



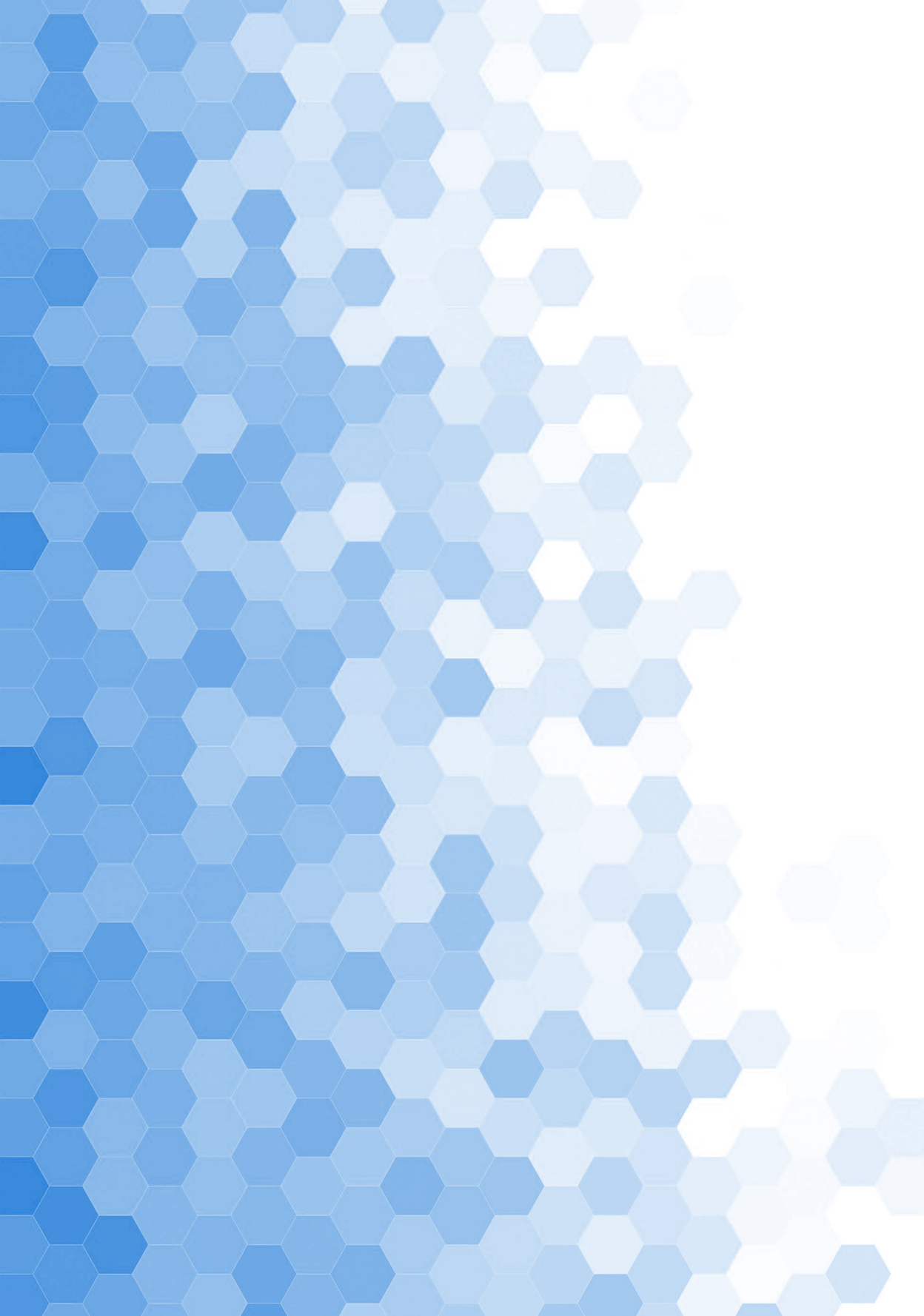
DIGITALNA TRANSFORMACIJA V LOGISTIKI IN MANAGEMENTU OSKRBOVALNIH VERIG

UREDNIK

Matevž
Obrecht



Univerzitetna založba
Univerze v Mariboru





Univerza v Mariboru

Fakulteta za logistiko

Digitalna transformacija v logistiki in managementu oskrbovalnih verig

Urednik
Matevž Obrecht

April 2025

Naslov <i>Title</i>	Digitalna transformacija v logistiki in managementu oskrbovalnih verig <i>Digital Transformation in Logistics and Supply Chain Management</i>
Urednik <i>Editor</i>	Matevž Obrecht (Univerza v Mariboru, Fakulteta za logistiko)
Recenzija <i>Review</i>	Benjamin Marcen (Univerza v Mariboru, Fakulteta za logistiko)
	Jure Erjavec (Univerza v Ljubljani, Ekonomska fakulteta)
Lektoriranje <i>Language editing</i>	Mateja Forte (Univerza v Mariboru, Fakulteta za logistiko)
Tehnični urednik <i>Technical editor</i>	Jan Perša (Univerza v Mariboru, Univerzitetna založba)
Oblikovanje ovitka <i>Cover designer</i>	Jan Perša (Univerza v Mariboru, Univerzitetna založba)
Grafika na ovitku <i>Cover graphic</i>	Logistics web, avtor: Gerd Altmann, pixabay.com, 2023
Grafične priloge <i>Graphic material</i>	Viri so lastni, razen če ni navedeno drugače. Avtorji prispevkov in Obrecht (urednik), 2025
Založnik <i>Published by</i>	Univerza v Mariboru Univerzitetna založba Slomškov trg 15, 2000 Maribor, Slovenija https://press.um.si , zalozba@um.si
Izdajatelj <i>Issued by</i>	Univerza v Mariboru Fakulteta za logistiko Mariborska cesta 7, 3000 Celje, Slovenija https://www.fl.um.si , info.fl@um.si
Izdaja <i>Edition</i>	Prva izdaja
Vrsta publikacije <i>Publication type</i>	E-knjiga
Dostopno na <i>Available at</i>	http://press.um.si/index.php/ump/catalog/book/944
Izdano <i>Published at</i>	Maribor, april 2025

Ime projekta Vzpostavitev okolja za izobraževanje zelene in digitalne logistike
Project name ter oskrbovalnih verig

Financer projekta Projekt sofinancirata Republika Slovenija, Ministrstvo za visoko
Project financier šolstvo, znanost in inovacije, in Evropska unija - NextGenerationEU. Projekt se izvaja skladno z načrtom v okviru razvojnega področja Pametna, trajnostna in vključujoča rast, komponente Krepitev kompetenc, zlasti digitalnih in tistih, ki jih zahtevajo novi poklici in zeleni prehod (C3 KS), za ukrep investicija F. Izvajanje pilotnih projektov, katerih rezultati bodo podlaga za pripravo izhodišč za reformo visokega šolstva za zelen in odporen prehod v Družbo S.O: projekt Pilotni projekti za prenovno visokega šolstva za zelen in odporen prehod. Projekt je del sheme NOO (Načrt za okrevanje in odpornost)



© **Univerza v Mariboru, Univerzitetna založba**
/ *University of Maribor, University Press*

Besedilo / *Text* © avtorji prispevkov in Obrecht (urednik), 2025

To delo je objavljeno pod licenco Creative Commons Priznanje avtorstva-Nekomercialno-Brez predelav 4.0 Mednarodna. / *This work is licensed under the Creative Commons Attribution-NonCommercialNoDerivs 4.0 International License.*

Uporabnikom je dovoljeno reproduciranje brez predelave avtorskega dela, distribuiranje, dajanje v najem in priobčitev javnosti samega izvirnega avtorskega dela, in sicer pod pogojem, da navedejo avtorja in da ne gre za komercialno uporabo.

Vsa gradiva tretjih oseb v tej knjigi so objavljena pod licenco Creative Commons, razen če to ni navedeno drugače. Če želite ponovno uporabiti gradivo tretjih oseb, ki ni zajeto v licenci Creative Commons, boste morali pridobiti dovoljenje neposredno od imetnika avtorskih pravic.

<https://creativecommons.org/licenses/by-nc-nd/4.0/>

CIP - Kataložni zapis o publikaciji
Univerzitetna knjižnica Maribor

658.286:004 (082) (0.034.2)

DIGITALNA transformacija v logistiki in managementu oskrbovalnih verig
[Elektronski vir] / urednik Matevž Obrecht. - 1. izd. - E-knjiga. - Maribor :
Univerza v Mariboru, Univerzitetna založba, 2025

Način dostopa (URL): <https://press.um.si/index.php/ump/catalog/book/944>

ISBN 978-961-286-971-7 (PDF)
doi: 10.18690/um.fl.2.2025
COBISS.SI-ID 231943171

ISBN 978-961-286-971-7 (pdf)
978-961-286-972-4 (trda vezava)

DOI <https://doi.org/10.18690/um.fl.2.2025>

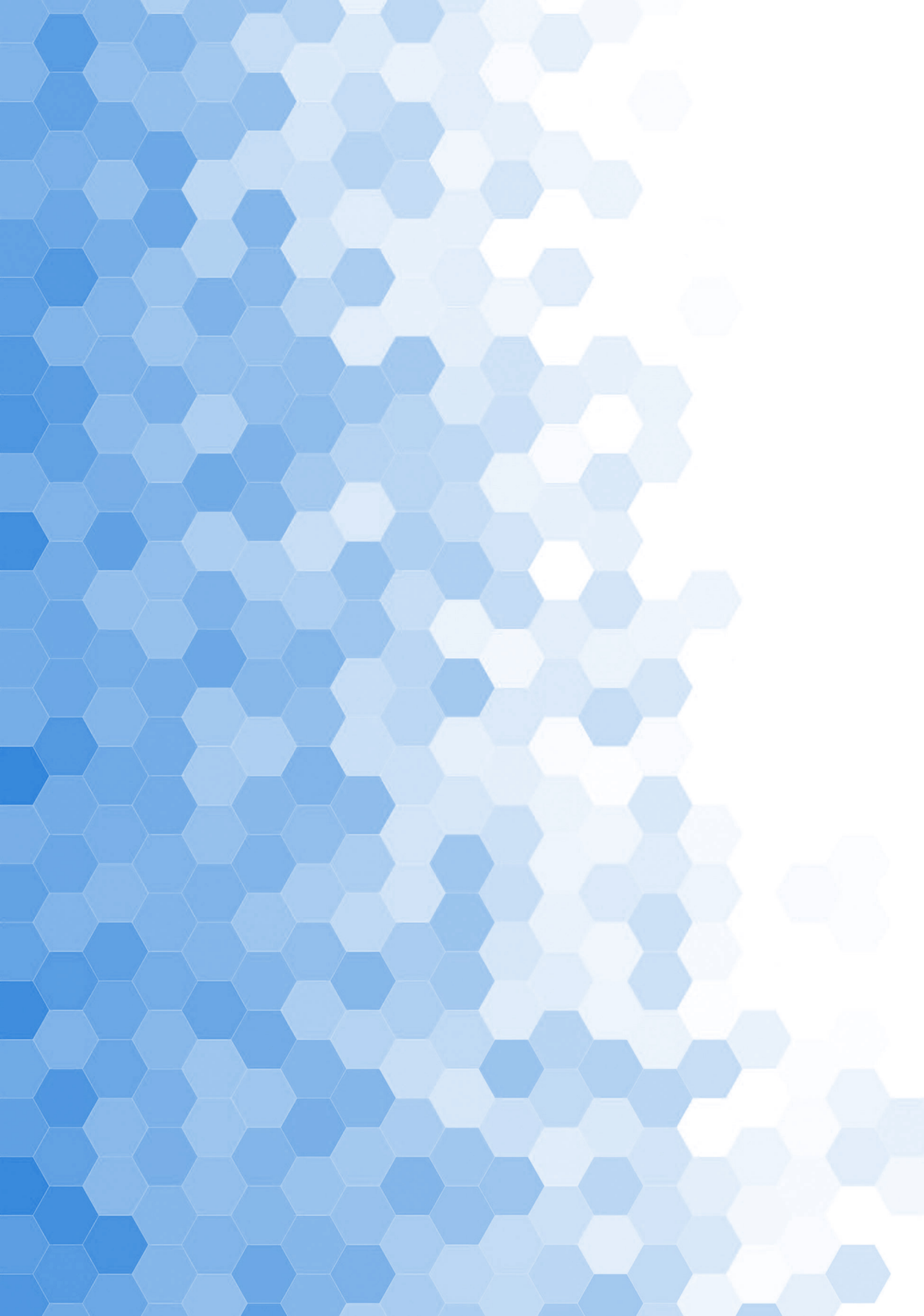
Cena
Price Brezplačni izvod

Odgovorna oseba založnika prof. dr. Zdravko Kacič,
For publisher rektor Univerze v Mariboru

Citiranje Obrecht, M. (ur.). (2025). *Digitalna transformacija v logistiki in*
Attribution managementu oskrbovalnih verig. Univerza v Mariboru,
Univerzitetna založba. doi: 10.18690/um.fl.2.2025

Kazalo

1	Digitalizacija – načrtovanje <i>Digitalization – Planning</i> Borut Jereb	1
2	Digitalizacija – izvajanje <i>Digitalization – Implementation</i> Borut Jereb	19
3	Informacijska in računalniška varnost <i>Information and Computer Security</i> Nena Orel Šanko	39
4	Poslovni informacijski sistemi <i>Business Information Systems</i> Bojan Rupnik	59
5	Podpora odločanja s simulacijami <i>Simulations in Decision Making</i> Bojan Rupnik	77
6	Avtonomna vozila v intralogistiki <i>Autonomous Vehicles in Intralogistics</i> Darko Hercog, Primož Bencak	93



DIGITALIZACIJA – NAČRTOVANJE

BORUT JEREB

Univerza v Mariboru, Fakulteta za logistiko, Celje, Slovenija
borut.jereb@um.si

Elektronsko poslovanje (e-poslovanje) igra ključno vlogo v sodobnem digitalnem okolju, preoblikuje poslovne prakse in odpira nove možnosti. Predstavljen je model vrednostne verige e-poslovanja, ki zajema podporne procese, vrednostno verigo in tehnološke rešitve. Poleg tega so obravnavani različni pristopi e-poslovanja, vključno z e-marketingom, e-dokumentacijo, e-plačili in e-upravljanjem s strankami. V nadaljevanju je poudarjena pomembnost informacijske in kibernetske varnosti v sodobnem poslovnem okolju. Varovanje digitalne pokrajine postaja ključno, pri čemer informacijska varnost zajema zaščito informacij, medtem ko kibernetska varnost obravnava zaščito digitalnih sistemov pred kibernetskimi grožnjami. Obe disciplini sta ključni za ohranjanje zaupanja in varnosti pri e-poslovanju. Na koncu prispevka je predstavljeno upravljanje IT tveganj s pomočjo standarda ISO/IEC 27005.

DOI

[https://doi.org/
10.18690/um.fl.2.2025.1](https://doi.org/10.18690/um.fl.2.2025.1)

ISBN

978-961-286-971-7

Ključne besede:

digitalizacija,
e-poslovanje,
informacijska varnost,
kibernetska varnost,
IT tveganja



Univerzitetna založba
Univerze v Mariboru

DOI
[https://doi.org/
10.18690/um.fl.2.2025.1](https://doi.org/10.18690/um.fl.2.2025.1)

ISBN
978-961-286-971-7

Keywords:
digitalization,
e-business,
information security,
cyber security,
IT risks

DIGITALIZATION – PLANNING

BORUT JEREB

University of Maribor, Faculty of Logistics, Celje, Slovenia
borut.jereb@um.si

E-business plays a crucial role in the modern digital environment, transforming business practices and opening new possibilities. The model of the e-business value chain is presented, encompassing supporting processes, the value chain, and technological solutions. Additionally, various e-business approaches are addressed, including e-marketing, e-documentation, e-payments, and e-customer management. The importance of information and cyber security in the contemporary business environment is emphasized. Safeguarding the digital landscape becomes crucial, with information security covering the protection of information, while cyber security addresses the protection of digital systems from cyber threats. Both disciplines are essential for maintaining trust and security in e-business. The article concludes with the presentation of IT risk management using the ISO/IEC 27005 standard.



University of Maribor Press

1 Uvod

V hitro spreminjajočem se okolju digitalne dobe se je elektronsko poslovanje ali e-poslovanje pojavilo kot usmeritev in pot, ki spreminja način, kako organizacije izvajajo svoje operacije in komunicirajo z deležniki. Pri podjetjih se e-poslovanje nanaša na uporabo digitalnih tehnologij in interneta za poenostavitev in izboljšanje različnih poslovnih procesov; od nakupovanja in prodaje blaga ter storitev do upravljanja notranjih operacij in sodelovanja s partnerji. Pri trgovanju pa, za razliko od tradicionalnih poslovnih modelov, e-poslovanje presega geografske omejitve in časovno omejenost, tako da zagotavlja globalno platformo za trgovino.

Obsega širok spekter spletnih dejavnosti, vključno z e-trgovino, e-marketingom, e-upravljanjem dobavnih verig in e-nabavo. Integracija tehnologije ne le omogoča bolj učinkovite in stroškovno smotrne poslovne prakse, temveč odpira tudi nove možnosti za inovacije in prilagajanje trgu.

Ključni elementi e-poslovanja vključujejo vzpostavitev prisotnosti na spletu, izvajanje varnih elektronskih transakcij, izkoriščanje podatkovne analitike za informirano odločanje ter prilagajanje nenehno spreminjajočemu se digitalnemu okolju. Uspeh podjetja v okolju e-poslovanja je odvisen od njegove sposobnosti ustvarjanja brezhibnih in privlačnih izkušenj za stranke, vzpostavljanja zaupanja in varnosti pri spletnih transakcijah ter izkoriščanja vpogledov, pridobljenih iz (največkrat masivnih) podatkov, da ostane podjetje konkurenčno na dinamično spreminjajočem se trgu.

Ker tehnologija nenehno napreduje in se spreminja, bo e-poslovanje igralo vse pomembnejšo vlogo pri oblikovanju prihodnosti poslovanja v podjetju in med podjetji – predvsem, ko govorimo o oskrbovalnih verigah. Ne glede na to, ali gre za zagonsko podjetje ali uveljavljeno multinacionalko, je razumevanje in izkoriščanje moči e-poslovanja ključno za uspeh pri poslovanju v okolju digitalne ekonomije. Pri tem podjetja ne smejo premagovati le tehnoloških izzivov, temveč tudi spreminjajoča se pričakovanja pri povezovanju z digitalno veščimi zaposlenimi in kupci znotraj in zunaj meja samega podjetja.

V nadaljevanju želimo bralca napotiti v iskanje poti za to, da bo znal:

- pregledati in analizirati tisti del poslovanja v njegovem okolju, ki bi ga bilo smiselno digitalizirati,
- prepoznati pomen informacijske in kibernetske varnosti in ju kot taki znati načrtovati v vlogi srednjega upravljaljskega sloja
- ter kritično ovrednotiti IT tveganja v vlogi srednjega upravljaljskega sloja.

2 e-poslovanje

E-poslovanje je celovit pristop k izvajanju poslovnih procesov s pomočjo elektronskih sredstev. To velja tudi za izvajanje poslovnih procesov, ki podpirajo izvajanje logističnih procesov. Obsega širok nabor dejavnosti, ki izkoriščajo digitalne tehnologije za optimizacijo operacij, izboljšanje izkušenj strank in povečanje splošne učinkovitosti poslovanja. E-poslovanje vključuje tako notranje kot zunanje interakcije organizacij in si prizadeva preoblikovati tradicionalne poslovne prakse s povezovanjem elektronskih sistemov in komunikacijskih kanalov. Koncept e-poslovanja spreminja način, kako organizacije izvajajo svoje operacije, komunicirajo s strankami in ustvarjajo vrednost. Predstavlja celovit premik k izvajanju poslovnih procesov z elektronskimi sredstvi, spodbuja učinkovitost, inovacije in globalni doseg.

Izvor e-poslovanja sega v zgodnje dni interneta. Z nastankom e-poslovanja (e-trgovine) je bila vpeljana zamisel o nakupovanju in prodaji izdelkov na spletu. Vendar se je s časom razvijala tudi zamisel o e-poslovanju, ki obsega množico dejavnosti, ki se raztezajo daleč preko digitalnih trgovin.

E-poslovanje je tako sestavljeno iz poslovanja, ki bazira na informacijsko-komunikacijskih tehnologijah (IKT). Nekatera ključna področja takšnega poslovanja so:

- **e-marketing:** uporaba digitalnih kanalov, kot so: socialna omrežja, e-poštni marketing, optimizacija spletnih iskalnikov (SEO) in spletno oglaševanje za promocijo izdelkov ali storitev ter dosego širšega občinstva.

- **E-trgovina:** kot že omenjeno, je e-trgovina pomemben del e-poslovanja. Vključuje spletno kupovanje in prodajo blaga ter storitev, zajema različne poslovne modele in platforme.
- **E-upravljanje s strankami (e-CRM):** upravljanje in negovanje odnosov s strankami s pomočjo digitalnih orodij in platform. To vključuje sledenje interakcijam s strankami, analizo podatkov za prilagajanje izkušenj ter zagotavljanje učinkovite podpore strankam preko spleta.
- **E-upravljanje oskrbovalne verige (e-SCM):** uporaba digitalnih tehnologij za optimizacijo procesov v oskrbovalni verigi; od nabave in upravljanja zalog do izpolnjevanja naročil in distribucije.
- **E-nabava:** uporaba elektronskih sistemov za upravljanje nabave blaga in storitev, vključno z izbiro dobaviteljev, izdajanjem naročil in upravljanjem odnosov z dobavitelji.
- **E-sodelovanje:** omogočanje sodelovanja med zaposlenimi in partnerji preko digitalnih platform, videokonferenc in orodij v oblaku.
- **E-upravljanje z znanjem:** upravljanje in deljenje organizacijskega znanja elektronsko za izboljšanje odločanja, reševanja problemov in inovacij.
- **E-analiza podatkov in poslovna inteligenca:** uporaba orodij za analizo podatkov za pridobivanje vpogleda iz obsežnih naborov podatkov, kar omogoča odločanje na podlagi podatkov.
- **E-plaćila in finančne transakcije:** obdelava elektronskih plačil, spletno izdajanje računov in varno upravljanje finančnih transakcij preko digitalnih platform.

V nadaljevanju so našteje nekatere koristi, ki so pogojene z značilnostmi e-poslovanja. Ključne sestavine in vplivi e-poslovanja so:

- **digitalna transformacija:** e-poslovanje je pospešilo proces digitalne transformacije v vseh panogah. Organizacije so prešle iz tradicionalnih poslovanj v integrirane digitalne ekosisteme, ki poenostavljajo procese, izboljšujejo izkušnje strank in povečujejo celotno učinkovitost.
- **Globalni doseg:** e-poslovanje omogoča podjetjem, da dosežejo globalno občinstvo brez omejitev geografskih meja.
- **Učinkovito nižanje stroškov:** digitalni procesi lahko znižajo operativne stroške, kot so dokumentacija na papirju in fizična infrastruktura. Priča smo

novim ekonomskim modelom in priložnostim za zaposlovanje. Začetniki in podjetniki lahko nastopajo in se vključujejo v globalne trge z minimalnimi vstopnimi ovirami, kar spodbuja gospodarsko rast.

- **Poudarek na strankah/partnerjih:** e-poslovanje omogoča prilagojene interakcije, hitre odzive in priročen dostop do informacij, kar povečuje zadovoljstvo strank. Stranke in/ali partnerji so v središču (poslovnih) operacij. S pomočjo podatkov, ki temeljijo na analitiki, organizacije razumejo želje, vedenje in potrebe strank in partnerjev, kar vodi v prilagojene interakcije in ponudbe.
- **Optimizirani procesi:** avtomatizacija nalog in procesov vodi v večjo učinkovitost in zmanjšanje števila človeških napak. Avtomatizacija, integracija in digitalizacija procesov povečujejo operativno učinkovitost. Od upravljanja dobavne verige do nadzora zalog in obdelave naročil, e-poslovanje optimizira uporabo virov in znižuje stroške.
- **Vpogledi v masovne podatke in odločanje na podlagi podatkov:** e-poslovanje ustvarja dragocene podatke, ki jih je mogoče analizirati, da bi dobili vpogled v obnašanje strank, trende na trgu in poslovno uspešnost.
- **Konkurenčna prednost:** organizacije, ki sprejemajo strategije e-poslovanja, so bolje pozicionirane za prilagajanje spreminjajočim se tržnim razmeram in preseganje konkurence.
- **Inovacije in agilnost:** e-poslovanje spodbuja okolje inovacij. Organizacije se hitro prilagajajo spreminjajočim se dinamikam trga, uvajajo nove storitve in izdelke ter preizkušajo nove poslovne modele brez zamud. Hitro in skoraj v realnem času.

Tako e-poslovanje zajema različne vidike sodobnih poslovnih operacij, ki izkoriščajo digitalne tehnologije za izboljšanje učinkovitosti, vključevanje strank ter splošno konkurenčnost. Gre za sprejemanje celostnega pristopa k upravljanju poslovanja v digitalni dobi.

E-poslovanje tako ponuja številne prednosti, kot so večji doseg, prihranek stroškov in udobje, ima pa tudi več negativnih vidikov, ki jih morajo podjetja upoštevati in obravnavati, da zagotovijo trajnostno in uspešno spletno poslovanje. To vključuje vlaganje v robustne varnostne ukrepe, učinkovito upravljanje logistike, zagotavljanje

skladnosti s pravnimi predpisi ter vzpostavljanje zaupanja in zadovoljstva strank z zanesljivimi storitvami in varnimi transakcijami.

Nekateri ključni negativni vidiki e-poslovanja, ki jih je potrebno še posebej pozorno nasloviti pri e-poslovanju, so:

- **varnostni izzivi:** e-poslovanje vključuje prenos občutljivih podatkov, vključno s finančnimi transakcijami in osebnimi informacijami. To pomeni, da je e-poslovanje tarča kibernetских napadov, kot so hekerski vdori, "phishing" in zlonamerna programska oprema. Podjetja morajo veliko vlagati v kibernetisko varnost, da zaščitijo podatke, kar je lahko drago in zapleteno.
- **Izziv zasebnosti:** z zbiranjem ogromnih količin podatkov o potrošnikih se pojavijo resni pomisleki glede zasebnosti. Podjetja morajo zagotoviti, da upoštevajo predpise o varstvu podatkov, kot je GDPR. Neupoštevanje teh predpisov lahko povzroči pravne posledice in izgubo zaupanja strank.
- **Tehnične težave:** e-poslovanje močno temelji na tehnologiji. Tehnične težave, kot so izpadi spletnih strani, programske napake ali počasno nalaganje, lahko motijo poslovanje, kar vodi do izgube prodaje in nezadovoljnih strank.
- **Visoki začetni stroški:** vzpostavitev robustne infrastrukture za e-poslovanje je lahko drago. To vključuje stroške razvoja uporabniku prijazne spletne strani, obratovanje varnih plačilnih sistemov in integracijo potrebnih zalednih sistemov. Ti začetni vložki so lahko ovira za mala podjetja.
- **Intenzivna konkurenca:** internet je v mnogih segmentih delovanja izenačil pogoje za delovanje največjih in najmanjših podjetij. Povečana konkurenca otežuje, da bi podjetja izstopala in privabljala stranke, kar pogosto zahteva znatne naložbe v trženje in strategije diferenciacije.
- **Logistični izzivi:** e-poslovna podjetja morajo še dodatno pozornost posvetiti upravljanju logističnih procesov. To vključuje skladiščenje, upravljanje zalog, pošiljanje in obdelavo vračil. Slabo upravljanje logistike lahko povzroči zamude pri dostavi in povišane stroške, kar negativno vpliva na zadovoljstvo strank.
- **Odvisnost od tehnologije:** pri e-poslovanju so podjetja zelo odvisna od tehnologije, kar pomeni, da lahko katerakoli tehnološka okvara ustavi

poslovanje. Podjetja morajo imeti robustno IT podporo in načrte za obnovitev po nesrečah, da bi zmanjšala IT tveganja.

- **Zaupanje in zadovoljstvo strank:** vzpostavljanje zaupanja s strankami je na spletu bolj zahtevno kot v fizičnih trgovinah. Težave, kot so nezmožnost fizičnega pregleda izdelkov pred nakupom, skrbi glede varnosti plačil in zamude pri odzivanju na poizvedbe strank, lahko zmanjšajo zadovoljstvo strank.
- **Pravna in regulativna skladnost:** pri e-poslovanju se morajo podjetja spoprijeti z zapleteno mrežo predpisov, ki se razlikujejo glede na regijo in industrijo. Ti vključujejo zakone o varstvu potrošnikov, predpise o elektronskem poslovanju in mednarodne trgovinske zakone. Neskladnost lahko privede do glob in drugih težav pri doseganju pravnih norm.
- **Pomanjkanje osebne interakcije:** pomanjkanje osebne interakcije v e-poslovanju otežuje vzpostavljanje poglobljenih odnosov s strankami. Osebnostno naravnane storitve in človeški stiki pogosto igrajo ključno vlogo pri zvestobi in zadovoljstvu strank.
- **Upravljanje vračil in povračil:** upravljanje vračil in povračil v e-poslovanju je lahko bolj zapleteno in drago kot v tradicionalni trgovini. Postopek vključuje obdelavo obratne logistike, ponovno založitev in obravnavanje morebitne izgube ali poškodbe vrnjenih predmetov.
- **Digitalni razkorak:** niso vsi potencialni kupci enako dostopni do interneta ali digitalnih naprav, kar vodi do digitalnega razkoraka. To omejuje doseg e-poslovanja podjetij, zlasti v regijah z nizko internetno penetracijo ali med demografskimi skupinami z manj tehnološke pismenosti.

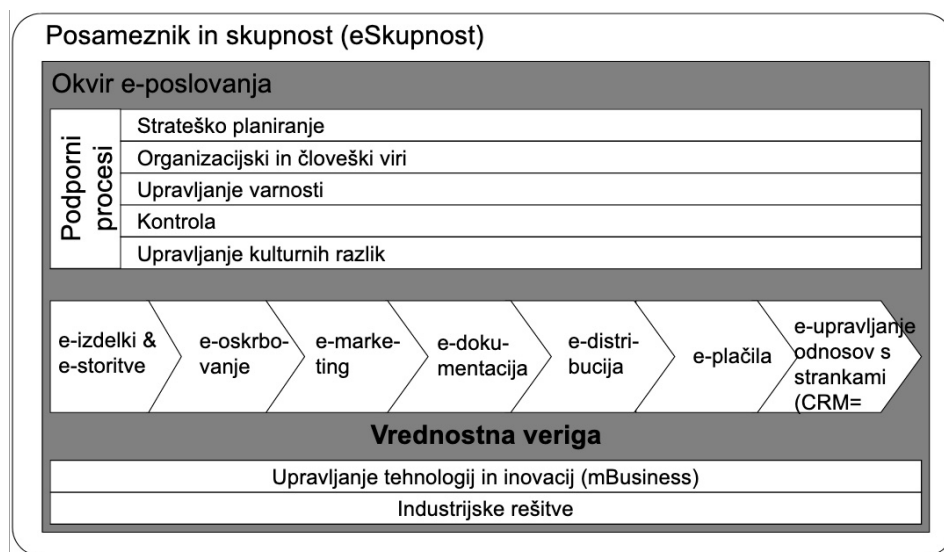
2.1 Model e-poslovanja

Na sliki 1.1 je prikazan model vrednostne verige e-poslovanja po knjigi Meier & Stormer (Meier, 2009). Slika prikazuje tri bistvene sestavine e-poslovanja, ki so:

- podporni procesi za izvajanje e-poslovanja,
- vrednostna veriga e-poslovanja,
- tehnično-tehnološke rešitve za podporo izvajanja e-poslovanja.

Podporne procese sestavljajo: strateško načrtovanje, organizacijski in kadrovski viri, upravljanje informacijske in kibernetske varnosti, kontrola ter upravljanje kulturnih razlik. Vsi ti procesi so pogojeni in so v zvezi z e-poslovanjem. Predpostavljamo, da je znanje o teh procesih že prisotno ali pa ga je treba pridobiti iz literature o managementu.

Vrednostno verigo sestavlja sedem različnih pristopov, ki pa se medsebojno dopolnjujejo in v vsakem od omenjenih pristopov je mogoče najti druge pristope. Pa vendar, na levi strani te vrednostne verige so pristopi, ki zahtevajo nižje vložke, praviloma tudi dajejo rezultate nižje vrednosti. Bolj, kot gremo proti desni, večji so vložki za realizacijo rešitve in pričakovane so večje koristi.



Slika 1.1: Model e-poslovanja

Vir: A. Meier & H. Stormer

Pri organizaciji elektronskih izdelkov in storitev je naloga organizacije najti ustrezno obliko sodelovanja s pomočjo poslovnega modela. Takšne oblike sodelovanja med organizacijami in morebitnimi kupci segajo od povsem enostavne in informativne predstavitve blaga, odprtih tržnic z blagom in njenimi vrednostmi, pa do bolj zaprtih sistemov, kjer deležniki takšne tržnice medsebojno sodelujejo.

Naslednji pristop pri e-poslovanju je namenjen elektronsko podprtim nabavnim postopkom. Načeloma obstaja vrsta rešitev za e-oskrbovanje. Rešitve se medsebojno razlikujejo glede na to, ali so katalogi izdelkov in storitev za izbiro in nabavo izdelkov na voljo na strani kupca (buy side) ali na strani dobavitelja (sell side). V tretji varianti (elektronski trg) tretja stranka zagotavlja programske rešitve in kataloge za nabavo. Tako se lahko uporabljajo primerjave in vrednotenje izdelkov in storitev. Upravljanje katalogov predstavlja poseben izziv.

e-marketing (ali spletni marketing) deluje tako, da s pomočjo elektronskih sredstev pridobivanja informacij in komuniciranja izkorišča tržne potenciale in neguje poslovne odnose. Segmentacija spletnih »kupcev« na kategorije omogoča izvajanje raznolikega marketinškega procesa in takojšnjega prilagajanja storitev spletnega marketinga. Prvi uspešni globalni primer tovrstnega e-poslovanja je bilo podjetje Google. Sledil je Facebook in ostali. Z ustreznimi ključnimi kazalci omogočajo merjenje učinkovitosti ponudb preko spleta (na primer z uporabo spletnega brskalnika), izračunavajo lahko stopnje interakcije (če govorimo, da je na drugi strani spletni potrošnik), spodbujajo spletne stranke k ustvarjanju njihovih (lahko navideznih) vrednosti, izvedejo poslovne transakcije (spletni kupec) ter vzdržujejo povezave s stranko (spletni ključni kupec). Pri tem je seveda treba preučiti in analizirati posebnosti spletnega oglaševanja.

Naslednji pristop se ukvarja s konceptom e-dokumentacije. Tu se elektronski dokument obravnava kot pravno veljaven dokument. Da bi to dosegli, je treba vzpostaviti zaupanja vredne centre, ki registrirajo dejanske osebe, izdajajo digitalna potrdila in zagotavljajo par elektronskih ključev za digitalni podpis. Asimetrični kriptografski postopki, ki uporabljajo zasebne in javne ključe, so osnovna zahteva pri uporabi takšnih potrdil in podpisov. Elektronski dokumenti se lahko elektronsko podpišejo na eni strani, na drugi strani pa se lahko izvede avtentikacija digitalnega podpisa. Dokumente lahko tudi ustrezno pretvorimo v elektronski kriptogram, ki dokaj dobro zaščiti dokument pred nezaželenimi vpogledi.

Pri elektronsko podprti distribuciji izdelka ali storitve, ki lahko nastopata v fizični ali elektronski obliki, govorimo o naslednji stopnji kompleksnosti elektronskega poslovanja. Če ima potrošnik za storitev pri roki mobilno napravo z internetno povezavo, lahko izkoristi časovno in lokacijsko neodvisen nakup ali storitev (spletna distribucija). Seveda, se tudi izdelki v elektronski obliki lahko distribuirajo na klasičen

način – to je ne po elektronski poti, saj ima tudi distribucija brez povezave v svetovni splet svoje prednosti. Poleg tega se lahko predstavljajo hibridne distribucijske oblike, ki kombinirajo spletno distribucijo z različico distribucije brez povezave. Distribucija je le del celovite oskrbovalne verige. Pri e-dobavi je potrebno s pomočjo referenčnega modela uskladiti korake načrtovanja, nabave, proizvodnje in dostave izdelkov in storitev.

Elektronsko plačevanje (e-plaćila) omogoča plačevanje majhnih vsot, ki vključujejo le nekaj centov (pikoplačilo), srednjih zneskov v nekaj evrih (mikroplačilo) in večjih zneskov (makroplačilo). Da bi zagotovili, da so transakcijski stroški za pikoplačila in mikroplačila dovolj nizki, da se izplačajo, so bile razvite metode, ki temeljijo na uporabi elektronskih kovancev. Poleg tega obstaja več računskih in lastniških postopkov za elektronska plačila. Da bi zagotovili varnost postopkov elektronskega plačevanja, je treba uporabljati kriptografske postopke in digitalne podpise. Tako na primer SET (varna elektronska transakcija) protokol zahteva uporabo dvojnega postopka podpisa, da so tako podatki o naročilu (v zvezi z trgovcem) kot tudi načini plačila (v zvezi z banko) varovani.

Pri e-upravljanju odnosov s strankami (e-Customer Relationship Management) se osredotočenost na same izdelke premakne k upravljanju s strankami. Poleg običajnih ključnih finančnih kazalnikov je poudarjeno, da je treba zajeti in ovrednotiti stranke, kupce ali na splošno deležnike. Relevantni podatki so shranjeni v skladišču podatkov o strankah, kar omogoča celovito analizo vedenja strank. Poleg analitičnega upravljanja odnosov s strankami uporabljamo tudi večkanalno upravljanje, ki predstavlja poseben izziv, saj je treba oceniti različne komunikacijske kanale s strankami in ugotoviti, kateri so primerni za uporabo. Ta pristop e-poslovanja zahteva največje vložke v realizacijo, vendar lahko zagotovi tudi največje donose. Ti donosi so lahko merjeni v denarju ali pa tudi drugače – na primer v poznavanju vedenja. V zadnjem času so bili vloženi veliki napor; predvsem v EU, v omejevanje zbiranja podatkov/informacij o posameznikih (kupcih) tako s strani posameznih podjetij kot tudi ostalih organizacij (na primer obveščevalnih služb).

3 Informacijska in kibernetska varnost

Varovanje digitalne pokrajine v hitro spreminjajoči se digitalni dobi, kjer so informacije in podatki v osrčju sodobnega delovanja, se je pomen informacijske varnosti in kibernetske varnosti povzpел na prvo mesto. Ti dve prepleteni disciplini sta namenjeni zagotavljanju razpoložljivosti, celovitosti in zaupnosti digitalnih informacij ter zaščiti posameznikov, organizacij in družb pred razširjenim svetom kibernetskih groženj. (Jereb, 2019) V nadaljevanju je predstavljen splošen pomen kibernetske varnosti v luči načrtovanja in izvajanja digitalizacije poslovanja.

Informacijska varnost obsega strategije, prakse in tehnologije, ki so uvedene za zaščito informacij pred nepooblaščenim dostopom, uporabo, razkritjem, motenjem, spreminjanjem ali uničenjem. Vključuje celosten pristop, ki obsega ljudi, procese in tehnologijo. Najpomembnejši ključni vidiki informacijske varnosti vključujejo:

- **razpoložljivost:** zagotavljanje, da so informacije in storitve dostopne in uporabne, kadar je to potrebno.
- **Celovitost:** ohranjanje natančnosti in zaupanja vrednosti podatkov s preprečevanjem nepooblaščenih sprememb.
- **Zaupnost:** zagotavljanje, da so informacije dostopne samo pooblaščenim posameznikom ali entitetam.
- **Avtentikacija in pooblastila:** preverjanje identitete uporabnikov in dodeljevanje ustrezne ravni dostopa.
- **Šifriranje podatkov:** pretvorba podatkov v neberljiv format, da se prepreči nepooblaščen dostop.
- **Upravljanje tveganj/ranljivosti:** identifikacija in naslavljanje ranljivosti, ki bi jih napadalci lahko izkoristili.
- **Usposabljanje zaposlenih:** izobraževanje zaposlenih o najboljših praksah varnosti in potencialnih tveganjih.

Kibernetska varnost se osredotoča na zaščito digitalnih sistemov, omrežij in naprav pred kibernetskimi grožnjami. Te grožnje obsegajo širok nabor zlonamernih dejavnosti, vključno s hekanjem, zlonamerno programsko opremo, izsiljevalsko programsko opremo, prevaro in še več. Ključni elementi kibernetske varnosti vključujejo:

- **varnost omrežja:** zaščita računalniških omrežij pred nepooblaščenim dostopom, vdorom v podatke in drugimi kibernetскими napadi.
- **Varnost končnih točk:** zavarovanje posameznih naprav (računalnikov, pametnih telefonov, naprav za internet stvari) pred zlonamerno programsko opremo in drugimi kibernetскими grožnjami.
- **Odziv na incidente:** razvijanje strategij za učinkovit odziv na kibernetiske incidente in zmanjšanje njihovega vpliva.
- **Ugotavljanje groženj:** zbiranje in analiziranje informacij o nastajajočih grožnjah, da bi napade predvideli in omilili.
- **Varnostna revizija in spremljanje:** redno ocenjevanje in spremljanje sistemov za znake vdorov ali sumljive dejavnosti.
- **Pravilniki in postopki kibernetiske varnosti:** ustvarjanje smernic in protokolov za zagotavljanje doslednih in učinkovitih varnostnih ukrepov.

V današnjem svetu, z medsebojno povezanimi organizacijami različnih tipov in velikosti, se pomembnost informacijske varnosti in kibernetiske varnosti ne more precenjevati. Kibernetiski napadi imajo potencial, da motijo kritično infrastrukturo, ogrozijo osebne podatke in škodujejo nacionalni varnosti. Izzivi na teh področjih se nenehno razvijajo zaradi naraščajoče kompleksnosti kibernetских kriminalcev, hitrega napredka tehnologije in vedno številčnejših možnosti za napad.

Pri reševanju informacijske in kibernetiske varnosti smo soočeni z izzivi, ki jih skušamo zaobiti z nekaterimi splošno sprejetimi strategijami zato, da bi si zagotovili varno digitalno okolje. Med temi strategijami so najpomembnejši proaktivni in celoviti pristopi, ki jih morajo sprejeti organizacije in posamezniki in vključujejo:

- **izobraževanje in usposabljanje:** neprekinjeno usposabljanje in programi ozaveščanja so ključni, da posameznike pooblastijo za prepoznavanje in odzivanje na kibernetiske grožnje.
- **Napredne tehnologije:** sprejemanje tehnologij, kot sta umetna inteligenca in strojno učenje za odkrivanje in preprečevanje kibernetских groženj v realnem času.
- **Sodelovanje:** deljenje informacij in obveščanje o grožnjah in najboljših praksah med organizacijami (tudi med vladami) za krepitev skupne kibernetiske varnosti.

- **Pravila in skladnost s predpisi:** spoštovanje predpisov in standardov za kibernetsko varnost za izboljšanje zaščite podatkov in zasebnosti.
- **Načrtovanje odpornosti:** razvijanje načrtov za odzivanje na incidente in obnovitev delovanja po nesrečah, da se zmanjša vpliv kibernetskih incidentov.

Bolj podroben opis zagotavljanja varnosti pred IT grožnjami in napadi predstavljamo v poglavju o informacijski in računalniški varnosti.

4 Upravljanje IT tveganj in investicij

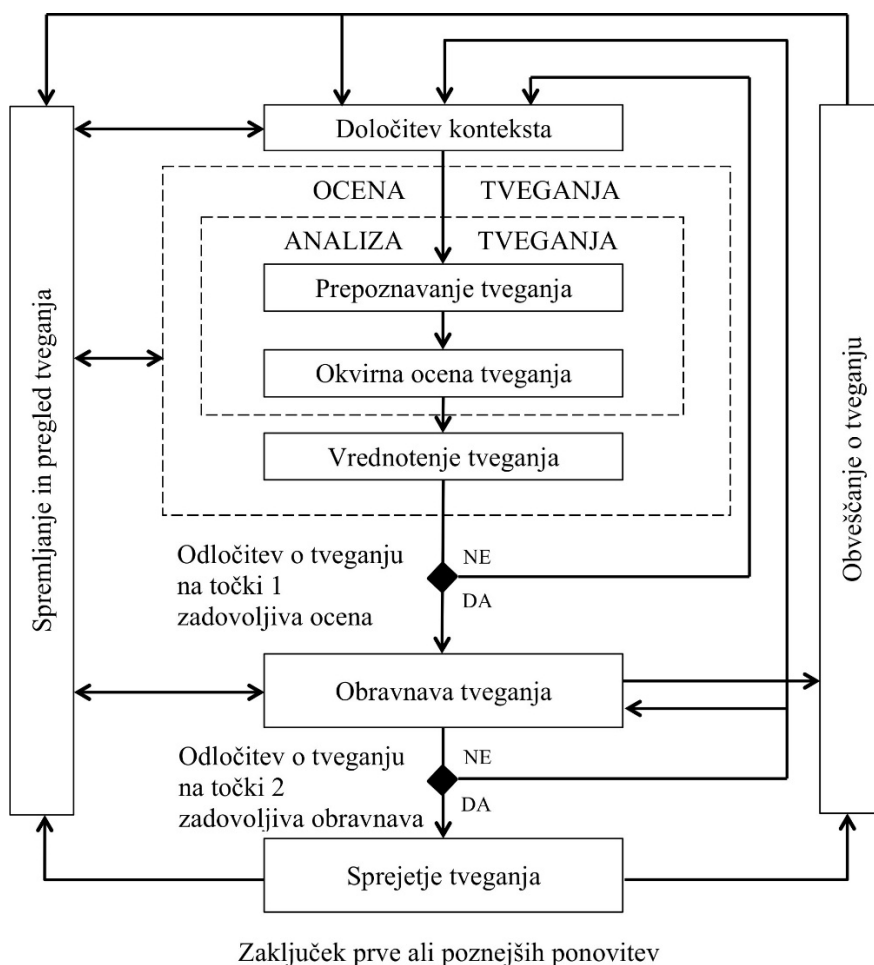
Pri vzpostavitvi sistema upravljanja varnosti morajo organizacije poskrbeti za sistematično upravljanje tveganj, ki mora biti skladno s potrebami, usmeritvami in okoljem, v katerem organizacija deluje. Navsezadnje mora biti upravljanje posameznih (operativnih, IT, tečajnih itd.) tveganj v skladu z upravljanjem vseh tveganj, s katerimi se organizacija srečuje. Varnostne usmeritve se nanašajo na pravočasno in učinkovito upravljanje s tveganji na področjih, kjer in kadar je to potrebno. Gre za proces, ki ga je potrebno vzpostaviti in ga po vzpostavitvi stalno izvajati in dopolnjevati.

Upravljanje IT tveganj je ključna sestavina celotnega upravljanja tveganj v organizaciji. Vključuje prepoznavanje, ocenjevanje in omilitev tveganj, povezanih z informacijsko tehnologijo, da se zagotovi razpoložljivost, zaupnost in celovitost informacij in sistemov. Ključni vidiki upravljanja tveganj informacijske tehnologije so predstavljeni na Sliki 1.2. Povzeti so po standardu ISO/IEC 27005:2022 (ISO/IEC, 2022), kar je standard, ki opisuje proces upravljanja s tveganji in njegove aktivnosti, s katerimi zagotavljamo informacijsko varnost.

Za izvajanje informacijske varnostne politike in sistema varnosti mora biti odgovoren najvišji upravljavski sloj organizacije. Pri tem izvaja proces upravljanja informacijskih tveganj tako, da upošteva kriterij zmanjševanja škode. Zelo groba ocena je, da pri zagotavljanju razpoložljivosti, celovitosti in zaupnosti informacij upošteva poslovni vpliv morebitnega varnostnega incidenta na poslovanje in realno verjetnost, da pride do informacijskega incidenta. (Jereb, 2019)

Ker se tveganjem ni smiselno povsem izogniti, niti se jim ne moremo, se je potrebno z njimi sprijazniti in se jih naučiti upravljati. Pri upravljanju tveganj se vodstva organizacij odločajo o naslednjih možnostih:

- tveganje je potrebno zmanjšati,
- tveganje sprejmemo brez dodatnega ukrepanja,
- tveganju se izognemo,
- tveganje prenesemo na pogodbene ali tretje osebe.



Slika 1.2: Aktivnosti pri upravljanju informacijskih tveganj

Vir: (Jereb, 2019)

Upravljanje informacijskih tveganj po ISO 27005 sestavljajo naslednje aktivnosti, ki jih prikazuje tudi Slika 2:

- **določitev konteksta** v katerem skušamo definirati okvir za upravljanje tveganj.
- **Oceno tveganja** kjer skušamo ovrednotiti nivo tveganja. Ta sklop vsebuje dve aktivnosti:
 - **analizo tveganja**, ki se ponovno deli na:
 - **prepoznavanje tveganja** in
 - **okvirno oceno tveganja** ter
 - **vrednotenje tveganja**.
- **Obravnava tveganja**, kjer je potrebno sprejeti ustrezne ukrepe tako, da se tveganjem izognemo, jih zmanjšamo, prenesemo na druge ali se odločimo, da jih v danem trenutku sprejmemo takšna, kot so.
- **Sprejetje tveganja**; sprejmemo odločitev za sprejetje ukrepov, povezanih s tveganji in določimo odgovornost za identifikacijo tveganj z utemeljitvami.
- **Obveščanje o tveganjih**, kjer zagotavljamo, da poteka stalna kakovostna izmenjava informacij med vsemi zainteresiranimi javnostmi in upravljavci tveganj o obstoju, naravi, obliki, verjetnosti, resnosti, sprejemljivosti in podobnih dejavnikih tveganj.
- **Spremljanje in pregled**, kjer tveganja in njihove dejavnike spremljamo in pregledujemo, da zaznamo vse spremembe v okviru organizacije ter vzdržujemo celosten vpogled v tveganje.

Praktična uporaba standarda ISO/IEC 27005 v različnih industrijah je ključnega pomena za zagotavljanje robustnega upravljanja IT tveganj. Nekateri hipotetični primeri študij ali primeri, kako bi se lahko ISO/IEC 27005 uporabljal v različnih industrijah, so naslednji.

- Finančni sektor:
 - Scenarij: finančna institucija ali podjetje pri izvajanju finančnih procesov želi izboljšati svoje procese upravljanja tveganj informacijske varnosti.

- Uporaba: ISO/IEC 27005 se lahko uvede za sistematično prepoznavanje in ocenjevanje tveganj, povezanih s podatki strank, finančnimi transakcijami in skladnostjo s predpisi. Institucija lahko nato izvede prilagojene strategije obvladovanja tveganj za zaščito občutljivih informacij in zagotovitev skladnosti s finančnimi predpisi.
- Zdravstveni sektor:
 - Scenarij: bolnišnica se zanima za varnost zdravstvenih kartonov in medicinskih podatkov.
 - Uporaba: ISO/IEC 27005 ponuja okvir za izvedbo ocenjevanja tveganj glede zaupnosti, celovitosti in razpoložljivosti zdravstvenih podatkov. Bolnišnica ga lahko uporabi za prepoznavanje ranljivosti, ocenjevanje potencialnih kršitev in izvajanje ukrepov za zaščito podatkov pacientov.
- Proizvodni sektor:
 - Scenarij: proizvodno podjetje si prizadeva zavarovati svojo intelektualno lastnino in proizvodne procese.
 - Uporaba: ISO/IEC 27005 lahko pomaga pri oceni tveganj, povezanih s krajo intelektualne lastnine, motnjami v dobavni verigi in prekinitvami operativnosti. Podjetje lahko izvede strategije za zmanjšanje tveganj za zaščito ključnih sredstev in zagotovitev kontinuitete proizvodnih procesov.
- Informacijske tehnologije (IT) storitve:
 - Scenarij: ponudnik IT storitev želi strankam dokazati svojo predanost informacijski varnosti.
 - Uporaba: ISO/IEC 27005 se lahko uporabi za celovito oceno tveganj v portfelju IT storitev. Z identifikacijo in obvladovanjem tveganj, povezanih z vdori v podatke, motnjami v storitvah in kibernetскими grožnjami, lahko podjetje okrepi svojo verodostojnost in strankam zagotovi predanost informacijski varnosti.
- Vladne agencije:
 - Scenarij: vladna agencija, odgovorna za podatke državljanov, želi okrepiti svoje varnostne ukrepe.
 - Uporaba: ISO/IEC 27005 lahko vodi agencijo pri oceni tveganj, povezanih s tajnostjo podatkov državljanov in razpoložljivostjo ključnih storitev. Agencija lahko razvije in izvede načrte za

obvladovanje tveganj, da zagotovi varno ravnanje s čezmejnimi informacijami.

- Trgovina:
 - Scenarij: trgovina izraža zaskrbljenost glede varnosti podatkov o plačilih strank.
 - Uporaba: ISO/IEC 27005 lahko pomaga trgovski verigi prepoznati tveganja, povezana s procesiranjem plačil, sistemi na prodajnem mestu in spletnimi transakcijami. Z izvajanjem varnostnih kontrol in rednim ocenjevanjem tveganj lahko podjetje zgradi zaupanje strank in zaščiti finančne transakcije.

V vsakem primeru je ključno prilagoditi uporabo ISO/IEC 27005 specifičnim IT tveganjem in zahtevam industrije. To vključuje razumevanje edinstvenih sredstev, groženj in ranljivosti, pomembnih za vsak sektor ter izvajanje učinkovitih strategij za obvladovanje IT tveganj in zmanjšanje potencialnih negativnih vplivov.

Literatura

- Meier, A. & Stormer, H. (2009). *eBusiness & eCommerce: Managing the Digital Value Chain*. Springer Berlin Heidelberg. ISBN 9783540893615
- Jereb, B. (2019). *Informatika in informacijska varnost: repertorij (1. izd)*. Maribor: Univerzitetna založba Univerze. DOI: 10.18690/978-961-286-251-0.
- ISO/IEC. (2022). ISO/IEC 27005:2022 - Information technology — Security techniques — Information security risk management. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).

DIGITALIZACIJA

– IZVAJANJE

BORUT JEREB

Univerza v Mariboru, Fakulteta za logistiko, Celje, Slovenija
borut.jereb@um.si

Programska oprema je nematerialna, njeno ustvarjenje je še vedno povezano s posamezniki pri digitalizaciji procesov. Ker je programska oprema postala zelo kompleksna, se organizacije, ki jo razvijajo in uporabljajo, srečujejo z novimi priložnostmi in izzivi skozi njen celoten življenjski cikel. ISO/IEC 12207:2011 je standard, ki zagotavlja okvir za opis življenjskega cikla sistemov programske opreme, ki temelji na interdisciplinarnem pristopu. Življenjski cikel programske opreme obsega procese; od zamisli za razvoj ali nakup, njeno testiranje, uvedbo, vzdrževanje do njenega umika. Poznavanje življenjskega cikla pomaga vsem deležnikom ustvarjati sistematično in organizirano upravljanje dela, povezanega s programsko opremo, kar je ključno za izboljšanje kakovosti in zmanjševanje težav pri digitalizaciji poslovnih procesov. Kakovost programske opreme - ključna za zadovoljstvo uporabnikov, se odraža v funkcionalnosti, zanesljivosti, učinkovitosti, uporabnosti, vzdržljivosti, prenosljivosti, varnosti in razširljivosti. ISO/IEC 25010:2017 je standard, ki opredeljuje celovit model kakovosti, omogoča oceno in izboljšanje programske opreme.

DOI

[https://doi.org/
10.18690/um.fl.2.2025.2](https://doi.org/10.18690/um.fl.2.2025.2)

ISBN

978-961-286-971-7

Ključne besede:

digitalizacija,
življenjski cikel
programske opreme,
kakovost programske
opreme,
ISO/IEC 12207,
ISO/IEC 25010



Univerzitetna založba
Univerze v Mariboru

DOI
[https://doi.org/
10.18690/um.fl.2.2025.2](https://doi.org/10.18690/um.fl.2.2025.2)

ISBN
978-961-286-971-7

Keywords:
digitalization,
software lifecycle,
software quality,
ISO/IEC 12207,
ISO/IEC 25010

DIGITALIZATION – IMPLEMENTATION

BORUT JEREB

University of Maribor, Faculty of Logistics, Celje, Slovenia
borut.jereb@um.si

Software is intangible, and its creation is still associated with individuals in the digitization of processes. As software has become highly complex, organizations developing and using it face new opportunities and challenges throughout its entire life cycle. ISO/IEC 12207:2011 is a standard that provides a framework for describing the life cycle of software systems based on an interdisciplinary approach. The software life cycle encompasses processes from conception to development or acquisition, through testing, deployment, maintenance, and eventual retirement. Understanding the life cycle helps all stakeholders establish systematic and organized management of software-related work, which is crucial for improving quality and reducing issues in the digitization of business processes. Software quality, crucial for user satisfaction, is reflected in functionality, reliability, performance, usability, maintainability, portability, security, and scalability. ISO/IEC 25010:2017 is a standard defining a comprehensive quality model, enabling the assessment and improvement of software.



University of Maribor Press

1 Uvod

Programska oprema je sestavljena iz niza navodil, ki se uporabljajo za izvajanje določenih nalog na računalnikih. Programska oprema je ključna sestavina sodobnih računalniških sistemov. Je nematerialna, kar pomeni, da nima fizične prisotnosti, kot jo ima strojna oprema. V veliki večini primerov še vedno velja, da je njen nastanek povezan s posameznikom (človekom) ali posamezniki, ki delujejo pri izvedbi skupnega projekta digitalizacije nekega procesa.

Programska oprema izboljšuje naše vsakodnevno življenje in spodbuja tehnološki napredek. Pri tem lahko gre za delo, zabavo, komunikacijo ali iskanje informacij. Programska oprema igra osrednjo vlogo pri uporabnosti računalnikov in digitalnih naprav ter tako omogoča avtomatizacijo različnih procesov, povečuje učinkovitost in zmanjšuje ročno delo.

Kompleksnost programske opreme je dosegla zelo visok nivo. Posledično pridobivamo s tem nove priložnosti in po drugi strani večje izzive za organizacije, ki ustvarjajo in uporabljajo sisteme programske opreme. Ti izzivi obstajajo skozi celoten življenjski cikel sistema in na vseh ravneh. ISO/IEC 12207 je standard, ki zagotavlja skupni procesni okvir za opis življenjskega cikla sistemov, temelječih na interdisciplinarnem pristopu.

Življenjski cikel razvoja programske opreme sestavljajo različni procesi, kot so: proces razvoja, testiranja, uvedbe in ukinitve. Cikel se lahko ponavlja, kar pomeni, da faze niso vedno zaporedne. Na primer, razvijalci se lahko vrnejo v fazo načrtovanja, če med implementacijo naletijo na težave. Pomembno je, da se zavedamo in poznamo življenjski cikel programske opreme, ker nam to vedenje pomaga zagotoviti, da je programska oprema razvita na sistematičen in organiziran način. To je predpogoj za izboljševanje kakovosti programske opreme ter zmanjševanje števila težav v vseh procesih njenega cikla.

Kakovost programske opreme je ključen vidik vsakega procesa razvoja programske opreme. Nanaša se na raven odličnosti ali primernosti namena programskega izdelka. Kakovost programske opreme je ključna, saj neposredno vpliva na zadovoljstvo uporabnikov, zanesljivost in celotni uspeh tistega procesa, ki ga digitaliziramo. Z osredotočanjem na: funkcionalnost, zanesljivost, zmogljivost,

uporabnost, vzdržljivost, prenosljivost, varnost in razširljivost lahko razvijalci zagotovijo zanesljive programske izdelke, ki ustrezajo uporabniškim pričakovanjem in poslovnim zahtevam. Redno testiranje, povratne informacije uporabnikov in kakovostne metrike pomagajo zagotoviti nenehno izboljševanje ter vzdrževanje visokih standardov kakovosti programske opreme. Kakovostna programska oprema ima visoko vrednost.

Kakovost programske opreme je torej ključna pri izvajanju vseh (poslovnih) procesov, saj zagotavlja, da programski izdelki izpolnjujejo uporabniška pričakovanja in tako zagotavlja nove vrednosti z digitalizacijo poslovanja. Organizacije se zanašajo na uveljavljene standarde in okvirje za učinkovito doseganje in ocenjevanje kakovosti programske opreme.

Družina standardov ISO/IEC 25000, znana tudi kot serija SQuaRE (Software Quality Requirements and Evaluation), zagotavlja celovit in mednarodno priznan nabor smernic za upravljanje kakovosti programske opreme. Serija ISO/IEC 25000 vključuje standarde in tehnična poročila, ki obravnavajo različne vidike značilnosti kakovosti programske opreme, vključno z modeli kakovosti, evalvacijskimi postopki in metodami merjenja.

ISO/IEC 25010 služi kot osnovni standard v seriji, ki opredeljuje celovit model kakovosti in nabor kakovostnih značilnosti. Značilnosti kakovosti zajemajo funkcionalnost, zanesljivost, uporabnost, učinkovitost, vzdržljivost in prenosljivost. S sledenjem tem značilnostim lahko organizacije ocenijo, merijo in izboljšajo kakovost svojih programskih izdelkov. Ta okvir prav tako zagotavlja sistematičen pristop, ki organizacijam omogoča določanje zahtev kakovosti, opredeljevanje meril evalvacije in izbiro ustrezne evalvacijske tehnike.

Ker tovrstni standardi spodbujajo doslednost in primerljivost pri ocenjevanju kakovosti programske opreme, omogočajo učinkovito komunikacijo med deležniki. Pomagajo izboljšati procese odločanja, omogočajo učinkovito upravljanje tveganj (vključno s stroški), krepijo zadovoljstvo strank in spodbujajo nenehno izboljševanje. Z njimi lahko organizacije dosežejo večjo preglednost, zanesljivost in interoperabilnost v svojih digitaliziranih poslovnih procesih.

Kakovost je tako vključena v vse življenjske cikle programske opreme. Med ostalim tudi v fazah, kot so:

- **načrtovanje:** kvalitetni vidiki naj bodo vključeni v načrtovanje projekta, da je zagotovljeno izpolnjevanje ciljev kakovosti.
- **Testiranje:** temeljito testiranje v različnih fazah življenjskega cikla zagotavlja, da se ohranjajo standardi kakovosti.
- **Povratne zanke:** redno prejemanje povratnih informacij od uporabnikov in deležnikov pomaga prepoznovati ter obravnavati težave s kakovostjo.
- **Neprekinjeno izboljševanje:** življenjski cikel programske opreme vsebuje ukrepe za nenehno izboljševanje, ki zagotavljajo, da se standardi kakovosti razvijajo skladno s spremenjenimi potrebami in tehnologijami.

Obe; življenjski cikel programske opreme in kakovost programske opreme, sta povezani področji, kjer so prakse zagotavljanja kakovosti vgrajene v celoten življenjski cikel, da bi zagotovili zanesljivost, funkcionalnost in visoko kakovost programske opreme.

2 Življenjski cikel programske opreme in ISO/IEC 12207:2017

ISO/IEC 12207:2017 je standard, ki ga uporabljamo za celoten življenjski cikel sistemov programske opreme, izdelkov in storitev, vključno s konceptualizacijo, razvojem, proizvodnjo, uporabo, podporo in ukinitvijo ter za njihovo dobavo, bodisi znotraj organizacije bodisi zunaj nje (ISO/IEC, 2017). Procesi življenjskega cikla iz tega dokumenta se lahko uporabljajo sočasno, ponavljajoče in rekurzivno za njegove sestavne dele.

Obstaja široka raznolikost programske opreme glede na njen namen, področje uporabe, kompleksnost, velikost, inovativnost, prilagodljivost, količine, lokacije, življenjsko dobo in razvoj. Standard to raznolikost podpira in je ne omejuje. Uporablja se pri enkratnih sistemih programske opreme, ki so napisani za posamezno in enkratno rešitev, za sisteme programske opreme za široko komercialno ali javno distribucijo ter za prilagodljive sisteme programske opreme. Prav tako se uporablja pri popolnoma samostojnih sistemih programske opreme in

pri sistemih programske opreme, ki so vgrajeni in integrirani v druge, večje, bolj kompleksne in celovite sisteme.

Sistemi programske opreme, obravnavani v tem standardu, so človeškega izvora, ustvarjeni in uporabljeni za zagotavljanje izdelkov ali storitev v določenih okoljih v korist uporabnikov in drugih deležnikov. Sistemi programske opreme lahko vključujejo naslednje elemente sistema: strojna oprema, programska oprema, podatki, ljudje, procesi (npr. postopki za zagotavljanje storitev uporabnikom), postopki (npr. navodila za operaterje), objekti, storitve, materiali in naravno nastale entitete. Glede na uporabnika so obravnavani sistemi programske opreme izdelki ali storitve.

Percepcija in definicija določenega sistema programske opreme, njegove arhitekture in elementov sistema sta odvisni od interesov in odgovornosti deležnikov. Sistem interesa enega deležnika se lahko obravnava kot element sistema v sistemu interesa drugega deležnika. Poleg tega se lahko sistem interesa obravnava kot del okolja za sistem interesa drugega deležnika.

Standard ISO/IEC 12207:2017 se uporablja v številnih organizacijah in panogah po vsem svetu, ki se ukvarjajo z razvojem, vzdrževanjem in upravljanjem programske opreme. Glavne skupine, ki uporabljajo ta standard, so:

- **informatika in informacijska tehnologija:** ta standard se najpogosteje uporablja v IT-industriji, kjer organizacije razvijajo programske rešitve, aplikacije, sisteme in storitve. To vključuje tako velika podjetja, ki razvijajo programske rešitve za široko javnost kot tudi specializirana IT-podjetja.
- **Telekomunikacije:** področje telekomunikacij pogosto uporablja standard ISO/IEC 12207 za razvoj programske opreme, ki se uporablja v omrežjih in komunikacijskih napravah.
- **Avtomobilska industrija:** avtomobilska industrija uporablja ta standard za razvoj vgrajene programske opreme v avtomobilih, kar vključuje nadzor motorja, varnostne sisteme in infotainment rešitve.
- **Zdravstvo:** v zdravstveni industriji se standard uporablja za razvoj programske opreme za medicinske naprave, elektronske zdravstvene kartoteke in druge informacijske sisteme.

- **Vojska:** vojaške organizacije uporabljajo ta standard za razvoj in vzdrževanje programske opreme za vojaške sisteme, vključno z obveščevalnimi, komunikacijskimi in nadzornimi sistemi.
- **Finančna industrija:** v finančni industriji se standard uporablja za razvoj programske opreme za finančne transakcije, bančne sisteme in upravljanje premoženja.
- **Letalstvo:** industrija letalske in vesoljske tehnologije uporablja ta standard za razvoj programske opreme za letalske naprave, satelite in vesoljske misije.
- **Energetika in drugi industrijski sektorji:** ta standard se lahko uporablja tudi v industrijskih sektorjih, kot so: proizvodnja, energetika in drugi; za razvoj programske opreme za nadzor in avtomatizacijo procesov.

ISO/IEC 12207:2017 se uporablja na vseh področjih, kjer je razvoj programske opreme ključnega pomena za delovanje organizacij in kjer je potrebno zagotoviti kakovostno upravljanje celotnega življenjskega cikla programske opreme; od koncepta do njene ukinitve. Tako med ostalim vključuje (ISO/IEC, 2017):

- **razvoj:** obravnava procese in dejavnosti, ki so vključeni v razvoj programske opreme; od začetne zasnove in opredelitve zahtev do oblikovanja, kodiranja, testiranja in implementacije.
- **Vzdrževanje:** naslavlja procese in dejavnosti, povezane z vzdrževanjem in izboljševanjem obstoječih sistemov programske opreme.
- **Dobavo:** vključuje procese za pridobivanje programske opreme od zunanjih dobaviteljev ali zagotavljanje programske opreme zunanjim strankam.
- **Zagotavljanje kakovosti:** določa procese za zagotavljanje kakovosti programske opreme skozi celoten življenjski cikel.
- **Izboljšave procesov:** omogoča osnovo za ocenjevanje in izboljšanje procesov, ki pomaga organizacijam izboljšati svoje procese razvoja in vzdrževanja programske opreme skozi celoten življenjski cikel.
- **Vodilo za dogovarjanje:** ponuja vodila za oblikovanje sporazumov med naročniki in dobavitelji v zvezi s procesi in dejavnostmi programske opreme.

- **Različne modele življenjskega cikla:** podpira različne modele življenjskega cikla programske opreme, vključno z iterativnimi, postopnimi in klasičnimi pristopi.

Prav tako se standard lahko uporablja v enem ali več načinih. Če je merilo področje uporabe, ga lahko uporabimo na strani (ISO/IEC, 2017):

- **organizacije** - za pomoč pri vzpostavitvi okolja zelenih procesov.
- **Projekta** - za pomoč pri izbiri, strukturiranju in uporabi elementov vzpostavljenega okolja za zagotavljanje izdelkov in storitev.
- **Naročnika in dobavitelja** - za pomoč pri razvoju sporazuma glede procesov in dejavnosti.
- **Presojevalcev procesov** - kot model referenčnih procesov za uporabo pri izvajanju presoj procesov, ki se lahko uporabljajo za podporo izboljšavam organizacijskih procesov.

Njegov namen je zagotoviti standardiziran okvir za procese življenjskega cikla programske opreme in kot tak služi več ključnim namenom (ISO/IEC, 2017):

- **standardizacija procesov:** ISO/IEC 12207 si prizadeva za standardizacijo procesov razvoja programske opreme; da bi jih naredil dosledne in ponovljive v različnih organizacijah in projektih. Ta standard pomaga vzpostaviti skupni jezik in nabor praks za inženiring programske opreme.
- **Zagotavljanje kakovosti:** spodbuja kakovost programske opreme in storitev z določitvijo procesov in dejavnosti, ki zagotavljajo, da programska oprema izpolnjuje določene zahteve in standarde. S sledenjem smernicam v ISO/IEC 12207 lahko organizacije izboljšajo kakovost svoje programske opreme.
- **Zmanjšanje tveganj:** standard pomaga zmanjšati tveganja, povezana z razvojem in vzdrževanjem programske opreme, saj zagotavlja strukturiran pristop. Pomaga pri prepoznavanju in omilitvi potencialnih težav že v zgodnjih fazah življenjskega cikla programske opreme.
- **Upravljanje življenjskega cikla:** ISO/IEC 12207 zajema celoten življenjski cikel programske opreme; od koncepta in zahtev preko oblikovanja, razvoja, testiranja, implementacije in vzdrževanja do umika.

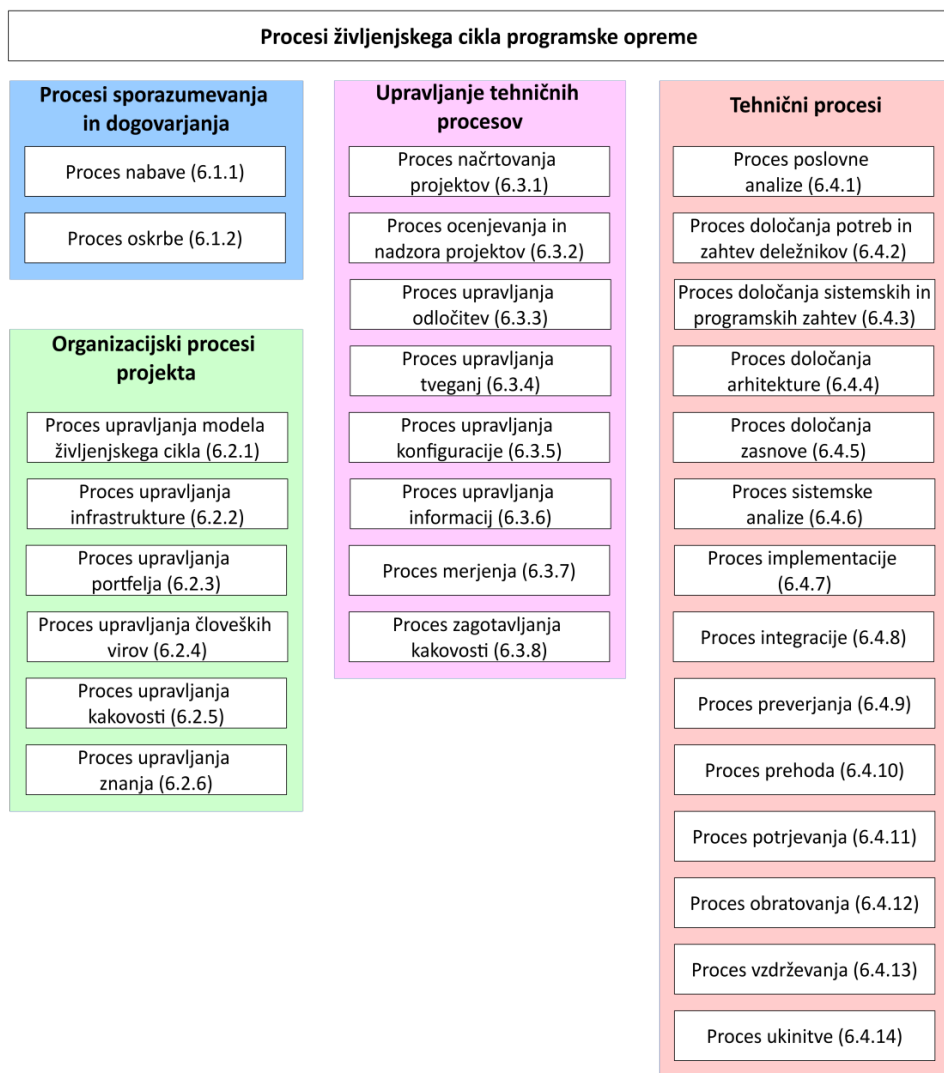
Zagotavlja celovit pristop k upravljanju programske opreme skozi celotno življenje.

- **Interoperabilnost:** z zagotavljanjem skupnega okvirja standard olajšuje interoperabilnost med različnimi komponentami programske opreme in sistemi, ki jih razvijajo različne organizacije. Poskrbi, da lahko programska oprema brez težav deluje skupaj.
- **Usklajenost z zahtevami deležnikov:** ISO/IEC 12207 poudarja pomen razumevanja in usklajevanja razvoja programske opreme z zahtevami deležnikov. To pomaga zagotoviti, da bodo izdelki programske opreme izpolnjevali pričakovanja in zahteve uporabnikov ter drugih relevantnih strani.
- **Izboljšanje procesov:** standard se lahko uporablja kot osnova za presojo in izboljševanje procesov. Organizacije ga lahko uporabijo za identifikacijo področij, kjer lahko izboljšajo svoje procese razvoja programske opreme.
- **Mednarodna združljivost:** ISO/IEC 12207 je mednarodni standard, kar ga naredi uporabnega in priznanega po vsem svetu. Ta globalna prepoznavnost je lahko še posebej koristna za organizacije, ki sodelujejo v mednarodnih sodelovanjih ali ponujajo programsko opremo na globalnem trgu.

2.1 Proces standarda ISO/IEC 12207:2017

Vsak proces v tem dokumentu je opisan glede na naslednje lastnosti:

- **imenovanje** procesa predstavlja obseg celotnega procesa,
- **namen** opisuje cilje izvajanja procesa,
- **rezultati** izražajo otipljive rezultate, ki se pričakujejo ob uspešnem izvajanju procesa,
- **aktivnosti** so skupine povezanih nalog v procesu,
- **naloge** so zahteve, priporočila ali dovoljena dejanja, namenjena podpori doseganja izidov.



Slika 2.1: Procesi in skupine procesov po ISO/IOC 12207:2017

Vir: (povzeto in prevedeno po ISO/IEC, 2017)

Standard združuje procese, ki se lahko izvajajo med življenjskim ciklom programskega sistema, in sicer v štiri skupine procesov. Vsak proces življenjskega cikla v teh skupinah je opisan glede na namen in želene izide s sklopom sorodnih dejavnosti in nalog, ki se lahko izvajajo za doseg teh izidov. Štiri skupine procesov in procesi, vključeni v vsako skupino, so prikazani na Sliki 2.1.

Skupine procesov so naslednje (ISO/IEC, 2017):

- **procesi sporazumevanja/dogovarjanja.** Organizacije so proizvajalci in uporabniki sistemov programske opreme. Ena organizacija (kot naročnik) lahko razporedi drugo organizacijo (kot dobavitelja) za izdelke ali storitve. To se doseže z uporabo sporazumov (ali pogodb). Sporazumi omogočajo tako naročnikom kot dobaviteljem, da uresničijo vrednost in podprejo poslovne strategije svojih organizacij. Procesi sporazumevanja so organizacijski procesi, ki se uporabljajo izven obsega življenjske dobe projekta, pa tudi med življenjsko dobo projekta. Praviloma organizacije delujejo sočasno ali zaporedoma tako naročniki kot dobavitelji sistemov programske opreme. Procesi sporazumevanja se lahko uporabljajo manj formalno, ko sta naročnik in dobavitelj v isti organizaciji. Prav tako se lahko uporabljajo znotraj organizacije za dogovor o odgovornostih organizacije, projekta in tehničnih funkcij. Glej Sliko 1.
- **Organizacijski procesi projekta.** Ti procesi se nanašajo na zagotavljanje virov, ki uredijo, da projekt izpolni potrebe in pričakovanja deležnikov organizacije. Običajno so usmerjeni na strateško raven upravljanja in izboljševanja poslovanja ali izvajanja dejavnosti organizacije. To realizirajo z zagotavljanjem in razporejanjem virov in z upravljanjem tveganj v konkurenčnih ali negotovih situacijah. Običajno se uporabljajo izven obsega življenjske dobe projekta, vendar lahko tudi med življenjsko dobo projekta. Vzpostavijo okolje, v katerem se izvajajo projekti. Organizacija določi procese in modele življenjskega cikla, ki jih uporabljajo projekti; ustanovi, preusmeri ali prekliče projekte, zagotovi potrebne vire, vključno z ljudmi in finančnimi sredstvi in določi ter spremlja merila kakovosti za sisteme programske opreme in drugih izdelkov, ki so plod razvoja za notranje in zunanje stranke. Organizacijski procesi projektov ustvarjajo poslovno podobo za številne organizacije in implicirajo komercialne in dobičkonosne motive. Enako so pomembni tudi za neprofitne organizacije, saj so tudi te odgovorne. Odgovorne so za vire in se srečujejo s tveganji pri svojih dejavnostih. Navedeni so tudi na Sliki 1.
- **Upravljanje tehničnih procesov.** Pri tem upravljanju se ukvarjamo z upravljanjem virov in sredstev za izvajanje tehničnih procesov, ki so nam na voljo in jih običajno dodeljuje upravljavski sloj organizacije. Z njihovo

uporabo dosegamo izpolnitev sporazumov, v katere je organizacija ali so organizacije vstopile. Procesi tehničnega upravljanja se nanašajo na tehnično izvajanje projektov, zlasti na načrtovanje v smislu stroškov, časovnih okvirjev in ciljev, na preverjanje dejanj za zagotavljanje skladnosti s plani in merili za uspešnost ter na identifikacijo in izbor ukrepov za odpravo pomanjkljivosti ali zakasnitev. Ti procesi se uporabljajo za vzpostavitev in izvajanje tehničnih planov za projekt, upravljanje informacij v timu tehničnega osebja, ocenjevanje tehničnega napredka glede na načrte za sistem programske opreme, izdelke ali storitve, nadzor tehničnih nalog do zaključka in za pomoč pri odločanju. Običajno bo v vsaki organizaciji soobstajalo več projektov. Procesi tehničnega upravljanja se lahko uporabljajo in izvajajo na korporativni ravni, da se izpolnijo zahteve in potrebe na nivoju celotne organizacije. Te procese prikazuje Slika 1.

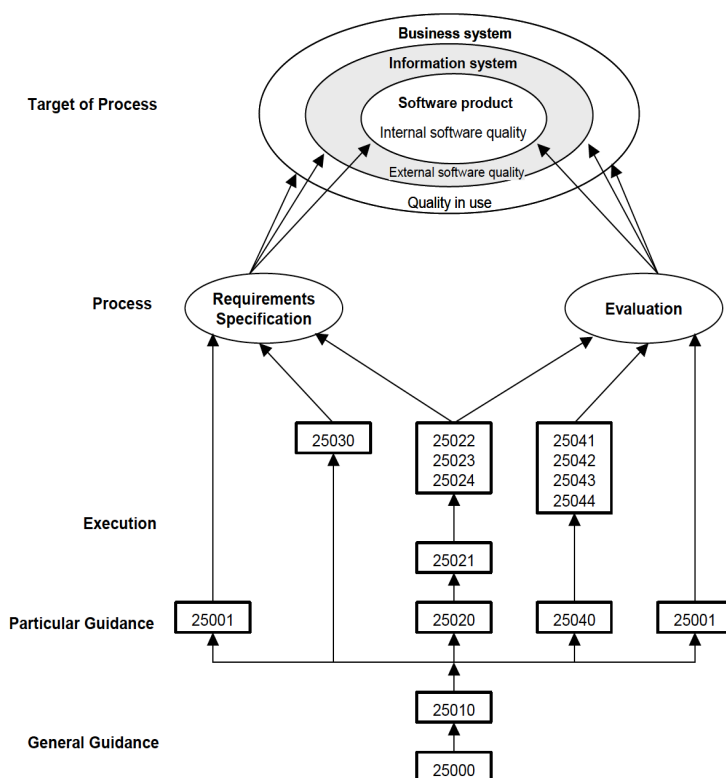
- **Tehnični procesi.** Ti procesi preoblikujejo potrebe deležnikov v izdelek ali storitev. Z uporabo izdelka ali upravljanjem storitve tehnični procesi zagotavljajo zmogljivosti; kadarkoli in kjerkoli je to potrebno, da izpolnijo zahteve (in zadovoljstvo) deležnikov. Tehnični procesi se uporabljajo za ustvarjanje in uporabo sistema programske opreme bodisi v obliki modela bodisi kot izdelka, ki je operativno uporaben. Tehnični procesi se uporabljajo na katerikoli ravni v hierarhiji strukture sistema programske opreme in na katerikoli stopnji v življenjskem ciklu. Na Sliki 1 so navedeni procesi, ki jih vsebuje ta skupina procesov.

Poleg predvidenih procesov si lahko definiramo dodatne procese, ki se za neko organizacijo izkažejo za potrebne in koristne. Vrstni red podpoglavij, v katerih so procesi opredeljeni v standardu, ne določa vrstnega reda, v katerem se procesi izvajajo med življenjskim ciklom sistema ali katerokoli od njegovih faz.

3 Model za zahteve in ocenjevanje kakovosti programske opreme ISO/IEC 25010:2011

ISO/IEC 25010 sodi v družino standardov ISO/IEC 250xx, ki je znana tudi pod imenom SQuaRE (Software Quality Requirements and Evaluation) (ISO/IEC, 2011). Pri tem je ISO/IEC 25000 temeljni standard, ki predstavlja celovit okvir za ocenjevanje in upravljanje kakovosti programske opreme. SQuaRE sta razvila Mednarodni standardizacijski organ (ISO) in Mednarodna elektrotehniška komisija

(IEC) z namenom zagotoviti strukturiran in dosleden pristop k ocenjevanju kakovosti programske opreme. Ta pristop pomaga organizacijam razumeti, opredeliti in oceniti kakovost svojih programskih izdelkov ter sprejemati odločitve o izboljšavah in optimizacijah le-teh. Celotna družina standardov vzpostavlja modele kakovosti, določa lastnosti kakovosti in opredeljuje zahteve kakovosti za programske izdelke. Ti modeli in lastnosti služijo kot orodja za ocenjevanje in merjenje različnih vidikov kakovosti programske opreme. Uporabljajo ga organizacije za razvoj programske opreme, drugi deležniki z namenom ocenjevanja, komuniciranja in izboljševanja kakovosti programskih izdelkov. Z upoštevanjem smernic in načel, določenih v teh standardih, lahko organizacije izboljšajo kakovost svojih programskih izdelkov, kar navsezadnje privede do povečanja zadovoljstva strank in uspešnih implementacij programske opreme. Osnovni referenčni model SQuaRE prikazuje Slika 2.2.



Slika 2.2: Referenčni model družine standardov za kakovost programske opreme SQuaRE

Vir: (ISO/IEC, 2011)

ISO/IEC 25010 zagotavlja podroben model kakovosti z določenimi značilnostmi in podznačilnostmi za ocenjevanje kakovosti programskega izdelka. ISO/IEC 25000 in ISO/IEC 25010 sta povezana standarda, vendar opravljata različne naloge znotraj širše serije SQuaRE. Tako je ISO/IEC 25000 informativni standard, ki uvaja širše koncepte in strukture za ocenjevanje kakovosti programske opreme. Hkrati je ISO/IEC 25010 normativni standard, ki jasno opredeljuje model kakovosti in merila za ocenjevanje kakovosti programskega izdelka. Ključne razlike med ISO/IEC 25000 in ISO/IEC 25010 predstavlja Tabela 1 (ISO/IEC, 2011).

Tabela 2.1: Ključne razlike med ISO/IEC 25000 in ISO/IEC 25010

	ISO/IEC 25000	ISO/IEC 25010
Obseg in namen	– osrednji standard v seriji SQuaRE, – zagotavlja okvir za zahteve in evalvacijo kakovosti programskega izdelka, – opredeljuje splošne koncepte, izraze in načela, povezana z upravljanjem kakovosti programske opreme, – uvaja modele kakovosti in metrike, uporabljene za ocenjevanje kakovosti programske opreme ter uporabnike vodi do drugih posebnih standardov v seriji, vključno z ISO/IEC 25010.	– specifičen standard znotraj serije SQuaRE, ki opredeljuje celovit model kakovosti, – poudarja kakovostne značilnosti in podznačilnosti, ki se lahko uporabljajo za ocenjevanje in merjenje kakovosti programskega izdelka, – se poglobi v različne vidike programske kakovosti, zagotavlja specifične kriterije za ocenjevanje programske opreme.
Vsebina	– gre za informativni standard, ki uvaja okvir kakovosti programskega izdelka, celotno strukturo kakovostnih značilnosti in podznačilnosti, – deluje kot usmerjevalni dokument za razumevanje ocenjevanja kakovosti programske opreme v okviru serije SQuaRE.	– normativni standard z določenimi zahtevami, namenjen neposredni uporabi pri ocenjevanju kakovosti programske opreme, – opredeljuje osem osnovnih kakovostnih značilnosti in njihove podznačilnosti (natančnost, skladnost, učinkovitost).
Uporaba	– uporablja se predvsem za zagotavljanje pregleda upravljanja kakovosti programske opreme in usmerjanje uporabnikov k drugim relevantnim standardom v seriji SQuaRE, – postavlja kontekst in terminologijo za modele kakovosti in metrike za ocenjevanje kakovosti programske opreme.	– se uporablja neposredno za ocenjevanje kakovosti programskega izdelka, – služi kot referenca za prakse, ki želijo oceniti in meriti kakovostne lastnosti programskega izdelka, – vodi izbiro relevantnih kakovostnih značilnosti in podznačilnosti za ocenjevanje glede na specifične potrebe in cilje ocenjevanja.

Vir: (ISO/IEC, 2011)

Model, ki ga opisuje ISO 25010:2011 predvideva (ISO/IEC, 2011):

- **model kakovosti**, ki zajema osem glavnih kakovostnih značilnosti, pri čemer vsaka predstavlja ključni vidik kakovosti programske opreme.
 - Funkcionalna primernost: vse sposobnosti v katerih programska oprema zagotavlja potrebne funkcije za izpolnjevanje določenih potreb.
 - Učinkovitost delovanja: sposobnost programske opreme, da se obnaša v pričakovanih časovnih okvirjih in s pričakovano uporabo ostalih IT virov, odzivnim časom in prenosom podatkov.
 - Združljivost: sposobnost programske opreme za delovanje z drugimi sistemi, programsko opremo ali strojno opremo.
 - Uporabnost: enostavnost uporabe programske opreme in uporabniška izkušnja.
 - Zanesljivost: sposobnost programske opreme, da ohrani svojo raven delovanja v določenih pogojih v določenem obdobju.
 - Varnost: sposobnost programske opreme, da ščiti podatke in funkcionalnosti pred neavtoriziranim dostopom in škodo.
 - Vzdržljivost: napor, potreben za izvedbo sprememb, odpravo napak ali prilagajanje programske opreme spremembam.
 - Prenosljivost: enostavnost, s katero je mogoče programsko opremo prenesti iz enega okolja v drugo.
- **Podznačilnosti**: vsaka, zgoraj naštetá značilnost, je razčlenjena na specifične podznačilnosti, kar olajša ocenjevanje in osredotočanje na določena področja ocenjevanja kakovosti.
- **Zahteve kakovosti**: vključuje niz zahtev kakovosti, ki lahko določijo želeno raven vsake kakovostne značilnosti in podznačilnosti za določen izdelek programske opreme.
- **Kakovost pri uporabi**: poudarja pomembnost ocenjevanja kakovosti na strani končnih uporabnikov, ki dojemajo kakovost programske opreme med dejansko uporabo.

(Sub)Characteristic	Reliability
Functional suitability	Maturity
Functional completeness	Availability
Functional correctness	Fault tolerance
Functional appropriateness	Recoverability
Performance efficiency	Security
Time behaviour	Confidentiality
Resource utilization	Integrity
Capacity	Non-repudiation
Compatibility	Accountability
Co-existence	Authenticity
Interoperability	Maintainability
Usability	Modularity
Appropriateness recognizability	Reusability
Learnability	Analysability
Operability	Modifiability
User error protection	Testability
User interface aesthetics	Portability
Accessibility	Adaptability
	Installability
	Replaceability

Slika 2.3: Značilnosti in podznačilnosti kakovosti programske opreme po ISO/IEC 25010:2011

Vir: (ISO/IEC, 2011)

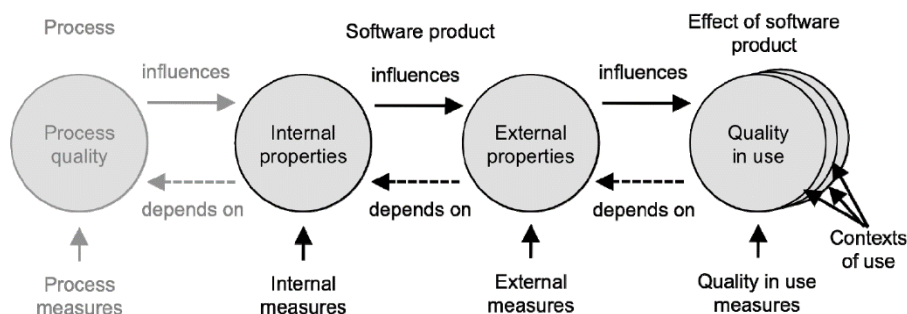
Effectiveness
Efficiency
Satisfaction
Usefulness
Trust
Pleasure
Comfort
Freedom from risk
Economic risk mitigation
Health and safety risk mitigation
Environmental risk mitigation
Context coverage
Context completeness
Flexibility

Slika 2.4: Značilnosti in podznačilnosti kakovosti pri uporabi programske opreme po ISO/IEC 25010:2011

Vir: (ISO/IEC, 2011)

Slika 2.3 in 2.4 prikazujeta množico značilnosti in podznačilnosti kakovosti programske opreme, kot jo definira model za ocenjevanje kakovosti ISO/IEC 25010:2011.

Kakovost programskega izdelka se lahko oceni z merjenjem internih lastnosti (običajno statične meritve vmesnih izdelkov), z merjenjem eksternih lastnosti (običajno z merjenjem obnašanja kode med izvajanjem) ali z merjenjem lastnosti kakovosti pri uporabi (ko je izdelek v dejanski ali simulirani uporabi). Glej Sliko 2 in Sliko 2.5.



Slika 2.5: Življenjski cikel kakovosti programske opreme

Vir: (ISO/IEC, 2011)

4 Komentar uporabnosti obeh standardov

Standarda ISO/IEC 12207 in ISO/IEC 25010 imata ključno vlogo pri digitalizaciji logističnih procesov, saj zagotavljata strukturo in smernice za učinkovito upravljanje razvoja programske opreme in zagotavljanja njene kakovosti. V nadaljevanju je kratko kritično ovrednotenje njunega pomena v kontekstu digitalizacije logističnih procesov.

ISO/IEC 12207 določa standardne procese za upravljanje življenjskega cikla programske opreme. Ta standard je pomemben za digitalizacijo logističnih procesov iz naslednjih razlogov:

- **strukturiran pristop k razvoju programske opreme:** ISO/IEC 12207 ponuja strukturiran okvir za načrtovanje, razvoj, vzdrževanje in upravljanje programske opreme. V kontekstu digitalizacije logistike to pomeni, da podjetja lahko učinkovito načrtujejo in izvajajo digitalne rešitve, ki so zanesljive in skladne z najboljšimi praksami.

- **Obvladovanje kompleksnosti:** logistični procesi so kompleksni in vključujejo številne udeležence ter tehnologije. ISO/IEC 12207 pomaga pri obvladovanju te kompleksnosti z jasnimi definicijami procesov, odgovornosti in aktivnosti v celotnem življenjskem ciklu programske opreme.
- **Zmanjšanje tveganj:** zaradi jasnih smernic za razvoj in vzdrževanje programske opreme, standard pomaga zmanjšati tveganja, povezana z napakami v programski opremi, kar je še posebej pomembno pri logistiki, kjer lahko napake povzročijo velike finančne izgube in motnje v oskrbovalni verigi.
- **Povečanje skladnosti in standardizacije:** uporaba ISO/IEC 12207 zagotavlja, da so procesi razvoja programske opreme skladni in standardizirani. To je ključnega pomena za interoperabilnost različnih sistemov in tehnologij, ki se uporabljajo v digitaliziranih logističnih procesih.

ISO/IEC 25010 določa model kakovosti programske opreme, ki vključuje različne značilnosti kakovosti, kot so: funkcionalnost, učinkovitost, zanesljivost, uporabnost in ostali kazalniki. Njegov pomen v digitalizaciji logističnih procesov je predvsem naslednji:

- **merjenje kakovosti:** ISO/IEC 25010 omogoča natančno merjenje in vrednotenje kakovosti programske opreme. V logistiki, kjer je natančnost in zanesljivost ključnega pomena, lahko podjetja uporabijo ta standard za zagotovitev, da digitalne rešitve ustrezajo visokim standardom kakovosti.
- **Izboljšanje uporabniške izkušnje:** kakovost programske opreme močno vpliva na uporabniško izkušnjo. ISO/IEC 25010 pomaga pri oblikovanju programske opreme, ki je enostavna za uporabo, učinkovita in prilagojena potrebam uporabnikov v logističnih procesih.
- **Zanesljivost in vzdržljivost:** zanesljivost in vzdržljivost sta ključni značilnosti kakovosti v logistiki, kjer okvare ali izpadi sistemov lahko povzročijo resne motnje. ISO/IEC 25010 pomaga zagotoviti, da so programske rešitve zanesljive in enostavne za vzdrževanje.
- **Podpora za odločanje:** standard ponuja jasna merila za ocenjevanje kakovosti programske opreme, kar lahko pomaga vodstvu pri odločanju o uvedbi novih digitalnih rešitev ali izboljšav obstoječih sistemov.

Ena izmed kritik obeh standardov je, da povzročata dodatne stroške in zahteve po virih. Mala in srednja podjetja v logistiki morda nimajo dovolj virov za popolno implementacijo teh standardov. Poleg tega sta lahko za neko sredino preveč kompleksna in zahtevna za razumevanje in implementacijo, kar lahko predstavlja oviro za podjetja, ki nimajo specializiranega znanja in izkušenj na področju systemskega inženiringa in kakovosti programske opreme.

Standarda ISO/IEC 12207 in ISO/IEC 25010 predstavljata pomembno pomoč pri digitalizaciji logističnih procesov, saj zagotavljata strukturiran pristop k razvoju in zagotavljanju kakovosti programske opreme. Njuna uporaba lahko izboljša učinkovitost, zanesljivost in kakovost digitalnih rešitev v logistiki. Vendar pa morajo biti podjetja pozorna na stroške, vire in prilagodljivost, povezano z implementacijo teh standardov ter se zavedati potencialnih izzivov in omejitev, ki jih lahko prineseta.

Literatura

- ISO/IEC. (2011). ISO/IEC 25010:2011 – Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).
- ISO/IEC. (2017). ISO/IEC/IEEE 12207:2017 - Systems and software engineering — Software life cycle processes. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).

INFORMACIJSKA IN RAČUNALNIŠKA PISMENOST

NENA OREL ŠANKO

Univerza v Mariboru, Fakulteta za logistiko, Celje, Slovenija
nena.orel@um.si

V današnjem času je varnost informacij in računalnikov izjemno pomembna iz več razlogov. Digitalizacija je omogočila ogromen pretok podatkov in informacij preko računalniških omrežij. Te informacije so pogosto občutljive narave, vključno s finančnimi podatki, osebnimi identifikacijami in poslovnimi skrivnostmi. Zato je nujno, da se informacije zaščitijo pred nepooblaščenim dostopom in zlorabo. V digitalnem svetu je veliko infrastrukture povezane z računalniškimi omrežji, to so šole, bolnišnice in prometni sistemi. Napadi na te sisteme lahko povzročijo resno finančno ali materialno škodo in ogrozijo življenja ljudi. Zato je pomembno zagotoviti, da so sistemi varni in odporni proti kibernetским napadom. Kibernetски napadi so postali vse bolj pogosti, sofisticirani ter izkoriščajo ranljivosti v računalniških sistemih in omrežjih za krajo podatkov, vohunjenje ter povzročanje škode. Zato je nujno nenehno nadgrajevanje varnostnih ukrepov in seznanjenost ljudi. Torej, varnost informacij in računalnikov je ključnega pomena za zaščito zasebnosti, gospodarske stabilnosti in nacionalne varnosti v sodobnem digitalnem svetu.

DOI

[https://doi.org/
10.18690/um.fl.2.2025.3](https://doi.org/10.18690/um.fl.2.2025.3)

ISBN

978-961-286-971-7

Ključne besede:

informacijska varnost,
računalniška varnost,
podatki,
informacije



Univerzitetna založba
Univerze v Mariboru

DOI
[https://doi.org/
10.18690/um.fl.2.2025.3](https://doi.org/10.18690/um.fl.2.2025.3)

ISBN
978-961-286-971-7

Keywords:
information security,
computer security,
data,
information

INFORMATION AND COMPUTER LITERACY

NENA OREL ŠANKO

University of Maribor, Faculty of Logistics, Celje, Slovenia
nena.orel@um.si

Today, information and computer security are extremely important for several reasons. Digitalisation has enabled a massive flow of data and information through computer networks, where information is often sensitive in nature, including financial data, personal identities, and business secrets. It is imperative to protect information from unauthorised access and misuse. In today's digital world, a lot of infrastructure is connected to computer networks, such as schools, hospitals, and transportation systems. Attacks on these systems can lead to significant financial or material damage and jeopardise people's lives. Hence, it is crucial to ensure systems' security and resiliency against cyber-attacks, which have become increasingly common, sophisticated, and exploit vulnerabilities to steal data, spy, and cause harm. Thus, constant upgrading of security measures and raising awareness among people are essential. Therefore, information and computer security are of paramount importance for safeguarding privacy, economic stability, and national security in the modern digital world.



University of Maribor Press

1 Uvod

Informacijska in računalniška varnost sta postali temeljna vprašanji v današnji digitalni dobi, kjer so podatki in informacije postali dragoceni viri, ki poganjajo tako zasebna kot poslovna okolja. S hitrim razvojem tehnologije in nenehnim povezovanjem preko interneta je varovanje podatkov postalo ključnega pomena, saj so se pojavile nove grožnje, ki ogrožajo tako posameznike kot organizacije. Varnostne kršitve, kot so: kraje identitete, hekerski napadi in izguba občutljivih informacij, predstavljajo resne posledice, ki lahko povzročijo nepopravljivo škodo tako na osebnem kot poslovnem nivoju. Zato je zaščita informacij in podatkov danes ključna naloga, ki varuje našo zasebnost, finančno stabilnost in poslovno konkurenčnost.

Na začetku pa je potrebno zavedanje, da sta obstoj in poslovanje vsake organizacije odvisna od virov informacijske tehnologije (v nadaljevanju: IT), brez katerih logistični procesi ter sistemi oskrbovalnih verig ne morejo (nemoteno) delovati (Jereb, 2017). Sem sodijo (Kajba et al., 2023): informacije, aplikacije (ali programska oprema), infrastruktura, neopredmetena sredstva in ljudje. IT viri so na voljo za implementacijo v različne IT procese (Jereb, 2017), razumemo pa jih lahko kot naložbe v te procese, kjer je pomembna tudi njihova primerna raven zaščite (Jereb et al., 2016). Trdimo lahko tudi, da so ti štirje IT viri temelj vsake tehnologije, kjer predstavljajo štiri soodvisne, soodločajoče ter enako pomembne komponente (Kabanda, 2019).

Za vsakega izmed IT virov pa je potrebno zagotavljati tudi IT zahteve, ki so že bile omenjene v poglavju Načrtovanje digitalizacije poslovanja. Glede na kontrolne cilje za informacijsko in sorodno tehnologijo (angl. Control Objectives for Information and related Technology) obstaja sedem poslovnih zahtev oziroma informacijskih kriterijev za IT vire (IT Governance Institute, 2007):

- uspešnost – se nanaša na informacije, pomembne za poslovni proces, ki so del tega poslovnega procesa ter njihovo pravočasno zagotovitev, pravilnost, skladnost in uporabnost,
- učinkovitost – se nanaša na zagotavljanje informacij z optimalno uporabo virov,

- zaupnost – se nanaša na varovanje občutljivih informacij pred razkritjem,
- celovitost – se nanaša na pravilnost in popolnost informacij, njihovo veljavnost v skladu s poslovno vrednostjo ter pričakovanji,
- razpoložljivost – se nanaša na informacije, ki morajo biti na razpolago, ko jih potrebujemo v poslovnih procesih, in varovanje potrebnih virov ter sorodnih zmogljivosti,
- skladnost – obravnava usklajitev z zakoni, predpisi in pogodbenimi dogovori (zunanja določena poslovna merila, notranje politike), ki veljajo za zadevni poslovni proces,
- zanesljivost – se nanaša na zagotavljanje ustreznih informacij za vodstvo, da lahko upravlja organizacijo in izvaja svoje odgovornosti iz naslova zaupnosti in vodenja.



Slika 3.1: Trikotnik CIA

Vir: lasten

Informatika, z vidika varnosti, zahteva predvsem, da so informacije na voljo, celovite in zaupne v obsegu, ki je potreben za izvedbo ter podporo poslovnim procesom. V primeru logistike to pomeni zagotavljanje *razpoložljivosti*, *celovitosti* in *zaupnosti* informacij, da je mogoče zagotoviti prave izdelke ali storitve v pravilni količini in kakovosti, dostavljene na pravo mesto in ob pravem času. (Kajba & Jereb, 2021) Te tri zahteve (razpoložljivost, celovitost in zaupnost) pa predstavljajo tudi trikotnik

CIA (angl. The CIA Triad: Confidentiality, Integrity and Availability) (Slika 1), kjer (Kemmerer, 2003):

- zaupnost zagotavlja, da se občutljive informacije ne razkrijejo nepooblaščenim prejemnikom,
- celovitost zagotavlja, da so podatki in programi spremenjeni ali uničeni samo na določen ter pooblaščen način,
- razpoložljivost zagotavlja, da bodo IT viri uporabni, kadarkoli jih potrebuje pooblaščen uporabnik.

2 Vrste varnosti in groženj, povezane z delovanjem IT

V poglavju Načrtovanje digitalizacije poslovanja je bila orisana splošna pomembnost informacijske in kibernetske varnosti z opisom ključnih elementov kibernetske varnosti ter proaktivnimi in celovitimi pristopi. V nadaljevanju sledi podroben opis vrst varnosti ter IT groženj.

2.1 Vrste varnosti, povezane z delovanjem IT

Potrebno je predstaviti vrste varnosti, povezane z delovanjem IT: informacijska varnost, IT varnost, kibernetska varnost, računalniška varnost in omrežna varnost.

Informacijska varnost (angl. Information Security, InfoSec) zajema orodja in postopke, ki jih organizacije uporabljajo za zaščito informacij ter preprečevanje nepooblaščenega dostopa do poslovnih ali osebnih informacij, vključno z nastavitvami pravilnika, ki nepooblaščenim ljudem preprečuje dostop do poslovnih ali osebnih podatkov. InfoSec je rastoče in razvijajoče se področje, ki zajema mnoge vidike; od preizkušanja, testiranja in revizije varnosti omrežja do infrastrukture. Ščiti občutljive podatke pred nepooblaščenimi dejavnostmi, vključno s pregledovanjem, spreminjanjem, snemanjem in kakršnokoli motnjo ali uničenjem. Glavni cilj je zagotoviti varnost in zasebnost kritičnih podatkov organizacij, kot so: podrobnosti o računih strank, finančnih podatkih ali intelektualni lastnini. Organizacije morajo dodeliti sredstva za zagotavljanje varnosti informacij in podatkov ter biti pripravljene na odkrivanje, odzivanje in proaktivno preprečevanje napadov, kot so: lažno predstavlanje, zlonamerna programska oprema, virusi, zlonamerni insajderji ter izsiljevalska programska oprema ('Information Security: The Ultimate Guide', n.d.).

IT varnost (angl. Information Technology Security, IT security) opisuje previdnostne ukrepe za zaščito računalnikov in omrežij pred nepooblaščenim dostopom. Postopki in procesi so zasnovani za preprečevanje kraje podatkov ali motenj v informacijskih sistemih. Visoka kakovost IT varnosti se osredotoča na varovanje celovitosti podatkov, ohranjanje zaupnosti informacij, shranjenih v omrežju, zagotavljanje dostopnosti podatkov in informacij pooblaščenemu osebju, preverjanje pristnosti uporabnikov, ki poskušajo dostopati do računalniških omrežij ter omogočanje varnega pošiljanja sporočil preko omrežij za uporabnike (The Upwork Team, 2021).

Medtem ko se tako IT varnost kot kibernetska varnost (angl. Cyber Security) osredotočata na zaščito podatkov o strankah, imata nekoliko drugačna pristopa. IT varnost se nanaša na širše razumevanje zaščite, raziskovanje korakov za zaščito poslovnih podatkov, vključno s fizičnimi podatki in informacijami v internih sistemih. Kibernetska varnost se bolj osredotoča na grožnje, s katerimi se organizacija lahko sreča preko interneta, ko se informacije in podatki prenašajo digitalno ali drugače uporabljajo na spletu (The Upwork Team, 2021). Kibernetska varnost zajema nabor orodij, politik, varnostnih konceptov, varnostnih ukrepov, smernic, pristopov k obvladovanju tveganj, dejanj, usposabljanja, najboljših praks, zagotovil ter tehnologij, ki se lahko uporabijo za zaščito kibernetskega okolja ter sredstev organizacije in uporabnikov (Von Solms & Van Niekerk, 2013).

Računalniška varnost se na splošno osredotoča na zaščito računalniških sistemov pred nepooblaščenim dostopom in uporabo. Strokovnjaki za računalniško varnost si prizadevajo vzpostaviti najboljše prakse računalniške varnosti, kar vključuje upravljanje računalniške varnosti in varnosti omrežja ter ustvarjanje kulture, osredotočene na varnost v organizaciji. Obstaja več različnih vrst računalniške varnosti, ki vplivajo na različne elemente fizične in digitalne infrastrukture organizacije. Posledično obstaja veliko različnih vrst varnosti, na katere se morajo osredotočiti strokovnjaki, vključno z (The Upwork Team, 2021; 'What Is Computer Security?', 2022):

- varnost aplikacij – opisuje korake, ki jih izvajajo razvijalci pri izdelavi aplikacije, da zagotovijo varnost uporabnikov in zmanjšajo ranljivosti v aplikaciji (pri tej vrsti varnosti je potrebno analizirati kodo aplikacije, da bi našli morebitne slabosti),

- informacijska varnost,
- varnost omrežja – ščiti digitalno infrastrukturo organizacije in preprečuje varnostne incidente v računalniških omrežjih, tako da lahko uporabniki nemoteno delajo,
- internetna varnost – ščiti brskalnike in informacije v aplikacijah, ki uporabljajo internet. Požarni zidovi in podobne vrste zaščite, ki samo pooblaščenim uporabnikom zagotavljajo dostop do zaščitene območij, veljajo za internetne varnostne storitve,
- varnost v oblaku – zagotavlja, da uporabniki, ki se povezujejo preko aplikacij v oblaku, ostanejo zaščiteni ter uporablja sisteme, kot je poenoteno upravljanje groženj (UTM) v oblaku, da ohranja varne povezave v oblaku,
- operativna varnost – opisuje prakse in analize, ki se uporabljajo pri rutinskih dejanjih za iskanje potencialnih ranljivosti, ki jih lahko hekerji izkoristijo. Cilj je videti redne akcije z vidika slabega akterja in ugotoviti, kje lahko izkoristijo prednost,
- varnost končne točke – s številom naprav, ki se uporabljajo v organizaciji (mobilni telefoni, tablice, prenosniki in računalniki), se varnost končnih točk osredotoča na zaščito teh sistemskih končnih točk in vključuje zaščito naprav pred okužbo z zlonamerno programsko opremo.

Vsaka od teh vrst računalniške varnosti vključuje več komponent, zaradi česar jih je mogoče obravnavati kot lastna specializirana področja. ('What Is Computer Security?', 2022) Prej omenjeni trikotnik CIA velja za industrijski standard računalniške varnosti že od razvoja glavnega centralnega procesorskega kompleksa¹ (Whitman & Mattord, 2011).

Razumevanje razlike med IT varnostjo in varnostjo omrežja (angl. Network Security) se osredotoča na razumevanje različne uporabe podatkov. IT varnost se osredotoča na vse podatke, s katerimi upravlja organizacija, medtem ko se varnost omrežja osredotoča na omrežne sisteme in njihovo zaščito pred vdori ter napadi na podatke. Ponudniki varnostnih storitev pogosto ščitijo infrastrukturo, ki organizacijam omogoča elektronsko sodelovanje. (The Upwork Team, 2021)

¹ Glavni centralni procesorski kompleks (angl. mainframe) - v svojem bistvu so »mainfram-i« visoko zmogljivi računalniki z veliko količino pomnilnika in podatkovnimi procesorji, ki obdelujejo milijarde preprostih izračunov ter transakcij v realnem času (IBM, n.d.).

2.2 Vrste IT groženj

Preden nadaljujemo z vrstami vdorov, je potrebno omeniti vrste groženj IT varnosti (The Upwork Team, 2021):

- kibernetiski kriminal – vključuje usmerjanje ali uporabo računalnikov ali računalniških sistemov za storitve kaznivih dejanj (kraja identitete ali izsiljevanje) za določeno vrsto finančne nagrade,
- kibernetiski napadi – obsežni digitalni napadi, ki lahko onеспособijo celoten računalniški sistem ali več računalniških sistemov (napadi lahko uporabljajo zlonamerno programsko opremo ali izsiljevalsko programsko opremo), da dosežejo cilj pridobivanja informacij o milijonih uporabnikov ali izvedejo napad z zavrnitvijo storitve (DoS),
- kibernetiski terorizem – uporablja orodja ter metode kibernetiskega kriminala in napadov, s čimer poskuša ciljati na kritično infrastrukturo držav ali drugače škodovati državam in povzročiti strah z nepooblaščenim dostopom do komunikacijske infrastrukture.

3 Zlonamerna programska oprema

Pogost izraz za zlonamerno programsko opremo je tudi zlonamerna koda ali »malware«. Vsako leto je poslovanje preplavljeno z napadi zlonamerne programske opreme, ki jih povzročajo vedno večje komunikacijske zmožljivosti računalnikov in telefonov. Značilnost vseh oblik zlonamerne programske opreme je, da je njihov obstoj nezaželen, neznan ali sovražen do napadenega uporabnika, ki prejme te programe. Še pred dvajsetimi leti se je zlonamerna koda širila izključno z disketami, ki so jih uporabniki prenašali iz računalnika v računalnik. S povečanjem komunikacijskih zmožnosti se je povečala tudi razširjenost zlonamerne kode. Danes se škodljivci radi širijo preko datotek, e-pošte, sistemov za takojšnje sporočanje in spletnih mest. (Šepec, 2018)

Zlonamerna programska oprema izkorišča varnostne pomanjkljivosti v operacijskih sistemih in aplikacijah za širjenje okužb. Uspešen prodor zlonamernih kod je posledica neustreznosti tradicionalnih obrambnih orodij, katerih način delovanja je predvsem reaktiven. Protivirusni in protivohunski programi so najuspešnejši v boju

proti znanim napadom. Ko se na spletu pojavi nova vrsta zlonamerne programske opreme, se lahko neovirano širi, dokler proizvajalci protivirusnih programov ne analizirajo napada in ustvarijo primerne »cepiva«. Pravilno konfigurirani požarni zidovi bi lahko odigrali bistveno vlogo v tem boju, vendar večina uporabnikov sploh ne ve, kaj je požarni zid.

3.1 Vrste zlonamerne programske opreme

Škodljive kode (angl. malicious software ali malware) se pojavljajo kot pomožno ali glavno sredstvo izvršitve pri številnih kaznivih dejanjih kibernetkega kriminala in so opredeljene kot škodljivi programi, posebej prirejeni za napade (škodanju) na informacijske sisteme, omrežja ali podatke. (Šepec, 2018) V današnji informacijski dobi, v kateri je možnost profiliranja posameznikov nekaj povsem običajnega in so posegi v informacijsko zasebnost posameznikov dosegli najvišjo raven v zgodovini, so vohunski programi vse prej kot nedolžni skupki kod. Škodljive kode, ki prevladujejo pri kaznivih dejanjih, preko katerih se vršijo različni načini, imajo za posledice različna motenja, poškodovanje in resno oviranje informacijskih sistemov ter e-podatkov. Značilno za vse oblike programov malware je, da je njihov obstoj nezaželen, nepoznan ali sovražen napadenemu uporabniku, ki te programe prejme (Šepec, 2018).

Ko kibernetki kriminalci načrtujejo napad na računalniška omrežja in sisteme, imajo na voljo različna orodja. Obstaja več načinov zlonamernih napadov, na katere morajo biti organizacije pozorne, ko razvijajo svoje strategije kibernetke varnosti in varnosti IT. Nekatere izmed vrst zlonamerne programske opreme bodo predstavljene v nadaljevanju; virusi, črvi, trojanski konj, vohunska programska oprema, oglaševalska programska oprema, izsiljevalska programska oprema in (distribuirana) zavrnitev storitve.

3.1.1 Virusi

Beseda VIRUS pomeni »Vitalni informacijski vir pod obleganjem« (angl. »Vital Information Resource under Siege«) (Maity & Dey, 2021). Vse vrste zlonamerne programske opreme se pogosto obravnavajo kot virusi, vendar so virusi le ena izmed oblik zlonamerne programske opreme, niso pa vse vrste virusi. Virus je računalniški

program, ki je bil sprva napisan za zabavo, danes pa povzroča predvsem neprecenljivo škodo informacijskim sistemom.

Izraz virus se v računalniškem žargonu uporablja po zgledu samopodvajajočih se bioloških virusov – virus je program ali koda, ki se samodejno razširi na druge datoteke, s katerimi pride v stik in izvaja zlonamerna opravila, kot je prikaz preprostih sporočilnih oken ali uničenje podatkov. Virus lahko opišemo kot program, ki okuži različne medije in spremeni delovanje računalnika ali omrežja (Šepec, 2018). Ali kot samorazmnoževalni program, ki lahko "okuži" druge programe tako, da spremeni njih ali njihovo okolje tako, da klic "okuženega" programa pomeni klic morda razvite ter v večini primerov funkcionalno podobne kopije virusa (Horton & Seberry, 1997).

Da se virusi aktivirajo in razširijo, je potrebna pomoč uporabnika, kar se zgodi ob klikanju na določeno datoteko, zagonu določenega programa ali klikanju na povezavo. Ko je okužena datoteka odprta, se virus razširi in lahko okuži druge programe, zagonski sektor trdega diska, njegovo particijo ali dokument. Ko je enkrat aktiviran, se prične širiti tudi na druge datoteke ali preko drugih komunikacijskih kanalov. Računalniški sistem se lahko okuži celo, če okuženega programa ne zaženemo, saj se nekateri virusi širijo že med kopiranjem. Virusi ne morejo okužiti računalnika, če gledamo le spletne strani – okužba se zgodi le, če dovolimo izvajanje spletnih programov. Dobro je vedeti, da virusi niso prisotni le v ukradenih ali razpokanih programih; zaradi nepazljivosti se lahko pojavijo tudi v legalnih programih. Zaradi programskih napak se nekateri virusi širijo tudi preko elektronske pošte brez prilog. (Šepec, 2018)

Virusi se na okuženem računalniku običajno nastanijo v posameznih izvršljivih programih, kar poveča velikost programa. Vsebina zaslona okuženega računalnika se nenadoma začne spreminjati, posamezni deli zaslona se lahko premikajo, pojavijo pa se tudi različne slike ali napisi, kot na primer: "Vaš računalnik je zdaj okužen." Okuženi računalnik lahko zahteva različna gesla in šifre ali kako drugače spremeni tipične ukaze, poslane preko tipkovnice ali miške. Prav tako je delovanje računalnika upočasnjeno (to ne pomeni, da je vsak počasen računalnik tudi okužen z virusom). Večina virusov je zasnovanih za uničenje računalnika ali podatkov. (Šepec, 2018)

Vsak virus ima sledeče komponente (Šepec, 2018):

- okužba: programski del, ki omogoča širjenje virusa,
- koristen tovor (angl. Payload): predstavlja glavno aktivnost virusa in je zasnovan za izvajanje posebnih funkcij, kot so brisanje, spreminjanje ter konfiguracija podatkov in namestitev programske opreme za oddaljeni dostop,
- prožilna funkcija: definira čas ali dogodek in izvede podporno komponento programa.

3.1.2 Črvi

Virusi se razlikujejo od črvov (angl. worms), saj njihov zagon zahteva aktivnost prejemnika v obliki izvajanja programa; uporabnik mora sam izvesti datoteko virusa (odpreti priponko v elektronski pošti, klikniti z miško na izvršljivo datoteko). Črvi izkoriščajo pomanjkljivosti v operacijskih sistemih (na primer: Windows in Linux) ter ne zahtevajo nobene aktivnosti s strani žrtve. (Šepec, 2018)

Tako je črv neodvisen program, ki lahko širi svoje kopije ali svoje dele na druge računalnike, običajno preko omrežnih povezav, te kopije pa so popolnoma funkcionalni neodvisni programi, ki se lahko bodisi širijo naprej in/ali komunicirajo z nadrejenim črvom (na primer za poročanje o rezultatih nekega izračuna) (Horton & Seberry, 1997). Pogosto napadejo pomembne sisteme in spletne strani. V primeru črvov je najopaznejša posledica povečan promet v omrežju.

Podobno kot virusi so tudi črvi samoreplicirajoči programi, ki se največkrat nenadzorovano širijo po računalniškem sistemu, internetu in drugih omrežjih (Šepec, 2018). Vendar so v primerjavi z virusi nekoliko bolj inteligentni, saj so sposobni samodejno najti primerne tarče za okužbo, širijo pa se brez pomoči uporabnika, saj uporabljajo napake v operacijskih sistemih in programih (Bhargava et al., 2022). Običajno so zelo uspešni pri širjenju, saj računalniški uporabniki ne nameščajo potrebnih varnostnih sistemov. Podobno kot virusi, črvi nosijo "tovor" (payload), ki jim omogoča nadzor nad okuženim računalnikom, brisanje datotek ali krajo osebnih informacij in podatkov. Leta 2004 je črv po imenu Blaster v samo petih urah okužil več kot 100.000 računalnikov. Drug črv, imenovan Mydoom, je

morda najhujši zlonamerni program v zgodovini, saj je leta 2004 povzročil več kot 38 milijard dolarjev škode (Paulo, 2022).

3.1.3 Trojanski konj

Trojanski konj nima možnosti samorepliciranja. Značilnost trojanskih konjev je, da pogosto vsebujejo neko nedolžno funkcijo (na primer prikaz ure in vremena na namizju računalniškega sistema) (Šepec, 2018), predstavljajoč majhen in škodljiv del nekega prvotnega, splošno uporabnega programa. Trojanski konj je za razliko od računalniškega virusa (ki se prilepi na drug program s katerokoli od številnih metod) samostojen program in ima lahko uporabniške funkcije za uporabnika. (Horton & Seberry, 1997)

Trojanski konj se lahko zlahka predstavi kot navidezno nedolžna datoteka, prenesena s spleta kot Word ali PDF dokument, priložen elektronski pošti (Bhargava et al., 2022). Ko je ta generični program nameščen, se z njim namesti tudi trojanski konj, kar omogoča napadalcu prevzem nad računalnikom. Čeprav se ta vrsta zlonamerne programske opreme ne razmnožuje, lahko izvaja številne škodljive dejavnosti. Za primarnim programom se skrivajo t. i. "zasilna vrata" (angl. trap door), ki omogočajo avtorju trojanskega konja, da izvede določeno funkcijo (dostop do informacijskega sistema uporabnika, pridobivanje datotek iz sistema ali namestitve škodljivih kod v sistem). Delujejo podobno kot virusi, saj zahtevajo neko predhodno aktivnost žrtve v obliki zagona izvršljive datoteke, obiska spletne strani ali odpiranja navidezno nedolžne datoteke, ki vsebuje kodo trojanskega konja. Glavni namen trojanskih konjev je ustvarjanje in kraja identitet v povezavi z dosego finančnega dobička. (Šepec, 2018)

3.1.4 Vohunska, oglaševalska in izsiljevalska programska oprema

Vohunski programi (angl. spyware) in oglasi (angl. adware) predstavljajo veliko nadlogo v računalniškem svetu. Obe sta vrsti zlonamerne programske opreme in se razlikujeta od virusov in črvov v tem, da se ne moreta širiti z enega računalniškega sistema na drugega.

Vohunski program je splošen izraz za različne vrste zlonamerne programske opreme, ki na določen način nadzira delovanje informacijskih sistemov ter zbira osebne podatke (Šepec, 2018). Je sklop kode, ki je nameščen v računalniškem sistemu in deluje kot vohun, se osredotoča na dejavnosti lastnika sistema ter zbira vse informacije, do katerih dostopa neavtorizirano (Maity & Dey, 2021). Vohunska programska oprema se namesti na računalnik med brskanjem po internetu, za okužbo računalnika pa izkorišča varnostne pomanjkljivosti v spletnem brskalniku. Zasede lahko različne oblike, od brezplačnih programov, zaslonov za zaščito zaslona, do različnih orodnih vrstic, pa vse do programov za deljenje datotek. Eden od priljubljenih trikov kriminalcev je preusmerjanje vašega brskalnika na neželene spletne strani, kar napadalcem omogoča izvrševanje dodatnih kaznivih dejanj. Namen vohunske programske opreme ni uničevanje, poškodovanje ali motenje podatkov in sistemov, temveč zbiranje različnih informacij o uporabniku (njegovih navadah in vedenju, pomnjenje in beleženje gesel ter drugih zaupnih informacij) preko spletnih mest, družbenih omrežij in spletnih trgovin, o čemer nato poroča nazaj na osrednji vir bodisi za zakonite bodisi nezakonite namene. (Šepec, 2018)

Oglaševalska programska oprema (angl. adware) zbira podatke o uporabnikih in njihovih spletnih navadah, svoje ugotovitve pa pošilja različnim agencijam, ki uporabnike zasipajo z oglasi in neželeno pošto. Adware lahko nenehno prikazuje pojavna okna, kar znatno upočasni delovanje računalnika. (Šepec, 2018)

Izsiljevalska programska oprema (angl. ransomware) ima sama po sebi razumljiv pomen – programi držijo ključne informacije za "talce", da bi prejeli odkupnino. Posledice lahko vključujejo izgubo podatkov ali neavtorizirano distribucijo podatkov v javnost, kar vpliva na prihodnje poslovanje organizacije (Šepec, 2018), njen ugled ali ugled osebe. Dandanes večina izsiljevalske programske opreme nastane kot posledica računalniškega črva, ki se lahko širi iz enega sistema v naslednjega in po omrežjih brez ukrepanja uporabnika (Bhargava et al., 2022). Izsiljevalska programska oprema lahko cilja na vse industrijske sektorje, kjer so nekateri bolj ranljivi od drugih. Na primer leta 2021 je izsiljevalska programska oprema najbolj prizadela (Fedor, 2022) pravne, proizvodne, finančne in kadrovske storitve (Cyberreason, 2022).

3.1.5 Zavrnitev storitve

Napad z zavrnitvijo storitve (angl. Denial of Service, v nadaljevanju DoS) je vrsta kibernetkega napada, pri katerem kriminalci naredijo določeno omrežje nedostopno uporabnikom in vstopijo v računalniški sistem, da zbirajo osebne podatke. Napad izvira iz enega samega sistema ali omrežja. Gre za poskus napadalcev, da preprečijo zakonitemu uporabniku storitve uporabo te storitve. Napad DoS se lahko izvede preko (Šepec, 2018):

- onemogočanja omrežnih preusmerjevalnikov, ki omogočajo dostop do interneta napadenega informacijskega sistema. Brezžične dostopne točke se reprogramirajo, da ne zagotavljajo več brezžične internetne povezave do napadenih IT sistemov,
- pošiljanja množice e-poštne sporočil (angl. mail bombing), kar preobremeni strežnik za elektronsko pošto,
- programov, ki se nenehno razmnožujejo ali drugih vrst virusnih kod, ki napadajo informacijski sistem.

Napad z distribuirano zavrnitvijo storitve (angl. Distributed Denial of Service, v nadaljevanju DDoS) je koordiniran preko več informacijskih sistemov, pri čemer vsak pošilja del podatkov za izvedbo napada hkrati iz več točk napada. Gre za distribuirano onemogočanje delovanja storitve informacijskega sistema. Napadalec lahko napade več podrejenih sistemov (sužnjev - angl. slaves), ki jih nadzira preko nadzornih sistemov (vodij - angl. masters). Napadi se pogosto izvajajo na bistveno večji ravni z več podrejenimi sistemi. (Šepec, 2018)

4 Ukrepi za zaščito pred IT grožnjami

Rek »bolje preventiva kot kurativa« velja tudi, kadar govorimo o informacijski in računalniški varnosti. V današnjem, visoko digitaliziranem in povezanem svetu, tako na posameznike kot podjetja na vsakem koraku prežijo najrazličnejše nevarnosti, zaradi česar je pomembno, da poznamo ukrepe, kako se zaščititi pred IT grožnjami ter zlonamernimi programskimi opremami. Različne strategije in metode v prvi vrsti sledijo postopku preprečevanja, odkrivanja ali zaznavanja ter odzivanja (Kemmerer, 2003) na IT grožnje. Pri tem se kibernetška varnost ukvarja predvsem z varovanjem

IT virov (informacije, aplikacije ali programska oprema, infrastruktura, neopredmetena sredstva in ljudje) pred nepooblaščenim razkritjem, spreminjanjem ali uničenjem. Na ta način se zagotovijo IT zahteve CIA trikotnika (razpoložljivost, celovitost in zaupnost).

Informacijska in računalniška varnost sta ključni temi, ki ju je potrebno obravnavati in implementirati v kateremkoli podjetju, da se zagotovi zaščito notranjih sredstev ter intelektualne lastnine (McFadzean et al., 2011). Večina podjetij (kot tudi posameznikov) posluje preko spleta, saj le-ta omogoča povezovanje in komunikacijo v realnem času (Chen et al., 2010). Obstajajo različni načini, kako se lahko podjetje zaščiti pred IT grožnjami ter napadi. V določenih primerih je potreben tudi finančni vložek, ki je odvisen od samega načina in ravni zaščite. V prvi vrsti je potrebno poučiti in izobraziti ljudi o primernem obnašanju v kibernetskem prostoru, saj so v večini primerov ravno ljudje odgovorni, da se napad sploh zgodi (odpiranje neprimernih strani, klikanje na spletne povezave ali priponke). V podpoglavjih je zajetih nekaj ukrepov, kako lahko podjetje zaščiti svoje IT vire s pomočjo zaposlenih pred IT grožnjami ter napadi. Enake ukrepe je mogoče uporabiti tudi v primeru fizičnega posameznika za varovanje osebnih naprav.

4.1 Ustvarjanje gesel

Za vsak uporabniški račun ter tudi nekatere aplikacije je potrebno ustvariti geslo. Veliko ljudi si določi zanje enostavno geslo, ki po navadi zajema kraj bivanja ali rojstni kraj, datume rojstnih dni, imena otrok ali ljubljencev in podobno. Prav tako se v geslih pogosto uporabijo besede iz slovarja. To nikakor ni primerna vsebina gesel, saj so lahko ugotovljiva in tudi dokaj kratka. Kadar napadalci poskušajo dostopati do računov, se poslužujejo napadov s surovo silo (angl. brute-force attack), kjer s pomočjo programske opreme "pregledajo" slovarje in uporabijo veliko število različnih gesel z upanjem, da bo eno izmed njih pravilno. (Kaspersky, 2023b)

Vsakoletno se podaljšuje tudi priporočljiva dolžina gesel, pri čemer se minimalno zahteva vsaj osem znakov. Daljša gesla so vedno boljša od kratkih – več, kot je znakov, dlje bo trajalo "razbijanje" gesla ali njegovo ugotavljanje. En dodaten znak (črka, številka ali simbol) lahko podaljša čas za razbijanje gesla za mesece ali celo leta. Zato je vedno bolje ustvariti daljša gesla, kot so minimalno zahtevana. Priporočljiva je uporaba gesel z vsaj 12 znaki. Pri tem je potrebno kombinirati velike in male črke,

številke ter simbole. Seveda moramo biti pozorni tudi na vrstni red, saj se vse pogostejše dogaja, da so gesla sestavljena iz (v tem zaporedju): ene velike črke, nabora malih črk, nabora števil in enega ali dveh simbolov. Zato je zelo pomembna uporaba »soljenja in popravljanja« gesel (The Upwork Team, 2021), kjer gre za naključno uporabo mešanice velikih in malih črk, števil ter simbolov, kar močno poveča stopnjo težavnosti in podaljša čas, ki je potreben za razbijanje gesla.

Zaradi preobremenjenosti smo ljudje nagnjeni k lenobi in enostavnosti, kadar ustvarjamo spletne račune, zaradi česar velikokrat uporabimo eno geslo za več računov, kar sploh ni priporočljivo. Kadar uporabljamo eno geslo za več računov ali naprav, lahko napadalci ob nepooblaščenem dostopu ali vdoru dostopajo do vseh teh računov in podatkov v njih. Če pa imamo za vsak račun in napravo drugačno geslo, je ogrožen samo en račun, drugi pa ne. Tako so naši podatki bolj varni in zaščiteni pred IT grožnjami ter napadi.

4.2 Zaščita računalniškega omrežja

Varovanje IT infrastrukture ter aplikacij ali programske opreme, posledično tudi informacij in ljudi v podjetju, je možno doseči na različne načine. Tabela 3.1 predstavlja nabor preventivnih ukrepov, katerih se lahko podjetje posluži za zaščito omenjenih IT virov ter njihov opis.

Tabela 3.1: Preventivni ukrepi za zaščito pred IT grožnjami

Ukrep	Opis
Namestitvev varnostnih IT okvirjev	Varnostni IT okvirji opisujejo dokumentirane in medsebojno razumljive politike, ki narekujejo upravljanje z občutljivimi informacijami v podjetju.
Ustvaritev belega seznama (angl. whitelist) aplikacij	Na podlagi seznama dovoljenih aplikacij lahko podjetje zaposlenim določi, katere aplikacije se smejo nameščati in/ali izvajati na službenih napravah.
Uporaba protivirusne programske opreme	Omogoča vzdrževanje "čistih" računalnikov in operacijskih sistemov na podlagi rednega preverjanja, zaznavanja, preprečevanja in odstranjevanja različne zlonamerne programske opreme.
Požarni zid (angl. firewalls)	Požarni zid določa pravila, ki urejajo promet podatkov ter nadzira vstop in izstop podatkov ter drugih naprav v in iz računalnika.
Uporaba sistema za zaznavanje vdorov v omrežje (NIDS)	Sistem za zaznavanje vdorov v omrežje (angl. network intrusion detection systems, v nadaljevanju NIDS) deluje podobno kot protivirusna programska oprema ter požarni zid; spremlja promet, ki poteka v in iz

Ukrep	Opis
	različnih naprav, povezanih v omrežje ter preverja izvajanje zlonamernih dejavnosti ali nepooblaščen dostope ter o tem obvesti lastnika omrežja.
Izvedba večstopenjske avtentikacije	Varnost informacij in podatkov se lahko zagotovi na podlagi večstopenjske avtentikacije, ki se zahteva za dostop do občutljivih informacij. V tem primeru lahko gre za kombinacijo vnosa različnih gesel, ki se jih prejme preko različnih naprav (telefon in računalnik) ali računov (e-pošta, telefonska številka).
Uporaba kriptiranja	Z asimetričnim kriptiranjem se zaščiti občutljive informacije, ki se prenašajo iz ene naprave v drugo bodisi preko spleta bodisi drugih naprav. Dokument ali datoteko s pomočjo javnega ključa kriptiramo (ustvarimo tajnopis), na drugi strani pa jo dekriptiramo z zasebnim ključem (spremenimo nazaj v čistopis).
Uporaba navidezno zasebnega omrežja (VPN)	Navidezno zasebno omrežje (angl. virtual private network, v nadaljevanju VPN) predstavlja način oblikovanja zasebnega mesta na spletu, ki uporabnikom pomaga ustvariti varno povezavo ter šifrira podatke, poslane preko omrežja. VPN je velikokrat vključen v protivirusno programsko opremo.
Uporaba „medenih loncev“ (angl. honeypots)	»Medeni lonci« predstavljajo umetno ustvarjeno tarčo, ki zajema nekoristne informacije. Medtem, ko napadalci nevede poskušajo dostopati do medenih loncev, so pomembne informacije in datoteke v računalniku zaščitene.
Izvedba ocene ranljivosti in penetracijskega testa	Izvedba ocene ranljivosti vključuje iskanje potencialnih težav v omrežju ali sistemu, ki bi lahko omogočile nepooblaščen zunanji dostop. Ranljivosti se odkrijejo, določi se njihova resnost in prednost razreševanja. Slednje se stori preko poskusa dostopa do omrežja ali sistema od zunaj, pri čemer lahko pomagajo etični hakerji.

Vir: (Chen et al., 2010; The Upwork Team, 2021; Vacca, 2013)

5 Sklep

Leta 2020 je bilo v povprečju odkritih 360.000 novih zlonamernih datotek (Kaspersky, 2023a), vsako leto pa postajajo njihovi avtorji bolj inovativni. Pojavljajo se nove vrste zlonamernih kod, ki lahko izkoriščajo varnostne pomanjkljivosti v operacijskih sistemih, programih za protivirusno zaščito in požarnih zidovih. Najpogostejše škodljive kode, ki prevladujejo v kriminalnih dejanjih, v katerih se izvajajo različne metode, so motnje, poškodbe in hudo oviranje informacijskih sistemov ter elektronskih podatkov (Šepec, 2018).

Internet je postal najpogostejše mesto za širjenje virusov. Zlonamerna programska oprema se lahko skriva v vsem, kar je preneseno s spletnih strani, brez ustreznega varnostnega sistema pa lahko povzroči veliko škodo. Zaradi hitre rasti pogostosti elektronske pošte so priloge postale najpogostejši razlog za širjenje računalniških virusov. Pomembno je omeniti, da obstaja veliko različnih vrst zlonamerne

programske opreme, ki se skoraj vsak dan izboljšujejo, množijo in se pojavljajo v novih oblikah ali variacijah.

Zato mora informacijska in računalniška varnost podjetij vključevati tudi zaščito pred socialnim inženiringom, kot so različne oblike phishinga (tudi smishing in vishing), saj napadalci pogosto ciljajo na človeški dejavnik kot najšibkejši člen v varnostni verigi. Phishing napadi, kjer se napadalci predstavljajo kot zaupanja vredni subjekti, da bi pridobili občutljive podatke ali dostop do sistemov, so še posebej nevarni v logistiki zaradi kompleksnih in razvejanih oskrbovalnih verig. Zaposleni lahko prejmejo lažna e-poštna sporočila, ki jih pozivajo k razkritju gesel, števil kreditnih kartic ali drugih zaupnih informacij podjetja, kar lahko vodi do resnih varnostnih incidentov in motenj v poslovanju. Zato je ključno, da podjetja izvajajo redna izobraževanja in ozaveščanja zaposlenih o prepoznavanju phishing poskusov ter uvajajo varnostne ukrepe, ki zmanjšujejo tveganje za tovrstne napade.

V kontekstu digitalizacije logistike imata informacijska in računalniška varnost ključno vlogo pri zagotavljanju nemotenega in varnega delovanja logističnih procesov. Digitalizacija prinaša številne prednosti, kot so povečana učinkovitost, boljša sledljivost pošilk in optimizacija zalog, obenem pa izpostavlja podjetja IT grožnjam in napadom. Kibernetski napadi, kot so: vdor v sisteme, kraja podatkov ali napadi z izsiljevalsko programsko opremo, lahko povzročijo resne motnje v oskrbovalnih verigah, kar vodi do zamud, finančnih izgub in splošne škode za ugled podjetij. Zato je nujno, da podjetja vlagajo v informacijsko in računalniško varnost skozi primerne rešitve ter ukrepe, predstavljene znotraj tega poglavja.

Informacijska varnost v logistiki se poleg zgoraj napisanega nanaša tudi na zaščito zaupnih podatkov, kot so: informacije o strankah, transakcijah, dobaviteljih ter poslovnih partnerjih in drugih. Učinkovito upravljanje podatkov je bistveno za vzdrževanje zaupanja med poslovnimi partnerji in končnimi uporabniki. Skladnost z zakonodajo in standardi varovanja podatkov, kot sta GDPR in ISO 27001, je pomemben vidik informacijske varnosti, ki zagotavlja, da podjetja delujejo v skladu z zakonskimi zahtevami in najboljšimi praksami. Varnostne politike in postopki, ki vključujejo redne varnostne preglede in ocene tveganja, so nujne za preprečevanje varnostnih incidentov in zmanjševanje tveganj pri digitalizaciji logistike.

Literatura

- Bhargava, P., Choudhary, R., & Gupta, A. (2022, May). A Review Study on Computer Virus. *World Journal of Research and Review (WJRR)*, 14(5), 39–44.
- Chen, R.-S., Chung, Y.-M., & Tsai, C.-H. (2010). A study of the performance evaluation of a network intrusion detection system. *Asian Journal on Quality*, 11(1), 28–38.
<https://doi.org/10.1108/15982681011051804>
- Cyberreason. (2022). *Ransomware: The True Cost to Business—A Global Study on Ransomware Business Impact*. <https://www.cybereason.com/hubfs/dam/collateral/reports/Ransomware-The-True-Cost-to-Business-2022.pdf>
- Fedor, O. (2022, November 3). *93 Must-Know Ransomware Statistics [2023]*. Antivirus Guide.
https://www.antivirusguide.com/cybersecurity/ransomware-statistics/?gclid=Cj0KCQjwi46iBhDyARIsAE3nVrYtrwBey_1ErcYLO6UBJVK3as7CfdxsGKVcHVkKjfM_Mcyvk92IIH0aAr3WEALw_wcB
- Horton, J., & Seberry, J. (1997). *Computer Viruses—An Introduction*. 19, 1, 122–131.
https://documents.uow.edu.au/~jennie/WEBPDF/1997_09.pdf
- IBM. (n.d.). *What is a mainframe?* IBM. Retrieved 4 October 2023, from
<https://www.ibm.com/topics/mainframe>
- Information Security: The Ultimate Guide. (n.d.). *Imperva*. Retrieved 3 October 2023, from
<https://www.imperva.com/learn/data-security/information-security-infosec/>
- IT Governance Institute. (2007). *COBIT 4.1: Framework, control objectives, management guidelines, maturity models*. IT Governance Institute.
- Jereb, B. (2017). Mastering logistics investment management. *Transformations in Business and Economics*, 16, 100–120.
- Jereb, B., Cvahte Ojsteršek, T., & Rosi, B. (2016). *Governance of Investments in Logistics* (pp. 236–247).
<https://doi.org/10.4018/978-1-5225-0001-8.ch011>
- Kabanda, G. (2019). *Trends in Information Technology Management*.
- Kajba, M., & Jereb, B. (2021). *Three Crucial Years of IT Trends in Logistics*. 187–198.
<https://www.elibrary.ru/item.asp?id=46600879&pff=1>
- Kajba, M., Jereb, B., & Obrecht, M. (2023). Considering IT Trends for Modelling Investments in Supply Chains by Prioritising Digital Twins. *Processes*, 11(1), Article 1.
<https://doi.org/10.3390/pr11010262>
- Kaspersky. (2023a, May 18). *The number of new malicious files detected every day increases by 5.2% to 360,000 in 2020*. WwW.Kaspersky.Com. https://www.kaspersky.com/about/press-releases/2020_the-number-of-new-malicious-files-detected-every-day-increases-by-52-to-360000-in-2020
- Kaspersky. (2023b, June 30). *Brute Force Attack: Definition and Examples*. WwW.Kaspersky.Com.
<https://www.kaspersky.com/resource-center/definitions/brute-force-attack>
- Kemmerer, R. A. (2003). Cybersecurity. *25th International Conference on Software Engineering, 2003. Proceedings.*, 705–715. <https://doi.org/10.1109/ICSE.2003.1201257>
- Maity, S., & Dey, D. (2021). Computer Virus Attacks. *La Pensée*, 51(3), 585–594.
<https://doi.org/10.6084/m9.figshare.19258763.v1>
- McFadzean, E., Ezingard, J.-N., & Birchall, D. (2011). Information Assurance and Corporate Strategy: A Delphi Study of Choices, Challenges, and Developments for the Future. *Information Systems Management*, 28(2), 102–129.
<https://doi.org/10.1080/10580530.2011.562127>
- Paulo. (2022, December 21). *Top 10 most dangerous computer viruses of all time*. Dynamic Solutions Group.
<https://www.dsolutionsgroup.com/top-10-most-dangerous-malware-of-all-time/>
- Šepec, M. (2018). Kibernetski kriminal: Kazniva dejanja in kazenskopravna analiza. In *Univerzitetna založba Univerze v Mariboru*. Univerzitetna založba Univerze v Mariboru.
<https://press.um.si/index.php/ump/catalog/book/335>

- The Upwork Team. (2021, June 8). *What Is IT Security? Examples and Best Practices for 2024*.
<https://www.upwork.com/resources/it-security>
- Vacca, J. R. (2013). *Cyber Security and IT Infrastructure Protection*. Syngress.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>
- What Is Computer Security? (And Why It's Important). (2022, August 23). *Berkeley Boot Camps*.
<https://bootcamp.berkeley.edu/blog/what-is-computer-security/>
- Whitman, M. E., & Mattord, H. J. (2011). *Principles of Information Security* (4th edition).
http://almuhammadi.com/sultan/sec_books/Whitman.pdf

POSLOVNI INFORMACIJSKI SISTEMI

BOJAN RUPNIK

Univerza v Mariboru, Fakulteta za logistiko, Celje, Slovenija
bojan.rupnik@um.si

Informacijski sistemi so postali nepogrešljiv steber sodobnih poslovnih operacij, ki omogočajo upravljanje podatkov, optimizacijo procesov in informirano odločanje. Ta povzetek raziskuje ključno vlogo informacijskih sistemov v poslovanju, s posebnim poudarkom na vplivu sistemov za načrtovanje virov podjetja (ERP). ERP sistemi delujejo kot integrirane platforme, ki usklajujejo različne funkcije podjetja, poenostavljajo procese in združujejo podatke v enotno dostopne zbirke. Organizacijam omogočajo neposredni dostop do podatkov v realnem času, kar pomaga pri učinkovitem dodeljevanju virov, zniževanju stroškov in izboljšanju storitev. ERP sistemi so neprecenljivi pri zagotavljanju vpogledov preko funkcij, ki omogočajo izboljšano komunikacijo in sodelovanje ter pri zagotavljanju varnosti podatkov in skladnosti. Poleg tega so ti sistemi gonilna sila za strateško načrtovanje, saj nudijo zmogljivost za odločanje na podlagi podatkov, napovedno analitiko in usklajevanje dolgoročnih ciljev. Sistemi ERP so preoblikovali način, kako podjetja delujejo, se prilagajajo spreminjajočemu se digitalnemu okolju in delujejo kot temeljni kamen za doseg operativne odličnosti in konkurenčne prednosti.

DOI

[https://doi.org/
10.18690/um.fl.2.2025.4](https://doi.org/10.18690/um.fl.2.2025.4)

ISBN

978-961-286-971-7

Ključne besede:

sistemi ERP,
informacijska podpora,
informacijski tok,
izbira in implementacija
ERP



Univerzitetna založba
Univerze v Mariboru

DOI
[https://doi.org/
10.18690/um.fl.2.2025.4](https://doi.org/10.18690/um.fl.2.2025.4)

ISBN
978-961-286-971-7

Keywords:
ERP systems,
information support,
information flow,
ERP selection and
implementation

BUSINESS INFORMATION SYSTEMS

BOJAN RUPNIK

University of Maribor, Faculty of Logistics, Celje, Slovenia
bojan.rupnik@um.si

Information systems have become an indispensable cornerstone of modern business operations, facilitating data management, process optimization, and informed decision-making. This abstract explores the pivotal role of information systems in business, with a specific focus on the pervasive influence of Enterprise Resource Planning (ERP) systems. ERP systems serve as integrated platforms that harmonize various business functions, streamlining processes and unifying data into a single, accessible repository. They empower organizations by providing centralized, real-time data, which aids in efficient resource allocation, cost reduction, and enhanced customer service. ERP systems are invaluable in driving cross-functional insights, fostering improved communication and collaboration, and ensuring data security and compliance. Moreover, these systems are a catalyst for strategic planning, offering the capacity for data-driven decision-making, predictive analytics, and long-term goal alignment. In essence, information systems, especially ERP, have revolutionized the way businesses operate, adapting to the ever-changing landscape of the digital age and serving as a cornerstone for achieving operational excellence and competitive advantage.



University of Maribor Press

1 Uvod

Moderen poslovni svet temelji na informacijah. Z razvojem tehnologije se pojavljajo vedno nove rešitve za posamezne poslovne procese. Vključevanje novih tehnologij omogoča boljši pregled, hitrejšo obvladovanje, večjo zanesljivost, varnost (pa tudi nevarnosti) procesov. Glede na obseg poslovanja lahko mala podjetja še upravljajo poslovanje z osnovnimi računalniškimi orodji, z večanjem obsega pa je prehod na kompleksnejše informacijske sisteme neobhoden. Pojem informacijskih sistemov je zelo obširen in lahko opisuje tako individualne rešitve za določene segmente poslovanja kot tudi celovite centralizirane sisteme, ki povezujejo različne podsisteme. Tudi količina informacij in izmenjave podatkov, ki se uporabljajo pri poslovanju, se je v zadnjem času izjemno povečala. Povezljivost sistemov znotraj podjetja kot tudi s poslovnimi partnerji predstavlja ne več konkurenčne prednosti, pač pa je mnogokrat lahko pogoj za poslovni obstoj. Medtem ko je klasična (papirna) komunikacija še vedno prisotna v mnogih segmentih, jo digitalizacija vztrajno izpodriva.

V tem poglavju predstavljamo osnovne poslovne informacijske sisteme, njihov pomen za poslovanje in integrirane rešitve za celovito vodenje poslovnih procesov.

2 Pregled poslovnih informacijskih sistemov

Ko govorimo o informacijskih sistemih, jih lahko razdelimo na različne načine glede na namembnost. Vsak informacijski sistem je namenjen opravljanju določenega poslovnega procesa ali dela procesa, pogosto pa so različni informacijski sistemi integrirani ter se ob upravljanju procesov dopolnjujejo. V glavnem lahko moderne poslovne informacijske sisteme razdelimo po področjih uporabe.

- Sistemi za **upravljanje virov** (ERP) po navadi predstavljajo integrirano rešitev, ki vključuje funkcionalnosti za upravljanje pglavitnih poslovnih procesov.
 - Upravljanje oskrbovalne verige (SCM - Supply Chain Management system).
 - Načrtovanje in vodenje proizvodnje.
 - Upravljanje človeških virov.
 - Finance in računovodstvo.

- Upravljanje zalog.
- Prodajni sistemi.
 - Upravljanje s strankami (CRM - Customer Relationship Management).
 - Prodaja in marketing.
 - E-poslovanje in spletna prodaja.
- Sistemi za poslovno inteligenco in podatkovno analitiko.
 - Podatkovne zbirke in sistemi za podatkovno rudarjenje.
 - Sistemi za poslovno inteligenco (BI - Business Intelligence).
- Dokumentni sistemi.
- Sistemi za upravljanje procesov.
 - Sistemi za izvajanje proizvodnje (MES - Manufacturing Execution System).
 - Procesni nadzorni sistemi (PCS - Process control system).
 - Skladiščni sistemi (WMS – warehouse management systems).
 - Sistemi za upravljanje transporta (transport management systems).
- Sistemi za napredno načrtovanje in razvrščanje (APS - Advanced Planning and Scheduling system).

Glede na razne rešitve so mnogi izmed naštetih sistemov lahko združeni v en celovit nadzorni sistem – ERP.

3 Pregled sistemov ERP

Začetki avtomatizacije poslovanja segajo v 60. in 70. leta 20. stoletja, ko so se pojavili prvi sistemi MRP (ang. Material Resource Planning), ki so služili načrtovanju zalog materiala in proizvodnje. Z razvojem so si ti sistemi razvili v MRP II, pri čemer so se dodajale funkcionalnosti za upravljanje dodatnih procesov oz. virov, kot so finance oz. računovodstvo in človeški viri za celovitejšo obravnavo poslovanja. V začetku 90. let so se obstoječi sistemi razvili v danes uveljavljene sisteme ERP, pri čemer je srž ideje v vključevanju vseh poglavitnih poslovnih procesov v celovit sistem.

Delež uporabe sistemov ERP v podjetjih se je v nadaljevanju le povečeval, tako da si danes pri večjih podjetjih poslovanja brez tovrstnih sistemov več ne moremo predstavljati.

Nadaljnji razvoj sistemov ERP je prvotno stremel k razvoju uporabniških vmesnikov (dostop preko spletnega brskalnika), v zadnjem času pa je opazen predvsem prehod na oblačne rešitve, kjer so funkcionalnosti dostopne na zunanjih stežnikih, s čimer se predvsem strošek strojne opreme in vzdrževanja prenese na ponudnika storitev ERP.

V trenutnem obdobju smo priča predvsem integraciji z ostalimi tehnologijami, kot so: internet stvari (IoT – Internet of Things), mobilne naprave, ipd., predvsem pa vključitvi strojnega učenja in umetne inteligence za avtomatizacijo rutinskih nalog in napovedovalno analitiko.

Ne glede na splošni razvoj so določene rešitve sistemov ERP osredotočene na posebnosti posameznih področij, kot npr. zdravstvo, proizvodnja, storitve itd.

Medtem ko lahko različne izvedbe sistemov ERP nudijo različne storitve, jih v glavnem lahko delimo glede na vrsto namestitve in glede na vrsto licence.

- **Lokalna namestitvev** - informacijski sistemi so nameščeni na lastni informacijski infrastrukturi podjetja. To omogoča večji nadzor in prilagodljivost sistema, lahko pa glede na potrebe predstavlja velik strošek za vzpostavitev in vzdrževanje potrebne infrastrukture. Veliko prednost predstavlja tudi večja varnost, saj se zaupni podatki nahajajo znotraj podjetja.
- **Oblachna rešitev** – ponudniki ERP sistemov lahko le-to nudijo tudi kot storitev, pri čemer je sistem postavljen na infrastrukturi ponudnika storitev ERP. Glede na to, da stroške strojne opreme prevzame ponudnik, lahko to predstavlja cenovno ugodnejšo možnost za mnoga podjetja. Lahko pa ta varianta predstavlja potencialno nevarnost za prestreganje zaupnih podatkov. Zaradi večje prilagodljivosti je lahko ta pristop ustrežnejši za mala in srednja oz. hitro spreminjajoča se podjetja.

- **Odprtokodne rešitve** omogočajo večji nadzor nad sistemom, saj lahko delovanje v veliki meri prilagodijo svojim potrebam. Tudi s stroškovnega vidika so odprtokodne rešitve lahko zastoj, stroški nastanejo predvsem pri vzdrževanju in podpori. Slednja je pri odprtokodnih rešitvah pogosto izvedena preko skupnosti uporabnikov. Pri tem lahko pomembno vlogo igra tudi neodvisnost od ponudnika sistema ERP, vpogled v kodo pa omogoča preglednost oz. transparentnost delovanja. Slabost je pogosto omejen nabor funkcionalnosti, prilagajanje zahtevam pa lahko predstavlja znaten strošek. Tudi težave z integracijo so po navadi pogostejše pri odprtokodnih rešitvah. Prelaganje podpore na skupnosti lahko predstavlja manj ažurno in zanesljivo podporo proti lastniškim možnostim.
- **Lastniške rešitve** večinoma omogočajo večji nabor funkcionalnosti že prilagojenih posameznim panogam. Za podporo skrbi ponudnik sam, kar lahko predstavlja pomemben dejavnik za mnoga podjetja. Tudi integracija z drugimi sistemi je pri lastniških ERP po navadi enostavnejša. Slabosti predstavljajo predvsem višji stroški nabave in vzdrževanja, odvisnost od izbranega ponudnika in v primerjavi z odprtokodnimi rešitvami, je večja možnost, da bo moralo podjetje prilagoditi poslovanje izbranemu sistemu namesto prilagoditvi ERP sistema poslovanju.

4 Izbira in implementacija sistemov ERP

Pri izbiri sistema ERP za podjetje nastopa mnogo dejavnikov, ki jih je potrebno upoštevati. V prvi vrsti je po navadi strošek uvedbe sistema, ki lahko vključuje:

- strošek nabave programske opreme,
- strošek nabave strojne opreme,
- strošek vzdrževanja programske in strojne opreme,
- strošek podpornih storitev,
- strošek implementacije in drugi.

Stroški uvedbe vsekakor niso edini dejavnik, ki ga je potrebno upoštevati. Pri postopku izbire je prvotno potrebno identificirati vse zahteve, ki izhajajo iz poslovnih procesov in postaviti kriterije ter ovrednotiti njihove prioritete. Prav tako je ključno tudi trajanje postavitve rešitve ERP.

V naslednjem koraku se glede na podane zahteve izdela tržna raziskava, v kateri se za obstoječe sisteme preveri njihova skladnost s podanimi zahtevami. Po izbiri potencialnih kandidatov sledijo pogajanja s ponudniki rešitev ERP.

Poleg stroškov ostale kriterije predstavljajo (Alanbay, 2005):

- prilagodljivost,
- zmožnost implementacije,
- vzdrževanje,
- odzivnost na spremembe v realnem času,
- porabniška izkušnja,
- sistemske zahteve,
- storitve podpore in usposabljanja,
- varnostno kopiranje podatkov in nastavitev,
- orodja za poročanje in analitiko,
- zanesljivost dobaviteljev,
- zmožnost integracije z drugimi sistemi,
- fleksibilnost financiranja.

Glede na raznolikost zahtev, je smiselno uporabiti večparametrsko odločitveno metodo kot na primer AHP (Podvezko, 2009). Pri tem je potrebno kriterije razvrstiti glede na vpliv oz. pomembnost za poslovanje.

Implementacija sistemov ERP predstavlja zahteven proces, pri katerem se poslovni procesi prilagodijo uporabi sistema (Pelphrey, 2015). Koraki, ki so vključeni v implementacijo, so.

1. **Projektni načrt;** znotraj katerega se določi projektna ekipa s predstavniki posameznih oddelkov, cilje in zahteve uspešnosti, načrt bistvenih nalog, rokov in potrebnih virov ter identifikacija možnih pasti pri prehodu na ERP. Poleg končnih uporabnikov pri načrtu sodelujejo tudi konzultanti ponudnika ERP rešitve.
2. **Načrt in konfiguracija sistema;** omogoča, da se izbran sistem ERP prilagodi specifikam posameznih procesov podjetja, v kolikor je to mogoče.

V mnogih primerih je potrebna tudi prilagoditev procesa rešitve ERP. Posamezni moduli sistema se nastavijo za delovanje v sklopu oddelkov s konfiguracijo lastnosti, postopkov in poročil. V tem sklopu se vzpostavijo tudi podatkovne strukture oz. podatkovne baze ter opravi integracija z ostalimi sistemi.

3. **Podatkovni prenos;** predstavlja še en ključni del pri prehodu na sistem ERP. V tem sklopu je potrebno obstoječe podatke prečistiti in pripraviti načrt prenosa na baze sistema ERP. Pri prenosu je potrebno zagotoviti natančnost in celovitost ter validacijo podatkov.
4. **Usposabljanje** zaposlenih je potrebno izvesti že pred samim prehodom na ERP. Pri tem se vzpostavi načrte za različne uporabnike in njihove pričakovane vloge. Pri usposabljanju je ključnega pomena, da zaposleni izpostavijo morebitne pomisleke, ki bi lahko vplivali na izvajanje procesov.
5. **Testiranje** je ključnega pomena za validacijo funkcionalnosti in učinkovitosti sistemov ERP. V tem sklopu se po navadi izvede testiranje enot (unit testing), testiranje integracije in testiranje celotnega sistema. Cilj je odkriti kakršnekoli napake in pomanjkljivosti, ki jih je nato potrebno odpraviti.
6. **Zagon** testiranega in validiranega sistema predstavlja prehod iz obstoječega na sistem ERP, pri čemer je tudi tu potreben načrt prehoda. Ob tem se beleži pravilnost delovanja in učinkovitost sistema, predvsem je pri tem koraku potrebna podpora uporabnikom ob prehodu.
7. **Zaključek implementacije in optimizacija;** je končna faza pri prehodu na poslovanje z ERP. Pri tem se oceni učinkovitost sistema, v sklopu katerega se preverja uspešnost projekta implementacije in odkriva morebitne težave. Glede na potrebe je tu možnost implementacije dodatnih funkcionalnosti. Ob zaključku prehoda se vzpostavijo še postopki vzdrževanja in podpore.

Za implementacijo sistemov ERP poznamo različne pristope, za katerega pa se podjetje odloči, pa je odvisno od velikosti podjetja, panoge, razpoložljivih sredstev, rokov in posamičnih potreb. Najbolj pogosti pristopi implementacije.

- **Pristop velikega poka** (Big Bang), pri katerem se ERP vzpostavi naenkrat v vseh oddelkih. Prednosti tega pristopa sta hitra vzpostavitev in takojšnji dostop do sistema, vendar pa lahko slednje predstavlja tveganje za

prekinitve poslovnih procesov, sploh v primeru nepopolne ali neuspešne implementacije.

- **Fazni pristop** predvideva postopno implementacijo posameznih funkcionalnosti ali pa po skupinah. Ta pristop tudi omogoča postopno prilagajanje sistema (ali procesa), s čimer se zmanjša tveganje za večje prekinitve. Ta pristop je načeloma bolj dolgotrajen ter lahko privede do težav pri integraciji med posameznimi funkcijami.
- **Vzporedna vzpostavitev** predvideva, da ob obstoječem (starem) sistemu vzporedno deluje tudi na novo vzpostavljeni ERP, dokler ni zagotovljeno učinkovito delovanje. Ta pristop sicer zahteva več virov za delovanje redundantnega sistema, vendar se s tem zelo zmanjša tveganje za prekinitve.
- **Modularni pristop** predvideva vzpostavitev vsakega modula, enega za drugim, podobno kot pri faznem pristopu. Razlika je predvsem poudarek na uvajanju posameznih funkcionalnosti pri faznem, medtem ko se pri modularnem pristopu funkcionalnosti vzpostavljajo v sklopu posameznih modulov. Pri tem dobijo prednost pomembnejši moduli, omogočen pa je lažji pregled nad procesom implementacije. Tudi pri modularnem pristopu lahko pride do težav z integracijo posameznih funkcionalnosti, saj so le-te lahko med moduli zelo prepletene.
- **Enotska vzpostavitev** je pristop, pri katerem vsaka poslovna enota oz. oddelok ERP vzpostavi samostojno. Pri tem se zmanjša verjetnost prekinitve drugih oddelkov, se pa lahko pojavi neskladje v prepletenih procesih posameznih oddelkov.

5 Osnovni procesi in upravljanje v ERP

V tem poglavju bomo podali tipske poslovne procese, ki jih upravljajo sistemi ERP. V sklopu modula prodaje sistemi ERP omogočajo med drugim:

- upravljanje kontaktov:
 - zajem in vodenje kontaktov (ang. leads),
 - posredovanje kontaktov prodajnikom za načrtovanje komunikacije,
 - beleženje komunikacije s potencialnimi strankami.
- Upravljanje priložnosti (opportunity):

- pretvorba kontaktov (potencialnih strank) v verjetne stranke,
 - beleženje prodajnega toka,
 - ocenjevanje pričakovanih vrednosti prodaje glede na verjetnost uspešne priložnosti.
- Vodenje ponudb in predračunov:
 - izdelava predračunov za izdelke ali storitve,
 - ustvarjanje ponudb in prodajnih nalogov,
 - dodajanje ključnih informacij o ponudbi.
- Obdelava prodajnih nalogov:
 - pretvorba potrjenih predračunov v prodajne naloge,
 - določanje podrobnosti naročil (izdelki, količine, cene, popusti itd.),
 - preverjanje zalog in dobavnih rokov.
- Upravljanje strank:
 - vodenje podatkov o strankah,
 - spremljanje nabav in komunikacij posameznih strank,
 - kategorizacija strank glede na kriterije.
- Cenovno vodenje:
 - določanje cenovnih struktur izdelkov,
 - določanje popustov glede na količino nakupa, akcije ipd.,
 - zagotavljanje skladnosti cen skozi različne prodajne kanale.
- Izdelava računov:
 - izdaja računa strankam,
 - povezava med prodajnim nalogom in dostavo,
 - vključitev davčnih podatkov in pogojev plačila.
- Obdelava plačila:
 - beleženje plačil stranke,
 - podpora plačilnim načinom (prenosi, kreditne kartice ipd.),
 - avtomatizacija plačil.
- Analitika in poročanje.
- Napovedovanje prodaje.
- Integracija z moduli upravljanja zalog, financ, CRM.

Display Standard order 4: Overview

Menu

Standard order: 4 Net Value: 20,092.50 USD

Sold-to Party: 1003064 Company The Bike Zone 203, 2144 N Orange Ave, Orlando FL 32804, USA

Ship-to Party: 1003064 Company The Bike Zone 203, 2144 N Orange Ave, Orlando FL 32804, USA

Cust. Reference: 203 Cust. Ref. Date: 10/26/2023

Sales Item Overview Item detail Ordering party Procurement Shipping Reason for rejection

Req. Deliv. Date: 11/26/2023 Deliver. Plant:

Complete Deliv.: Total Weight: 57,170 G

Delivery Block: Volume: 0.000

Billing Block: Pricing Date: 10/26/2023

Pym Terms: 0001 Pay immediately w/o deduction

Inco. Version:

Incoterms: FOB

Inco. Location1: Miami

All Items

Item	Material	Req. Segment	Order Quantity	Un	S	Item Description
10	DXTR1203		5	EA		Deluxe Touring Bike (black)
20	PRTR1203		2	EA		Professional Touring Bike (black)

Slika 4.1: Primer prodajnega naloga v sistemu SAP

V sklopu modula proizvodnje se izvajajo osnovni procesi:

- upravljanje kosovnic:
 - izdelava kosovnic za posamezne izdelke,
 - definiranje razmerij in struktur med posameznimi komponentami izdelkov.
- Usmerjanje (routing) in upravljanje delovnih središč:
 - definiranje proizvodnih smeri, zaporedja postopkov za izdelavo izdelkov,
 - določitev delovnih središč in virov potrebnih za proizvodni proces.
- Načrtovanje proizvodnje:
 - izdelava urnikov proizvodnje glede na napoved zahtev, obstoječe prodajne naloge ali druge zahteve,

- optimizacija razvrščanja za izravnavo porabe virov in upoštevanje rokov.
- Načrtovanje materialov:
 - izračun in načrtovanje zahtevanih materialov/surovin za proizvodnjo,
 - zagotavljanje zadostne količine surovin in komponent za potrebe proizvodnje.
- Upravljanje delovnih nalogov:
 - ustvarjanje in vodenje delovnih nalogov za proizvodnjo,
 - spremljanje statusa delovnih nalogov glede na proizvodni načrt.
- Načrtovanje zmogljivosti:
 - ocenjevanje in vodenje zmogljivosti delovnih središč, virov in strojev,
 - preprečevanje preobremenjevanja ali nizke izkoriščenosti proizvodnih virov.
- Vodenje proizvodnih aktivnosti:
 - spremljanje in beleženje proizvodnih aktivnosti v proizvodni hali,
 - zajem podatkov proizvodnje, izkoriščenosti virov in strojev v realnem času.
- Preverjanje kakovosti:
 - vzpostavitev ukrepov za preverjanje kakovosti izdelkov,
 - izvedba inšpekcij za zagotavljanje kakovosti.
- Upravljanje zalog:
 - osveževanje zalog v realnem času ob uporabi surovin in komponent ter izdelavi končnih izdelkov,
 - komisioniranje in vodenje zalog na podlagi naročil.
- Integracija z modulom upravljanja zalog, financ, skladiščnega sistema.

TRWA1600
Touring Aluminum Wheel Assembly, Plant:Plant Dallas, BOM Usage:Production, Alternative:01

Selected Date: 10/27/2023 Select Change Number: No change number... View Change Records

Components Header Attributes Header Attachments Header Long Text

Item No...	Item Category	Component	Prelimina...	Component Quantity	Subitems	Component Description	Valid From	Valid To
0010	Stock Item (L)	TRTR1600		1.000 EA	Maintain	Touring Tire	01/01/2010	12/31/9999
0020	Stock Item (L)	TRTB1600		1.000 EA	Maintain	Touring Tube	01/01/2010	12/31/9999
0030	Stock Item (L)	TRWH1600		1.000 EA	Maintain	Touring Aluminum Wheel	01/01/2010	12/31/9999
0040	Stock Item (L)	HXNT1600		1.000 EA	Maintain	Hex Nut 5 mm	01/01/2010	12/31/9999
0050	Stock Item (L)	LWSH1600		2.000 EA	Maintain	Lock Washer 5 mm	01/01/2010	12/31/9999
0060	Stock Item (L)	BOLT1600		1.000 EA	Maintain	Socket Head Bolt 5x20mm	01/01/2010	12/31/9999

Slika 4.2: Primer kosovnice za izdelek v sistemu SAP

V sklopu vodenja človeških virov ERP podpira:

- vodenje podatkov o zaposlenih:
 - podatkovna baza s podatki o zaposlenih,
 - zajem in osveževanje osebnih podatkov,
 - vzdrževanje profilov in zgodovine.
- Zaposlovanje in spremljanje kandidatov:
 - ustvarjanje delovnih mest in zaposlovanje,
 - spremljanje prošenj,
 - organiziranje razgovorov in ocenjevanje kandidatov.
- Ocenjevanje zaposlenih:
 - postavljanje pričakovanih uspešnosti,
 - izvajanje ocenjevanja uspešnosti zaposlenih,
 - spremljanje uspešnosti zaposlenih.
- Beleženje prisotnosti:
 - beleženje prihodov in odhodov,
 - spremljanje odsotnosti/dopustov/bolniških,
 - ustvarjanje poročila prisotnosti za plačilne liste.
- Izplačila:

- izračun in izplačila plač,
- odvajanje davkov in ugodnosti,
- generiranje plačilnih list.

Create Personal data

Menu

Personnel No:

* Start: * To:

Name

Title:

* Last Name:

* First Name:

Middle name:

Designation:

Suffix:

Name:

Name Format:

Birth name:

Initials:

Nickname:

HR data

* SSN:

* Date of Birth:

Language:

Nationality:

Marital status:

Gender:

Slika 4.3: Primer vnosa za novega zaposlenega v sistemu SAP

Glavne naloge, ki jih ERP podpira na področju nabave, so:

- upravljanje dobaviteljev:
 - vodenje podatkov o dobaviteljih, kontaktih, zgodovine poslovanja,
 - ocenjevanje in kategorizacija dobaviteljev glede na zanesljivost, stroške, kakovost storitev.
- Iskanje dobaviteljev in zahteve za ponudbe:
 - iskanje možnih dobaviteljev za izdelek ali storitve,
 - ustvarjanje zahtev za ponudbe (Request for quotation) in njihovo vodenje,
 - ocenjevanje in primerjava ponudb.

- Nabava:
 - izvedba nakupa na podlagi potreb,
 - določanje izdelkov oz. storitev in količin,
 - priprava sredstev in pooblastil.
- Nabavni nalog:
 - ustvarjanje in potrjevanje nabavnih nalogov izbranim dobaviteljem,
 - določanje podrobnosti (količine, cene, pogoji plačil in dostave),
 - posredovanje nabavnega naloga ponudniku in notranjim službam za odobritev.
- Definiranje postopkov odobritev:
 - določitev deležnikov potrjevanja oz. odobritev,
 - določitev odobritvenih pristojnosti in usmerjanja potrditev,
 - zagotavljanje skladnosti s postopki poslovnega procesa.
- Pogajanja z dobavitelji in upravljanje pogodb:
 - vodenje pogajanj za doseganje ugodnih pogojev,
 - ustvarjanje in upravljanje pogodb z dobavitelji,
 - spremljanje izvajanja pogodb in njihovo podaljševanje.
- Prevzem in pregled izdelkov:
 - beleženje prejetih izdelkov s strani dobaviteljev,
 - pregled kakovosti in skladnosti z zahtevami,
 - osveževanje zalog in financ.
- Računovodstvo:
 - preverjanje skladnosti računov in prejetih pošilk,
 - potrjevanje cen, količin in pogojev,
 - potrjevanje računov in plačil.

Pri vseh dejavnostih je bistvena povezava med dejanskim dogajanjem in informacijskim tokom, ki spremlja to dogajanje. Za vsako aktivnost pri poslovanju mora obstajati povezava med dejanskim in informacijskim tokom. Vsako izvedeno aktivnost je tako potrebno v sistemu ERP zabeležiti ali potrditi, prav tako pa ERP podaja, katere aktivnosti se morajo izvesti.

Kakor se dejanski materialni tokovi, izvedene storitve in druge aktivnosti v realnem času zaležijo v sistemu ERP, tako se na primer pri odpremi pošiljke (in potrditvi aktivnosti) preračunajo zaloge.

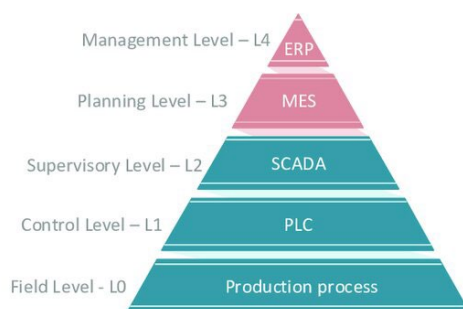
Sistemi ERP s centralnim delovanjem zagotavljajo, da vsak oddelek dobi na razpolago ažurne podatke ter le tiste, do katerih smejo posamezni udeleženci procesa dostopati.

Ker po navadi obstaja medsebojna odvisnost pri aktivnostih posameznih oddelkov, je v sistemih ERP pomembna tudi skladnost podatkov. Tako se lahko načrt proizvodnje tvori glede na potrjena naročila prodaje, posledično se ustvarijo nabavni nalogi za potrebne surovine.

Dodatna prednost, ki jo tu nudijo sistemi ERP, je avtomatizacija postopkov. Tako se na primer lahko po potrditvi naročila samodejno tvori prodajni nalog, ali pa ustvari proizvodni načrt glede na naročila. Seveda je še vedno na ključnih stopnjah potrebna potrditev pooblaščenega zaposlenega na ustreznem oddelku.

6 Integracija sistemov

Glede na vrsto lahko podjetja uporabljajo sistem ERP kot samostojno orodje, v mnogih primerih pa je potrebna integracija z drugimi. Slika 4 prikazuje primer nivojev avtomatizacije in sistemov. Sistemi ERP tu predstavljajo vrhovni managerski nivo, ki nadzira delovanje celotnega poslovanja.



Slika 4.4: Avtomatizacija po ANSI/ISA-95

Vir: . (Pospisil, 2021)

Podporni sistemi so postavljeni glede na nivo uporabe. Tako na najnižjem nivoju govorimo o proizvodnem procesu na strojnem nivoju. Sistemi PLC (Programmable Logic Controller) omogočajo nadzor oz. krmiljenje posameznih strojev in so osnova za avtomatizacijo proizvodnje. Za nadzor dogajanja skrbijo sistemi SCADA (Supervisory Control and Data Acquisition), ki zbirajo in prikazujejo podatke naprav in senzorjev ter omogočajo oddaljeno upravljanje. Sistemi MES (Manufacturing Execution System) upravljajo in nadzorujejo proizvodne. S povezavo PLC omogoča globok vpogled v izvajanje procesa ter skrbi za zvezno izmenjavo podatkov o proizvodnih nalogih, zalogah, preverjanju kakovosti in drugih ključnih proizvodnih kazalnikih v realnem času.

Zasnova sistemov ERP mora biti kompatibilna z obstoječimi preostalimi sistemskimi rešitvami, zato je v mnogih primerih potrebna tudi horizontalna integracija. To lahko zajema povezljivost z uporabniško programsko opremo, kot so pisarniške rešitve, komunikacijske aplikacije ipd. Predvsem pa je tu bistveno ustrezno deljenje podatkov in dostopov do njih med posameznimi oddelki. Pri horizontalni integraciji je potrebno skrbno načrtovati delovanje na osnovi poslovnih procesov.

7 Zaključek

ERP in njihovi podporni sistemi so za današnje poslovanje ključnega pomena, saj ne predstavljajo več konkurenčne prednosti, temveč so neobhodni za uspešno poslovanje. Z integracijo tovrstnih sistemov je mogoče zagotoviti ne le informacijske podpore poslovnim procesom, temveč tudi njihovo izvajanje z visoko stopnjo avtomatizacije. Prav avtomatizacija pogostih rutinskih aktivnosti pripomore k povečanju učinkovitosti poslovnih aktivnosti. Poenoten dostop omogoča visoko stopnjo preglednosti ter s tem poveča tudi zanesljivost procesov in pogosto z zmanjšanjem človeškega vpliva tudi zmanjša verjetnost napak. Glede na obsežno podatkovno oz. informacijsko podporo sistemi omogočajo napredne analize poslovanja ter podporo odločanju na operativnem, taktičnem in strateškem nivoju.

Literatura

Alanbay, O. (2005). ERP selection using expert choice software. Honolulu, Hawaii, July, 8(10).

- Podvezko, V. (2009). Application of AHP technique. *Journal of Business Economics and Management*, (2), 181-189.
- Pelphrey, M. W. (2015). *Directing the ERP implementation: A best practice guide to avoiding program failure traps while tuning system performance*. CRC Press.
- Pospisil, O., Blazek, P., Kuchar, K., Fajdiak, R., & Misurec, J. (2021). Application perspective on cybersecurity testbed for industrial control systems. *Sensors*, 21(23), 8119.

PODPORA ODLOČANJA S SIMULACIJAMI

BOJAN RUPNIK

Univerza v Mariboru, Fakulteta za logistiko, Celje, Slovenija
bojan.rupnik@um.si

Logistični, proizvodni, transportni in vsi sorodni problemi v osnovi potekajo po sorodnih procesih, pri katerih je ključni dejavnik čas. Glede na kompleksnost procesov je nekatere mogoče dokaj enostavno analizirati, bolj pa kot so procesi prepleteni, težje jih je dobro povzeti s klasičnimi analitičnimi pristopi. Pri tem so simulacije tiste, ki omogočajo globlji vpogled v potek tovrstnih procesov, omogočajo analizo učinkovitosti, pomanjkljivosti, predvsem pa preverjanje in analizo obstoječih sistemov ob različnih pogojih brez poseganja v njihovo delovanje. Poleg dobrega poznavanja procesov je za simulacije ključnega pomena podatkovna podpora, ki lahko vključuje od beleženja zgodovinskih podatkov pa do napovedovanja prihodnjega dogajanja z možnimi alternativnimi scenariji. Z možnostjo sprotnega beleženja podatkov med izvajanjem procesa in posredovanja aktivni simulaciji, ki podatke sproti obdeluje, lahko zgradimo digitalni dvojček. V sklopu tega poglavja udeleženci spoznajo strežne sisteme in čakalne vrste, simulacije diskretnih dogodkov in orodja, ki jih podpirajo ter primere uporabe v proizvodnih, logističnih in transportnih primerih.

DOI

[https://doi.org/
10.18690/um.fl.2.2025.5](https://doi.org/10.18690/um.fl.2.2025.5)

ISBN

978-961-286-971-7

Ključne besede:

poslovno odločanje,
podatki,
obdelava podatkov,
prikazovanje podatkov,
statistične analize



Univerzitetna založba
Univerze v Mariboru

DOI
[https://doi.org/
10.18690/um.fl.2.2025.5](https://doi.org/10.18690/um.fl.2.2025.5)

ISBN
978-961-286-971-7

Keywords:
simulations,
discrete event simulation,
digital twin,
material flow,
queuing systems

SIMULATIONS IN DECISION MAKING

BOJAN RUPNIK

University of Maribor, Faculty of Logistics, Celje, Slovenia
bojan.rupnik@um.si

Logistical, production, transportation, and all related issues in the industry follow similar processes, with time being the crucial factor. While some processes can be relatively easily analysed due to their simplicity, the more interconnected the processes are, the more challenging it becomes to describe them accurately using traditional analytical approaches. Simulations, in this regard, provide a deeper insight into the flow of such processes. They enable the analysis of efficiency, shortcomings, and, most importantly, allow for the examination of existing systems under different conditions without interfering with their operation. Besides having a good understanding of the processes, data support is crucial for simulation. This support can involve the recording of historical data and predicting future events with possible alternative scenarios. By enabling real-time data logging during process execution and providing the data to an active simulation that processes it in real-time, a digital twin can be created. Within the scope of this subject, participants familiarize themselves with server systems, queuing systems, discrete event simulations, and the tools that support them, along with examples of their application in manufacturing, logistics, and transportation scenarios.



University of Maribor Press

1 Uvod

S simulacijami poskušamo preslikati dogajanje iz resničnega sveta v matematični oz. računalniški model, s katerim lahko to dogajanje ponavljamo, ga spreminjamo ter opazujemo, kako se to dogajanje obnaša ob različnih pogojih. Večino področij iz poslovnega sveta je mogoče analizirati s simulacijami, kot so na primer materialni tokovi v proizvodnih obratih ali skladiščih, simulacije transportnih tokov, informacijskih ali finančnih tokov. Simulacije nam tako služijo ne le za analizo tovrstnih sistemov, ampak tudi za optimizacijo – sploh, kadar so sistemi preveč računsko kompleksni, da bi jih bilo mogoče v ustreznem času optimizirati s klasičnimi optimizacijskimi metodami.

Glede na vrsto problemov, ki jih rešujemo in namen optimizacije, obstaja več različnih simulacijskih pristopov:

- 3D/realno-časovne simulacije (npr. simulacije za učenje pilotov),
- sistemska dinamika (simulacije kompleksnih, celovitih sistemov),
- simulacija agentov (opazovanje ljudi, entitet ob interakcijah v prostoru in času),
- simulacija diskretnih dogodkov.

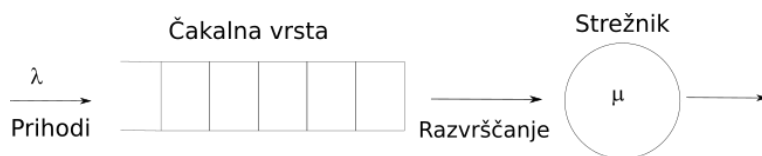
Prav slednji pristop je v ospredju tega dela. Simulacije diskretnih dogodkov omogočajo opisovanje kakršnihkoli sistemov, kjer posamezni dogodki vplivajo na nadaljnje obnašanje dogajanja. Sama metoda je v osnovi preprosta. Celoten sistem je zasnovan s stanji, ki jih spremenijo le dogodki ob vnaprej določenih časih. Za razliko od zveznih simulacij je med posameznimi dogodki, ne glede na pretečen čas, stanje vedno nespremenjeno. Dogodki so lahko definirani vnaprej (npr. predvideni prihodi strank), lahko pa tudi sami generirajo nove dogodke.

2 Modeliranje in simulacija procesov

Ne glede na področje vsi procesi vključujejo časovno komponento. Tako glede na obnašanje opazujemo, kaj se v določenem sistemu dogaja in kako dolgo kaj traja. Tu lahko upoštevamo vhodne tokove, kot so npr. prihodi strank v trgovino, trajanje nakupa, čakanje pred blagajno. Ta primer lahko preslikamo na številne druge, pri katerih govorimo o vhodih, obdelavi in na koncu izhodu iz sistema.

2.1 Strežni sistemi in čakalne vrste

Osnovni primer (Slika 5.1) strežnega sistema (Thomopoulos, 2012) vključuje čakalno vrsto, v kateri entitete čakajo na obdelavo in strežnik, ki te naloge obdeluje, delovanje sistema pa je odvisno od strežne zmogljivosti strežnika, intenzitete prihodov nalog in kapacitete čakalne vrste. Entitete lahko glede na naravo simulacije predstavljajo naloge, pakete, stranke, informacije, obdelovance oz. praktično vsak element, ki v sklopu simulacije vpliva na dogajanje.



Slika 5.1: Osnovni strežni sistem s čakalno vrsto

Vir: lasten

Intenziteta prihodov določa, s kakšno frekvenco prihajajo entitete v čakalno vrsto. V glavnem lahko intenziteto prihodov podamo kot:

$$\lambda = \frac{N}{T} \quad (1)$$

kjer je λ intenziteta, N število prihodov in T časovni interval prihodov.

Po postopku se vsaka entiteta postavi v čakalno vrsto, iz katere se posreduje strežniku, v kolikor je ta razpoložljiv. V primeru več čakajočih entitet je izbira naslednje, ki se posreduje, lahko izvedena po različnih pristopih:

- FIFO (First-in, First-out) pristop, kjer se vsaka naloga posreduje strežniku po vrstnem redu v katerem pride.
- LIFO (Last-in, Fast-out) pristop, kjer se zadnja naloga, ki vstopi v vrsto, prva posreduje na strežnik.
- Prioritetne vrste omogočajo postavitev prioritete obravnave za določene naloge oz. skupine nalog. Tako se entitete z višjimi prioritetaми posredujejo na strežnik pred tistimi z nižjimi.
- Naključni pristop določi naključno entiteto v čakalni vrsti.

Glede na intenziteto prihodov in razpoložljivost strežnika se lahko entitete v čakalni vrsti kopičijo, zmanjšujejo ali pa povprečno enakomerno dolgo čakajo v čakalni vrsti. Pri modeliranju sistemov je navadno iskana prav slednja varianta, saj omogoča stabilne sisteme.

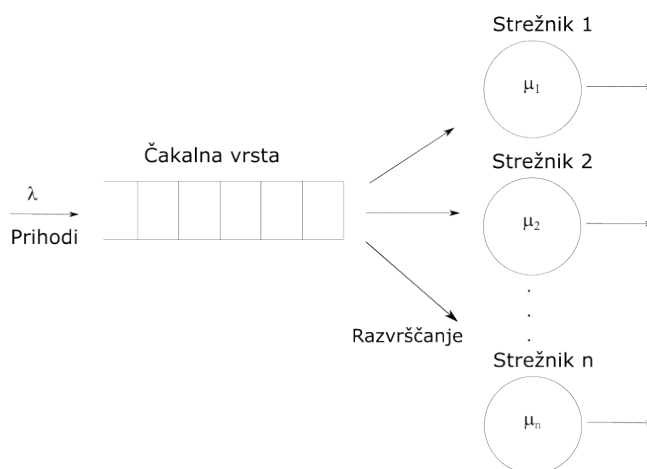
Poleg intenzitete prihodov je ključni dejavnik tudi hitrost strežbe μ , ki je podana s številom entitet, ki jih je strežnik zmožen obdelati na časovno enoto. Strežna hitrost je tako podana kot obratna vrednost strežnega časa.

$$\mu = \frac{1}{s} \quad (2)$$

S predstavlja strežni čas. Podobno kot pri prihodih je tudi strežni čas lahko podvržen naključnosti. Tako ločimo hitrosti strežbe na:

- deterministične in
- stohastične.

V nekaterih primerih je strežni čas konstanten in znan vnaprej, pri drugih pa odvisen od dejavnikov in naključen. Modeliranju strežnih časov navadno ustrezata eksponentna ali normalna porazdelitev glede na vrsto procesa.



Slika 5.2: Strežni sistem z več strežniki

Vir: lasten

Predstavljeni model omogoča simulacijo čisto osnovnega procesa z eno čakalno vrsto in enim strežnikom. Posnemanje primerov iz realnega sveta pa zahteva gradnjo kompleksnejših mrež, kjer lahko ima vsak gradnik več vhodov in izhodov. Glede na zahtevnost primera, ki ga želimo modelirati, lahko tako nastanejo kompleksni modeli, kjer na potek vplivajo, ne le povezanost med gradniki, temveč tudi pravila razvrščanja po posameznih, pogojno določenih prihodih in strežna pravila. Modeliranje in simulacijo tovrstnih primerov je zato smiselno izvesti v ustreznih namenskih orodjih.

Za opis glavnih karakteristik strežnih sistemov s čakalnimi vrstami je v uporabi Kendallova označba (Bolch et al., 2006). Osnovna označba je v naslednji obliki:

$$A/B/c/K/m/Q,$$

kjer predstavlja:

A – porazdelitev časov prihodov,

B – porazdelitev časov strežbe,

c – število strežnikov,

K – kapaciteto čakalnih vrst,

m – velikost populacije,

Q – strežno strategijo.

Vrednosti, ki jih tako zavzemata komponenti A in B , so:

- M – eksponentna porazdelitev,
- D – deterministična porazdelitev,
- E – Erlangova porazdelitev,
- G – splošna porazdelitev.

Število strežnikov c podaja podatek, na koliko strežnikov se lahko paralelno izvajajo strežbe.

Kapaciteta K določa maksimalno število strank v sistemu tako v čakalnih vrstah kot tudi na strežbi, medtem ko m predstavlja pričakovano število strank. Že prej omenjene strežne strategije (FIFO, LIFO) pa določajo, na kakšen način se entitete posredujejo iz čakalnih vrst.

2.2 Simulacija diskretnih dogodkov

Medtem ko strežni sistemi s čakalnimi vrstami predstavljajo predvsem abstraktno predstavitev, je za modeliranje kompleksnejših sistemov potreben naprednejši pristop. Simulacije diskretnih dogodkov (Fishman, 2001) poleg npr. sistemske dinamike ali agentske simulacije predstavljajo enega izmed najbolj uporabljenih pristopov. Med drugim je pogosta uporaba pri simuliranju problemov iz proizvodnje, zdravstva, transporta in logistike, energijskih sistemov, oskrbovalnih verig in sorodnih.

Strežni sistemi s čakalnimi vrstami predvidevajo dokaj neposreden tok med prihodi in obdelavo. Pri modeliranju diskretnih dogodkov pa se poleg samih entitet, vrst in strežnikov upoštevajo tudi karakteristike, pravila, viri in dogodki. V sklopu simulacije se na podlagi modela zgradi seznam vseh dogodkov in njihov predvideni čas. Dogodek predstavlja kakršnokoli spremembo sistema, kot npr. vstop stranke v čakalno vrsto, začetek oz. konec obdelave izdelka na stroju ali sprememba lastnosti entitete. Vsak dogodek spremeni stanje simuliranega sistema.

Izvajanje simulacije poteka po simulacijskem času, ki ne teče po realnem času, ampak diskretno preskakuje čase med posameznimi dogodki. Posamezni dogodki lahko tvorijo tudi nove dogodke, ki se prav tako umestijo v seznam bodočih dogodkov, zaradi česar se lahko nekateri, že načrtovani dogodki, tudi prestavijo.

Med samim izvajanjem simulacije se beležijo statistike čakalnih vrst, izkoriščenosti strežnikov, pretočnost in drugi parametri, s katerimi je mogoče podati ustrezno analizo simuliranih sistemov.

Še dva ključna elementa pri izvajanju simulacij sta verifikacija in validacija. Z verifikacijo preverimo pravilnost posameznih implementiranih funkcionalnosti, formul za izračune, logike. Z validacijo preverjamo, kako dobro model posnema realni sistem. Rezultate simulacije v ta namen primerjamo s pričakovanim

obnašanjem realnega sistema, ki je pridobljeno iz meritev ali ekspertne ocene. Verifikacija in validacija sta ponavljajoča se procesa, ki vodita k večji natančnosti in zanesljivosti izdelanega modela. Z analizo senzitivnosti lahko ocenimo tudi območja negotovosti.

2.3 Modeliranje simulacijskih parametrov

Načini modeliranja vhodnih parametrov simulacije so odvisni od vrste simuliranega sistema in od razpoložljivih podatkov. Pri tem je v prvi fazi potrebno dobro razumevanje procesov, na podlagi katerih je možno modelirati materialni tok. Tako je potrebno identificirati vse dejavnike (procese ali parametre), ki lahko vplivajo na obnašanje sistema, kot so:

- entitete in njihove lastnosti – kateri so ključni elementi simulacije, kako lahko njihove lastnosti vplivajo na materialni tok (entitete z različnimi lastnostmi imajo npr. različne tokove skozi omrežje).
- Simulacijski objekti – kakršnikoli gradniki simulacijskega orodja, ki vplivajo na stanje sistema – izvori, ponori, strežniki oz. procesorji, čakalne vrste, objekti za združevanje oz. razdruževanje entitet, objekti za spreminjanje lastnosti entitet, generatorji dogodkov-
- Materialni tok – povezave med vsemi objekti iz oz. do katerih se entitete lahko premikajo. Ob tem je potrebno skrbno določiti pogoje preusmeritev iz posameznih objektov na naslednike.
- Vhodne intenzitete – primer, podan na začetku poglavja, je le ena izmed možnosti za modeliranje vhodov. Ob modeliranju vhodov iz realnih sistemov lahko uporabimo:
 - deterministične vrednosti – pri sistemih, kjer so dobro določene količine in časi (npr. vozni redi vlakov, urniki sestankov itd.).
 - Dinamične prihode – vhodne obremenitve so lahko odvisne od raznih dejavnikov kot npr. količina vozil ob prometnih špicah.
 - Prileganje statističnim porazdelitvam – kadar imamo na razpolago ustrezne podatke, lahko vhodne obremenitve modeliramo s prileganjem statističnim porazdelitvam.

- Zgodovinske podatke – kjer imamo na voljo beleženje dogajanja v sistemih (npr. sistemi MES), lahko opravimo analizo s privilegjem statističnim porazdelitvam.
- Ekspertne ocene – ob pomanjkanju zapisov lahko oceno obnašanja posameznih gradnikov ocenimo na podlagi izkustvenih ocen ekspertov.
- Naključne vrednosti – naključnost predstavlja ključni element simulacij. Pri modeliranju prihodov se sicer naključne vrednosti uporabljajo znotraj ustreznih razponov oz. se naključne vrednosti tvorijo po ustreznih porazdelitvah.
- Analizo občutljivosti - vhodne parametre lahko spreminjamo, da ocenimo, kakšno je obnašanje sistema ob različnih začetnih nastavitvah ob predpostavki.
- Strežne hitrosti – pridobitev strežnih hitrosti je podobna kot pri vhodnih intenzitetah. Pogosto je možno strežne hitrosti pridobiti iz poznavanja trajanja procesov kot npr. specifikacije proizvodnih strojev, hitrosti transporta itd.

Ne glede na to, kateri pristop je uporabljen, je glede na modeliran sistem, potrebno skrbno preučiti vse izbrane parametre (validacija modela).

2.4 Naključne vrednosti

Tvorba naključnih vrednosti predstavlja enega izmed temeljnih konceptov pri simulacijah, zato ji tudi namenjamo lastno poglavje. Ustvarjanje naključnega števila (L'Ecuyer, 2012) je sicer matematično preprosta operacija, vendar lahko ob nerodnem pristopu pripelje do pojava vzorcev. Pojav vzorcev pri tvorbi naključnih števil lahko privede do neustreznega obnašanja simulacije, saj se lahko pojavijo nezaželene odvisnosti v simulacijskem toku, ki ga sicer v realnem sistemu ne bi bilo pričakovati.

Računalniški sistemi za tvorjenje naključnih vrednosti uporabljajo generatorje psevdo-naključnih števil, kjer se izračun naključne vrednosti izvede s funkcijo z vhodno spremenljivko. Primer enostavnega linearne kongruenčnega generatorja podamo s formulo:

$$X_{n+1} = (aX_n + c) \% m \quad (3)$$

Tu predstavljajo:

X_n - seme generatorja,

a - množitelj – določa periodo in kakovost naključnosti,

c - inkrement – premik sekvence za večjo raznolikost ustvarjenih števil,

m - delitelj – določa obseg ustvarjenih števil.

Lastnosti zaporedja naključnih števil, ustvarjenega s takšnim generatorjem, so odvisne od izbire danih parametrov. Namen generatorjev je ustvariti čim večjo entropijo oz. nepredvidljivost stanj, zato je tudi izbira semena pomembna. Ob uporabi enakega semena bo funkcija vedno ustvarila enako zaporedje psevdonaključnih vrednosti. Glede na potrebe je to lahko zaželeno, kot na primer pri izvedbi različnih konfiguracij ob enakih inicialnih vseh ali pri verifikaciji. V večini primerov pa je zaželeno naključne vrednosti čim bolj razpršiti. V takih primerih je smiselno tudi seme generatorja izbrati čim bolj naključno, na primer iz trenutnega procesorskega časa ob izvršitvi generiranja naključne vrednosti. Linearni kongruenčni generator tvori cela števila na intervalu $[0, m - 1]$, pogosto pa je želena tvorba realnih števil na intervalu $[0, 1]$, predvsem v namene normalizacije vrednosti. V ta namen novo število delimo z m .

Pri modeliranju večine problemov iz realnega sveta intenziteta prihodov poteka naključno, kljub temu pa lahko to naključnost navadno postavimo v meje. Intenziteto prihodov tako pogosto modeliramo s porazdelitvami, kjer so prihodi neodvisni in povprečno sledijo v enakih razmikih. Modeliranje naključnih procesov iz realnega sveta pogosto izvajamo po Poissonovi porazdelitvi:

$$P(X = k) = \frac{(\lambda^k e^{-\lambda})}{k!}, \quad (4)$$

kjer je $(P(X = k))$ verjetnost pojavitve k dogodkov, λ povprečna intenziteta prihodov v časovnem intervalu in k število dogodkov za kolikor želimo poiskati verjetnost. Poissonova porazdelitev je uporabna pri opisu dogodkov, kot so:

- modeliranje prihodov strank v trgovino v določenem časovnem obdobju,
- analiza števila okvar pri proizvodnji,
- napovedovanje števila nesreč na odseku znotraj časovnega obdobja,
- prihodi sporočil pri e-pošti.

Modeliranje vhodnih tokov ali strežnih hitrosti izvajamo s prileganjem statističnim porazdelitvam (Johnson, 1987), kot sta Poissonova ali normalna. Te lahko določimo s statističnimi testi, oceno oblike histogramov, metodo minimalnih kvadratov in drugimi pristopi. Ko imamo porazdelitve procesov znane, lahko na njihovi podlagi ustvarimo naključne dogodke, ki se odvijajo po enakih statističnih karakteristikah kot preučeni sistemi.

Primer izračuna naključno generiranih vrednosti po Poissonovi porazdelitvi s povprečno vrednostjo λ prikazuje naslednji postopek:

function *Poisson*(λ)

$L = e^{-\lambda}$

$k \leftarrow 0$

$p \leftarrow 1$

while ($p > L$) **do**

$k \leftarrow k + 1$

$p = p * rand()$

end

Poisson = k

Psevdokoda 1: generator naključnih vrednosti po Poissonovi porazdelitvi

3 Simulacijski primer

Za simulacijski primer vzemimo trgovino, v katero stopajo stranke, ki različno dolgo iščejo izdelke in jih na koncu kupijo na blagajni. Definirajmo lastnosti sistema:

- povprečno vstopi 5 strank na minuto,
- št. Blagajn: 5,
- povprečno trajanje nakupa: 15 min,

- transakcija na blagajni traja povprečno 5 minut.

Po Kendallov notaciji bi lahko osnovni strežni sistem opisali z:

M/M/5/30/3000/FIFO,

pri čemer predpostavimo prihode strank in strežbo po eksponentni porazdelitvi, upoštevamo 5 blagajn, ocenjeno kapaciteto trgovine za 30 strank, skupno število strank pa zaokrožimo na 3000 (ocena za en delovni dan). Za strežno strategijo izberemo FIFO, se pravi, da se stranke strežejo glede na njihov čas prihoda (in nakupa).

Vhodni parameter tu predstavlja povprečni čas prihoda med dvema zaporednima strankama. Če privzamemo, da so prihodi strank Poissonov proces, lahko naključne čase prihodov modeliramo na naslednji način:

$$t_i = \frac{-\ln \text{rnd}()}{\lambda} \quad (5)$$

Tabela 5.1: Primer naključno določenih prihodov po eksponentni porazdelitvi

	Naključni čas [s]	Naslednji prihod [s]
1	0,010422473	0,625348364
2	0,44356782	27,23941755
3	0,047033142	30,06140609
4	0,561568412	63,7555108
5	0,416494108	88,74515728
6	0,083158277	93,73465391
7	0,023527478	95,14630261
8	0,052567808	98,30037111
9	0,130142537	106,1089233
10	0,055501926	109,4390389
11	0,010422473	144,9275279
12	0,44356782	152,8945772
	...	...

Vir: lasten

Podan simulacijski primer lahko analiziramo s strežnimi sistemi s čakalnimi vrstami, vendar se z vsakim dodanim elementom kompleksnost poveča. Zato je smotno za tovrstne probleme uporabiti ustrezna simulacijska orodja. Pri simulacijskih orodjih ni pričakovati, da bodo rezultati simulacije popolnoma skladni s teoretičnimi izračuni

zaradi zaokrožitvenih napak in naključnosti, vendar bi se morali pri dobro načrtovanem simulacijskem modelu rezultati dobro približati teoretičnim izračunom.

Iz zastavljenega primera simulacije lahko hitro ugotovimo, da sistem ni vzdržen; ob povprečnem številu 5 strank na minuto in 5 blagajnami s strežno hitrostjo 5 minut. Čas nakupovanja pri tem predstavlja primer, ki ga stranke opravljajo istočasno. Če bi s Kendallovno notacijo podali samo ta del, bi ga lahko opisali kot proces, ga lahko poenostavljeno podamo z:

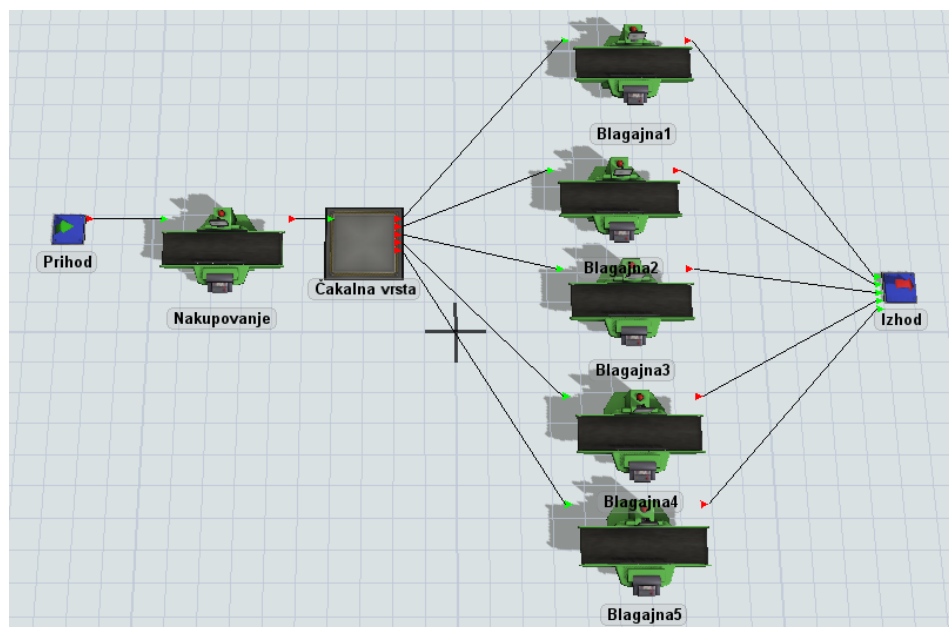
$$M/M/\infty,$$

saj pri nakupovanju vsaka stranka opravlja svoj nakup in pri tem niti ne rabi vstopati v čakalno vrsto. Zato lahko ta segment upoštevamo kot neomejen (vsaka stranka ima svoj takoj razpoložljiv strežnik). Prihodi strank predstavljajo prihode, kot so generirani, za strežno hitrost upoštevamo po zadanih parametrih povprečno 15 min na stranko. Stranke po opravljenem nakupu vstopijo v čakalno vrsto (oz. čakalne vrste pred posameznimi blagajnami). Pri konkretni simulaciji bi morali seveda upoštevati razne faktorje, kot so delovni čas, pavze in malice, obremenitve ob različnih časih tekom dneva itd.

Predstavljeni primer lahko modeliramo v simulacijskih orodjih (Slika 5.3) ter se izogibamo množici izračunov pri večanju kompleksnosti strežnih sistemov s čakalnimi vrstami.

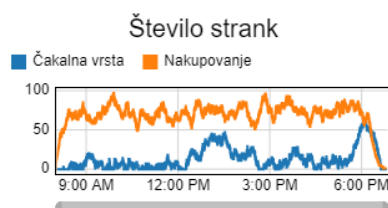
Ker je zastavljeni primer nestabilen (nenehno naraščanje čakalne vrste in nenehna zasedenost blagajn), preverimo, kako bi lahko spremenili sistem v vzdržnega. V glavnem lahko uporabimo dva pristopa. Lahko dodamo dodatne blagajne ali pa jih zamenjamo za hitrejše. Za ta scenarij pustimo vse nastavitve in karakteristike enake, le blagajne pohitrimo za faktor 5 (še vedno po eksponentni porazdelitvi).

Cilj vsake simulacije je ugotoviti zmogljivosti modeliranega sistema, kamor spadajo razne karakteristike. V tem primeru se osredotočimo na velikost čakalne vrste (Slika 5.4) in čakalne čase v njej (Slika 5.5) ter izkoriščenost blagajn (Slika 5.6).



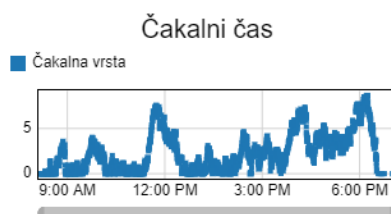
Slika 5.3: Simulacijski model trgovine v orodju FlexSim

Vir: lasten



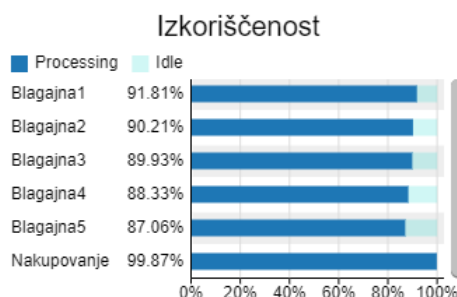
Slika 5.4: Dolžina čakalne vrste

Vir: lasten



Slika 5.5: Čakalni časi v čakalni vrsti

Vir: lasten



Slika 5.6: Izkoriščenost blagajn

Vir: lasten

Rezultati simulacije ob spremenjenih karakteristikah pokažejo (relativno) stabilen sistem, saj nimamo nenehno naraščajočih čakalnih vrst in čakalnih časov. Pogosto je pri simulacijah kompleksnih sistemov potrebno poiskati rešitve, kjer se izognemo ozkim grlom in neizkoriščenim virom.

4 Zaključek

Predstavljeni primer kaže le delček zmožnosti, ki jih simulacije nudijo. Velika uporabnost simulacij pride do izraza predvsem pri preučevanju kompleksnih sistemov, kjer je govora o navidezno nepovezanih parametrih. Tako se simulacije uporabljajo na logističnem, finančnem, informacijskem, proizvodnem oz. pravzaprav kakršnekoli sorodnem področju. Na področju logistike simulacije predstavljajo stroškovno ugoden pristop pri analizi proizvodnih procesov, transportnih poti in usmerjanja, prometnih vzorcev ipd. S spreminjanjem parametrov simulacije oz. simulacijskih scenarijev je možno kompleksne sisteme opazovati z različnih vidikov, kar omogoča učinkovito odločanje na podlagi smotrnih analiz.

Izvedba simulacij omogoča cenovno učinkovit pristop za analizo kompleksnih sistemov brez potrebe po prekinitvi procesov. V današnjih tehnoloških sistemih je opaziti vedno večjo integracijo raznovrstnih rešitev, od sistemov ERP, MES, PLC, SCADA in drugih. Medtem ko tovrstni sistemi v glavnem beležijo in tudi lahko v veliki meri vodijo procese, predstavlja simulacija alternativno možnost za optimizacijo s primerjavo alternativ in podporo odločanju. V zadnjem obdobju v

ospredje prihajajo digitalni dvojčki, ki omogočajo celovit vpogled v razne procese podjetij. Digitalni dvojčki zajemajo dogajanje procesov podjetja v realnem času iz senzorjev, strojev, naprav in drugih virov (internet stvari) ter na podlagi teh zgradijo virtualno predstavo. Simulacije, izvedene nad virtualno podobo realnega sistema, omogočajo globlji vpogled v delovanje in poslovanje ter predstavljajo dodano vrednost pri poslovnem odločanju na vseh nivojih.

Literatura

- Thomopoulos, N. T. (2012). Fundamentals of queuing systems: statistical methods for analyzing queuing models. Springer Science & Business Media.
- Bolch, G., Greiner, S., De Meer, H., & Trivedi, K. S. (2006). Queueing networks and Markov chains: modeling and performance evaluation with computer science applications. John Wiley & Sons.
- Fishman, G. S. (2001). Discrete-event simulation: modeling, programming, and analysis (Vol. 537). New York: Springer.
- Johnson, M. E. (1987). Multivariate statistical simulation: A guide to selecting and generating continuous multivariate distributions (Vol. 192). John Wiley & Sons.
- L'Ecuyer, P. (2012). Random number generation (pp. 35-71). Springer Berlin Heidelberg.

AVTONOMNA VOZILA V INTRALOGISTIKI

DARKO HERCOG,¹ PRIMOŽ BENČAK²

¹ Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko,
Maribor, Slovenija
darko.hercog@um.si

² Univerza v Mariboru, Fakulteta za logistiko, Celje, Slovenija
primoz.bencak1@um.si

Avtomatsko vodena in avtonomna vozila se vedno bolj uporabljajo v intralogističnih procesih v namene transporta blaga ali podpore pri komisioniranju. Publikacija podaja kratek pregled področij avtomatskih in avtonomnih vozil, njihove razlike ter možnosti uporabe v intralogistiki. Bralcu poda osnovno teorijo s področja delovanja posameznih (pod)sistemov (pogon, senzorji, lokalizacija in navigacija) avtonomnih mobilnih robotov. Za lažje razumevanje so dodane spletne povezave do videoposnetkov, ki teorijo podkrepijo s praktičnimi prikazi. Nazadnje je s primerom avtonomnega mobilnega robota MiR100 predstavljeno upravljanje mobilnega robota in njegove funkcije.

DOI

[https://doi.org/
10.18690/um.fl.2.2025.6](https://doi.org/10.18690/um.fl.2.2025.6)

ISBN

978-961-286-971-7

Ključne besede:

avtonomna vozila,
avtonomni mobilni roboti,
AMR,
avtomatsko vodena vozila,
AGV,
intralogistika



Univerzitetna založba
Univerze v Mariboru

DOI
[https://doi.org/
10.18690/um.fl.2.2025.6](https://doi.org/10.18690/um.fl.2.2025.6)

ISBN
978-961-286-971-7

Keywords:

autonomous vehicles,
autonomous mobile robots,
AMR,
automated guided vehicles,
AGV,
intralogistics

AUTONOMOUS VEHICLES IN INTRALOGISTICS

DARKO HERCOG,¹ PRIMOŽ BENČAK²

¹ University of Maribor, Faculty of Electrical Engineering and Computer Science,
Maribor, Slovenia
darko.hercog@um.si

² University of Maribor, Faculty of Logistics, Celje, Slovenia
primoz.bencak1@um.si

Automated guided and autonomous vehicles are increasingly used in intralogistics processes to transport goods or support order picking. The publication provides a brief overview of the areas of automated and autonomous vehicles, their differences, and potential applications in intralogistics. The reader is introduced to the basic theory of the operation of autonomous mobile robots' (sub)systems (drive, sensors, localization, and navigation). For ease of understanding, web links to videos are added, which support the theory with a practical demonstration. Finally, in an example of the autonomous mobile robot MiR100, the operation of the mobile robot and its functions are presented.



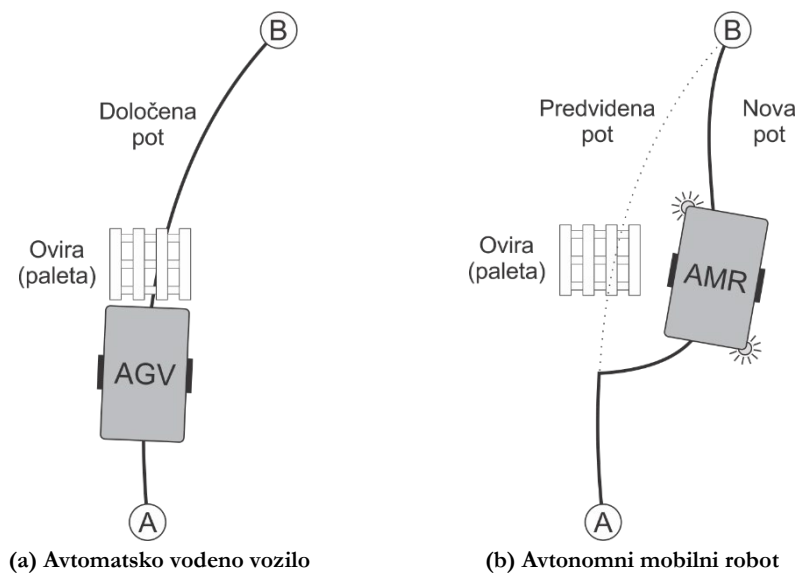
University of Maribor Press

1 Uvod

Avtonomna in avtomatsko vodena vozila omogočajo samostojen transport različnega tovora znotraj proizvodnih ali logističnih procesov. Avtomatsko vodena vozila, za katere se v uporablja kratica AGV (ang. Automated Guided Vehicles), so na tržišču prisotna že precej časa; prvo takšno vozilo je bilo namreč izdelano že leta 1950. Avtomatsko vodena vozila sledijo fiksnim in vnaprej označenim potem (slika 6.1-a), pri čemer se za označitev poti uporabljajo različni sistemi, kot so npr. sledilne žice ali magnetni trakovi. Vozilo s pomočjo nameščenih senzorjev detektira označeno pot, nato pa s pomočjo pogonskega in krmilnega sistema tej poti sledi. Dodatno pa ta vozila vsebujejo tudi senzorje za detekcijo prisotnosti ovir na označeni poti. V primeru zaznane ovire se mora vozilo ustaviti in počakati na odstranitev te ovire (slika 6.1-a). Avtomatsko vodena vozila predstavljajo dokaj preprosto in cenovno ugodno rešitev samostojnega notranjega transporta, saj bazirajo na relativno preprostih sistemih zaznavanja, procesiranja in odločanja. Imajo pa ta vozila kar nekaj pomanjkljivosti, in sicer: (1) sledijo fiksnim in vnaprej določenim potem, (2) v primeru nepričakovane ovire na poti se vozilo zaustavi, (3) za delovanje vozil je potrebna sprememba infrastrukture in kasneje tudi vzdrževanje te infrastrukture itd. Navkljub navedenim pomanjkljivostim se ta vozila dandanes v industriji precej uporabljajo in sicer za manj kompleksne prevoze tovora iz ene do druge lokacije.

Pred slabim desetletjem so se na tržišču začela pojavljati novejša vozila, za katere se uporablja termin avtonomni mobilni roboti oz. kratica AMR (ang. Autonomous Mobile Robots). Ta vozila imajo določeno stopnjo inteligence in lahko samostojno sprejemajo odločitve, ko zaidejo v nove ali nepredvidene situacije. Avtonomni mobilni roboti izvajajo lokalizacijo in navigacijo s pomočjo senzorjev in naprednih algoritmov ter naloženega zemljevida oz. karte prostora, v katerem izvajajo transportna opravila (Siegwart, Nourbakhsh, & Scaramuzza, 2011). Avtonomni mobilni roboti vsebujejo številne senzorske sisteme, med katerimi so še posebej pomembni varnostni laserski skenerji. Posledično lahko obratujejo v neposredni bližini ljudi in ostalih dinamičnih ovir, zmožni so peljati tudi skozi vrata, hodnike in uporabljati dvigala. Z vgrajenimi senzorji in dovršeno programsko in strojno opremo zaznavajo objekte v svoji neposredni okolici in z uporabo naprednih algoritmov samostojno izračunajo optimalno pot do cilja. V primeru zaznane ovire na predvideni poti, ta vozila samostojno poiščejo alternativno pot in po njej nadaljujejo

z dostavo tovora do ciljne lokacije (slika 6.1-b). V nadaljevanju bo za vozila AMR uporabljen tudi termin avtonomna vozila, za vozila AGV pa avtomatska vozila.



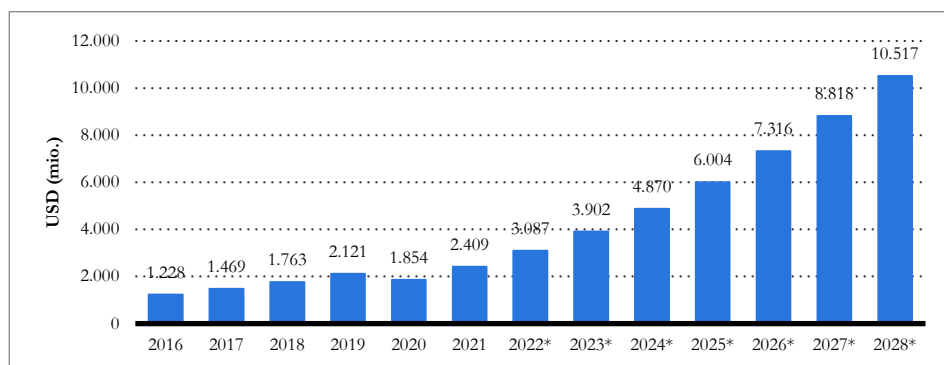
Slika 6.1: Pot avtomatsko vodenega (levo) in avtonomnega vozila (desno)

Vir: lasten.

Zaradi številnih dobrih lastnosti prodaja avtonomnih mobilnih robotov strmo narašča. Letni promet trenutno znaša dobre 3 milijarde ameriških dolarjev, v naslednjih petih letih pa bi naj narasel celo preko 10 milijard (slika 6.2).

Avtonomna vozila so prilagodljiva, saj se prilagajajo spremembam v okolju. Relativno enostavno jih je mogoče programirati in prilagoditi za izvajanje različnih opravil. Avtomatsko vodena vozila pa so zasnovana za vnaprej določene poti in opravila, zato so manj prilagodljiva spremembam v okolju. Sprememba njihovih poti ali opravil zahteva spremembo fizične infrastrukture. Vpeljava avtonomnih vozil vključuje kartiranje oz. kreiranje karte prostora, v katerem bo vozilo delovalo, konfiguracijo vozila in programiranje transportnih opravil. Vpeljava teh vozil ne zahteva namestitve fizičnih poti ali kakšnih drugih posegov v obstoječo infrastrukturo. Pri vpeljavi avtomatsko vodenih vozil pa je potrebno okolje prilagoditi in namestiti sledilne poti, kar pa je lahko precej dolgotrajno in cenovno zahtevno. Avtonomna vozila so primerna za izvajanje nalog v dinamičnih okoljih,

kot so skladišča ali proizvodni obrati, kjer se vozila gibljejo v neposredni bližini ljudi, opreme in drugih ovir. Avtomatska vozila pa se uporabljajo v transportnih procesih, kjer so poti v naprej točno določene in se praviloma s časom ne spreminjajo. Avtonomna vozila veljajo za dolgoročno stroškovno bolj učinkovita, saj zahtevajo manj investicij v infrastrukturo in se lahko prilagajajo spreminjajočim se potrebam.



Slika 6.2: Velikost svetovnega trga avtonomnih mobilnih robotov (AMR) od leta 2016 do 2021 z napovedjo do leta 2028

Vir: (Statista., 2023).

1.1 Vrste vozil

Na tržišču obstaja precej različnih vrst avtonomnih in avtomatsko vodenih vozil, med drugim (Wikipedija, 2023):

- Paletni vozički (ang. Pallet Trucks); ta vozila se primarno uporabljajo za transport palet in ne vsebujejo mehanizma za avtomatsko nalaganje/odlaganje tovora. Vozila vsebujejo le mehanizem, ki omogoča dvig in spust palet v območju nekaj centimetrov.
- Viličarji (ang. Fork Trucks); le-ti so opremljeni z vilicami in se primarno uporabljajo za samostojen transport tovora na paletah. Uporabljajo se predvsem pri transportih, kjer obstaja višinska razlika med nalaganjem in odlaganjem. Ta vrsta vozil sodi med dražja vozila.
- Vlečna vozila (ang. Towing Trucks); ta vozila so zasnovana za vleko pasivnih vozičkov ali prikolic, naloženih z različnim tovorom. Pogosto se

uporabljajo v proizvodnih procesih za oskrbo montažnih linijah s potrebnim materialom.

- Unit Load vozila so zasnovana za prevoz različnega tovora, kot so palete, zaboji ali kontejnerji. Vozila vsebujejo ploščad, ki vključuje mehanizem za dviganje/spuščanje tovora, transportne valjčke z/brez pogona, tračne transporterje itd.
- Vozila za lažji tovor (ang. Light Load) so vozila z nosilnostjo do 500 kg. Uporabljajo se za prevoz lažjih predmetov, kot so škatle, košare, ali drugi materiali.
- Specializirana vozila (ang. Specialized Trucks); ta vozila so prilagojena posebnim aplikacijam, kot so na primer izvajanje transporta v čistih sobah, nevarnih snovi v kemičnih obratih itd.

V tabeli 6.1 so zbrane povezave do YouTube videoposnetkov, ki prikazujejo različne vrste vozil. Do videoposnetkov je mogoče dostopati s klikom na YouTube ikono. V kolikor povezava ne deluje, je mogoče videoposnetek poiskati na portalu YouTube z uporabo pripadajočih ključnih besed.

Tabela 6.1: Primeri različnih vrst avtonomnih in avtomatsko vodenih vozil

Vrsta vozila	Video	Ključne besede
Paletni vozički		Nipper B.V., Nipper AGV
viličarji		Jungheinrich UK, AGV Forklift Trucks by Jungheinrich
vlečna Vozila		DF Automation, AGV towing multiple trolleys
		JD Universal, Unidirectional Towing AGV for Logistics Transportation
Unit Load		Dematic, Unit Load AGV - Warehouse Automation by Egemin Automation Inc.
		IBG Automation, AGV - Automated Guided Vehicle
Vozila za lažji tovor		SSI SCHAEFER Group, Automated Guided Vehicle Weasel®, E-Commerce, Supply Chain, Hermes Fulfilment GmbH

1.2 Uporaba avtonomnih vozil v intralogistiki

Avtonomni mobilni roboti se v intralogistiki in skladiščih uporabljajo za različne namene, kot so:

- oskrba proizvodnih delovnih mest,
- prevoz blaga v skladiščih in distribucijskih centrih,
- podpora pri procesu komisioniranja,
- itd.

V industriji se avtonomni mobilni roboti uporabljajo predvsem za oskrbo proizvodnih delovnih postaj s potrebnim materialom. To oskrbo zagotavljajo namenska avtonomna vozila, kot so na primer avtonomni viličarji, ali pa univerzalna avtonomna vozila, ki se jim z gornjim modulom (ang. top module) spremeni funkcionalnost, ter na tak način prilagodi specifičnim nalogam. Za oskrbo proizvodnih delovnih mest v praksi najpogosteje zasledimo: (a) vlečna vozila, (b) vozila s policičnim regalom, (c) s transportnim sistemom in (d) z dvizžno mizo.

V skladiščih in distribucijskih centrih se avtonomna vozila uporabljajo predvsem za podporo pri komisioniranju. Pri komisioniranju tipa »blago k človeku« se uporabljajo mobilni regali in avtonomni mobilni roboti z dviznim mehanizmom. Vozilo v skladišču dvigne celoten regal in ga prenese do delovne postaje, kjer se nahaja komisionar. Ko le-ta pobere zahtevane izdelke iz regala, AMR prenese regal nazaj v skladišče. Pri komisioniranju tipa "človek k blagu" pa avtonomna vozila nudijo podporo komisionarju. Komisionarji se premikajo po hodnikih med regali s policami in pobirajo blago v skladu z naročilom v delovnem nalogu. Komisionarji poberejo blago s polic in ga odložijo v škatle, ki se nahajajo na avtonomnem vozilu, le-to pa poskrbi za transport blaga do vhodno/izhodnega območja skladišča.

2 Avtonomni mobilni roboti

Avtonomni mobilni roboti vsebujejo številne komponente (podsisteme), ki omogočajo avtonomno zaznavanje okolja, lokalizacijo, navigacijo in izvajanje transportnih opravil. Med pomembnejšimi so.

- Senzorski sistem; le-ta vsebuje številne senzorje (inercialni, optični, 3D kamere, ultrazvočni senzorji itd.), s pomočjo katerih vozilo zaznava okolico. Dodatno imajo k osnovnim senzorjem nekatera vozila tudi druge senzorje, ki se uporabljajo za posebne naloge, kot so: čitalniki črtne kode, čitalniki

radiofrekvenčne identifikacije (ang. Radio Frequency Identification, RFID) ali okoljski senzorji.

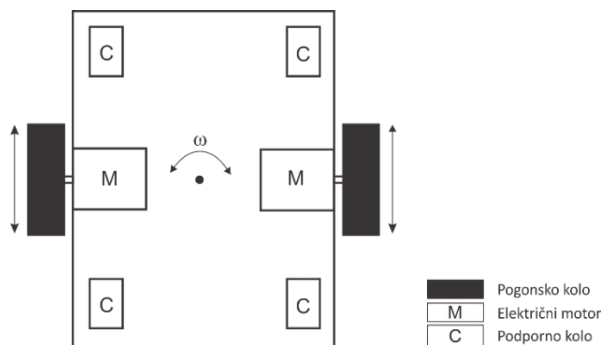
- Lokacijski sistem; avtonomni mobilni roboti morajo poznati svojo točno lokacijo v okolju, v katerem se nahajajo. To zagotavlja lokalizacijski sistem, ki na podlagi podatkov, pridobljenih iz različnih senzorjev, oceni trenutni položaj in orientacijo robota glede na njegovo interno karto.
- Navigacijski sistem; navigacijski sistem predstavlja ključno komponento za avtonomno delovanje vozil, saj je ta sistem zadolžen za načrtovanje poti. Na osnovi začetne in končne lokacije ter ob upoštevanju omejitev prostora (zidovi, prepovedana območja itd.) navigacijski sistem izračuna optimalno pot robota. V primeru zaznane ovire na izračunani poti pa poišče alternativno.
- Varnostni sistem; avtonomna vozila v nobenem primeru ne smejo ogrožati varnosti ljudi in/ali opreme. Posledično vozila vključujejo različne varnostne komponente, kot so varnostni laserski skenerji, senzorji za zaznavanje trkov, gumbi za zaustavitev v sili, ki zagotavljajo varno delovanje vozila tudi v neposredni bližini ljudi.
- Sistem za upravljanje baterij; avtonomni mobilni roboti so praviloma baterijsko napajani. Sistem za upravljanje baterij zagotavlja optimalno delovanje baterij z namenom doseganja čim daljše življenjske dobe le-teh.
- Komunikacijski sistem; le-ta omogoča komunikacijo z drugimi sistemi. Pri avtonomnih mobilnih robotih se najpogosteje uporabljajo moduli za brezžično komunikacijo (npr. Wi-Fi ali Bluetooth).
- Uporabniški vmesnik; uporabniški vmesnik, ki je praviloma dosegljiv preko posebnega zaslona na dotik ali spletnega vmesnika, omogoča spremljanje trenutnega stanja robota, ročno upravljanje robota, prikaz obvestil in opozoril, prikaz karte območja, programiranje robota itd.
- Pogonski sistem; pogonski sistem vključuje pogonske motorje, reduktorje, kolesa in krmilnike pogonskih motorjev. Z ustreznim krmiljenjem pogonskih koles vozilo sledi predhodno izračunani poti.
- Sistem strojnega učenja in umetne inteligence; nekatera napredna vozila vključujejo tudi sisteme strojnega učenja in umetne inteligence. Ti sistemi se uporabljajo za prepoznavanje predmetov, optimizacijo poti, opravil itd.

2.1 Konfiguracije pogonskega in krmilnega sistema

Avtonomna in avtomatsko vodena vozila vsebujejo pogonski in krmilni sistem. Pogonski sistem omogoča pomik vozila v vzdolžni smeri, krmilni pa zasuk vozila. Generalno gledano obstajajo štiri osnovne konfiguracije pogonskega in krmilnega sistema (Roboteq Inc., 2013):

1. Diferencialni pogon (ang. Differential drive):
 - s štirimi pogonskimi kolesi.
 - z dvema pogonskima kolesoma in enim ali več podpornih koles (ang. Castor wheel).
2. Kolesni pogon (ang. Steer drive): vsebuje kolo, ki je hkrati pogonsko in krmilno.
3. Avtomobilski (ang. Ackerman) pogon. Pri tej konfiguraciji sta zadnji kolesi pogonski, sprednji pa krmilni.
4. Mecanum (ang. Mecanum) konfiguracija je podobna tisti pri diferencialnem pogonu s štirimi pogonskimi kolesi, namesto navadnih koles pa so uporabljena t. i. mecanum oz. švedska kolesa. Z ustreznim vodenjem teh koles je mogoče doseči pomik mobilnega robota v poljubni smeri.

Pri avtonomnih in avtomatsko vodenih vozilih je najpogosteje uporabljen diferencialni pogon z dvema pogonskima kolesoma (slika 6.3), saj je ta konfiguracija precej preprosta za izvedbo in hkrati omogoča dovolj natančno krmiljenje vozila. Ta konfiguracija diferencialnega pogona vključuje tudi eno ali več podpornih koles, ki preprečujejo prevračanje vozila. Pogonski kolesi sta vpeti na isti osi, hitrost vrtenja posameznega kolesa pa je določena s hitrostjo vrtenja pripadajočega električnega motorja. Če se pogonski kolesi vrtita z enako hitrostjo, vozilo pelje naravnost, v nasprotnem primeru pa vozilo zavija v smeri kolesa, ki se vrti počasneje. Vozilo z diferencialnim pogonom se lahko tudi zavrti na mestu (okrog osi vrtenja), in sicer tedaj, ko se kolesi vrtita z enako hitrostjo, pri čemer pa se eno vrti naprej, drugo pa nazaj.



Slika 6.3: Diferencialni pogon z dvema pogonskima in štirimi podpornimi kolesi

Vir: lasten.

Tabela 6.2 vsebuje povezave do YouTube video vsebin, v katerih so prikazani principi delovanja različnih konfiguracij pogonskega in krmilnega sistema.

Tabela 6.2: Primeri konfiguracij pogonskega in krmilnega sistema

Konfiguracija	Video	Ključne besede
Diferencialni pogon		Kollmorgen – Autonomous Mobile Solutions, AGV Vehicle Types, Differential drive
Kolesni pogon		Kollmorgen – Autonomous Mobile Solutions, AGV Vehicle Types, Steer drive
		SICK AG, Monitoring automated guided vehicles (AGV) - with Safe Motion Control from SICK
Mecanum		ERobtic, ERobtic Mecanum Wheel
		Torwegge GmbH & Co. KG, TORsten Mecanum Rad Animation TORWEGGE
		KUKA - Robots & Automation, Clever Autonomy for Mobile Robots - KUKA Navigation Solution
		Neobotix GmbH , Neobotix mobile Roboterplattformen

2.2 Zunanji in notranji senzorji

Avtonomna vozila vsebujejo številne zunanje in notranje senzorje. Zunanji senzorji se uporabljajo za zaznavanje okolice, notranji pa za detekcijo notranjih procesnih veličin. Za zaznavanje okolja, lokalizacijo in navigacijo se uporabljajo kombinacije podatkov, pridobljenih iz različnih senzorjev. Najpogosteje uporabljeni senzorji so:

- Inercialne merilne enote (ang. Inertial Measurement Units, IMUs). Le-te se uporabljajo pri ohranjanju stabilnosti vozila in pri lokalizacijskih ter navigacijskih algoritmihi. IMU vključujejo tri osnovne senzorje, in sicer: (1) 3-osni merilnik pospeška (ang. Accelerometer), ki meri pospeške vozila v vseh treh smereh (x, y, z), (2) 3-osni žiroskop (ang. Gyroscope), ki meri kotno hitrost oz. hitrost vrtenja vozila okoli posamezne osi, (3) 3-osni magnetometer (ang. Magnetometer), ki meri jakost in smer magnetnega polja v vseh treh oseh. V kombinaciji z drugimi senzorji podatki inercialne merilne enote izboljšajo natančnost ocene lokacije robota.
- LiDAR senzorji (ang. Light Detection And Ranging). Ti senzorji so ključna senzorska komponenta, ki se v avtonomnih mobilnih robotih uporablja za navigacijo, zaznavanje ovir, kartiranje in lokalizacijo. LiDAR senzorji z uporabo laserskih žarkov merijo razdalje do predmetov v okolici robota, kar omogoča natančno kartiranje prostora in navigacijo.
- Senzorji pogonskih koles; le-ti so nameščeni na pogonskih motorjih in tako zajemajo hitrost ter položaj pogonskih koles. Ti senzorji omogočajo grobo določitev smeri in hitrosti gibanja vozila. Zaradi različnih pogreškov (naključnega drsenja pogonskih koles, geometričnih napak, ločljivosti inkrementalnih dajalnikov ...) takšen sistem določanja hitrosti vozila ni absolutno točen, zato so potrebni dodatni senzorji (merilniki pospeška, žiroskopi itd.), ki oceno o hitrosti gibanja dopolnjujejo z natančnejšimi meritvami. Senzorji pogonskih koles zagotavljajo informacije, ki pomagajo pri lokalizaciji vozila, predvsem pri algoritmihi, ki temeljijo na odometriji (ang. Odometry).
- Ultrazvočni senzorji (ang. Ultrasonic Sensors) oddajajo zvočne valove in merijo čas, v katerem se oddani valovi odbijejo od zaznanih objektov. Uporabljajo se predvsem za detekcijo transparentnih objektov, kot so npr.

steklena vrata, ki jih optični senzorji (LiDAR, kamere) težje ali pa sploh ne zaznajo.

- Sistemi kamer se uporabljajo za vizualno zaznavanje objektov, predvsem tistih, ki jih z drugimi senzorji ni mogoče zaznati. LiDAR senzorji zaznavajo objekte v ravnini, ki je za določeno razdaljo odmaknjena od tal (višina je odvisna od namestitve senzorja na mobilno platformo). Objektov, ki se nahajajo višje ali nižje od te ravnine, LiDAR senzorji ne zaznajo. Za zaznavo takšnih objektov se uporabljajo 3D kamere, ki so praviloma nameščene na sprednji strani vozila.
- Radarski senzorji (ang. Radar Sensors) oddajajo radijske valove in merijo čas preleta od oddaje do sprejema. Radarji uporabljajo radiofrekvenčne (RF) signale, običajno v mikrovalovnem pasu in omogočajo zaznavo predmetov na razmeroma velikih razdaljah. V primerjavi z optičnimi senzorji, kot so LiDAR ali kamere, na radar manj vplivajo neugodne vremenske razmere, kot so dež, megla ali sneg, zato so primerni za avtonomna vozila, ki delujejo na prostem. Imajo pa radarji na splošno manjšo ločljivost v primerjavi z LiDAR senzorji, zato so manj primerni za kartiranje prostora ali zaznavanje manjših predmetov.
- Senzorji dotika (ang. Touch sensors); ti senzorji se uporabljajo za zaznavo trkov s predmeti. V splošnem se za detekcijo ovir uporabljajo brezkontaktni in kontaktni sistemi. Slednji se uporabljajo pri avtomatsko vodenih vozilih, pri avtonomnih pa se praviloma uporabljajo brezkontaktni sistemi. Kot kontaktni sistem se uporabljajo varnostni odbijači, znotraj katerih so nameščeni senzorji dotika. Ti senzorji se aktivirajo, ko pride do neposrednega stika vozila z oviro.
- Globalni sistem za določanje položaja (ang. Global Positioning System, GPS). V nekaterih avtonomnih mobilnih robotih se uporablja tehnologija globalnega sistema za določanje položaja, ki zagotavlja podatke o globalnem položaju vozila, kjer koli na zemeljski obli. To je še posebej uporabno pri vozilih, ki se uporabljajo na prostem, kot je npr. kmetijstvo ali dostava v zadnji milj. Signali GPS ne morejo prodreti v notranjost zgradb, zato se v vozilih, ki delujejo v zaprtih prostorih, ne uporabljajo.
- Ostali senzorji; odvisno od namena uporabe lahko avtonomna vozila vsebuje tudi ostale senzorje, kot so npr. senzorje za merjenje zunanjih

veličin (temperatura, vlažnost, koncentracija plinov), senzorje za detekcijo črtnih kod, RFID oznak itd.

2.2.1 Varnostni laserski skenerji

Varnostni laserski skenerji (slika 6.4) omogočajo brezkontaktno detekcijo objektov o okolici mobilnega robota. Ti senzorji imajo t. i. varno območje (ang. Safety zone) in dve ali več opozorilnih območij (ang. Warning zones), ki so nastavljiva in namenjena različnim podpornim funkcijam, kot je npr. opozorilni zvok. Če vozilo zazna oviro znotraj opozorilnega območja (rumeno in oranžno območje) v smeri gibanja, mora začeti z normalnim zaviranjem. Če se zaznan objekt nahaja znotraj varnega območja (rdeče območje), pa se mora vozilo zasilno zaustavi z uporabo vgrajene zavore (Wikipedija, 2023). Sodobni varnostni laserski skenerji omogočajo konfiguracijo več območij, in sicer s pomočjo pripadajoče programske opreme. AMR-ji praviloma vsebujejo dva ali več varnostnih laserskih skenerjev. Najpogosteje se uporabljata dva, ki sta nameščena na diagonalnih robovih vozila. Takšna namestitvev omogoča 360° zaznavanje okolice vozila, kar pomeni, da lahko AMR zaznava tudi objekte, ki se nahajajo ob boku vozila. To je še posebej pomembno v primeru zasuka robota na mestu.



Slika 6.4: Primer varnostnega laserskega skenerja

Vir: (SICK AG, 2018)

Varnostni laserski skenerji se uporabljajo za brezkontaktno detekcijo objektov na številnih področjih (tabela 6.3), zelo pogosto jih zasledimo na področju varovanja delovnih območij industrijskih robotov.

Tabela 6.3: Primeri delovanja in uporabe varnostnih laserskih skenerjev

Področje uporabe	Video	Ključne besede
Mobilni roboti		SICK AG , Monitoring automated guided vehicles (AGV) - with Safe Motion Control from SICK
Robotske celice		SICK Sensor Intelligence, Safe Robotics: Safe sequence monitoring
		SICK AG, Safe Robotics: Palletizing application

2.3 Lokacijski in navigacijski sistemi

Avtonomna in avtomatsko vodena vozila vsebujejo lokacijski in navigacijski sistem, Pri avtomatsko vodenih vozilih je le-ta precej preprosto, saj vozila le sledijo vnaprej določenim putem. Avtonomna vozila pa vsebujejo širok nabor senzorjev in napredne navigacijske algoritme, kar jim omogoča prilagajanje transportnim putem v spreminjajočem okolju.

2.3.1 Avtomatsko vodena vozila

Pri avtomatsko vodenih vozilih se za označitev poti najpogosteje uporabljajo sledilne žice in sledilni trakovi (tabela 6.4). Sledilna žica je najstarejši sistem za usmerjanje vozil in se še danes uporablja, predvsem zaradi svoje visoke natančnosti in zanesljivosti. Vendar pa ima ta sistem eno pomembno omejitev; žico je namreč potrebno namestiti v posebno režo pod površino tal, približno 1 cm globoko. To pomeni, da je potrebno izvesti fizične posege v infrastrukturo na območju, kjer bo vozilo izvajalo transportne naloge. Podoben poseg v infrastrukturo pa je potrebno izvesti tudi ob vsaki spremembi poti. Za razliko od sledilnih žic se sledilni trakovi nameščajo na površino tal. Njihova ključna prednost je predvsem v tem, da jih je mogoče enostavno odstraniti ali premestiti. Sledilni trakovi so lahko barvni ali magnetni. Najpogosteje se uporabljajo magnetni sledilni trakovi, saj so precej manj občutljivi na poškodbe in umazanijo.

Za detekcijo poti pa se uporabljajo tudi t. i. inercialni navigacijski sistemi (tabela 6.4), pri katerih ni potrebno označiti celotne poti vozila, temveč le določene točke. Inercialni sistemi temeljijo na merjenju pospeškov v vseh treh smereh (x , y , z) in kotov zasuka okrog vzdolžne, prečne in navpične osi vozila (Wikipedija. Prosta enciklopedija). Na podlagi izmerjenih pospeškov in kotov zasuka se s pomočjo

integracijskih metod oceni trenuten položaj vozila v prostoru. Zaradi različnih pogrškov (pogreški senzorjev, pogršek integracijske metode itd.) prihaja do razlik med dejanskim in ocenjenim položajem vozila, zato se pri tej navigaciji praviloma uporabljajo dodatne talne oznake. Ko vozilo prečka takšno oznako, s senzorjem zazna njen točen položaj in popravi ocenjen položaj vozila. Praviloma se kot oznake uporabljajo majhni trajni magneti, obstajajo tudi rešitve, kjer se uporabljajo RFID ali QR oznake.

2.3.2 Avtonomna vozila

Pri avtonomnih vozilih se za lokalizacijo in navigacijo pogosto uporabljata dve metodi, in sicer 2D lasersko skeniranje in SLAM (ang. Simultaneous Localization and Mapping).

2D lasersko skeniranje deluje na principu merjenja odboja laserskega žarka od fiksno nameščenih odsevnikov v prostoru. Na podlagi odboja laserskih žarkov iz različnih odsevnikov se s pomočjo triangulacije določi trenuten položaj vozila. Laserska tehnologija zagotavlja visoko odpornost na lažne refleksije in visoko natančnost določitve položaja. Običajno se ta tehnologija uporablja na nekoliko višjih platformah, na primer v viličarjih, saj je v teh primerih laser nameščen dokaj visoko in posledično ob prisotnosti ljudi ne prihaja do prekinitev laserskih žarkov.

Pri uporabi SLAM algoritmov si vozilo izgradi konsistentno karto območja, v katerem se nahaja, hkrati pa tudi določi trenutno lokacijo na tej karti. SLAM pogosto vključuje združevanje senzorjev, pri katerem se združujejo podatki iz več senzorjev, da se izboljša natančnost kartiranja in lokalizacije. SLAM algoritme klasificiramo na osnovi senzorjev, ki jih le-ti primarno uporabljajo. LiDAR SLAM prioriteto uporablja LiDAR za zaznavo okolice, medtem ko npr. Visual SLAM uporablja sistem strojnega vida oz. kamere kot primarnega senzorja. SLAM je primeren za neznana ali dinamična okolja, kjer se lahko postavitev obratov s časom spreminja. Algoritmi SLAM so računsko zelo potratni in posledično zahtevajo veliko procesorske moči in pomnilnika. SLAM je odvisen od kakovosti in natančnosti senzorjev, zato je kalibracija senzorjev ključnega pomena.

Tabela 6.4: Primeri delovanja različnih lokacijsko-navigacijskih sistemov

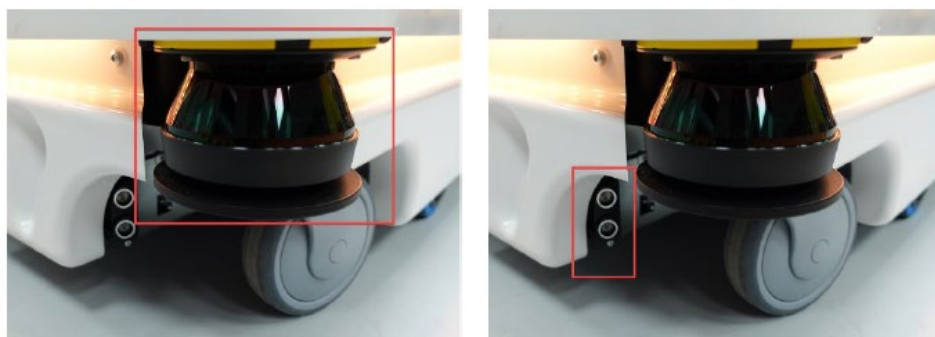
Lokacijski in navigacijski sistem	Video	Ključne besede
Sledilna žica		Jungheinrich AG, Jungheinrich Inductive Guidance for Forklift Trucks
		Götting KG, Götting FTF Spurführungstechnologien / AGV Track Guidance Technologies
Sledilni trakovi		Götting KG, Götting FTF Spurführungstechnologien / AGV Track Guidance Technologies
		Roboteq, Magnetic track following Mobile Robot demonstrator
Inercialni sistem		DS AUTOMOTION, Magnetic Navigation by DS AUTOMOTION GmbH - Automated Guided Vehicle (AGV)
2D laser		Götting KG, Götting FTF Spurführungstechnologien / AGV Track Guidance Technologies
		DS AUTOMOTION, Laser navigation by DS AUTOMOTION GmbH - Automated Guided Vehicle (AGV)
SLAM		cygbot lab, 2D / 3D Dual SLAM Robot using ROS and LiDAR with Raspberry Pi

3 Avtonomno vozilo MiR100

MiR100 (Mobile Industrial Robots., 2023a) je avtonomno vozilo z nosilnostjo do 100 kg proizvajalca Mobile Industrial Robots. Uporabljati ga je mogoče izključno v zaprtih proizvodnih prostorih, v skladiščih ali znotraj drugih industrijskih objektov. MiR100 (slika 6.5) ima vgrajena dva varnostna laserska skenerja (slika 6.6), ki sta nameščena na diagonalnih robovih robota in tako omogočata skeniranje celotnega območja v njegovi okolici. Vozilo vsebuje tudi ultrazvočne senzorje (slika 6.6) in 3D kamero. Posledično lahko vozilo MiR100 obratuje v neposredni bližini ljudi in ostalih dinamičnih ovir, zmožno je peljati skozi ožje hodnike ali vrata. MiR100 deluje na diferencialni pogon in sicer ima dve pogonski kolesi in štiri podporna kolesa (ang. Castor wheel). Vozilo je možno ročno upravljati preko vgrajenega spletnega vmesnika, primarno pa je vsekakor namenjen samostojnemu izvajanju različnih transportnih nalog. Robot izvaja lokalizacijo in navigacijo preko zemljevida, ki se lahko uvozi ali ustvari ob prvem zagonu.

**Slika 6.5: MiR100**

Vir: lasten.

**Slika 6.6: Varnostni laserski skener (levo) in ultrazvočni senzor (desno)**

Vir: lasten.

MiR100 predstavlja osnovno mobilno platformo, na katero je mogoče namestiti različne zgornje module (ang. Top Modules) in s tem spremeniti funkcionalnost vozila (slika 6.7). Dodatek MiR Hook 100, na primer, spremeni vozilo MiR100 v vlečno vozilo in tako omogoča vleko tovora, ki se nahaja na pripetih vozičkih. Primeri nekaterih dodanih zgornjih modulov za vozilo MiR100 so navedeni v spodnji tabeli 6.5.



Slika 6.7: Primer zgornjega zaklepnega modula.

Vir: lasten.

Tabela 6.5: Primeri gornjih modulov za vozilo MiR100

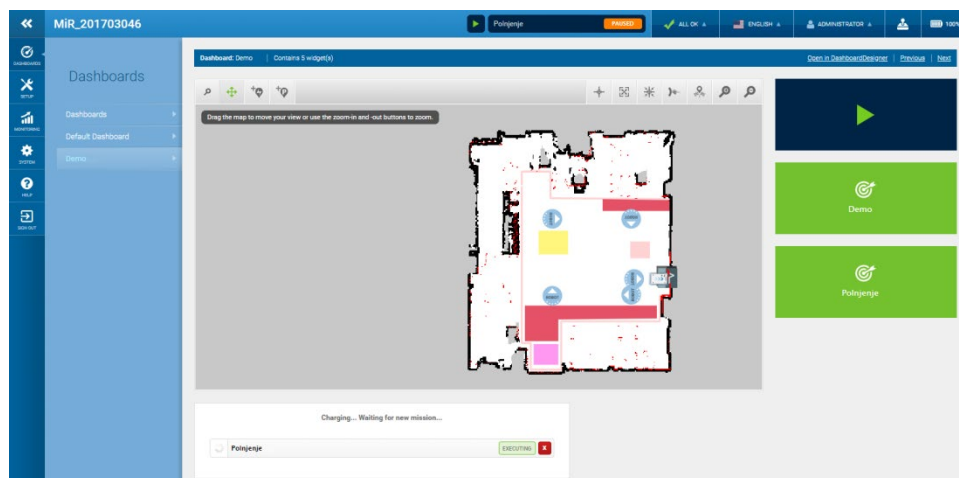
Gornji modul	Video	Ključne besede
Valjčni, tračni	 	Omni Automation, MiR 100 Robot - Top Module Roller Conveyor Mobile Industrial Robots, Mir100 hos SAXE på Elmia Automation 2016
Zaklepni		Robotcenter, Clamp top module for MiR100/MiR200
Vlečni		Mobile Industrial Robots, MiR 100 Hooking a Trailer Automatically
S sodelujočo robotsko roko		Mobile Industrial Robots, MiR100 with UR cobot arm at SGIMRI

3.1 Uporabniški vmesnik

Roboti MiR imajo vgrajeno Wi-Fi dostopno točko, preko katere je mogoče dostopati do uporabniškega vmesnika robota. Uporabniški vmesnik, ki je zasnovan v obliki spletne strani, omogoča: (1) kreiranje nadzornih plošč, (2) kartiranje prostora, (3) kreiranje misij, (4) spremljanje trenutnega stanja robota, (5) upravljanje uporabnikov, (6) ročno vodenje robota, (7) posodobitve programske opreme itd.

Nadzorne plošče omogočajo neposreden dostop do posameznih ključnih funkcij robota in so predvsem namenjene različnim skupinam uporabnikov. Posamezna nadzorna plošča je sestavljena iz vizualnih gradnikov (ang. Widget), ki predstavljajo

značilnosti sistema, kot je npr. določena misija, zemljevid, trenutna čakalna vrsta misij itd. Nadzorne plošče je mogoče kreirati in urejati z vgrajenim urejevalnikom nadzornih plošč (ang. Dashboard designer). Primer nadzorne plošče je prikazan na spodnji sliki (slika 6.8).



Slika 6.8: Primer izdelane nadzorne plošče

Vir: lasten.

Vozilo je mogoče ročno upravljati s pomočjo virtualne igralne palice (ang. Joystick), ki je sestavni del uporabniškega vmesnika. Preko uporabniškega vmesnika je mogoče kreirati več uporabniških računov z različnimi dovoljenji, kar omogoča nadzorovan dostop do posameznih funkcij robota. Preko uporabniškega vmesnika je mogoče spremljati tudi trenutno stanje robota (njegova lokacijo na zemljevidu, stanje baterije, sporočila o napakah in opozorilih itd).

3.2 Kartiranje in urejanje kart

Kartiranje oz. izdelovanje zemljevidov območja je najpomembnejši postopek, ki vozilu omogoča samostojno delovanje v izbranem prostoru. Izdelava karte poteka v dveh korakih. V prvem koraku se na robota naloži CAD datoteko obstoječe karte prostora, ali pa se karto kreira z ročnim vodenjem robota. V drugem koraku pa se karto uredi z uporabo vgrajenega urejevalnika. Vgrajena funkcionalnost kartiranja omogoča kreiranje zemljevida z ročnim premikanjem robota po prostoru z uporabo

vgrajene virtualne igralne palice. Med premikanjem se zajemajo podatki iz varnostnih laserskih skenerjev in na podlagi le-teh robot izdelava karto prostora. Po zajemu karte sledi urejanje. Dodatno k nepremičnim objektom (npr. stene) so v procesu kreiranja namreč zajeti tudi t. i. dinamični objekti (ljudje, viličarji, vozički, stoli, palete itd.), ki se v trenutku zajemanja nahajajo v okolici vozila. Te objekte je potrebno odstraniti, saj lahko v nasprotnem primeru podaljšajo dolžino poti vozila. Pri skeniranju lahko pride tudi do napak pri zaznavanju nepremičnih objektov (npr. sten) in posledično se objekti na karti prikažejo kot prekinjene črte. V tem primeru je takšne objekte treba z uporabo vgrajenih orodij na karti popraviti ali dodatno narisati.

Na urejeni karti je z uporabo dodatnih orodij možno določiti: (1) priporočljiva območja vozila (ang. Preferred zones), (2) nepriporočljiva območja (ang. Unpreferred zones), (3) nedovoljena oz. prepovedana območja vozila (ang. Forbidden zones), (4) kritična območja (ang. Critical zones), (5) hitrostna območja (ang. Speed zones), (6) območja signalizacije (ang. Blink zones, Beep zones) itd.

Posamezna območja imajo naslednji pomen:

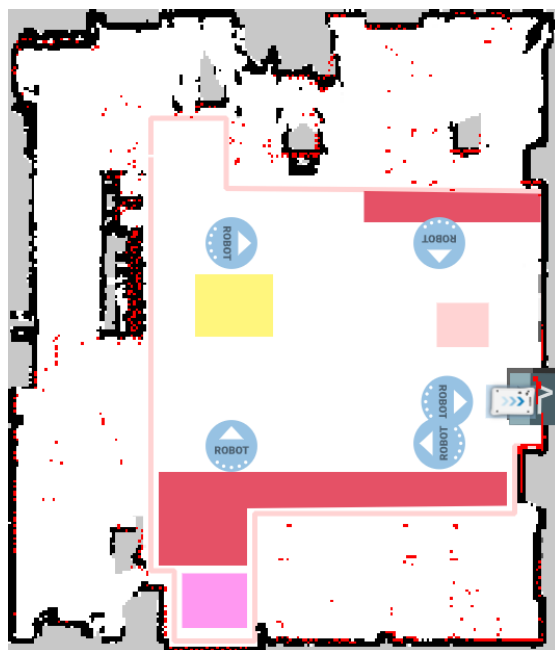
- Priporočljivo območje (ang. Preferred zones): robot vedno poskuša peljati po tem območju.
- Nepriporočljivo območje (ang. Unpreferred zones): robot se poskuša izogniti temu območju, vendar, če ni druge možnosti, lahko pelje tudi po tem območju.
- Prepovedano območje (ang. Forbidden zones): v to območje robot ne sme nikoli vstopiti.
- Kritična območja (ang. Critical zones): ovire, ki so zaznane s pomočjo nameščenih kamer ali skenerjev, so v tem območju prezrte. To robotu omogoča, da se lahko približa oviram brez sprožitve varnostnega sistema zaustavitve. Ko robot zapusti to območje, se zaščitne funkcije ponovno aktivirajo. To območje je uporabno npr. pri ozkih prehodih, vratih itd.
- Usmerjevalna območja (ang. Directional zones): določajo smer gibanja robota. Robot se v tem območju lahko premika le v izbrani smeri.
- Hitrostna območja (ang. Speed zones): v teh območjih je možno povečati ali zmanjšati hitrost vozila. Zmanjšanje hitrosti se npr. uporabi, če se vozilo

nahaja v območju z veliko ljudmi. Privzeta hitrost robota je 1 m/s, minimalna 0,1 m/s in maksimalna 1,5 m/s.

- Območja signalizacije (ang. Blink zones, Beep zones): med vožnjo v tem območju lahko robot predvaja izbran zvok in/ali ustrezno signalizira z vgrajenim LED svetlobnim trakom. Signalizacija se primarno uporablja za opozarjanje ljudi na prisotnost robota.
- Območje I/O modula: ob vstopu v to območje robot aktivira vhodno/izhodni (ang. Input / Output) modul.

Na spodnji sliki (slika 6.9) je prikazan primer urejene karte z dodanimi posebnimi območji.

Pred kreiranjem transportnih opravil (misij) je na kreirani karti potrebno določiti še pozicijske točke (markerje); to so točke v prostoru, do katerih se robot lahko zapelje. Posamezna točka vsebuje ime, X in Y koordinato točke v metrih ter orientacijo vozila v stopinjah.



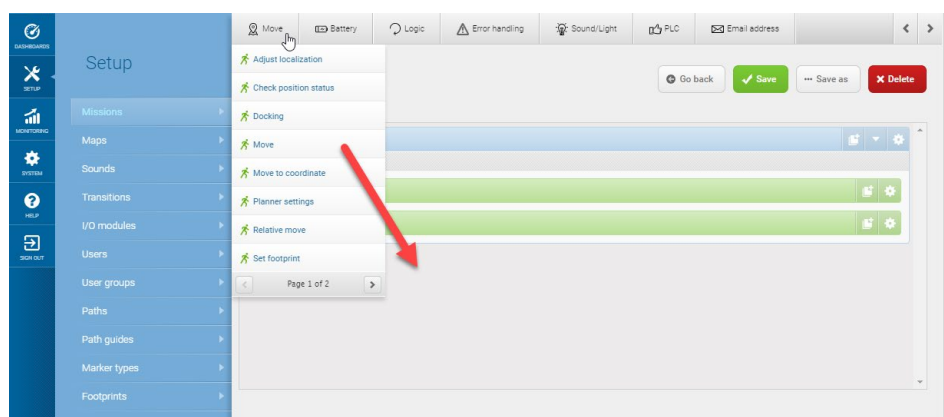
Slika 6.9: Primer urejene karte z dodanimi posebnimi območji

Vir: lasten.

3.3 Kreiranje misij

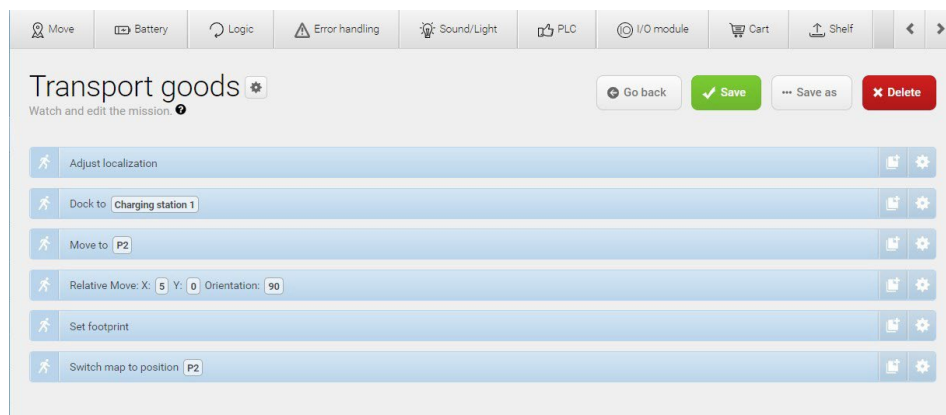
Po kreiranju karte sledi programiranje vozila oz. kreiranje t. i. misij (ang. Missions). Misija je sestavljena iz različnih dejanj, kot so: premik vozila, vklop/izklop digitalnega signala, priklop/odklop vozička itd. Posamezna dejanja predstavljajo osnovne gradnike za oblikovanje misij, le-te pa je možno uporabiti tudi znotraj drugih misij. Večina dejanj ima nastavljive parametre.

Misija je sestavljena iz posameznih dejanj oz. ukazov, ki jih je možno izbrati v menijih urejevalnika misij (ang. Mission Editor), slika 6.10. Ukazi so združeni v podmenije *Move*, *Battery*, *Logic* itd. Ukaz se v misijo doda tako, da se povleče v spodnji del urejevalnika, slika 6.10. Ukazi se izvajajo v zaporedju, in sicer od zgoraj navzdol. Parametre izbranega ukaza je možno spremeniti z izbiro ikone (zobnik), ki se nahaja na skrajno desni strani posameznega ukaza (slika 6.11).



Slika 6.10: Urejevalnik misij (Mission Editor)

Vir: lasten.

**Slika 6.11: Primer kreiranja misije**

Vir: lasten.

4 Zaključek

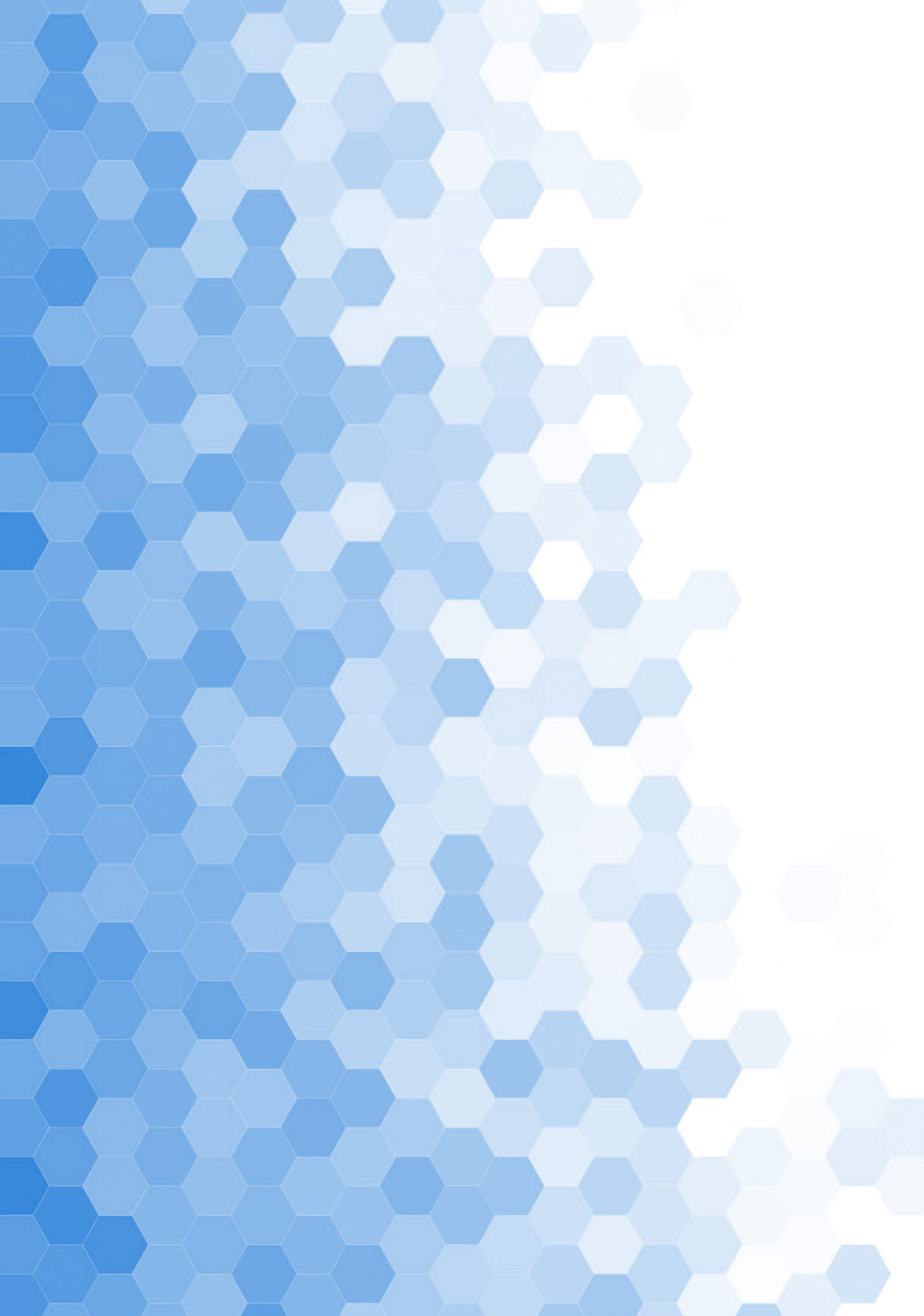
Poglavje podaja bralcu osnovne informacije o delovanju avtomatsko vodenih in avtonomnih vozil ter opisuje praktične primere aplikacij. V kratkem pregledu področja avtomatsko vodenih in avtonomna vozila je moč opaziti, da eni in drugi uporabljajo različne senzorske sisteme za zaznavanje okolice in ovir. Z uporabo različnih pogonov dosegamo različne načine premikanja ter posledično kinematične in dinamične lastnosti vozil. Glavna razlika med avtomatskimi in avtonomnimi vozili je prisotna predvsem v sistemih odločanja, ki pa so neposredno povezani s sistemi zaznavanja. Na praktičnem primeru avtonomnega mobilnega robota MiR 100 je prikazano delovanje uporabniškega vmesnika ter osnovnih funkcij za delovanje v intralogističnih aplikacijah. Ugotovimo lahko, da je MiR 100 osnovna avtonomna platforma, ki pa za naprednejše aplikacije potrebuje dodatne module. Predvidevamo, da se bo uporaba avtonomnih mobilnih robotov v prihodnosti zvišala predvsem na račun nadgradnje obstoječih avtomatsko vodenih vozil ter avtomatizacije ročnih procesov.

Literatura

- Mobile Industrial Robots. (2023a). MiR100 User guide. Retrieved from <https://www.mobile-industrial-robots.com/>
- Mobile Industrial Robots. (2023b). Mobile Industrial Robots Web Site. Retrieved from <https://www.mobile-industrial-robots.com/>

- Roboteq Inc. (2013). Building a Magnetic Track Guided AGV, Application Note AN1326. Retrieved from <https://www.roboteq.com/index.php/applications/100-how-to/278-building-a-magnetic-track-guided-agv>
- SICK AG. (2018). SICK Web Site. Retrieved from <https://www.sick.com>
- Siegwart, R., Nourbakhsh, I. R., & Scaramuzza, D. (2011). *Introduction to autonomous mobile robots*: MIT press.
- Statista. (2023). Global autonomous mobile robot market size 2016-2028. Retrieved from <https://www.statista.com/statistics/1285835/worldwide-autonomous-robots-market-size>
- Wikipedija. (2023). Automated Guided Vehicle. Retrieved from https://en.wikipedia.org/wiki/Automated_guided_vehicle
- Wikipedija. Prosta enciklopedija. Inercialna navigacija. Retrieved from https://sl.wikipedia.org/wiki/Inercialna_navigacija





DIGITALNA TRANSFORMACIJA V LOGISTIKI IN MANAGEMENTU OSKRBOVALNIH VERIG

MATEVŽ OBRECHT (UR.)

Univerza v Mariboru, Fakulteta za logistiko, Celje, Slovenija
matevz.obrecht@um.si

Visokošolski učbenik "Digitalna transformacija v logistiki in managementu oskrbovalnih verig" je celovit vodnik, namenjen podpiranju digitalizacije in digitalnih pristopov v logistiki. Poudarek je na digitalizaciji procesov, uporabi orodij za digitalno obdelavo podatkov in simulacije ter na avtonomnih vozilih ter strojnem učenju v logističnih procesih in kibernetiki varnosti. Interdisciplinarni pristop združuje znanja iz več področij - računalništva, informatike, mehatronike, strojnega učenja in simulacijskih postopkov ter poslovnega odločanja, kar omogoča celovito razumevanje izzivov digitalne logistike in aplikacijo uporabnih znanj tudi na področja izven logistike in oskrbovalnih verig. Bralci so opremljeni s praktičnimi znanji in veščinami za izboljšanje učinkovitosti, preglednosti posameznih procesov. Učbenik pokriva teme, kot so: 1) Digitalizacija procesov - načrtovanje; 2) Digitalizacija procesov - izvedba; 3) Poslovno-informacijski sistemi; 4) Simulacije in digitalni dvojčki; 5) Avtonomna vozila v logistiki in 6) Informacijska varnost. Celotna vsebina je usmerjena v krepitev digitalnih kompetenc, ki so ključne za uspešno upravljanje sodobnih logističnih podjetij in odpornih oskrbovalnih verig.

DOI
[https://doi.org/
10.18690/um.fl.2.2025](https://doi.org/10.18690/um.fl.2.2025)

ISBN
978-961-286-971-7

Ključne besede:
avtonomna vozila,
digitalizacija procesov,
interdisciplinarna znanja,
digitalna logistika,
zeleni in digitalni prehod,
informacijska varnost

DOI
[https://doi.org/
10.18690/um.fl.2.2025](https://doi.org/10.18690/um.fl.2.2025)

ISBN
978-961-286-971-7

Keywords:

autonomous vehicle,
digitalization,
interdisciplinary knowledge,
digital logistics,
green and digital transition,
cyber security

DIGITAL TRANSFORMATION IN LOGISTICS AND SUPPLY CHAIN MANAGEMENT

MATEVŽ OBRECHT (ED.)

University of Maribor, Faculty of Logistics, Celje, Slovenia
matevz.obrecht@um.si

The higher education textbook *"Digital Transformation in Logistics and Supply Chain Management"* is a comprehensive guide aimed at supporting digitization and digital approaches in logistics. It focuses on process digitalization, the use of tools for digital data processing and simulations, autonomous vehicles, machine learning in logistics processes, and cybersecurity. This interdisciplinary approach combines knowledge from various fields—computer science, information technology, mechatronics, machine learning, simulation methods, and business decision-making, providing a thorough understanding of digital logistics challenges and the application of practical knowledge to areas beyond logistics and supply chains. Readers are equipped with practical knowledge and skills to improve the efficiency and transparency of individual processes. The textbook covers topics such as: 1) Process Digitization - Planning; 2) Process Digitization - Execution; 3) Business Information Systems; 4) Simulations and Digital Twins; 5) Autonomous Vehicles in Logistics; and 6) Information Security. The entire content is focused on strengthening digital competencies essential for effectively managing modern logistics companies and building resilient supply chains.





Univerza v Mariboru

Fakulteta za logistiko



Digitalizacija – načrtovanje

Borut Jereb

Digitalizacija – izvajanje

Borut Jereb

Informacijska in računalniška varnost

Nena Orel Šanko

Poslovni informacijski sistemi

Bojan Rupnik

Podpora odločanja s simulacijami

Bojan Rupnik

Avtonomna vozila v intralogistiki

Darko Hercog, Primož Bencak



NAČRT ZA
OKREVANJE
IN ODORNOST



Univerza v Mariboru



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA VISOKO ŠOLSTVO,
ZNANOST IN INOVACIJE



Financira
Evropska unija
NextGenerationEU