DINAMINIO RIZIKOS VERTINIMO PLĖTRA IR POVEIKIS DARBUOTOJŲ SAUGAI IR SVEIKATAI

ĮŽANGA

Rizikos vertinimas – tai kertinis Europos lygmens požiūrio į darbuotojų saugą ir sveikatą (DSS) pagrindas (EU-OSHA, 2020). Valstybių narių darbdaviai privalo atlikti rizikos vertinimą darbo vietoje, kuris leistų nustatyti, įvertinti ir valdyti riziką darbuotojų saugai ir sveikatai (Darbuotojų saugos ir sveikatos pamatinės direktyvos 89/391/EEB 9 straipsnio 1 dalies a punktas). Vis dėlto per 2019 m. atliktą trečiąją Europos įmonių apklausą apie naują ir kylančią riziką (ESENER) paaiškėjo, kad faktinis darboviečių, kuriose nuolat atliekamas rizikos vertinimas, skaičius įvairiose ES valstybėse narėse svyruoja nuo apytiksliai 42 % iki 94 % (EU-OSHA, 2020). Šiuos skirtumus ne taip lengva paaiškinti, tačiau iš ESENER apklausos matyti, kad visoje Europoje esama teigiamo ryšio tarp darbovietės dydžio ir atitikties lygio: kuo didesnė darbovietė, tuo didesnė tikimybė, kad joje bus atliktas nuolat peržiūrimas ir patvirtinamas rizikos vertinimas. MVĮ dažnai sunkiau pasiekti (EU-OSHA, 2020), ir kai kurios apskritai niekada neatlieka rizikos vertinimo dėl kompetencijos, išteklių ar supratimo stokos. Tai kelia problemų ne tik reguliavimo požiūriu, bet ir darbuotojams.

Vienas būdas padėti įmonėms atlikti rizikos vertinimus yra pasiūlyti tinkamas lengvai naudojamas (elektronines) priemones, kurios gali palengvinti rizikos vertinimo procesą. Pagrindinis lengvai prieinamų priemonių privalumas yra tas, kad jas naudojant galima greitai gauti pakankamai tikslius rezultatus. Pavyzdžiui, Europos darbuotojų saugos ir sveikatos agentūra (EU-OSHA) sukūrė įvairias internetines interaktyvias rizikos vertinimo priemones, vadinamas OiRA (https://OiRAproject.eu/en). OiRA gali būti taikoma daugybei įvairių įmonių ir veiklos rūšių, ir dabar ją naudoja tūkstančiai įmonių visoje ES (EU-OSHA, 2021a). Nacionaliniu lygmeniu sukurtos įvairios papildomos priemonės, pvz.,

- „BeSmart.ie“: https://www.besmart.ie/,
- „Rie.nl“: https://www.rie.nl/,
- „Prevencion10.es“: https://www.prevencion10.es/.

Be to, sukurta nemažai pagalbinių skaitmeninių priemonių, orientuotų į konkrečią riziką, kuriomis galima veiksmingai pasinaudoti atliekant rizikos vertinimą, pvz.,

- triukšmo riziką: https://www.av.se/en/health-and-safety/noise/mata-ljud-och-buller/noise-exposure-app/,
- cheminių medžiagų riziką: https://www.seirich.fr/seirich-web/index.xhtml.

Tokios skaitmeninės priemonės naudojamos vis platesniu mastu, todėl esama tam tikro pasitikėjimo, kad jos bus sėkmingai panaudotos Europos darbo vietose. Kartu su stebėsenos technologijų, jutiklių ir dirbtinio intelekto (DI) plėtra darbuotojų saugos ir sveikatos srityje, dabar tinkamas laikas įvertinti ateities skaitmenines rizikos vertinimo technologijas. Šiame dokumente nagrinėjama, kokius kitus žingsnius įmonės ir pramonė žengia rizikos vertinimo srityje. Iš tiesų, jų pažanga yra tokia reikšminga, kad jai apibūdinti reikalingas atskiras terminas – dinaminis rizikos vertinimas.

Šiame dokumente pateikiamos su dinaminiu rizikos vertinimu susijusios įžvalgos ir aptariami toliau išvardyti klausimai.

1. Kas yra dinaminis rizikos vertinimas ir kuo jis skiriasi nuo dabartinės rizikos vertinimo sampratos?
2. Kokia yra dinaminio rizikos vertinimo nauda darbuotojų saugai ir sveikatai (DSS) ir kokie yra tinkami tokio vertinimo plėtojimo atskaitos taškai?
3. Kokias nepageidaujamas pasekmes dinaminis rizikos vertinimas sukelia DSS ir kaip galima sušvelninti šias pasekmes?

4. Kokias pasekmes dinaminis rizikos vertinimas sukeltų darbdaviams, darbuotojams, DSS ekspertams ir politikos formuotojams?

Siekiant atsakyti į šiuos klausimus, šiame dokumente problema nagrinėjama dviem aspektais. Pirmas aspektas yra pagrįstas McKinsey verslo požiūriu į rizikos valdymą (Jain *et al.*, 2020). Šiam aspektui būdingas tam tikras skubos pojūtis, būtent todėl prie rizikos vertinimo sąvokos pridedamas žodis „dinaminis“.

Remiantis antruoju aspektu, procesų saugos pramonės įmonės vertinamos kaip pirmaujančios taikant dinaminio rizikos vertinimo metodus. Šiose įmonėse buvo jaučiamas poreikis imtis pokyčių po rimtų incidentų, įvykusių XXI amžiaus pradžioje, ir požiūris į riziką, kaip į dinamiškesnį reiškinį, buvo vienas iš būdų gerinti rizikos vertinimą ir prevenciją.

Bet prieš tai šiame dokumente bus aptartas pagrindinių rizikos ir rizikos vertinimo sąvokų ryšys, kuris padės suprasti pagrindinius dinaminio rizikos vertinimo aspektus.

Pagrindinių sąvokų ryšys

Siekiant pasinaudoti kitose srityse, kuriose rizika vertinama iš kitos perspektyvos, taikomos praktikos ir aplinkybių privalumais, būtinas gana platus supratimas; konkrečiau, diskusija „dinaminio rizikos valdymo“ klausimais bus paprastesnė paaiškinus sąvokų tarp rizikos, valdymo, vertinimo, kliūčių ir DSS poreikio ryšį.

Kadangi pamatinėje direktyvoje (Pamatinė direktyva 89/391/EEB) rizikos sąvoka neapibrėžta, remiamės ISO standartais, būtent ISO 31000 ir ISO 45001 standartais, kurie padeda suformuluoti išsamią DSS sričiai tinkamą apibrėžtį: DSS rizika – tai su darbu susijusio pavojingo įvykio arba poveikio tikimybės ir sužalojimo ar sveikatos sutrikimo, kurį gali sukelti įvykis ar poveikis, sunkumo derinys.

ISO standartuose nustatyta tarptautinė rizikos apibrėžties perspektyva, kuri naudinga šioje diskusijoje. Tačiau svarbu tai, kad standartais nustatomos išsamesnės organizacinės sąlygos, užduotys, metodai ir pareigos, kurias organizacijos gali nuspręsti prisiimti, siekdamos užtikrinti rizikos kontrolę. Tai padeda **rizikos valdymą** apibrėžti kaip išsamų organizacinių ypatumų ir priemonių, kurių dauguma nėra būdingi tik rizikos sričiai, rinkinį. Tokie aspektai kaip komunikacija, vadovavimas, suinteresuotųjų subjektų dalyvavimas, dizainas ir kompetencija, yra svarbūs ne tik rizikos valdymo, bet ir kitose srityse (pvz., finansų valdymo ir našumo srityse). **Rizikos vertinimas** – unikalus rizikos valdymo procesas. Rizikos vertinimo vaidmuo sistemoje – tiksliai paaiškinti, kokia rizika yra paplitusi konkrečioje darbo vietoje, ar ji yra svarbi atsižvelgiant į kitus rizikos veiksnius ir kaip ji ilgainiui kinta. Vertinimo metu taip pat gali būti atliekamas tikėtinas apsaugos priemonių poveikis. Vertinimo tikslas – pateikti įrodymus, kuriais pagrindžiami sprendimai, ar reikia šalinti riziką ir kaip tai padaryti. Šiuo atveju kalbama apie darbdavių pareigą priimti sprendimą dėl savo darbuotojų apsaugos priemonių ir suteikti būtiną įrangą bei mokymą.

ISO standartuose iš esmės nustatyta, kad rizikos valdymas ir vertinimas yra **dinamiškos** sąvokos. Pagal ISO 45001 standartą dinamiškumo problemai spręsti pasitelktas „Plan-Do-Check-Act“ (planuoti, daryti, tikrinti, veikti) ciklas. Pamatinėje direktyvoje (89/391/EEB) taip pat pripažįstami dinaminiai procesai: 6 straipsnio 1 dalyje nustatyta, kad darbdaviai turi koreguoti darbuotojų saugos ir sveikatos priemones pasikeitus aplinkybėms ir siekti gerinti darbuotojų saugą ir sveikatą. Žinoma, koregavimo dažnumas nėra griežtai apibrėžtas.

Apibendrinant galima teigti, kad rizikos valdymas yra plačiausia sąvoka, apimanti daugybę organizacijų pastangų pašalinti arba sumažinti bet kurios rūšies riziką. DSS (rizikos) valdymas yra orientuotas į profesinės rizikos kontrolę. Rizikos vertinimas yra konkretus rizikos valdymo procesas, skirtas rizikai ištirti ir palengvinti sisteminių sprendimų dėl prevencinių priemonių priėmimą. Dinaminio rizikos vertinimo sąvoką reikia suprasti remiantis būtent šia sistema; tikrasis pokytį lemiantis aspektas – tai žodžio „dinaminis“ įterpimas. Kyla klausimas, kodėl įvairūs subjektai apskritai pasisako už rizikos „dinamiškumą“?

Įžvalgos dėl dinaminės rizikos

Pirmoji įžvalga kyla iš verslo aplinkos, kurioje stengiamasi patenkinti poreikį keistis. Nepaisant akivaizdžių skirtumų DSS srityje, darbuotojų saugai ir sveikatai atsirandančios pasekmės yra svarbios. Naujausioje ataskaitoje, kurioje pateikiamos per konsultacijas su įmonėmis gautos įžvalgos, paaiškinama, kodėl reikia pakeisti rizikos metodus ir kodėl jie turi tapti daug dinamiškesni (Jain *et al.*, 2020). Pateikiant argumentus, pirmiausia nurodoma tai, kad verslo aplinka pasikeitė iš esmės: skaitmeninė revoliucija, klimato kaita, geopolitinės galios pokyčiai ir kintantys suinteresuotųjų subjektų lūkesčiai lemia **didesnį** organizacijų **lankstumą, greitesnę reakciją ir didesnį veiksmingumą.** Ataskaitoje siūloma šalinant riziką imtis pokyčių šiose srityse:

- hiperdinaminio rizikos nustatymo siekiant neatsilikti nuo greitai kintančios verslo aplinkos;
- dinaminio rizikos vertinimo ir sprendimų priėmimo siekiant susidoroti su sparčiais rinkos poreikių pokyčiais, socialine atsakomybe ir darbu; bei
- dinaminio sprendimų dėl tinkamos rizikos kontrolės ir prevencinių priemonių priėmimo.

Dėl pastarojo aspekto pažymėtina, kad dinaminis sprendimų dėl rizikos kontrolės priėmimas gali būti siejamas su **atsparumo** sąvoka: organizacijos turi būti atsparios greitų (technologinių) verslo pokyčių akivaizdoje ir greitai bei veiksmingai įdiegti arba pašalinti kontrolės priemones. Aktualus su DSS susijęs pavyzdys yra skubaus veido kaukių dalijimo arba prisitaikymo prie nuotolinio darbo (darbo iš namų) praktika, kaip dalis kovos su COVID-19 pandemija priemonių. DSS specialistai iš esmės pernakt privalėjo išspręsti veido kaukių dėvėjimo saugos ir saugių darbo vietų namuose problemas. Atsižvelgiant į spartų šių pokyčių tempą, reikia ne tik greitai įvertinti riziką, bet ir nustatyti naujas arba geresnes valdymo struktūras; viena iš dažniau naudojamų struktūrų – aktyvesnė sąveika su suinteresuotaisiais subjektais, sprendimų priėmėjais ir teisės aktų leidėjais ir, nepamirškime, mokymasis apie COVID-19 keliamą riziką. Šios DSS saugos priemonės buvo įdiegtos labai greitai, dažnai atmetant arba apeinant standartinius DSS procesus. Sprendimų priėmimas pagal komitetuose vykdomas procedūras trunka ilgai, todėl, siekiant greitai ir veiksmingai sumažinti riziką, reikia nustatyti veiksmingesnius sprendimų priėmimo būdus (Jain *et al.*, 2020).

Antrasis dinaminio rizikos vertinimo aspektas yra susijęs su sparčiais ir esminiais organizacijų veiklos pokyčiais. Dabar organizacijose vyksta daugybė pokyčių. Grįžtant prie mūsų DSS ekspertų per COVID-19 krizę pavyzdžio, pažymėtina, kad organizacijos turėjo labai greitai įvertinti ir nuspręsti, kurie darbuotojai yra svarb įmonei (ir turėtų atvykti į darbo vietą), o kurie galėtų dirbti namuose.

Taip prieiname prie pirmos išvados: hiperdinaminis rizikos nustatymas reikalingas tam, kad būtų atsižvelgta į greitai kintančią aplinką. Pagrindinis aspektas yra tas, kad organizacijos, visų pirma veikiančios smarkiai svyruojančiose rinkose, privalo numatyti, įvertinti ir stebėti grėsmes, remdamosi neužtikrinta vidaus ir išorės informacija. Dar kartą grįžtant prie DSS per COVID-19 krizę klausimo pažymėtina, kad rizika buvo susijusi ne tik su viruso poveikiu, bet ir su namuose dirbančių žmonių nusiskundimais dėl raumenų ir kaulų sistemos sutrikimų, psichikos sveikatos problemų, kurias sukėlė saviizoliacija, ir pavojų, kylančių dėvint veido kaukes. Šiuo atveju taip pat reikia nuspėti rizikos ateitį: kaip rizika keisis ateityje ir ką galime nuveikti, kad sumažintume jos poveikį?

Apskritai rizikos nustatymas, rizikos vertinimas ir prevencinių priemonių valdymas turi būti reaktyvesnis ir lankstesnis (Jain *et al.*, 2020). Be to, kaip nurodyta toje pačioje ataskaitoje, pokyčius galima palengvinti penkiais būdais.

Pirmasis būdas – **rizikos valdymą versle paversti svarbiausia priemone**, padedančia priimti strateginius sprendimus. Kartu su antru sprendimu nustatyti **gyvybingą praktiką**, kuri padėtų greitai suprasti rizikos pobūdį, tai reiškia, kad rizika turi būti įvertinta greičiau, platesniu mastu ir užtikrinant didesnę kokybę. Tai reiškia, kad DSS ekspertai turi turėti iš anksto prieinamą rizikai įvertinti reikalingą svarbiausią informaciją apie profesinę riziką, kuri turi būti suderinta su kitų rizikos sričių pagrindine informacija, be to, DSS ekspertai turi greitai rasti kūrybingus DSS sprendimus ir greitai juos pritaikyti.

Trečias sprendimas – **rizikos vertinimo ir valdymo skaitmeninimas**. Duomenys apie DSS riziką turi būti daug lengviau prieinami ir analizuojami greičiau, be to, pasinaudojant technologijomis, reikėtų užtikrinti nuolatinį duomenų srautą, kuris padėtų parengti apibendrintą rizikos profilį kartu su kitais rizikos veiksniais (pvz., finansine rizika ir procesų rizika). Tie duomenys gali būti gauti iš DSS duomenų

sistemų, pvz., įvade aprašytų e. priemonių, tačiau lygiai taip pat naudingos gali būti pranešimo apie incidentus sistemos ir išorės DSS duomenų šaltiniai: pramonės duomenų bazės, duomenys iš statistikos biurų, visuomenės sveikatos duomenys ir kiti stebėsenos duomenys.

Ketvirtas sprendimas – **DSS specialistai ir riziką valdantys asmenys turi būti geriau pasirengę naujoms skaitmeninimo realijoms** ir šiuolaikinio **verslo dinamikai**, atsižvelgiant į skubų poreikį ir didėjančias stebėsenos technologijų galimybes bei duomenų rinkimą per daiktų internetą ir pan. Siekiant neatsilikti nuo skaitmenizuoto pasaulio realijų, jų mokymą reikia atnaujinti įtraukiant duomenų analitiką, taip pat praplečiant jų požiūrį, kad būtų įgytas supratimas apie įvairesnėse srityse kylančią riziką. Kartu reikia ugdyti tvirtesnius vadovavimo įgūdžius, įskaitant kitus netechninio pobūdžio įgūdžius, kurie būtų naudingi vadovaujant įvairių specialistų grupėms ir gaunant atitinkamas žinias iš bendradarbių ir suinteresuotųjų subjektų.

Penktas sprendimas, kuris jau paplitęs tarp DSS ekspertų, – sukurti **tvirtą rizikos kultūrą, kurioje pagrindinį vaidmenį atliktų saugos ir rizikos ekspertai**, o vykdomąsias pareigas einantys asmenys atsakytų už sveikos rizikos kultūros puoselėjimą kartu užtikrinant visišką darbuotojų dalyvavimą. Atrodo, kad šioje verslo įžvalgoje pražiūrėta tai, kas ilgai domino DSS ekspertus.

Lengva suprasti, kodėl šis požiūris yra patrauklus didelėms organizacijoms, visų pirma veikiančioms rizikingose pramonės sektoriuose; nenuostabu, kad didelės cheminių medžiagų įmonės pirmosios ėmėsi veiksmų dinaminio rizikos vertinimo srityje. Mažesnėms organizacijoms, kurios, atrodo, dažnai atsilieka įgyvendindamos rizikos vertinimo priemones (taip pat žr. mūsų įvadą), tokie sprendimai galėtų būti labai naudingi, tačiau jie vis tiek yra pernelyg brangūs. Šiuo atžvilgiu sektoriaus arba pramonės asociacijos gali būti pakankamo dydžio, kad padėtų kurti savo sektoriams skaitmeninius DSS sprendimus. Reikėtų sukurti MVĮ skirtus pažangesnius nacionalinius skaitmenizuotus DSS sprendimus siekiant pažangos arba tai daryti ES lygmeniu (OiRAproject.eu).

Šiame dokumente pasirenkama viena verslo perspektyva, paaiškinanti, kad idėjos apie riziką keičiasi. Šiai nuomonei pritaria kiti verslo lyderiai (Kaul *et al.*, 2018; Terblanche & O'Donnell, 2021), nepaisant to, kad jie suformulavo savo pačių įžvalgas. Juos vienija mintis, kad rizikos analizę reikia atlikti daug greičiau, remiantis duomenimis, ir reaguoti į staigius ir esminius pokyčius organizacijoje.

DSS srityje, kuri yra gana uždara darbo sritis, skaitmeninės priemonės patenka į rinką (žr. įvade pateiktus pavyzdžius dėl e. priemonių), tačiau, atrodo, kad poreikis veikti operatyviai nėra toks svarbus. Kartu į DSS ekspertų kompetencijos sritį patenka pasiūlymai dėl kultūros puoselėjimo, rizikos vertinimo metodų nustatymo ir rizikos analizės svarbos. Žvelgiant iš šios perspektyvos, galima daryti prielaidą, kad procesus reikia pagreitinti naudojant skaitmenines priemones.

Dinamiškumą skatina procesų sauga

Termino „dinamiškas rizikos valdymas“ kilmė tiek, kiek ji susijusi su sauga, kildinama iš procesų saugos. Procesų sauga yra orientuota į nuotėkio, gaisro ir sprogimo prevenciją cheminių medžiagų gamyklose, siekiant užkirsti kelią žmonių sužalojimui darbe (pagal Pamatinę direktyvą 89/391/EEB) ir žalai aplinkai (Seveso direktyva 2012/18/ES, Europos Komisija, 2012). Kadangi pramonę iš esmės sudaro didelės, finansiškai stabilios įmonės, veikiančios ypač pavojingoje aplinkoje, nieko stebėtino, kad jos stato „dinamiškesnės“ rizikos srities pamatus. Pirmasis dokumentas yra tiesiogiai susijęs su 2005 m. „Texas City“ naftos perdirbimo gamykloje įvykusiu sprogimu. Praėjus penkeriems metams po incidento, Kalantatina *et al.* (2010) paskelbė dokumentą, kuriame matematiniai rizikos modeliai buvo derinami su įrašais apie incidentus 11 metų laikotarpiu, siekiant išsiaiškinti, ar nelaimingo atsitikimo rizika nuolatos didėjo iki 37 kartų, palyginti su pradine rizika. Autorė matematinį modelį sujungė su duomenimis ir sukūrė „mokymosi modelį“, kuriuo įrodoma, kad įrangos blogėjimas ir aplaidumas prižiūrint sistemas lėmė dinamiškai didėjančią riziką.

Pasman ir Rogers (2014) rėmėsi tuo pačiu nelaimingu atsitikimu, t. y. 2005 m. sprogimu „Texas City“ naftos perdirbimo gamykloje, ir siekė įrodyti, kad saugos kontrolei yra naudinga nuolatinė procesų saugos rodiklių (pageidautina pagrindinių rodiklių) stebėsena. Šie autoriai taip pat pasiūlė atnaujinti matematinius modelius naudojant duomenis, nors šį kartą tai buvo cheminių medžiagų apdirbimo gamyklose taikomi matematiniai modeliai.

„Deepwater Horizon“ katastrofa 2010 m., atrodo, padidino susidomėjimą duomenimis grindžiamais rizikos valdymo metodais, nes po tos nelaimės parašyta daugiau dokumentų (pvz., Khakzad *et al.,* 2012, 2013; Vinnem *et al*., 2012). Šiuose dokumentuose iš esmės pradedama nauja matematinių požiūrių į rizikos vertinimą analizės ir optimizavimo tradicija. Norvegijos mokyklos atstovai kartu su Vinnem analizavo valdymo paramos sistemas (2012 m. atvejis), kad suprastų riziką sukeliančius veiksnius ir planuotų saugesnes priežiūros užduotis, o Kanados mokyklos atstovai kartu su Khakzad ir Kahn dirbo tobulindami matematines vertinimo priemones.

Iki 2016 m. parengta pakankamai dokumentų, kad būtų galima atlikti peržiūrą šia tema (Khan *et al.*, 2016). Šiame dokumente vartojamas terminas **dinaminis rizikos vertinimas,** kuriuo siekiama paaiškinti rizikos modelių atnaujinimą, kaip nuolatinę užduotį, įskaitant automatizuotą duomenų sąsają su galutiniu tikslu. Vėlgi, matematiniai rizikos vertinimo modeliai atlieka pagrindinį vaidmenį. Tais pačiais metais Pitblado *et al.* (2016) nustatė duomenų sistemų ir dinaminio rizikos vertinimo ryšį, naudodamas duomenis, skirtus rizikos vertinimui atnaujinti, atsižvelgiant į prašymus dėl leidimo dirbti, kad juos būtų galima priimti arba atmesti, remiantis tikslinės rizikos lygiais, taip užtikrinant, kad rizikos lygis niekada neviršytų tam tikro ribinio lygio. Šiuo požiūriu sąvoka „dinaminis“ taip pat apima skaitmenizuotas saugos valdymo sistemas, o metodai išplito kitose rizikos srityse.

Šiuose dokumentuose parodoma, kaip didelės nelaimės paskatino cheminių procesų saugos ekspertus greičiau suformuoti dinaminį požiūrį į riziką. Šių ankstyvųjų dokumentų tikslas buvo suprasti prastėjančius saugos standartus, nustatyti, kad laikas yra svarbus matematinių rizikos vertinimo metodų veiksnys vertinant rizikos lygius ir kuo labiau sumažinant riziką darbo vietoje. Pažymėtina, kad šis pokytis galėtų įvykti greičiau, jei dažniau būtų naudojami jutiklių tinklai, kuriuose matuojami visų rūšių rizikos parametrai. Dabar su dinaminiu rizikos valdymu arba dinaminiu rizikos vertinimu susiję metodai techninės rizikos analizės srityje yra pakankamai nusistovėję ir dauguma metodų šiuo klausimu yra paskelbti viešai, nepaisant to, kad terminologija nebūtinai pasikartoja.

Svarbi su DSS susijusi įžvalga yra ta, kad su dinaminės rizikos analize susiję interesai ir paskatos procesų pramonės sektoriuje yra panašūs į DSS srities interesus ir paskatas: blogėjančios būklės sistemų kontrolė, darbuotojams kylančios rizikos kontrolė ir pagrįstų sprendimų saugos klausimais priėmimas. Pagrindinis skirtumą lemiantis veiksnys yra tas, kad cheminių procesų saugai reikalinga išsami likusių techninių sistemų analizė, o DSS valdymo srityje to nereikia. Dėl šios priežasties gali būti mažiau galimybių atlikti sudėtingus matematinius vertinimus DSS srityje. Kita vertus, DSS valdymas yra susijęs su sudėtinga techninių, žmogiškųjų ir aplinkos veiksnių sąveika, o plėtojant stebėjimo technologijas, jutiklius ir dirbtinį intelektą, siekiant juos panaudoti darbuotojų saugos ir sveikatos srityje, vis daugiau duomenų galima panaudoti DSS tikslais. 1 ir 2 teksto languose pavaizduota, kaip dinaminis rizikos vertinimas galėtų atrodyti valdant DSS.

1 langas. Dinaminės rizikos vertinimas naudojant rizikos matricą

Rizikos matrica parengta remiantis Jungtinių Valstijų gynybos departamento kariniu standartu Nr. 882, kuris buvo tikslinamas ne mažiau kaip penkis kartus (2012). Saugos srityje ją visų pirma naudoja DSS ekspertai, taip pat darbdaviai ir politikos formuotojai, kad riziką vizualizuotų lentelėje. Jei politikos formuotojai nereikalauja naudoti matricos, darbdaviai gali patys nuspręsti ją naudoti savo organizacijoje.

Rizikos matrica nurodo sunkumą horizontalioje ašyje (keturiais etapais: katastrofiška, kritinė, ribinė ir nereikšminga) ir tikimybę vertikalioje ašyje (šešiais etapais: dažnas, tikėtinas, atsitiktinis, nuotolinis, mažai tikėtinas ir pašalintas). Kiekvienam matricos langeliui priskiriami rizikos sunkumo lygiai (penkiais etapais: didelis, sunkus, vidutinis, žemas ir pašalintas), kur kiekvienas lygis skatina priimti skirtingus sprendimus, kaip elgtis konkrečioje rizikos situacijoje.

Šiame pavyzdyje naudojama galima konfigūracija, įskaitant hipotetinius DSS pavojus, kylančius sandėliavimo srityje. Šioje vietoje pridedamos trys pavojingos situacijos: ugnis, šakinių keltuvų susidūrimas ir šlapios grindys, ant kurių pėstieji gali paslysti, suklupti, nukristi (PSN).

1 paveikslas. Hipotetinė sandėlio rizikos matrica

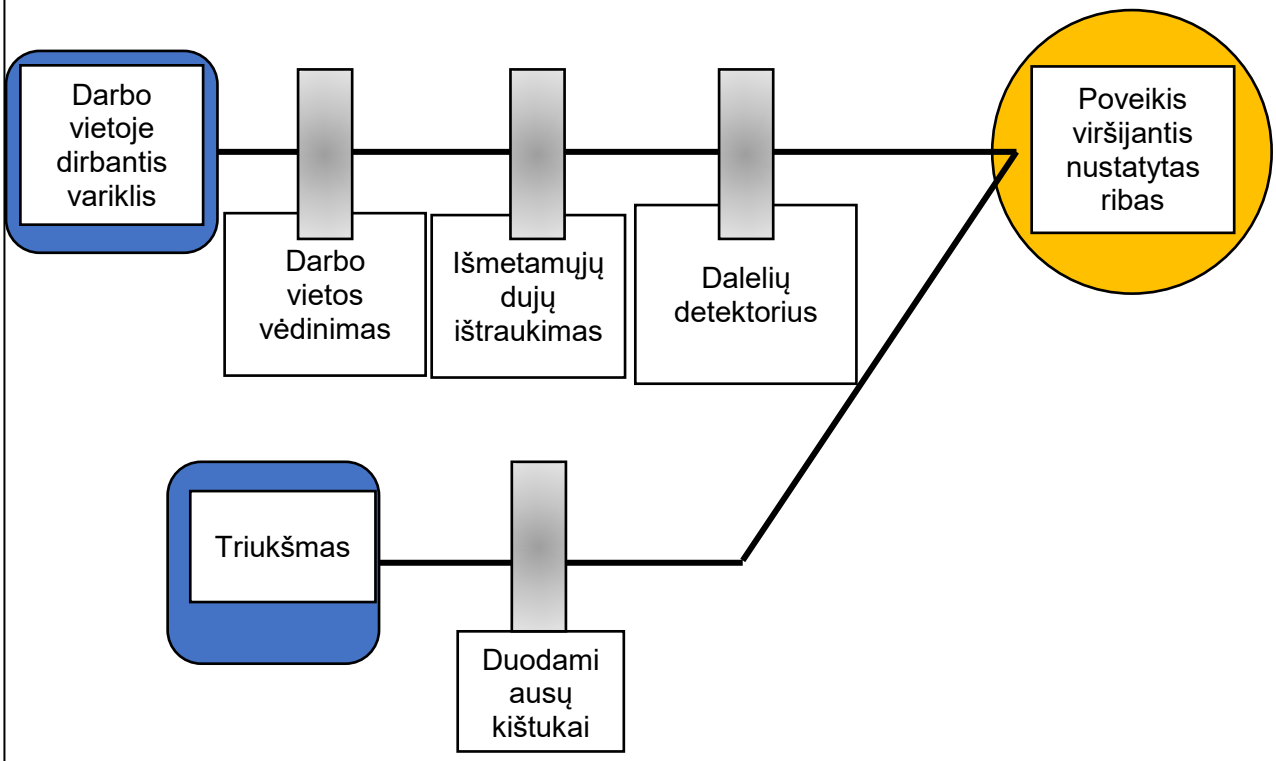
	Katastrofiška	Kritinė	Ribinė		Nereikšminga
Dažnas					
Tikėtinas					
Atsitiktinis		šakinio keltuvo avarija			
Nedažnas			Slidi danga (PSN)		
Retas	gaisras				

DSS ekspertai lentelėse pavaizduoja visas situacijas, kuriose gali pasireikšti DSS pavojai, ir naudoja nuorodų sąrašus nuspręsdami, kuriame rizikos matricos langelyje turi būti rodoma situacija; šis procesas gali būti skaitmeninamas naudojant skaitmeninius įrodymus, taip pagrindžiant faktinį rizikos vertinimą. Ši nuostata grindžiama mintimi, kad įrodymai atrenkant konkretų langelį rizikos matricoje dažnai saugomi skaitmeninėje laikmenoje; pvz., įrašuose apie incidentus, dėl kurių buvo suteikta daugiau laikinojo nedarbingumo dienų (tai įpareigoja Pamatinė direktyva), tačiau dinaminio rizikos vertinimo atveju daug įdomiau sugretinti vos neįvykusius incidentus, techninės priežiūros ataskaitas ir skundus. Tokių duomenų bazių sąsaja turėtų suteikti geresnę įžvalgą dėl incidentų, susijusių su nustatytais pavojais, dažnumo ir iš esmės suteikti įrodymų dėl jų įtraukimo į tinkamą rizikos matricos langelį. Tą patį metodą galima naudoti stebint ir nustatant konkrečios rizikos (pvz., šakinio keltuvo avarijos) kitimą laikui bėgant, galbūt dėl to, kad pranešimų apie incidentus skaičius didėja arba galbūt dėl to, kad konkrečią dieną gamykloje dirba per daug nepatyrusių darbuotojų. Turint pakankamai duomenų (iš vienos organizacijos, pramonės sektoriaus arba nacionaliniu lygmeniu), algoritmai galėtų būti naudojami dinaminiams rodikliams nustatyti siekiant stebėti visas pavojingas situacijas.

2 langas. Prevencinių priemonių stebėsena

Didžioji dalis DSS specialistų darbo yra susijusi su saugos lygių arba prevencinių priemonių (kurios procesų saugos srityje vadinamos kliūtimis) priežiūra. „Peteliškės“ analizėje (angl. *BowTies*) pateikiamas vienas nuoseklaus prevencinių priemonių stebėsenos būdas. Šiame pavyzdyje pavaizduotas dyzelino suodžių poveikis garažuose; 2 paveiksle parodyta hipotetinė „peteliškės“ analizės dalis.

2 paveikslas. „Peteliškės“ analizės dalis, susijusi su pavojingų medžiagų poveikiu



Pilkos spalvos juostos – tai prevencinės priemonės (kliūtys), kurios gali būti nustatytos atlikus rizikos vertinimo procesą, ir parodo, kad, siekiant išlaikyti priimtiną rizikos lygį, būtinos kontrolės priemonės. Pats rizikos vertinimas galėjo būti atliktas naudojant duomenimis grindžiamus metodus, pvz., aprašytus 1 teksto lange, tačiau šioje vietoje dėmesį skiriame duomenų, gautų taikant prevencines priemones, integracijai. Šiuo atveju dalelių detektorius yra nuolatinė stebėsenos sistema, kuri kiekvieną minutę atlieka dalelių masės kubiniame metre skaičiavimus. Jis yra sujungtas su skaitmenine sistema, kuri perskaito matavimus. Šiame pavyzdyje duomenys, naudojami apskaičiuojant bendrą poveikį, yra oro kokybės pakaitiniai duomenys; nustačius pakankamas ribas, kokybę galima pavaizduoti naudojant šviesoforo spalvas (raudona, geltona, žalia). Lygiai taip pat stebimas vėdinimo srauto rodiklis, tą patį galima pasakyti apie išmetamųjų dujų aktyvavimo skaičių, kuris atitinka informaciją apie tos konkrečios prevencinės priemonės būseną. Tačiau kiekvienas iš šių naudojamų duomenų srautų „dinamiškas“ yra būtent todėl, kad gali būti panaudojamas prevencinių priemonių sąlygoms ir veiksmingumui stebėti beveik tikruoju laiku, o tai sudaro sąlygas tikruoju laiku imtis intervencinių veiksmų anksčiau nei tai pradeda kelti susirūpinimą.

Jeigu, naudojant šį ir kitus detektorius, galima surinkti pakankamai duomenų, poveikio (ir rizikos) lygis gali būti nuspėjamas, remiantis oro sąlygomis, darbo krūviu arba testuojamu automobiliu. Lygiai taip pat jį galima panaudoti apskaičiuojant poveikio darbuotojams lygį ir nuspėjant ilgalaikį poveikį sveikatai. Asmeniniai aptikimo prietaisai pinga, todėl jie tampa patraukliais duomenų šaltiniais dinaminio rizikos vertinimo ir rizikos valdymo srityje.

Aptarimas

Šiame dokumente siekiama paaiškinti, kokie yra nauji dinaminio rizikos vertinimo aspektai, kokią reikšmę jie galėtų turėti DSS srityje, ir ar galima perimti patirtį iš srities pirmūnų bei kaip tai padaryti. Akivaizdu, kad rizikos valdymas yra dinaminio pobūdžio; Pamatinė direktyva (89/391/EEB) ir ISO 45001 tai aiškiai parodo. Nieko stebėtino, kad dirbant DSS srityje rizikos valdymą, vertinimus ir kontrolės priemones reikia atnaujinti gavus naujų įžvalgų, įvykus rimtiems nelaimingiems atsitikimams, pasikeitus įstatymams arba sukūrus naujus saugos sprendimus. Tačiau pokyčiai kitose srityse verčia mus galvoti apie būsimą rizikos vertinimą DSS darbo aplinkoje. Šiame skirsnyje aptariami aktualesni klausimai.

Dinaminis rizikos vertinimas kaip ateities vizija

Iš verslo rizikos perspektyvos matyti, kad turime būti dinamiškesni, nes pasaulis tampa dinamiškesnis. Verslo tempai greitėja, taigi ir pati rizika tapo dinamiškesnė nei anksčiau. Tendencijos priežastis yra skaitmenizavimas, kuris paspartina verslo operacijas ir sprendimų priėmimą. DSS ekspertų žinutė yra ta, kad procesai turi būti greitesni, lankstesni ir pagrįsti skaitmeninių įrodymų sistemomis.

Su procesų sauga susiję požiūriai patvirtina verslo požiūrį, tačiau yra praktiškesnio pobūdžio. Šis pramonės sektorius sukūrė metodus, kad paremtų dinaminį rizikos vertinimą ir rizikos valdymą.

Ši ateities vizija sulaukia DSS ekspertų kritikos. Didėjant sistemų sudėtingumui, DSS ekspertai gali susidurti su automatizavimu ir skaitmeninimu, keliantį pavojų saugai (EU-OSHA, 2018). Vis dėlto atrodo, kad DSS srityje reikia sekti rinkoje naudojamų e. priemonių pavyzdžiu, tačiau beveik kiekvienas skaitmeninimo aspektas turės būti patikrintas ir tik paskui taikomas.

Privalumai

Verslo ir procesų saugos požiūriuose atsispindi dinaminio rizikos vertinimo privalumai, bet jie apima keletą pagrindinių naudos aspektų. Šie privalumai praplečia ne tik Europos darbdavių (ir MVĮ) prieigą prie rizikos vertinimo, bet ir galėtų padėti įmonėms (geriau) prisitaikyti prie greitai kintančios verslo ar technologijų dinamikos. Todėl organizacijos atsiduria geresnėje padėtyje, kurioje gali reaguoti į verslo procesų pokyčius ir su jais susijusią DSS riziką.

Kitas privalumas yra tas, kad skaitmeninė sistema padeda užtikrinti griežtą rizikos vertinimą ir rizikos valdymą. Nustačius ribines vertes, programuojamos užduotys ir planuojami patikrinimai, vykdymas yra patikimas, o nukrypimai lengvai nustatomi. Tai padeda užtikrinti nuoseklią ir atsekamą rizikos kontrolę (prevencines priemones). Galiausiai dėl skaitmeninimo padidėja procesų sparta ir tuo pat metu stipriai sumažinamos žmogaus pastangos.

Skaitmeninėse sistemose taip pat neišvengiamai taikomi nuoseklūs duomenų rinkimo metodai. Atsiradus daugybei duomenų galimybių, leidžiančių aptikti silpnus signalus, ryšys tarp rizikos veiksnių, kurie įprastoje veikloje buvo nepastebimi, tapo matomi. Be to, tuo atveju, kai lyginami dideli duomenų kiekiai, gali būti įmanoma atlikti tam tikrą rizikos prognozavimą, tačiau tai itin priklauso nuo duomenų kokybės. Analizes galėtų atlikti trečiosios šalys (t. y. ne darbdaviai), pasinaudodamos pažangiųjų technologijų privalumais (pvz., ypač sudėtingais algoritmais, didžiaisiais duomenimis, galingais procesoriais ir pan.), kad mažiausiomis pastangomis būtų atliekami kokybiški vertinimai.

Įdiegus skaitmenines sistemas, taip pat atsiranda galimybės tiesioginei sąsajai su kitomis skaitmeninėmis sistemomis, kuriose gali būti atitinkama informacija. Darbo grafikas, oro prognozės, priežiūros ataskaitos, leidimo dirbti programinė įranga ir audito programinė įranga galėtų suteikti naudingos informacijos, reikalingos pagrįstam rizikos vertinimui, įskaitant daug platesnę žinių bazę nei anksčiau.

Trūkumai

Kartu esama ir reikšmingų trūkumų. Kai kurių labai svarbių DSS procesų dar negalima skaitmeninti. Saugos kultūra yra vienas iš šių procesų: saugos kultūra, kurią neabejotinai sudėtinga išmatuoti ir dar sunkiau įtakoti, gerinimas ir toliau iš esmės priklauso nuo žmogaus pastangų. Tą patį galima pasakyti apie vadovavimą; DSS vadovo įgūdžiai vadovauti savo organizacijai užtikrinant aukščiausio lygio saugą iš esmės yra susiję su žmogaus pastangomis. Komunikacija ir pasitikėjimas yra panašūs dalykai, tačiau šioje srityje naudos gali duoti socialiniai tinklai. Pripažindamas šiuos žmogaus įgūdžius, DSS ekspertas

gali naudoti duomenų sistemas, kad konkrečiau pritaikytų savo veiksmus prie konkrečių DSS klausimų. Jeigu iš duomenų sistemų matyti, kad veido kaukės naudojamos nepavyzdingai, DSS ekspertas gali imtis veiksmų tuo konkrečiu klausimu, užuot susitelkęs į saugos kultūros gerinimą. Tačiau prie intervencinių veiksmų turi prisidėti ir žmogus.

Kitas trūkumas (kurį pirmaujančios organizacijos nuslepia) gali būti susijęs su sąnaudomis. Ne visos organizacijos, ypač MVĮ, gali norėti arba sugebėti išleisti pinigus specialiai DSS programinei įrangai. Šiuo atveju programinės įrangos kūrėjai susiduria su problema: jie privalo sukurti sistemas, kurios padėtų veiksmingai užtikrinti DSS ir būtų naudingos naudotojų grupei. Kartu jie privalo įrodyti, kad duomenis naudoja patikimai ir, kad užtikrinama gera duomenų apsauga. Net jeigu organizacijos atnaujina rizikos valdymą, kad jis atliktų svarbesnį vaidmenį, ir atitinkamai skiria finansavimą duomenų sistemoms (kaip siūlo McKinsey), tai nebūtinai reiškia, kad susirūpinimą keliantys DSS klausimai organizacijai tapo svarbesni. Spręsdamos išlaidų apribojimo klausimą, organizacijos gali pasirinkti kitą būdą, t. y. bendradarbiauti profesinėse asociacijose arba, galbūt, nacionaliniu lygmeniu. Šiuo atveju taip pat kiltų suderinamumo klausimai, tačiau galėtų atsirasti ir galimybių pasimokyti iš vienas kito incidentų saugos srityje.

Kita problema – DSS teisės aktai dažnai keičiami lėtai: DSS reglamentai gali galioti ištisus metus, o kartais net ir dešimtmečius. Pavyzdžiui, Pamatinė direktyva 89/391/EEB galioja ilgiau nei 30 metų. Nieko stebėtino, nes pagrindiniai teisiniai požiūriai į sužalojimus ir mirtį darbe greitai nepakeičiami. Tokia padėtis darbuotojams gali būti priimtina; jiems ne itin svarbu, ar jų sveikatai turi įtakos XIX amžiaus staklės ar futuristinis kobotas. Tačiau programinės įrangos sprendimų, kurie gali būti pakeisti pernakt, atveju galėtų būti naudinga turėti tam tikras rekomendacijas (pvz., mašinų skaitomos apibrėžtys arba mašinų skaitomas teisinis tekstas).

Be to, nereikia pamiršti ir kultūrinio aspekto. Ne visi DSS ekspertai teigiamai vertina savo darbo skaitmeninimą, nes dėl to jie vis labiau atitolsta nuo žmonių ir jiems rūpimų (DSS) klausimų. Dėl skaitmeninių sistemų duomenys tampa vis labiau prieinami, todėl greičiau priimami geresni sprendimai dėl rizikos, tačiau daugiau laiko praleidžiama dirbant su kompiuteriais, o ne su žmonėmis. Stebina tai, kad konsultavimo bendrovės iš tiesų teigia, kad rizikos valdymas įmonėse atlieka vis svarbesnį vaidmenį ir nėra tik slaptas specializuotas departamentas, tačiau veikia kaip pagrindinis sprendimų priėmimo procesų dalyvis organizacijose. Net jeigu šiuo atveju nekalbama apie DSS rizikos valdymą, akivaizdu, kad tai yra galimybė DSS ekspertams atitinkamai reaguoti. Tačiau tai reiškia nuolatinį DSS darbuotojų kvalifikacijos kėlimą, kad jie galėtų dirbti su šiuolaikinėmis skaitmenizuotomis sistemomis, perspektyviais projektais ir prisiimti daug daugiau atsakomybės.

Politikos formuotojams, visų pirma veikiantiems nacionaliniu arba tarptautiniu lygmeniu, sudėtinga suprasti, kokie svarbūs pokyčiai trumpuoju laikotarpiu turėtų jiems įtakos. Žvelgiant iš platesnės nei pradiniai procesai perspektyvos, pažymėtina, kad skaitmeninimas neturi tokio reikšmingo poveikio darbuotojų saugos ir sveikatos reikalavimams arba sistemoms, kurias naudojant stebimi veiklos rezultatai. Žvelgiant iš politikos formuotojų perspektyvos, galima apsvarstyti galimybę skaitmeninti jų stebėsenos sistemas siekiant neatsilikti nuo spartesnės DSS dinamikos. Be to, jie turi atsižvelgti į tai, kaip DSS duomenimis pažeidžiamas privatumas, kaip tai yra daugumoje politikos sričių visoje Europoje.

Trumpai apie dirbtinį intelektą

Dabar bet kokia pažanga skaitmeninimo srityje neatsiejama nuo kylančių diskusijų dėl DI. Surinkus duomenis, visuomet patrauklu rizikos prognozavimui taikyti mokymosi algoritmus. Tačiau dėl DI kyla visiškai nauja diskusija ir EU-OSHA ne vienintelė sprendžia darbo vietoje DI sukeliamas problemas (EU-OSHA, 2018): Tarptautinė darbo organizacija (TDO) klausimą aptarė savo ataskaitoje „derybos dėl algoritmo“ (angl. „*Negotiating the algorithm*“) (De Stefano, 2018);Tarptautinė elektrotechnikos komisija (IEC) paskelbė leidinį „Sauga ateityje“ (angl. „*Safety in the future*“) (IEC, 2020), o Europos Komisija savo baltojoje knygoje dėl dirbtinio intelekto paskelbė bendresnio pobūdžio požiūrį į DI (Europos Komisija, 2020). Atrodo įmanoma, kad diskusijos dėl dinaminio rizikos vertinimo arba valdymo ir DI gali būti sujungtos į vieną.

Išvada ir perspektyva

Dinaminis rizikos vertinimas – tai terminas, vartojamas siekiant parodyti, kad rizikos vertinimas tapo galingu skaitmeniniu ir šiuolaikiniu įrankiu, padedančiu tvarkyti skaitmeninius duomenis ir šalinti greitai kintančią riziką. Svarbų postūmį pokyčiams suteikia verslo lyderiai, kurie savo paslaugas siūlo plataus masto skaitmeninimo, kuris vyksta visoje visuomenėje, srityje. Mokslinė pažanga procesų sektoriuje jau padėjo sukurti dinaminio rizikos vertinimo įgyvendinimo metodus, nepaisant jų konkrečios paskirties. DSS srityje dinaminė rizikos analizė primena, kad esama poreikio atsinaujinti.

Akivaizdi dinaminio rizikos vertinimo **nauda** – gyvybinga dinaminė darbo aplinka, kurioje sprendžiamos sudėtinės ir sudėtingos rizikos vertinimo problemos, sparta ir nuoseklumas. **Trūkumai** yra tokie pat kaip ir bet kurioje IRT sistemoje: įgūdžių spragos, priklausomybė nuo kompetencijos IRT srityje, kibernetinis saugumas ir išlaidos. Nepaisant trūkumų, sukurta keletas skaitmeninio rizikos vertinimo priemonių, o tai rodo, kad DSS ekspertai įvairiose Europos vietose žengia į skaitmeninį pasaulį.

Įvairiems DSS suinteresuotiesiems subjektams daromas įvairus poveikis. Didžiausias poveikis daromas **DSS ekspertams**, kadangi jie savo kompetenciją turės papildyti tam tikrais skaitmeniniais įgūdžiais. Jie turės suprasti, kokie duomenys įvedami į sistemą, ir koks yra jų ryšys su saugos turiniu, taip pat turės suprasti, kada sistemoje įvyksta klaidos. Be to, labai tikėtina, kad jie dalyvaus kuriant naujas sistemas ir dirbs su IT ekspertais. Labai tikėtina, kad **darbdaviai** dalyvaus aktyviai, nes jie priima sprendimus dėl investicijų, tačiau jie neprivalo žinoti tikslios informacijos. **Be to**, darbdaviams daromas didžiausias poveikis, atsižvelgiant į jų vadovaujantį vaidmenį įgyvendinant pertvarkos projektą, pašalinant įgūdžių spragas ir kontroliuojant išlaidas. Labiausiai tikėtina, kad darbuotojai bus naudotojai, todėl jiems nereikia turėti daug žinių apie sistemas, tačiau jiems reikės su jomis dirbti. Vis dėlto darbuotojai, kaip galutiniai naudotojai, neprivalo dalyvauti kuriant ir įgyvendinant naudotojo reikalavimus, sprendžiant privatumo klausimus ir kitus rūpimus aspektus, kurie jiems gali kilti.

Politikos formuotojams artimiausioje ateityje gali ir nebūti daug darbo, išskyrus kylančią riziką, susijusią su asmens duomenų naudojimu. Be to, jie paprastai dalyvauja sprendžiant su veiksmingumo standartais susijusius klausimus arba tais atvejais, kai reikia pritarti konkretiems sprendimams. Jų vaidmuo ateityje gali būti susijęs su pastangų suderinimu, geresnės praktikos nustatymu ir veikla skaitmeniniu formatu.

Apibendrinant galima teigti, kad žvelgiant į iš DSS perspektyvos dinaminis rizikos vertinimas – tai perėjimas prie skaitmeninio rizikos vertinimo siekiant daug greičiau spręsti su dinamine rizika susijusius klausimus nei anksčiau. Patirtis kitose srityse rodo, kad požiūris yra sėkmingas, o tai reiškia, kad DSS rizikos vertinimas gali būti grindžiamas tik remiantis tose srityse suformuota praktika. Turėdami keletą DSS rizikos vertinimo priemonių Europoje (pvz., OiRA, „BeSafe“ ir RIE), jau žengiame į skaitmeninę ateitį, tačiau paskatos veiksniai yra kitokie; jeigu DSS platformos yra orientuotos į tai, kad būtų pasiektas didesnis procentinis rodiklis darboviečių, kuriose atliekamas privalomas rizikos vertinimas, dinaminis rizikos vertinimas yra orientuotas į greitesnį veikimą. Pažymėtina, kad Pamatinėje direktyvoje ar kitame teisės akte nėra jokio esminio teisinio reikalavimo, pagal kurį rizikos vertinimas turėtų būti atliktas naudojant skaitmenines sistemas; atrodo, kad paskata yra finansinė arba paprasčiausiai susijusi su tuo, kad stengiamasi dirbti neatsiliekant nuo naujausių technologijų suteikiamų galimybių.

Autorius Coen van Gulijk, „TNO Healthy Living“, Hadersfildo universitetas, Delfto technologijų universitetas.
Projektą administravo: Annick Starren, Europos darbuotojų saugos ir sveikatos agentūra (EU-OSHA).

Šį diskusijoms skirtą dokumentą užsakė Europos darbuotojų saugos ir sveikatos agentūra (EU-OSHA). Santrauką, taip pat visas joje pateiktas nuomones ir (arba) išvadas, parengė autoriai ir jų turinys nebūtinai atitinka EU-OSHA nuomonę.

Bibliografija ir nuorodos

CCPS (Cheminių procesų saugos centras) (2018). *Bow ties in risk management: A concept book for process safety*. John Wiley & Sons.

De Stefano, V. (2018). *„Negotiating the algorithm“: Automation, artificial intelligence and labour protection*. EMPLOYMENT Working Paper No. 246. Tarptautinė darbo organizacija. Skelbiama adresu: https://www.ilo.org/employment/Whatwedo/Publications/working-papers/WCMS_634157/lang--en/index.htm

1989 m. birželio 12 d. Europos bendrijų direktyva 89/391/EEB dėl priemonių darbuotojų saugai ir sveikatos apsaugai darbe gerinti nustatymo. Skelbiama adresu: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A31989L0391
Taip pat žr.: https://osha.europa.eu/en/legislation/directives/the-osh-framework-directive/

2006 m. gegužės 17 d. Europos Parlamento ir Tarybos direktyvą 2006/42/EB dėl mašinų, iš dalies keičiančią Direktyvą 95/16/EB (nauja redakcija). Skelbiama adresu: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0042

2012 m. liepos 4 d. Europos Parlamento ir Tarybos direktyva 96/82/EB dėl didelių, su pavojingomis medžiagomis susijusių avarijų pavojaus kontrolės (nauja redakcija). Skelbiama adresu: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012L0018

2016 m. gegužės 11 d. Europos Parlamento ir Tarybos direktyva 2016/798 dėl geležinkelių saugos. Skelbiama adresu: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0798

EU-OSHA (Europos darbuotojų saugos ir sveikatos agentūra) (2018) *Prognozės dėl naujos ir atsirandančios rizikos, susijusios su skaitmeninimu iki 2025 m.* Europos rizikos stebėjimo tarnybos ataskaita. Europos Sąjungos leidinių biuras, Liuksemburgas. Skelbiama adresu: https://osha.europa.eu/en/publications/foresight-new-and-emerging-occupational-safety-and-health-risks-associated

EU-OSHA (Europos darbuotojų saugos ir sveikatos agentūra) (2020) *Europos įmonių apklausa apie naują ir kylančią riziką (ESENER 2019). Informacinis pranešimas*. Skelbiama adresu: https://osha.europa.eu/en/publications/european-survey-enterprises-new-and-emerging-risks-esener-2019-background-briefing

EU-OSHA (Europos darbuotojų saugos ir sveikatos agentūra (2021a). *OiRA ir kitos nacionalinėse DSS strategijose ir teisės aktuose numatytos rizikos vertinimo priemonės.* Skelbiama adresu: https://oshwiki.eu/wiki/OiRA_and_other_online_risk_assessment_tools_in_national_OSH_strategies_and_legislation#cite_note-20

EU-OSHA (Europos darbuotojų saugos ir sveikatos agentūra (2021b). *Kas yra rizikos vertinimas?* Skelbiama adresu: https://oiraproject.eu/en/what-risk-assessment

Europos Komisija (2020). *Dirbtinis intelektas. Europos požiūris į kompetenciją ir pasitikėjimą* [baltoji knyga]. COM(2020) 65 *final*. Skelbiama adresu: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

Europos elektrotechninės standartizacijos komitetas (CENELEC) (2017). *Railway applications - The specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 1: Generic RAMS Process.* Standard No EN 50126–1:2017. Skelbiama adresu: https://www.cenelec.eu/dyn/www/f?p=104:110:1185783283395501::::FSP_ORG_ID,FSP_PROJECT,FSP_LANG_ID:1257173,60236,25

IBM (2018). *IBM data risk manager*. Skelbiama adresu: https://www.ibm.com/downloads/cas/XEMQ1MDK

IEC (Tarptautinė elektrotechnikos komisija) (2020). *Safety in the future* [White Paper]. Skelbiama adresu: https://www.iec.ch/basecamp/safety-future

Tarptautinė standartizacijos organizacija (ISO) (2018). *Occupational health and safety management systems — Requirements with guidance for use* (ISO Standard No 45001:2018). Skelbiama adresu: https://www.iso.org/iso-45001-occupational-health-and-safety.html

Jain, R., Nauck, F., Poppensieker, T., & White, O. (2020 m. lapkričio 17 d.). *Meeting the future: Dynamic risk management for uncertain times*. McKinsey & Company. Skelbiama adresu: https://www.mckinsey.com/business-functions/risk/our-insights/meeting-the-future-dynamic-risk-management-for-uncertain-times

Kalantarnia, M., Khan, F., & Hawboldt, K. (2010). Modelling of BP Texas City refinery accident using dynamic risk assessment approach. *Process Safety and Environmental Protection*, *88*(3), 191–199. https://doi.org/10.1016/j.psep.2010.01.004

Kaul, N., Lodha, A., Countryman, T., & Patel, P. (2018). *Digitizing operational risk for improved safety performance*. Gauta 2021 m. kovo 24 d. adresu: https://www.accenture.com/t20180711t081149z__w__/tw-en/_acnmedia/pdf-82/accenture-pov-digital-barrier-management.pdf

Khakzad, N., Khan, F., & Amyotte, P. (2012). Dynamic risk analysis using bow-tie approach. *Reliability Engineering & System Safety*, *104*, 36–44. https://doi.org/10.1016/j.ress.2012.04.003

Khakzad, N., Khan, F., & Amyotte, P. (2013). Quantitative risk analysis of offshore drilling operations: A Bayesian approach. *Safety Science, 57*, 108–117. https://doi.org/10.1016/j.ssci.2013.01.022

Khan, F., Hashemi, S.J., Paltrinieri, N., Amyotte, P., Cozzani, V., & Reniers, G. (2016). Dynamic risk management: A contemporary approach to process safety management. *Current Opinion in Chemical Engineering*, *14*, 9–17. http://dx.doi.org/10.1016/j.coche.2016.07.006

Pasman, H., & Rogers, W. (2014). How can we use the information provided by process safety performance indicators? Possibilities and limitations. *Journal of Loss Prevention in the Process Industries*, *30*, 197–206. https://doi.org/10.1016/j.jlp.2013.06.001

Pitblado, R., Fisher, M., Nelson, B., Fløtaker, H., Molazemi, K., & Stokke, A. (2016). Concepts for dynamic barrier management. *Journal of Loss Prevention in the Process Industries*, *43*, 741–746. http://dx.doi.org/10.1016/j.jlp.2016.07.005

Terblanche, A., & O'Donnell, R. (2018). *Dynamic risk assessment. The power of four*. KPMG International Cooperative. Skelbiama adresu: https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/03/dynamic-risk-assessment-for-audit-brochure.pdf

Jungtinių Valstijų gynybos departamentas (2012 m. gegužės 11 d.). *System safety*. MIL-STD-882 E. Skelbiama adresu: https://www.acqnotes.com/Attachments/MIL-STD-882E%20System%20Safety%205%20Nov%202012.pdf

Vinnem, J., Bye, R., Gran, B., Kongsvik, T., Nyheim, O., Okstadd, H., Seljelid, J., & Vatn, J. (2012). Risk modelling of maintenance work on major process equipment on offshore petroleum installations. *Journal of Loss Prevention in the Process Industries*, *25*(2), 274–292. https://doi.org/10.1016/j.jlp.2011.11.001