pet od istega proizvajalca, tako da gre predpostaviti, da lahko odpovedo tudi druge [31]) [20]. Pri tem pa je treba poudariti, da so posamezni dogodki v drevesu odpovedi med seboj neodvisni[53] [31].

Korak 5: Kvantitativna analiza drevesa

Zadnji korak obravnavanega postopka predstavlja kvantitativna analiza drevesa odpovedi, kjer na osnovi pogostosti nastanka neželenega dogodka v preteklosti izračunamo verjetnost neželenega glavnega dogodka [16, 20].

Najprej se oceni oz. iz dostopnih virov poišče verjetnost pojava vseh osnovnih in neraziskanih dogodkov, nato na osnovi Boolove algebre izračunamo verjetnost dogodkov.

[53] Rausand, M., Chapter 3 and 4: Fault Tree Analysiss, RAMS Group, NTNU – Trondheim, Wiley, 2004, vir: https://www.ntnu.edu/documents/624876/1277590549/chapt03-fta.pdf/c2e449ab-3221-472c-b3d7-3310942ee511

Za logična vrata ALI uporabimo enačbo:

$p_{ALI} = p1 + p2 – (p1 \times p2)$
p_{ALI} – verjetnost dogodka, če vrata povezujejo dva dogodka
$p_{ALI2} = 1-[(1-p1)x \ldots \ldots (1-pn)]$
p_{ALI2} – verjetnost dogodka, če vrata povezujejo »n« dogodkov

Za logična vrata IN uporabimo enačbo:

$p_{IN} = p1 \times p2x \ldots \ldots pn$
p_{IN} – verjetnost dogodka

Pri tem posamezno verjetnost dogodka izračunamo tako, da upoštevamo čas misije. Če gre za trajno obratovanje (torej nas ne zanimajo dogodki, ki zahtevajo pojav na zahtevo) in je čas misije enak, lahko izračune opravimo kar s pogostostjo odpovedi (λ); tako je opravljen tudi izračun v dodatku. V splošnem pa bomo seveda izračunavali verjetnost.

Pri izračunu verjetnosti glavnega dogodka se uporabi pristop *line-to-line*. Obstajajo tudi drugi kompleksnejše postopki, ki pa se uporabljajo za zelo velika drevesa odpovedi. Po postopku začnemo izračune na dnu drevesa in nadaljujemo proti vrhu. Vsi vhodi na logična vrata morajo biti predhodno definirani, da lahko izračunamo izhod. Sočasno pa morajo biti definirana vsa nižja vrata, preden nadaljujemo na višji nivo [16, 20, 23, 24].

Pri pregledu slike 20 lahko ugotovimo, da Z1 ne bo dobavljena, če se bo zgodilo eno od naslednjega:

- odpoved P11 in P12,
- odpoved V4,
- odpoved P2.

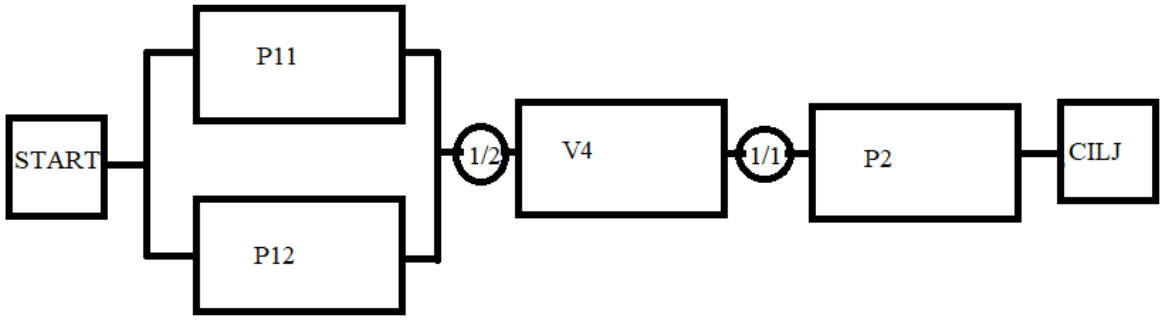
To so hkrati minimalne poti odpovedi.

Te poti odpovedi lahko prikažemo tudi v obliki blokovnih diagramov; o tem več v nadaljevanju.

3.5 Drevesa dogodkov in blokovni diagrami

Čeprav se analiza drevesa odpovedi večinoma uporablja za kalkulacijo sistemskih napak, obstajata še dve alternativni tehniki. To sta analiza drevesa dogodkov (ETA[54]) in postopek blokovnih diagramov. Vsi trije postopki uporabljajo enak matematični princip, tj. Boolovo algebro. Vse tri tehnike morajo dati enake numerične odgovore na enak problem. Razlike med njimi so v analitikovem načinu vizualizacije (prikaza) vodstvu in sodelavcem ter načinu razumevanja in interpretiranja rezultatov [9].

Poglejmo najprej blokovni diagram. Blokovni diagram je logični prikaz serije gradnikov, ki predstavljajo »ovire« v logični povezavi. Konkretno bi bil za obravnavan primer blokovni diagram videti takole:



Slika 21: Blokovni diagram primera

Potek je od leve proti desni. Številke v krogu pomenijo, koliko blokov mora biti prehodnih, da je pogoj izpolnjen. V konkretnem primeru mora delovati bodisi P11 bodisi P12, torej 1 od 2, delovati mora V4 v celoti, prav tako pa mora biti prepusten zadnji blok.

Blokovne diagrame lahko neposredno spremenimo v funkcije Boolove algebre, npr.

Uspeh = (P11∨P12)∧V4∧P2

Vrednost funkcije Uspeh vrne 1, če so 1 P11 ali P12 ter hkrati V4 ter hkrati P2, to je kriterij uspeha.

[54] ETA – analiza drevesa dogodkov (angl. *Event Tree Analysis*)

Kot alternativa postopkoma drevesa odpovedi in drevesa dogodkov lahko blokovni diagram uporabimo tudi za kalkulacijo sistemskega tveganja. Glavna prednost tega postopka je ta, da ima blok diagram enak generalni koncept kot procesni blok diagram in je zaradi tega lažje razumljiv. To je še posebej pomembno, če je rezultate analize treba predstaviti ljudem, ki jim to področje analiz tveganja ni znano [23].

Drevesa dogodkov ocenjujejo možnost nezgode kot rezultat odpovedi posamezne naprave ali procesa, pri čemer je ta dogodek znan kot začetni dogodek. Gre za induktivni proces, pri katerem se razvijajo morebitne posledice. Začetni dogodek je dogodek, ki predstavlja neko aktivnost ali odpoved opreme, ki bo, če se z njo ne bo pravilno ravnalo, privedla do naslednjega koraka pri odpovedi celotnega sistema.

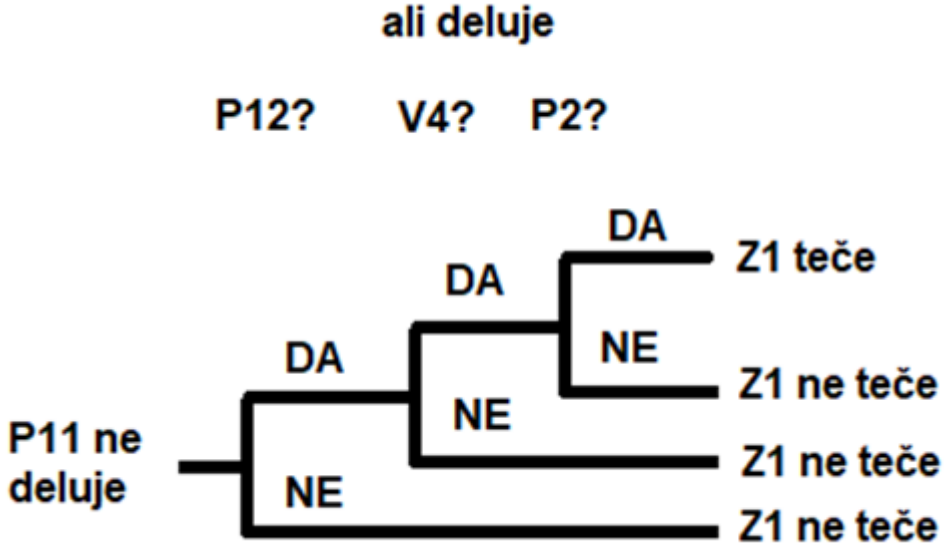
Začetni dogodek je torej dogodek, ki povzroči motnje v obratu in lahko vodi do poškodbe obrata, če upoštevamo uspešno delovanje različnih blažilnih sistemov v obratu ali ne. Začetni dogodek je torej incident, ki zahteva samodejno dejanje ali ukrep, ki ga sproži operater, da se obrat pripelje v varno in stabilno stanje, pri čemer lahko v odsotnosti takšnih ukrepov zaskrbljujoča stanja v obratu povzročijo resne poškodbe obrata. Začetni dogodki so običajno razvrščeni na notranje in zunanje iniciatorje, ki kažajo izvor dogodkov[55] [31].

Začetnemu dogodku sledi več takojšnjih akcij oz. aktivnosti, ki so načrtovane z namenom preprečitve ali zmanjšanja učinka začetnega dogodka, če je to potrebno. Drevo dogodkov se od začetnega dogodka razvije na dve veji – ena za uspešno oz. pravilno delovanje, druga za nepravilno delovanje. Dogovorjeno je, da zgornja veja predstavlja pravilno delovanja, spodnja pa nepravilno oz. odpoved.

Naš primer je prikazan na sliki 22. Tu imamo začetni dogodek (odpoved črpalke P11) in nato vmesne korake. Zgornje veje kažejo na delovanje sistema oziroma posameznega elementa, spodnje veje pa kažejo negativni odziv, ki povzroči sistemsko odpoved. V praksi bi za vsak naslov (P12, V4, P2) izdelali drevo odpovedi, da bi izračunali pogostost odpovedi za posamezen element (v splošnem pa gre za sisteme)[56] [31].

[55] PRA PROCEDURES GUIDE (NUREG/CR-2300): A Guide to the performance of Probabilistic Risk Assessments for Nuclear Power Plant. (vir prvega dela je https://www.nrc.gov/docs/ML0635/ML063560439.pdf, vir drugi dela pa je: https://www.nrc.gov/docs/ML0635/ML063560440.pdf

[56] Rausand M., Chapter 3: Event Tree Analysis, RAMS Group, NTNU – Tronmdheim, vir: https://www.ntnu.edu/documents/624876/1277590549/chapt03-eta.pdf/6f3e1b19-4824-4812-adc8-9762d2201c22



Slika 22: Drevo dogodkov za obravnavani sistem

Drevo dogodkov je zahtevna kvantitativna tehnika, ki zahteva dobro poznavanje sistema in predvsem zadostno mero inženirske natančnosti pri sledenju morebitnim scenarijem.

Kombinacija pristopa drevo dogodkov/drevo odpovedi se pogosto uporablja v nuklearni industriji.

Ker vsi trije poprej predstavljeni postopki uporabljajo enak matematični princip in ker je razlika predvsem v načinu razumevanja, je odločitev, kateri postopek v določeni situaciji izbrati, prepuščena uporabniku.

Univerzitetna založba
Univerze v Mariboru

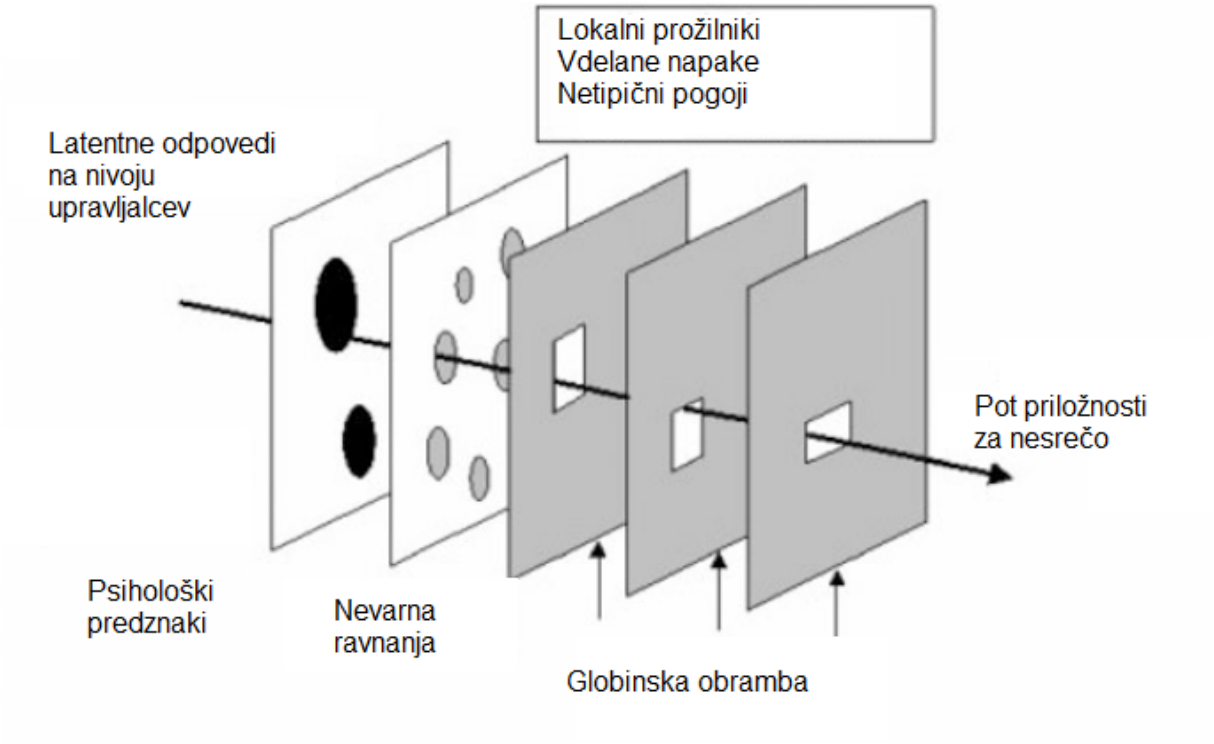
4 Ugotavljanje človeškega vpliva na varnost – človeška napaka

4.1 Stanje na področju analiz človeške zanesljivosti (HRA[57])

Sredi prejšnjega stoletja se je zgodil velik preobrat v miselnosti zasnove, izgradnje in vzdrževanja tehnoloških sistemov. Po letu 1940 je tehnološki razvoj dosegel stanje, v katerem je človek začel predstavljati omejitveni faktor pri celotnem delovanju nekega sistema [11].

[57] HRA – Analiza človeške zanesljivosti (angl. *Human Reliability Analysis*)

Na področju HRA je pomemben prispevek Jamesa Reasona[58], ki je razvil prikaz »ementalec« analize globinske obrambe pred človeškimi napakami:



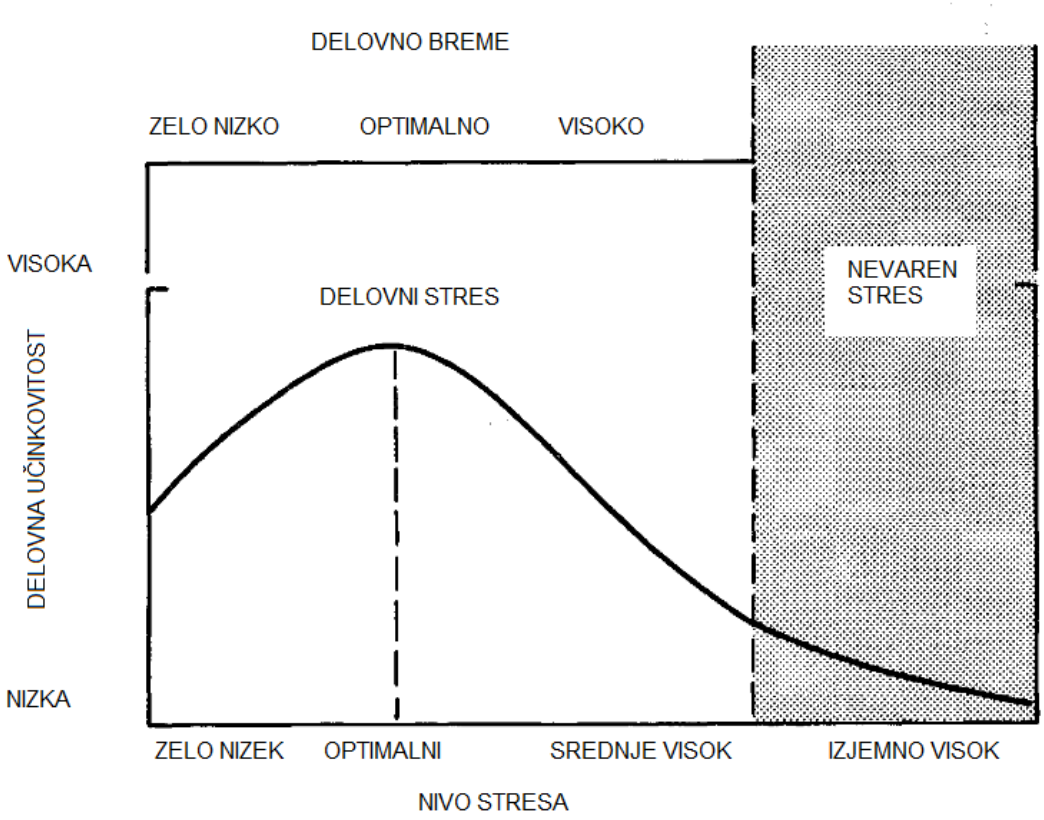
Slika 23: Prikaz »ementalec« analize globinske obrambe

Ta pojasnjuje, da obstaja možnost t. i. globinske obrambe pred človeškimi napakami kljub številnim pomanjkljivosti sistema, ki so videti kot ementalec (angl. *Swiss cheese*).

Začetek opisa tovrstnih metod je najti v uporabniškem priročniku oziroma pregledu postopkov HRA [59], kjer je najti sliko 24, ki zelo dobro opisuje povezavo med dejavniki stresa in odzivi nanj.

[58] Več o tem: Justin Larouzée. Human Error and Defense in Depth: From the "Clambake" to the "Swiss Cheese". Prof. Dr. Joonhong Ahn, Prof. Dr. Franck Guarnieri, Prof. Dr. Kazuo Furuta. Resilience: A New Paradigm of Nuclear Safety. From Accident Mitigation to Resilient Society Facing Extreme Situations , Springer International Publishing - Available under Open Access, pp. 257–267, 2017, Print ISBN 978-3-319-58767-7 Online ISBN 978-3-319-58768-4. 10.1007/978-3-319-58768-4_22. hal-01574818

[59] Swain, A.D., Guttman, H., Handbook of Human Reliability Analysis With Emphasis on Nuclear Power Plant Applications, https://www.osti.gov/servlets/purl/5752058 .



Slika 24: Povezava med dejavniki stresa in odzivi nanj

Dandanes najdemo sodobne tehnološke sisteme na vseh področjih, npr. proizvodnih, transportnih, zdravstvenih, finančnih in tudi administrativnih. S posodabljanjem sistemov nam le-ti omogočajo zmeraj nove možnosti in racionalnejšo izrabo virov. Možnosti posodabljanja tehnoloških sistemov za doseganje večjega učinka s težnjo po iskanju večjih donosov so neizmerne. Zaradi tega postajajo zmeraj bolj kompleksni in zahtevnejši glede na strukturo. Že desetletja nazaj je bilo jasno, da človeška dejanja v vsakodnevnem procesu predstavljajo glavnico dejanj v povezanem tehnološkem sistemu, ne glede na obseg in zahtevnost sistema, pri čemer povzročajo skrbi samo tista človeška dejanja, ki so napačna, zmotna ali neuporabna. V strokovni literaturi so takšna dejanja zapisana kot »človeška napaka«, kar bi lahko poimenovali tudi drugače: »človekova zmotna dejanja« [16].

Kvantitativnih podatkov s področja verjetnosti človeških napak je zelo malo. Razlog pomanjkljivosti obstoječih podatkov je v tem, da so zelo splošni in ne upoštevajo vrsto opravil, pogojev delovnega okolja ipd. V splošnem velja, da so verjetnosti pojava človeških napak bistveno večje od verjetnosti tehničnih napak [11].

Več virov navaja, da direktne in indirektne človeške napake predstavljajo kar 60–90 % vseh napak/odpovedi sistemov [10, 11]. Svetovni analitiki ocenjujejo, da nezgodam pri jedrskih centralah botruje človeški faktor v 50–70 %, pri letalskih nezgodah v najmanj 50 %, v procesni industriji pa je ta odstotek še višji [10]. V zadnjih desetletjih delež nezgod, katerih vzrok je človeška napaka, narašča. To ne pomeni, da povzročamo ljudje čedalje več napak, ampak da prihajajo s tehnološkim razvojem vedno bolj do izraza [11].

Prepoznava tveganj in nato reagiranje na tveganje je zaradi izjemne zapletenosti delovanja človeka zahtevna naloga. Reakcije ali odločitve so poleg splošnih lastnosti in izkušenj posameznika lahko odvisne tudi od veliko drugih zunanjih vplivov ter od trenutnega fizičnega in psihičnega stanja izbranega subjekta [10].

Večina današnjih tehnoloških sistemov je odvisna od interakcij z ljudmi, ki zagotavljajo nemoten proces. Pomembnost medsebojnega delovanja tehnoloških sistemov in človeka je bila še pred časom razpoznavna samo v delu pri izvajanju nadzora v večjih sistemih (nuklearna in letalska industrija), saj se je vsakdo zavedal katastrofalnih posledic za človeka in okolico. V praksi se je hitro izkazalo, da ta pomembnost ni omejena zgolj na nadzor, ampak je pomembna tudi v drugih dejavnostih, kot npr. proizvodnji, upravljanju, vzdrževanju itd. [16].

4.1.1 Prepoznavanje človeških napak

Raziskava vplivov človeških napak sega na več področij, pri čemer je potencial ali indeks vpliva na nastanek možnega pojava človeške napake v posameznih dejavnostih različen [11].

Nekateri strokovnjaki navajajo, da ima človeško zmotno ravnanje pri celoviti izvedbi nekega procesnega okolja ali naprave največji vpliv v dejavniku nepravilnega obratovanja (35 %), projektiranja (30 %), izvajanja (20 %) in vzdrževanja (15 %) [16].

Človeški dejavnik ima že v fazi izdelave osnutka novega sistema velik vpliv na zanesljivost in varnost delovanja sistema. Zato je treba identificirati morebitne nevarnosti, ki lahko vplivajo na življenjsko dobo in porušitev sistema.

Človeško zmotno ravnanje ima pomemben vpliv na zanesljivost tudi pri izvedbi projekta, in sicer zaradi neustreznega porekla izdelkov, neustrezne izvedbe postavitve, npr. tehnološke opreme, neustreznega pregleda ipd.

Dejavnik, ki je najbolj občutljiv na človeško zmotno ravnanje, je način obratovanja. To je zagotovo faza, v kateri lahko človeško zmotno ravnanje povzroči takojšni nastanek napake (začasna ali kontinuirana prekinitev). Zmotno ravnanje lahko nastane zaradi nepravilnega izvajanja postopkov, izvajanja nadzora, zagotavljanja varnostnih ukrepov ipd. [16].

Neustrezno vzdrževanje je tudi eden izmed dejavnikov, ki posledično vpliva na zmanjšanje zanesljivosti samega sistema. Zato lahko človeški faktor odločujoče vpliva na vrsto opravil v vzdrževalnem ciklusu [11].

4.1.2 Verjetnostna analiza

Ker je v praksi za ugotavljanje vpliva človeške napake, celo za enostaven sistem, nemogoče izvesti deterministično analizo, uporabimo analizo verjetnosti (angl. *Probabalistic Analysis*), pri čemer iščemo povezave med pomembnejšimi vzroki in pomembnejšimi posledicami.

Glavna cilja verjetnostne analize sta:

1. zmanjšati verjetnost do te mere, da se napaka ne pojavi,
2. minimalizirati posledice neželenih motenj oz. situacij.

Če želimo vnaprej predvideti morebitne odpovedi sistema, moramo iz preteklih izkušenj vedeti, kaj je temu lahko vzrok, ali identificirati načine, pod katerimi se lahko pojavijo motnje, upoštevajoč, kako je bil sistem vzpostavljen.

Analiza človeške zanesljivosti (HRA) zajema predpostavko, da človeški faktor lahko v nekem sistemu odpove. Leta 1990 je Ed Dougherty zraven analize človeške zanesljivosti prve generacije (klasični postopek) predstavil tudi analizo HRA druge generacije (moderni postopek oz. CREAM – Cognitive[60] Reliability and Error Analysis Method) [11].
Obe sta podrobneje predstavljeni v nadaljevanju.

Večina pristopov HRA prve generacije temelji na naslednjem postopku: analiza najprej prikaže razliko med uspešnimi in neuspešnimi procesi nekega sistema, nakar se za vsakega od njih izračuna verjetnost napake (glavni cilj). Če redno izvajamo te kalkulacije, se je treba ozirati na sistemske napake, ki so se že zgodile v preteklosti, in jih upoštevati. Ta opis se

[60] Cognition – spoznati/poznati oz. izraz pomeni, da če želiš razumeti sposobnost nekega človeka, moraš (s)poznati njegovo znanje, izkušnje, čutenja.

nanaša na model zanesljivosti[61], ki predstavlja poznavanje določenega sistema in je v primeru analize človeške (ne)zanesljivosti to človek [9]. To je razvidno tudi s slike 25.

Slika 25: Vloga modela zanesljivosti [9]

4.2 Analiza človeške zanesljivosti – HRA prve generacije

Izhodišča analize človeške zanesljivosti – HRA prve generacije so bila predstavljena v prejšnji točki, zato smo se v nadaljevanju osredotočili predvsem na različne pristope oz. postopke te analize.

Trenutno obstaja okrog 35–40 kvalitetnih HRA-postopkov, pri čemer pa lahko predvidevamo, da nekateri postopki uporabljajo identične pristope in bi bilo zaradi tega realno število postopkov manjše [11].

4.2.1 Postopki HRA prve generacije

Večina postopkov analize človeške zanesljivosti je bila razvitih okrog leta 1980, pri čemer v nadaljevanju navajamo le nekatere najpogosteje uporabljene [11]:

Analiza preiskave nesreče in progresije (AIPA[62])

Tehnika te analize temelji na določitvi verjetnosti, če bi se neka aktivnost izvedla, glede odziva operaterja sistema. Ta postopek je prejšnja verzija postopka *Time-Reliability-Correlation*.

[61] Model zanesljivosti (angl. *reliability model*)
[62] AIPA – Accident Investigation and Progression Analysis

Matrika zmede (angl. *Confusion Matrix*)
Tehnika matrike zmede je uporabna za določevanje verjetnosti operaterjevega napačnega ocenjevanja začetnega dogodka. Matrika zmede zajema običajno vse aktivnosti vseh faz dogodka, ki dopolnjujejo avtomatsko delovanje sistema, izključuje pa akcije zunaj ustaljenega delovanja sistema, kot so napake, narejene v času testiranja, in aktivnosti vzdrževanja.

Drevo akcije operaterja (OAT[63])

Drevo akcije operaterja temelji na premisi, da je lahko reakcija na dogodek opisana v treh stopnjah:

1. opazovanje ali beleženje dogodka,
2. diagnosticiranje ali razmišljanje o dogodku,
3. reagiranje na dogodek.

Napake, ki bi lahko nastale v tretji fazi, niso najpomembnejše. Primarna skrb mora biti posvečena napakam, ki lahko nastanejo v drugi fazi, tj. med diagnosticiranjem. Postopek je skoncentriran na verjetnosti, da operater pravilno oceni napako in določi akcije, ki so nujne za delovanje sistema [28].

Sociološko-tehnična presoja človeške zanesljivosti (STAHR[64])

Postopek se na mnogo načinov razlikuje od drugih postopkov analize človeške zanesljivosti. Predstavlja postopek presoje človeške zanesljivosti v kompleksnem tehničnem sistemu in se sestoji iz tehnične in socialne komponente. Tehnična komponenta je diagram, ki kaže vzroke in efekte, ki povežejo faktorje do izhodne situacije. Socialna komponenta teži k spodbujanju soglasja skupine in presoje strokovnjakov o vplivu različnih pogojev na verjetnost.

[63] OAT – Operator Action Tree
[64] STAHR – Socio-Technical Assessment of Human Reliability

Tehnika za napoved velikosti človeške napake (THERP[65])

Namen te tehnike je izračun verjetnosti uspešne izvršitve več aktivnosti, ki so bile potrebne za izpolnitev naloge. Izračuni temeljijo na predhodno določeni velikosti napake. Rezultat je definiran kot dopolnilo k verjetnosti nastanka napake. Tehnika vključuje izdelavo analiz za določitev karakteristik izvršitve človeških nalog, ki so analizirane.

Ocena eksperta (angl. *Expert Estimation*)

Ocene eksperta se poslužujejo strokovnjaki presojevalci za določevanje verjetnosti človeške napake v nekem sistemu.

Zanesljivost človeške kognitivnosti (HCR[66])

Postopek ustreza namenu kvantifikacije časovno odvisnih verjetnosti operaterja v kontrolni sobi, ki reagira v primeru nesreče. Ime postopka, zanesljivost človeške kognitivnosti, kaže na tri različne tipe »kognitivnega oplemenitenja«, ki se nanašajo na spretnost, pravila in znanje.

Simulacija vzdrževanja učinkovitosti zaposlenih (MAPPS[67])

Računalniški model MAPPS je bil razvit z namenom analiziranja vzdrževalnih aktivnosti zaposlenih v nuklearnih elektrarnah. Namen modela je zagotavljati zanesljive podatke vzdrževalnih aktivnosti zaposlenih za analizo zanesljivosti procesov[68] [11].

4.2.2 CREAM[69] postopek – HRA druge generacije

V prejšnjih točkah smo prikazali osnovne principe postopkov človeške zanesljivosti, ki se uporabljajo za analiziranje obstoječega stanja nekega sistema ali pa za ugotavljanje verjetnosti nastanka napak sistema. Večina strokovnjakov tega področja navaja, da je bila HRA-postopek prve generacije razvit z namenom dajanja hitrih praktičnih odgovorov situacije sistema, čeprav zanesljivost rezultatov varira.

---

[65] THERP – Technique for Human Error Rate Prediction
[66] HCR – Human Cognitive Reliability
[67] MAPPS – Maintenance Personnel Performance Simulation
[68] PRA – analiza zanesljivosti procesov (angl. *Performance Reliability Analysis*)
[69] CREAM – Cognitive Reliability and Error Analysis Method

Postopek CREAM/postopek kognitivne (spoznavne) zanesljivosti in analize odpovedi je bil razvita na podlagi principov modelov analiz merjenja človeške zanesljivosti – HRA prve generacije. Osnovni princip pri razvoju tega postopka predstavlja praktični pristop do analize učinkovitosti (PA[70]) in analize verjetnosti ter je popolnoma dvosmeren (angl. *bi-directional*). To pomeni, da je enak princip lahko uporabljen tudi za retrogradno analizo, in sicer pri iskanju vzrokov in napovedovanju učinkov sistema [11].

Uporablja se na več različnih načinov [2]:

- kot samostojna analiza, in sicer za retrospektivne ali prospektivne analize,
- kot del večjega postopka načrtovanja kompleksnih, interaktivnih sistemov,
- kot HRA v okviru celostne varnostne analize (ISA[71]) ali verjetnostno varnostne analize (PSA[72]).

Za pravilno uporabo in izvedbo postopka CREAM je treba dobro poznati obravnavani primer (proces, napravo ipd.), vključno s podrobnejšimi informacijami, parametri, načini delovanja ipd. [2].

Tehnika CREAM uporablja pristop h kvantifikaciji z dveh ravni, pri čemer lahko rečemo, da poznamo dva postopka kognitivne zanesljivosti in analize odpovedi:

1. osnovni CREAM-postopek
   (angl. *Basic Cognitive Reliability and Error Analysis Method*),
2. razširjeni CREAM-postopek
   (angl. *Extended Cognitive Reliability and Error Analysis Method*).

Postopka sta povzeta po Hollnagelu [11] in sta v nadaljevanju v osnovi predstavljena, podrobneje pa med izvedbo analize.

[70] PA – Performance Analysis
[71] ISA – Integrated Safety Analysis
[72] PSA – Probabilistic Safety Analysis

4.3.1 Programska podpora

V okviru našega preverjanja razpoložljivih/obstoječih programskih orodij za izvedbo CREAM-analize smo ugotovili, da slednje obstaja in se imenuje CREAM Navigator [19]. Orodje CREAM Navigator že omogoča izdelavo osnovnih analiz z nekaj osnovnimi dogodki (bazirano na nekaj primerih testiranja), vendar zaenkrat zgolj za demonstracijske namene, saj je razvoj slednjega še vedno v polnem teku [19]. Čez nekaj let pa najverjetneje lahko pričakujemo preverjeno in polno delujoče programsko orodje, ki bo bistveno olajšala delo izvajalcu CREAM-analize.

Pri manjših sistemih se lahko izvedbe analize lotimo ročno, kar je koristno tudi, če želimo izdelati referenčni primer za upravljalce kompleksnih sistemov oz. za njih v praksi uporabno metodologijo analiziranja manjših sistemov s stališča njihove varnosti in zanesljivosti.

4.3.2 Osnovni postopek CREAM

Namen osnovnega postopka CREAM[73] je določitev ocene izvedbene zanesljivosti za določeno nalogo oz. aktivnost. Ocena je izražena z osnovnim dejanjem verjetnosti napake, npr. ocena verjetnosti izvedbe nepravilnega dejanja za celotno nalogo. Ta podaja prvo projekcijo naloge, in to za celotno nalogo ali za posamezne glavne odseke naloge.

Projekcija se lahko uporabi za odločitev dejanja. Z njo npr. ugotovimo, ali je pri določenem segmentu nalog ali pri specifičnih dejanj treba nadaljevati s podrobno analizo.

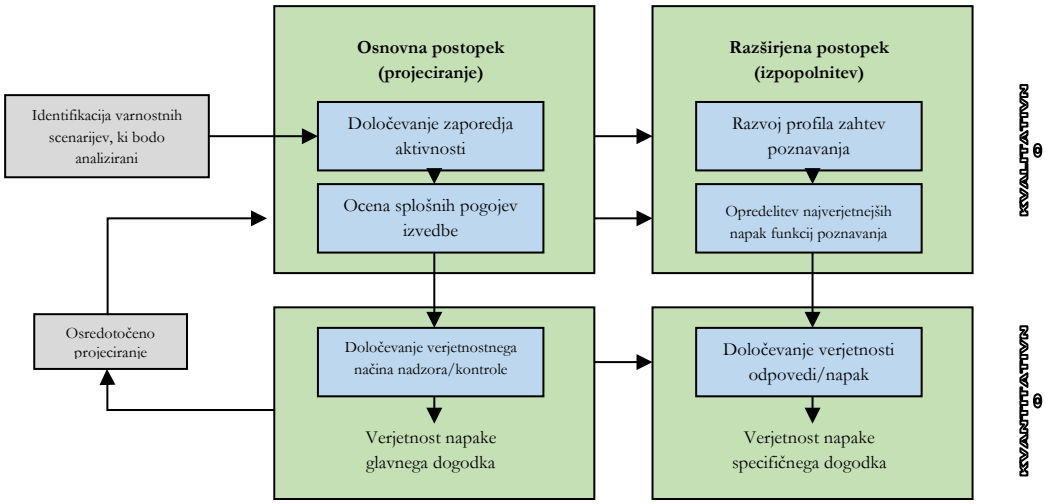
Osnovni postopek je uporaben predvsem za hitro, pavšalno oceno reda velikosti napake in je sestavljen iz naslednjih *treh korakov* [11, 28]:

1. določevanje zaporedja aktivnosti (opis naloge/dela naloge, ki se analizira),
2. ocena splošnih izvedbenih pogojev/pogojev izvedbe (CPC[74]),
3. verjetnostni način nadzora/kontrole (COCOM[75]).

[73] Osnovni CREAM-postopek (angl. *Basic Cognitive Reliability and Error Analysis Method*)
[74] CPC – Common Performance Conditions
[75] COCOM – Cognitive Control Model

Med osnovnim postopkom CREAM in drugimi projekcijskimi postopki obstajata dve večji razliki. Prva je karakteristika situacije, ki lahko vpliva na izvedbo in predstavlja izhodiščno stanje za ocenitev zanesljivosti skupaj z analizo nalog. Zanesljivost ali verjetnost napake posameznega dejanja se upošteva, kadar je situacija kot celota primerno opisana. Druga karakteristika predstavlja projekcijo, ki se nanaša na eksplicitni, običajno enostavni in poznavalni model. Ta model predstavlja temeljni princip za rezultate [11, 28].

Za lažje razumevanje zgoraj navedenega je v pomoč shematski prikaz poteka obeh postopkov – osnovnega in razširjenega CREAM-postopek (v nadaljevanju).



Slika 26: Shematski prikaz poteka postopkov osnovnega in razširjenega CREAM-postopka [11]

4.3.3 Razširjeni CREAM-postopek

Razširjeni CREAM-postopek[76] uporablja kot vhodne podatke izhodišča/rezultate osnovnega CREAM-postopka. Njen namen je določiti verjetnosti napake za vsako posamezno akcijo oz. dogodek upravljalca (operaterja). Uporablja se, kadar je verjetnost nastanka človeške odpovedi/napake po osnovnem CREAM-postopku enaka (oziroma večja) od verjetnosti nastanka tehnične odpovedi/napake.

Razširjeni CREAM-postopek zajema naslednje stopnje:

1. določevanje aktivnosti poznavanja ter razvoj profila zahtev poznavanja,
2. opredelitev najverjetnejših napak funkcij poznavanja,
3. določevanje verjetnosti odpovedi/napak posameznega specifičnega dogodka [11, 28].

[76] Razširjen CREAM-postopek (angl. Extended Cognitive Reliability and Error Analysis Method)

Nadaljnja teoretična izhodišča tako za osnoven kot za razširjen CREAM-postopek so navedena v nadaljevanju tega dela, in sicer med izvedbo analize.

Univerzitetna založba
Univerze v Mariboru

Seznam uporabljenih virov

[1] CPR – Committee for the Prevention of Disasters. *PGS 3 edition – Guidelines for quantitative risk assessment : CRP18E "Purple Book"*. Hague : Committee for the Prevention of Disaster. 2005.

[2] *CREAM (Cognitive Reliability Error Analysis Method)* [svetovni splet]. Wikipedia. Dostopno na WWW: https://en.wikipedia.org/wiki/CREAM [21.3.2016].

[3] Djeddou Messaoud. *Rate failure prediction in Wastewater Treatment Plant using Artificial Neural Networks*. Biskra : Mohamed Kheider University of Biskra, 2014

[4] *Edraw Max - Proffesional All-In-One Visualization Software* [svetovni splet]. *Edraw Visualization Solutions*. Dostopno na WWW: http://www. edrawsoft.com/ [21. 1. 2015].

[5] *ELSEVIER - World leading, multiple-media publisher of scientific, technical and health information products and services* [svetovni splet]. Reed Elsevier Group plc.. Dostopno na WWW: http://www.elsevier.com/wps/ [14. 9. 2014].

[6] Terje Aven: Risk assessment and risk management: Review of recent advances on their foundation, European Journal of Operational Research, Vol. 253, pp 1–13, 2016 https://doi.org/10.1016/j.ejor.2015.12.023

[7] Flemish government. *Background information : Appendix to Handbook failure frequencies 2009, for drawing up a safety report*. Brussel : Flemish Government, LNE Department, Environment, Nature and Energy Policy Unit, Safety Reporting Division

[8] Flemish government. *Handbook failure frequencies 2009, for drawing up a safety report*. Brussel : Flemish Government, LNE Department, Environment, Nature and Energy Policy Unit, Safety Reporting Division

[9] Fras Matjaž. *Izgradnja infrastrukture Centralne Čistilne Naprave Dogoše-Maribor s koncesijo po BOT modelu : diplomsko delo*. Maribor : Fakulteta za strojništvo, 2001.

[10] Fras Matjaž. *Postopki določevanja verjetnosti tehnične in človeške napake v procesni tehniki : seminarska naloga pri predmetu Varnost in zanesljivost v procesni tehniki*. Maribor : Fakulteta za strojništvo, 2006.

[11] Gspan Primož. *Analiza in presoja varnosti pri delu*. Ljubljana : Zavod Republike Slovenije za varstvo pri delu, 1996.

[12] Hollnagel Erik. *Cognitive reliabilitv and error analysis method*. Halden : Institutt for Energiteknikk, Elsevier Science, 1998.

[13] HSE – health and Safety Executive Gov.UK. *Failure Rate and Event Data for use within Risk Assessments (28/06/2012)*. Merseyside : HSE, 2012

[14] *IDRO – Soluzioni per l'ambiente* [svetovni splet]. Idrodepurazione Srl.. Dostopno na WWW: http://www.idro.net/ [27. 9. 2014].

[15] *IDRO – Soluzioni per l'ambiente. Wastewater Treatment Plants : Internal documentation*. Seregno : Idrodepurazione Srl., 2014.

[16] *Integrated Reliability Engineering software* [svetovni splet]. ISOGRAPH. Dostopno na WWW: http://www.isograph-software.com/ [17. 4. 2014].

[17] Koletnik Dejan. *Analiza vpliva človeške napake na zanesljivost slovenskega prenosnega omrežja zemeljskega plina : magistrsko delo*. Maribor : Fakulteta za strojništvo, 2006.
[18] Korošec Goran. *Kanalizacija v delu naselja Plintovec : diplomsko delo*. Maribor : Fakulteta za gradbeništvo, prometno inženirstvo in arhitekturo, 2010.
[19] Muhlbauer W. Kent. *Pipeline Risk Management Manual : Ideas, Techniques and Resources - third edition*, Oxford : Elsevier Inc., 2004.
[20] Murthy Mahesh, Serikova Nellya. Selection of failure frequency and its impact on risk assessment – A case study from plot plan optimisation. *Journal of Loss Prevention in the Process Industries* (2016), vol. 10.1016/j.jlp.2016.05.001.
[21] Novak-Pintarič Zorka. *Varnost kemijskih procesov : zbrano gradivo*. Maribor : Fakulteta za kemijo in kemijsko tehnologijo, 2005.
[22] Servwy Roger. CREAM Navigator : software tool under development [svetovni splet]. Illinois : University of Illinois at Urbana-Champaign. Dostopno na WWW: http:// http://www.ews.uiuc.edu/~serwy/cream/ [19. 5. 2016].
[23] SINTEF Industrial Management. *OREDA – Offshore Reliability Data Handbook : 4th Edition*. Trondheim : Det Norske Veritas, 2002.
[24] Sutton S. Ian. *Process Reliability and Risk Management*. New York : Van Nostrand Reinhold, 1992.
[25] Sutton S. Ian. *Process Risk and Reliability Management, Second Edition*. Oxford : Elsevier Inc., 2015.
[26] Taheriyoun Masoud, Moradinejad Saber. *Reliability analysis of a wastewater treatment plant using fault tree analysis and Monte Carlo simulation : Environ Monit Assess 187:4186*. Switzerland : Springer International Publishing, 2014.
[27] Uradni list RS št. 64/2012. *Uredba o emisiji snovi in toplote pri odvajanju odpadnih voda v vode in javno kanalizacijo* [svetovni splet]. Uradni list RS. Dostopno na WWW: http://www.uradnilist.si/1/content?id=109650 [25. 11. 2015].
[28] Uradni list RS št. 98/2007. *Uredba o emisiji snovi pri odvajanju odpadne vode iz malih komunalnih čistilnih naprav* [svetovni splet]. Uradni list RS. Dostopno na WWW: http://www.uradnilist.si/1/objava.jsp?urlid=200798&stevilka=4857 [24. 11. 2015].
[29] Zupančič Janja. *Varnost in zanesljivost rektifikacijske kolone plina : magistrsko delo*. Maribor : Fakulteta za strojništvo, 2002.
[30] Fras. Matjaž. *Varnost in zanesljivost čistilne naprave : magistrsko delo. Maribor*: [M. Fras], 105 f., ilustr. https://dk.um.si/IzpisGradiva.php?id=60004. [COBISS.SI-ID 20166934], 2016.
[31] Kožuh, Mitja. Osebna komunikacija, 2021.

VARNOST IN ZANESLJIVOST V OKOLJSKI TEHNIKI

JURE MARN, MATJAŽ FRAS IN JURIJ ILJAŽ
Univerza v Mariboru, Fakulteta za strojništvo, Maribor, Slovenija.
E-pošta: jure.marn@um.si, matjaz.fras@um.si, jurij.iljaz@um.si

Ključne besede:
varnost,
zanesljivost,
okoljska tehnika,
procesna tehnika,
drevesa odpovedi

Povzetek Delo predstavlja prvi pogled v varnostno kulturo, zlasti varnost in zanesljivost v okoljski tehniki in širše. Predstavljeni so osnovni koncepti kot so varnost, zanesljivost, tveganje, odpovedi, napake in osnovni mehanizmi za njihovo analizo kot so drevesa odpoved in drevesa dogodkov.

Univerzitetna založba Univerze v Mariboru
DOI https://doi.org/10.18690/978-961-286-477-4
ISBN 978-961-286-477-4

SAFETY AND RELIABILITY IN ENVIRONMENTAL ENGINEEERING

JURE MARN, MATJAŽ FRAS & JURIJ ILJAŽ
University of Maribor, Faculty of Mechanical Engineering, Maribor, Slovenia.
E-mail: jure.marn@um.si, matjaz.fras@um.si, jurij.iljaz@um.si

Keywords:
safety, reliability, environmental engineering, process engineering, fault trees

Abstract This work represents first view into safety culture, in particular safety and reliability in the area of environmental engineering, and wider. Basic concepts such as safety, reliability, risk, failure, error and basic mechanism for their analysis such as fault tree and event tree are discussed.

DOI https://doi.org/10.18690/978-961-286-477-4 ISBN 978-961-286-477-4
University of Maribor Press

Univerza v Mariboru

Fakulteta za strojništvo