Standarda SIST ISO/IEC 31000 in SIST ISO/IEC 31010

Standarda SIST ISO/IEC 31000:2011 in 31010:2011 se nanašata na procesno varnost, ker pa sta procesna varnost ter varnost in zdravje pri delu med seboj soodvisni, sta standarda pomembna tudi za stroko varnosti in zdravja pri delu.

Avtor:
Primož Gspan
Na jami 11
Ljubljana

Uvod

Osnovni standard SIST ISO/IEC 31000:2011 Obvladovanje tveganj – Načela in smernice za obvladovanje tveganja obravnava splošna načela in principe uveljavljanja varnosti, in ker je v slovenščini, vsebuje tudi posebej slovensko izrazje s področja varnosti. Njemu podrejen standard SIST ISO/IEC 31010:2011 Obvladovanje tveganj – Tehnike obvladovanja tveganja navaja načine izvajanja in tehnike zagotavljanja varnosti. Ker sta procesna varnost in varnost zaposlenih funkcionalno povezani, je smiselno opozoriti na vsebino tudi teh dveh standardov, ki sicer za uporabo pri nas nista obvezna, tako kot so obvezni predpisi s področja varnosti in zdravja pri delu.

Standarda SIST ISO/IEC 31000:2011 in 31010:2011

Organizacije vseh vrst in velikosti se srečujejo z notranjimi ali zunanjimi dejavniki, ki povzročajo negotovost, ali bodo in kdaj bodo doseženi postavljeni cilji. Vpliv te negotovosti na doseganje ciljev organizacije je tveganje. Pri vodenju dejavnosti je zato treba že pri zasnovi in nadalje med delovanjem obvladovati in zagotoviti »procesno varnost« in pri deviacijah od začrtanega poteka usmerjati dejavnost proti zastavljenim ciljem. Standard SIST ISO/IEC 31000:2011[1] je temeljni standard o tveganjih za odstopanja od predvidenih ciljev. Dopolnilni standard SIST ISO/IEC 31010:20112 pa obravnava predvsem postopke in tehnike za nadzorovanje tveganj.

Zakonodaja s področja varnosti in zdravja pri delu (v nadaljevanju: ZVZD–13) je na drugi strani usmerjena posebej na varnost in ohranitev zdravja pri delu (v nadaljevanju: VZD) in za zagotovitev delovne zmožnosti celo delovno dobo poklicnih izvajalcev dejavnosti, torej na zaposlene. ZVZD–1 nalaga generalno odgovornost za varnost in zdravje pri delu delodajalcu, od odgovornosti pa ne odvezuje niti zaposlenih. Kot temeljno orodje ZVZD–1 uvaja obvezno izjavo o varnosti z oceno

tveganja (v nadaljevanju: IzVOT), ki jo v sodelovanju z zaposlenimi pripravi in jo odgovorno podpiše delodajalec.

Organizacija ima tudi druge cilje v okviru varnosti. Eden od njih je procesna varnost. Ta naj zagotavlja nemoteno delovanje sistema, kakovosten proizvod, ekonomsko in kompatitativno učinkovitost, visoko boniteto, varovanje okolja idr. Vsi ti cilji neposredno ali posredno vplivajo tudi na VZD udeleženih v dejavnosti. In obratno. Zato procesne varnosti sistema, ki je temeljni predmet obeh omenjenih standardov, ni mogoče obravnavati ločeno od VZD. Procesna napaka oziroma napaka v tehnološkem postopku lahko neposredno ali posredno vpliva tudi na VZD zaposlenega in obratno. Zato sta procesna varnost in varnost in zdravje pri delu posebna primera celovite (integralne) varnosti.

Od leta 2011 imamo v seznamu SIST-ov tudi slovenska standarda: SIST /IEC 31000:2011 Obvladovanje tveganj – Načela in smernice ter SIST ISO/IEC 31010:2011 Obvladovanje tveganj – Tehnike. Prvi je v slovenščini, drugi ni predviden za prevod v slovenski jezik.

Pomen obeh standardov so zlasti splošna načela za zagotavljanje varnosti, deloma tudi na parcialnih področjih, kot je VZD, in sistematičen pregled splošno priznanih postopkov in tehnik za obvladovanja tveganj. Na prvi, prevedeni standard, ki vsebuje tudi slovensko izrazje s področja varnosti in tveganj, se lahko sklicujemo tudi na področju VZD, da se izognemo včasih napačni rabi ali rabi nepreciznih slovenskih izrazov ali definicij, tudi v predpisih.

Oba standarda sta med seboj povezana, zato je nanju smiselno posebej opozoriti delavce s področja VZD. Razumljivo je, da v obsegu tega sestavka lahko samo grobo opozorimo na vsebino, za podrobnosti je treba standardoma nameniti pozornost v celoti.

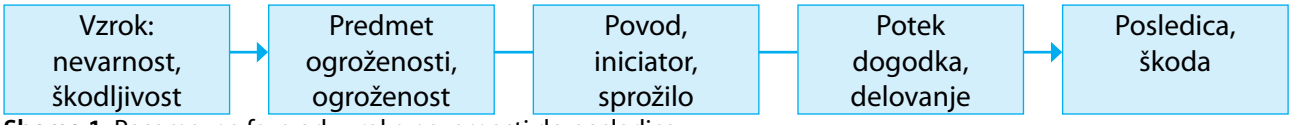
Potek neželenega odmika od cilja dejavnosti

Za obvladovanje tveganja je treba najprej (s)poznati in identificirati možne vzroke tveganj za motnje.[4] Spoznati je treba, kaj lahko gre in ali sploh lahko gre kaj narobe. Pri analizi moramo predvideti verjeten scenariji poteka neželenega dogodka.

Postopki in metode analize so različni. Za preprečevanje posledic (ukrepanje) si veliko pomagamo, če razdelimo potek dogajanja na posamezne značilne faze oziroma elemente. Te elemente ponazarja spodnja shema.[5]

Izhodiščni in temeljni element je nevarnost oziroma vzrok (eksplozivna zmes, sile, hitrost, strupenost idr.). Za nadaljnji potek mora biti v dosegu nevarnosti/vzroka predmet ogroženosti (človek, cilj, okolje, finančni uspeh itd.). Dogodek ostane latenten, dokler delovanja nevarnosti/škodljivosti na predmet ogroženosti ne aktivira povod/sprožilo (vžig, napačno ravnanje upravljavca, tehnična odpoved itd.). Z aktiviranjem (povod/sprožilo) se sproži nadaljnji potek dogodka, ki privede do končne posledice/škode (nezgoda, poškodba osebe, okolja, materialna/finančna škoda, kazenska odgovornost idr.).

Potek dogodka pogosto ni vedno



Shema 1: Posamezne faze od vzroka nevarnosti do posledice

tako preprost,[4] ampak lahko vsebuje na različne načine serijsko, paralelno ali drugače kompleksno povezanih dejavnikov. Praviloma pa se dajo tudi bolj kompleksni dogodki prevesti na opisane osnovne elemente.

Neželenim posledicam dogodka se lahko izognemo z vgradnjo varoval (varnostne plasti) med naštetimi elementi. Vzemimo na primer, da odpove tehnični element v danem procesu. Če lahko ima odpoved resne posledice, za varnostni ukrep vgradimo indikator napake in zagotovimo stalnega upravljavca sistema, ki ob indikaciji tehnične napake ustrezno ukrepa. Lahko se zgodi, da pride do več neugodnih istočasnih naključij. Recimo da je ob signalu napake upravljavec odsoten ali nepazljiv. Lahko tudi napačno ukrepa: lahko oceni, da gre za lažni alarm. Čeprav v zadnjem primeru nastane posledica zaradi več istočasnih vzrokov (odpoved, odsotnost/napačno ravnanje), lahko celoten dogodek štejemo kot enotno verigo vzrok–ogroženost–povod–potek–škoda po predstavljeni shemi. Za sprejemljivo varnost se zato praviloma ne zadovoljimo s posamezno »varovalko« (indikator napake – pričakovana korekcija upravljavca), ampak v sistem vgradimo ustrezno več varovalk, redundančnih sistemov ipd.

Poznavanje scenarija poteka dogodka in povezave med temeljnimi elementi poteka dogodka je bistveno za obvladovanje tveganja, zato da izberemo in na primernih mestih vgradimo posamezne ali večkratne ukrepe za prekinitev neželenega poteka.

Postopki za analizo možnih napak, potekov dogodkov in posledic so odvisni od sistema, cilja, podatkov, možnosti, izvedljivosti, odločanja idr. Če kvantitativno poznamo tveganja in zanesljivost posamezne varovalke, lahko tudi kvantitativno ocenimo celotno varnost in s primerjavo z zahtevami ocenimo, ali je tveganje sprejemljivo ali ni.

Na temelju opisane sheme se je izoblikoval splošno priznan prioritetni vrstni red ukrepov:

- iz obravnavanega sistema izločiti ali zmanjšati nevarnost,
- iz območja nevarnosti umakniti cilj/predmet morebitne ogroženosti,
- odstraniti ali zmanjšati možnost aktivacije/povoda poteka dogodka in
- preprečiti ali omejiti škodo, na primer, z ukrepi na poti do cilja ali na cilju (preusmeritev poteka dogodka v nenevarno območje, omejiti učinek na cilj, osebna varovalna oprema) itd.

SIST ISO/IEC 31000:2011 Obvladovanje tveganj – Načela in smernice za obvladovanje tveganja

StandardSISTISO/IEC31000:2011[1] je temeljni standard za obvladovanje tveganj, povezanih z določenim procesom. Ta standard postavlja in priporoča načela, ki morajo biti izpolnjena za uspešno obvladovanje tveganj. Na začetek uvršča »vzpostavljanje konteksta« obvladovanja tveganj v organizaciji in navaja prednosti upoštevanja v standardu definiranih načel za organizacijo. Sistematično predstavlja prepletanje načel (točka standarda 3), okvira (točka 4) in procesa obvladovanje tveganj (točka 5 standarda).

Med načeli poudarja, da obvladovanje tveganj ustvarja in varuje vrednost, da je obvladovanje tveganj sestavina vseh organiziranih procesov, da je del odločanja, da

je treba izrecno obravnavati negotovost, da mora biti obvladovanje tveganja sistematično, strukturirano in pravočasno, da obvladovanje temelji na najboljših razpoložljivih informacijah, da je prilagojeno in usklajeno z zunanjim in notranjim kontekstom organizacije ter s profilom tveganja, da upošteva človeške in kulturne dejavnike, da je pregledno in vključujoče do deležnikov, da je dinamično, ponovljivo, da se odziva na spremembe in da omogoča nenehno izboljševanje organizacije.

V okviru so razdelane naloge v obravnavani organizaciji, pooblastila in zavezanosti v zvezi z obvladovanjem tveganj: zasnova za obvladovanje tveganja, izvajanje obvladovanja tveganja, spremljanje, pregled in nenehno izboljševanje okvira.

V procesu standard SIST ISO/IEC 31000:2011 obravnava in navaja posamezne elemente in njihovo medsebojno povezanost, kot so: komuniciranje z zunanjimi in notranjimi deležniki v vseh fazah procesa, spremljanje in pregled kot načrtovani sestavini procesa obvladovanja tveganja, ki vključujeta redno preverjanje in nadzor. Komuniciranje in spremljanje povezujeta vzpostavljanje okolja in ocenjevanje tveganja; zadnje vsebuje identifikacijo tveganja, analizo tveganja, obravnavo in ovrednotenje tveganja.

Standard 31000 vsebuje informativni dodatek A – Lastnosti okrepljenega obvladovanja tveganj. Pri tem kot cilj vsake organizacije navaja ustrezno raven delovanje okvira z navedbo ključnega cilja ter z obravnavanjem lastnosti učinkovitega obvladovanja tveganj. Pod lastnosti šteje: nenehno izboljševanje obvladovanja tveganj z določanjem ciljev, delovanje organizacije, merjenje, pregled ter poznejše spremembe procesov, sistemov, virov, zmogljivosti, spretnosti in znanja. Nadalje med lastnosti prišteva odgovornost in poudarja celovitost, popolno opredeljeno in v celoti sprejeto odgovornost za tveganja, ukrepe in naloge. Vse to morajo vsebovati tudi opisi delovnih mest, hkrati pa naj bo varnost tudi del uvajalnih programov organizacije. Vsako odločanje naj vključuje tudi upoštevanje tveganj in njihovo obvladovanje. Med lastnostmi poudarja tudi zahtevo po stalni komunikaciji z zunanjimi in notranjimi deležniki. Obvladovanje tveganja je v smislu tega standarda osrednja aktivnost vseh procesov vodenja, ker na tem temeljita upravljavska struktura in delovanje sistema.

SIST ISO/IEC 31000:2011 vsebuje tudi poslovenjene izraze in definicije v zvezi s tveganjem. Nekatere od pogosteje uporabljenih izrazov navajamo tukaj v celoti, ostali izrazi so na tem mestu le taksativno našteti:

- tveganje – vpliv negotovosti na doseganje ciljev (s petimi opombami),
- obravnavanje tveganja – proces primerjave analize tveganja z merili tveganja, da se ugotovi, ali sta tveganje in/ali njegova velikost sprejemljivi oziroma dopustni,
- okvir za obvladovanja tveganja,
- politika obvladovanja tveganja – izjava o celovitih namerah in usmeritvi,
- organizacije v zvezi z obvladovanjem tveganja,
- odnos do tveganja – pristop organizacije k ocenjevanju in morebitnemu spreminjanju, ohranitvi, sprejetju ali odvračanju od tveganj,
- načrt obvladovanja tveganj,
- skrbnik tveganja,
- proces obvladovanja tveganja – sistematična uporaba politik, postopkov in praks obvladovanja pri aktivnostih komuniciranja, posvetovanja, vzpostavljanje konteksta ter identifikacija,

analiziranja, vrednotenja, obravnavanja, spremljanja in pregledovanja tveganja,
- vzpostavljanje konteksta,
- zunanji kontekst,
- notranji kontekst,
- komuniciranje in posvetovanje,
- déležnik,
- ocena tveganja – celovit proces identifikacije tveganja, analize tveganja in ovrednotenje tveganja,
- identifikacija tveganja – proces ugotavljanja, priznavanja in opisovanja tveganja,
- vir tveganja – element, ki je sam ali v kombinaciji z drugimi elementi sposoben povzročiti tveganje,
- dogodek – pojav ali sprememba določenega spleta okoliščin,
- posledica – izid nekega dogodka,
- verjetnost – možnost, da se bo nekaj zgodilo,
- profil tveganja,
- analiza tveganja – proces, ki pomaga razumeti naravo tveganja in opredeliti raven tveganja,
- merila tveganja,
- raven tveganja,
- ovrednotenje tveganja,
- obravnavanje tveganja,
- ukrep za obvladovanje tveganja – ukrep, ki spreminja tveganje,
- preostalo tveganje,
- spremljanje,
- pregled …

SIST ISO/IEC 31010:2011 Obvladovanje tveganj – Tehnike obvladovanja tveganja

SIST ISO/IEC 31010:2011[2] dopolnjuje osnovni standard 31000. Tehnike (metode) za obvladovanja tveganja so tehnični pripomočki v smislu identifikacije in vrednotenja, sprejemljivosti tveganja in izbire optimalnih ukrepov pri načrtovanju ter vodenju sistema, za primerjanje izvedljivosti, uporabnosti in učinkovitosti ukrepov. Tehnike so različne in so odvisne od vrste pričakovanih tveganj in ciljev, razpoložljivih podatkov, namena obvladovanja, negotovosti in zahtevnosti ukrepov ter pričakovanih rezultatov.

Standard SIST ISO/IEC 31010:2011 definira koncept ocenjevanja tveganj, ki vsebuje namen in prednosti, okvir ocenjevanja tveganj in obvladovanje tveganj ter obravnava postopke ocenjevanja in obvladovanja tveganj.

Ta standard opisuje namen in koristi. Med številnimi koristmi ocenjevanja tveganja navaja na prvem mestu razumevanje tveganja in njegov vpliv na cilje organizacije.

Standard podrobno obravnava okvir ocene tveganja ter postopek ocenjevanja in obvladovanja tveganja (glej tudi SIST ISO/IEC 31000:2011), ki naj seznanja odločujoče in odgovorne v organizaciji s poglobljenim razumevanjem tveganj, ki lahko vplivajo na doseganje ciljev in usmerjajo ukrepe. Posebej opozarja na negotovost analiz tveganja in na občutljivost rezultatov na posamezne parametre.

V splošnem delu standard SIST ISO/IEC 31010:2011 tudi podrobno govori o izbiri tehnik za ocenjevanje tveganj glede na razpoložljive podatke, naravo in stopnjo negotovosti, glede na kompleksnost sistema ter glede na uporabo ocene tveganja v življenjski dobi sistema.

V informativnem dodatku A standard primerja tehnike ocenjevanja glede na uporabnost in našteva značilne lastnosti posameznih orodij za ocenjevanje tveganj. V informativnem dodatku B so sistematično razdelane najbolj znane tehnike za ocenjevanje tveganja. Pri vsaki od navedenih tehnik so posebej navedeni: pregled obravnavane metode, uporabnost metode, potrebni vhodni podatki, postopek, učinek, zmogljivost in omejitve obravnavane metode. Po tem sistemu je podrobno opi-

sanih naslednjih 28 tehnik oziroma metod: 1. »viharjenje možganov« (brainstorming), 2. metoda strukturiranih ali polstrukturiranih intervalov (structured or semi-structured intervals), 3. metoda Delphi, 4. kontrolne preglednice (check-lists), 5. predhodne analize tveganja (PHA-preliminary hazard analysis), 6. HAZOP (hazard and operability study), 7. analiza nevarnosti in kritične kontrolne točke (HACCP-hazard analysis and critical control points), 8. ocena strupenosti (toxicity assessment), 9. strukturirana metode »kaj če« (tehnika SWIFT), 10. analiza scenarijev (scenario analysis), 11. vpliv na posel (BIA-business impact analysis), 12. analiza temeljnih vzrokov (RCA-root cause analysis in RCFA-roor cause failure analysis), 13. analiza vrste napak in posledic (FMEA-failure modes and effects analysis) ter analiza vrste napak in kritična analiza (FMECA-failure modes and effects nad criticaly analysis), 14. drevo napak (FTA-fault tree analysis), 15. drevo dogodkov (ETA-event tree analysis), 16. analiza vzrokov in posledic (cause-consequences analysis), 17. analiza vzroka in učinka (cause-and-effect analysis; kombinacija FTA in ETA), 18. analiza varnostnih plasti (LOPA-layers of protection analysis), 19. drevo odločanja (decision tree analysis), 20. zanesljivost človeka (HRA-human reliability assessment), 21. analiza metuljčka (bow tie analysis), 22. vzdrževanje, osredotočeno na zanesljivost (RCM-reliability centered maintenance),

23. analiza vtihotapljenosti (SA-sneak analysis) in krožna analiza vtihotapljenosti (SCI-sneak circuit analysis), 24. Markova analiza (Markov analysis), 25. simulacija Monte Carlo, 26. Bayesova statistika in Bayesove mreže (bayesian statistics and bayesian nets), 27. krivulje FN (FN curves) in 28. indeksi tveganja (risk indices, matrika tveganja).
Vse naštete metode so sistematično razdelane po že prej naštetih točkah v standardu.

Diskusija in zaključki

Omenjeno je že, da varnost in zdravje za zaposlene v sistemu poklicnega dela nista odvisna samo od področja, ki ga ureja ZVZD, ampak širše od integralne varnosti določenega sistema oziroma procesa. Čeprav standarda SIST ISO/IEC 31000:2011 in SIT ISO/IEC 31010:2011 v prvi vrsti obravnavata »procesno varnost«, torej nemoteno delovanje sistema, lahko varnost sistema neposredno ali posredno vpliva tudi na zaposlene v sistemu ali širše, na primer na okolje, učinkovitost, gospodarjenje idr. Zato procesno varnost in VZD, kot našo osnovno strokovno usmeritev, štejemo kot med seboj povezani sestavini integralne varnosti. In obratno. Posebej procesna varnost in VZD sta organsko prepleteni in soodvisni.
Kljub temu da standarda SIST ISO/IEC 31000:2011 in SIST ISO/IEC 31010:2011 pri nas za uporabo nista obvezna, sta koristni dopolnili za celovitejše razumevanje in sistematično obravnavo varnosti danega sistema. Omenjena standarda moramo šteti kot pregledno urejene splošne napotke za vodenje varnosti.
Za konkretno praktično uporabo v določenem primeru pa so potrebna še druga, praviloma formalno pridobljena znanja, in praktične izkušnje za učinkovito obvladovanje procesnih tveganj in v zvezi z njimi tudi za zagotavljanje VZD udeleženih v vodenju danega sistema, za varnost širšega okolja in za zagotavljanje integralne varnosti delovanja obravnavanega sistema.

Literatura

1. SIST ISO/IEC 31000:2011 Obvladovanje tveganj – načela in smernice za obvladovanje tveganja.
2. SIST ISO/IEC 31010:2011 Obvladovanje tveganj – tehnike obvladovanja tveganja.
3. Zakon o varnosti in zdravju pri delu ZVZD–1. Ur. l. RS, št. 43/2011.
4. Gspan, P. (1996). Analiza in presoja varnosti pri delu. Ljubljana: ZRSVD.
5. Compes, P. C. (1994). Analyse und Prävention von Schäden in der Produktion. Zbornik s posveta Kakovost proizvodnje in varnost, Bled.