RISK MANAGEMENT SOFTVER BAZIRAN NA AI I CPS PREDIKCIJI

DOI: *10.70329/2744-2403.2025.5.9.1*

Naučni rad

Edin Garaplija [1]
Muhamed Durakovic [2]

Sažetak:
Ovaj rad se fokusira na upotrebu mašinskog učenja i korištenje namjenskih baza podataka vještačke inteligencije u svrhu kreiranja rješenja zasnovanih na unaprijeđenom algoritmu za preventivno upravljanje rizicima i predikciju rizika u realnom vremenu. U radu se analiziraju postojeći standardi, njihovi nedostaci i moguća rješenja za unapređenje, kao i struktura i algoritamska osnova ovih sistema, te njihova integracija u postojeće sigurnosne arhitekture i platforme. Obuhvaćena je detekcija prijetnji na osnovu anomalija i analiza ustaljenog korisničkog ponašanja prema zadanim obrascima, procjena rizika i proaktivna detekcija napada. Pravovremena identifikacija i upravljanje rizicima postaju ključni faktori održivosti kompanija i sigurnosti poslovnih i informacionih sistema. Prediktivna analitika, zasnovana na vještačkoj inteligenciji, mašinskom učenju i analizi velikih skupova podataka, donosi transformacijske mogućnosti u oblastima poput industrije, finansija i zdravstva, koje su u savremenoj eri povezane sajber sigurnošću i predikcijom rizika, a koje pomažu donosiocima odluka da efikasnije upravljaju sistemima i zaštite ih. Integrativni pristup usklađivanju ovih tehnologija, posebno u kontekstu organizacione strukture i pravnog okvira, obuhvata pitanja pouzdanosti i transparentnosti modela, odgovornosti za automatizovane odluke, zaštite privatnosti i usklađenosti sa zakonodavstvom. Cilj rada je pružiti sveobuhvatan pregled tehnoloških i metodoloških inovacija u prediktivnoj zaštiti od sajber rizika, te identifikovati pravce budućeg razvoja sa posebnim fokusom na sigurnost, etiku i pouzdanost AI sistema.

Ključne riječi: *Rizik, AI Predikcija, Cyber sigurnost*

---

[1] Edin Garaplija, PhD in security Science, President of INZA Institute of the Risk Management
[2] Muhamed Durakovic, IT Eng., IT Development engineer of the INZA Group

1. Uvod

Upravljanje rizicima u sistemima kritične infrastrukture postaje sve zahtjevniji zadatak, posebno u kontekstu ubrzanog tehnološkog razvoja, povećane međusobne povezanosti samih sistema i sve sofisticiranijih sajber prijetnji. Dosadašnji pristupi, koji se najčešće oslanjaju na mjere koje zanemaruju prevenciju u najranijoj fazi, više nisu dovoljni da odgovore na savremene sigurnosne izazove u korporativnom okruženju. U tom kontekstu, vještačka inteligencija (AI) i mašinsko učenje nude nove perspektive i mogućnosti za unapređenje postojećih sigurnosnih sistema, prvenstveno kroz uvođenje prediktivnih modela koji omogućavaju pravovremeno prepoznavanje prijetnji prije nego što izazovu štetu.Poseban fokus biće stavljen na način integracije algoritama u postojeće procese, s ciljem unapređenja standardnih pristupa i omogućavanja blagovremenih reakcija u složenim okruženjima. Osim tehničkih aspekata, rad će se baviti i širim pitanjima koja prate primjenu ovih tehnologija, od etičkih i pravnih izazova, do pitanja transparentnosti, zaštite podataka i usklađenosti sa zakonima i internim regulativama. Ova dimenzija je ključna kako bi se osigurala odgovorna i dugoročno održiva upotreba AI sistema u poslovnoj praksi.Današnji procesi digitalne transformacije značajno doprinose većoj povezanosti i operativnoj efikasnosti, ali istovremeno otvaraju prostor za nove ranjivosti. Napadi na informacione sisteme sve više se oslanjaju na kombinaciju tehničkih propusta i ljudskih faktora. Stoga savremeni pristupi sigurnosti moraju prevazići tradicionalnu zaštitu mrežnih granica i obuhvatiti širu analizu rizika u svakodnevnom poslovanju. Potrebna je proširena vizija sigurnosti, koja povezuje tehničke, organizacione i ljudske faktore u jedinstven sistem za rano upozoravanje i preventivno djelovanje.Platforma INZA Risk Management za upravljanje rizicima razvijena je upravo s tom vizijom, kao odgovor na globalne izazove te nudi skalabilno i inteligentno rješenje koje se može prilagoditi specifičnim potrebama različitih organizacija u procesu upravljanja kritičnom infrastrukturom.

2. Teorijski okvir

U današnjem poslovnom okruženju, gdje digitalne tehnologije čine temelj gotovo svakog sektora, upravljanje rizicima sve više postaje sastavni dio šire strategije opstanka i rasta. Umjesto da se reaguje tek nakon što dođe do incidenta, sve veći naglasak stavlja se na pravovremeno prepoznavanje prijetnji i adekvatan odgovor na njih. Smatra se da spektakularan napredak u razvoju sajber-fizičkih sistema (CPS) i tehnologije interneta stvari (IoT) predstavlja osnovu za Industriju 4.0 (Whalster, W., 2013). Teorija CPS-a proistekla je iz teorije upravljanja i inženjerstva upravljačkih sistema, a fokusira se na međusobno povezivanje

fizičkih komponenti i upotrebu kompleksnih softverskih entiteta kako bi se uspostavile nove mrežne i sistemske mogućnosti. CPS-ovi povezuju fizičke i inženjerske sisteme te spajaju sajber svijet s fizičkim. Suprotno tome, teorija IoT-a proizašla je iz računarskih nauka i internetskih tehnologija, te je prvenstveno usmjerena na međusobnu povezanost, interoperabilnost i integraciju fizičkih komponenti putem interneta. Očekuje se da će s potpunom tržišnom integracijom IoT-a u narednoj deceniji doći do razvoja poput automatizacije CPS-ova putem IoT-a (Dworschak, B., Zaiser, H., 2014).

Ovo je posebno značajno u kontekstu sajber sigurnosti, gdje jedan jedini propust može izazvati ozbiljnu tehničku, ali i reputacijsku štetu. U svojoj suštini, upravljanje rizicima podrazumijeva identifikaciju prijetnji, njihovu procjenu, donošenje odluka o načinu odgovora i praćenje promjena tokom vremena. Standardi poput ISO 31000 nude koristan okvir, ali se u praksi često pokazuje da klasični modeli ne odgovaraju u potpunosti složenosti savremenog digitalnog okruženja. Oni se oslanjaju na procjene koje su ponekad subjektivne i teško prilagodljive brzini promjena.Pojava naprednih tehnologija, poput vještačke inteligencije, donijela je značajne promjene u ovom pristupu. Algoritmi danas mogu analizirati ogromne količine podataka, otkrivati obrasce koji su ranije ostajali neprimijećeni i upozoravati na potencijalne probleme prije nego što prerastu u ozbiljne incidente. Takvi sistemi su naročito korisni za prepoznavanje odstupanja u ponašanju; bilo korisnika, bilo uređaja – koja mogu ukazivati na greške, zloupotrebe ili sigurnosne napade.

Platforma INZA za upravljanje rizicima razvijena je na tim principima, ne funkcioniše samo kao alat za nadzor rizika, već kao sistem koji aktivno uči iz prethodnih iskustava i prilagođava se novim situacijama. Na osnovu stvarnih podataka i ponašanja korisnika, sistem može mnogo ranije upozoriti na sumnjive aktivnosti nego što bi to mogli klasični mehanizmi. Na taj način se značajno skraćuje vrijeme reakcije i smanjuju potencijalne štete.Osim toga, platforma koristi metode prediktivne analize, pristup koji omogućava izvlačenje korisnih obrazaca iz prošlih događaja za potrebe budućih procjena. To uključuje analizu situacije, procjenu tokom koje se predlažu preventivne mjere, kreiranje scenarija rizika, te na kraju ključnu analizu troškova i koristi, koja pokazuje koliko angažman u preventivne mjere u konačnici smanjuje mogućnost havarije, ali i koliko u ekonomskom smislu donosi koristi samoj organizaciji.

Na kraju, INZA Risk Management predstavlja spoj dugogodišnjeg iskustva i inovacije, a njena snaga ogleda se u sposobnosti prilagođavanja svakom okruženju, posebno onima koji su već zakoračili na put digitalizacije i traže načine da pametnije i dugoročnije zaštite svoje sisteme.

3. Sigurnosni sistemi bazirani na umjetnoj inteligenciji

Upotreba vještačke inteligencije u savremenim sigurnosnim sistemima postaje sve češći odgovor na izazove koje postavlja zaštita složenih informacionih mreža. Iako se klasične mjere poput vatrozida, antivirusnih alata i ručne kontrole pristupa i dalje koriste, praksa pokazuje da one često ne mogu pratiti brzinu i nepredvidivost savremenih napada. Današnji napadi nisu lako uočljivi; često se odvijaju kroz suptilne promjene i obrasce ponašanja koji mogu proći neopaženo. Zbog toga se sve veća pažnja usmjerava ka sistemima koji ne zavise od unaprijed definisanih pravila, već imaju sposobnost samostalnog prepoznavanja odstupanja u ponašanju.

Table 3 The applications and technologies related to artificial intelligence for CPS

Connection	SAAS	BDP, mCPS	CBM	Self-maintain
Conversion	LCM	HMI, MaC	PHM	Self-aware
	AMAT	LTTA, SDC		
Cyber (analytic solutions)	EaPS	RTD, FoM, AA, PtPM	CPS	Self-compare
Cognition	SCRM	POD, SOPS	DSS	Self-predict
	ISaDS	ACD, MLA, HPC, ISR		Self-optimise
Configuration	TaT	CoA	RCS	Self-organise
	FPR	KPI		
	AMaAC	CPPS		Self-configure

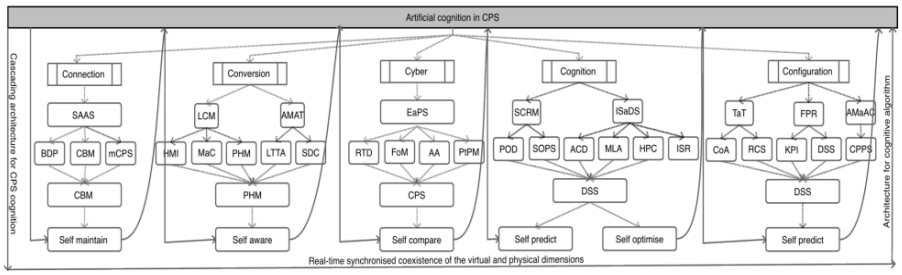


Fig. 2 Cascading framework for artificial intelligence for CPS

SN Applied Sciences
A SPRINGER NATURE journal

Slika 1.: Radanliev, P. (2020). *„Vještačka inteligencija i mašinsko učenje u dinamičkoj analitici sajber rizika na ivici mreže“*, SN Applied Science, časopis izdavača Springer Nature.

Kaskadni okvir prikazan na slici 2 predstavlja novi pristup u dizajniranju dinamičkih i automatiziranih prediktivnih sistema koji su podržani inteligencijom u realnom vremenu. Ovaj okvir omogućava procjenu potencijala za primjenu kognitivnih AI mehanizama u prikupljanju podataka i analitici s dinamičkim povratnim informacijama u realnom vremenu.

Takvi mehanizmi mogu omogućiti prediktivnu inteligenciju o učestalosti prijetnji i potencijalnoj veličini gubitaka koji iz njih proizilaze. Nesumnjivo je da se, kako

bi se osigurala ova funkcionalnost, algoritmi dubokog učenja moraju integrisati u kognitivne mehanizme kako bi formirali dinamičke intervale povjerenja i vremenski definisane granice na osnovu podataka u realnom vremenu. Kada se ove sposobnosti postignu, kaskadni okvir sa slike 2 postaje savremeni alat za analitiku rizika. (Radanliev, P., 2020)

Algoritmi vještačke inteligencije analiziraju velike količine podataka u realnom vremenu i traže znakove koji odstupaju od uobičajenog toka aktivnosti, čime omogućavaju otkrivanje prijetnji koje nisu evidentirane u postojećim bazama podataka. Korištene tehnike uključuju različite pristupe poput klasifikacije, klasterovanja podataka i neuronskih mreža, koje omogućavaju vrlo precizno prepoznavanje nepravilnosti u sistemu.

Napredni AI programi mogu brzo pregledati velike količine informacija kako bi prepoznali i odgovorili na potencijalne prijetnje te prema potrebi prilagodili sigurnosne mehanizme. Ove tehnologije koriste napredne algoritme za analizu velikih skupova podataka s ciljem identifikacije rizika, obrazaca i anomalija. Ovo poboljšanje u donošenju odluka i raspodjeli resursa može se uporediti s ulogom AI sistema u drugim oblastima, poput komunikacije o klimatskim promjenama, gdje su se AI glasovi pokazali jednako efikasnim kao i ljudski (Ni, B., 2023).

U okviru platforme INZA Risk Management, vještačka inteligencija se primjenjuje na više nivoa zaštite. Prvi sloj uključuje analizu stanja, gdje se stalno prate promjene u obrascima korištenja s ciljem otkrivanja neuobičajenih aktivnosti. Osim toga, sistem kontinuirano nadzire ponašanje svih komponenti kritične infrastrukture, bilježi njihove „normalne“ režime rada i prepoznaje odstupanja. Kada se pojavi takva situacija, sistem odmah reaguje, šalje obavijest i predlaže korake za preventivno djelovanje.

Posebna vrijednost INZA Risk Management sistema ogleda se u njegovoj sposobnosti povezivanja s vanjskim izvorima podataka, poput globalnih baza poznatih prijetnji i prethodnih incidenata, kao i u korištenju vlastite istorije kako bi bolje razumio specifičnosti okruženja u kojem se koristi. Na taj način, sistem reaguje ne samo na ono što vidi, već i na ono što zna, oslanjajući se na iskustvo kombinovano s aktuelnim podacima.

Automatizacija ima ključnu ulogu. Kada se rizik otkrije, sistem odmah obavještava odgovorne osobe i nudi preventivne mjere, čime se vrijeme reakcije svodi na minimum. Upravo ta brzina često odlučuje hoće li incident biti uspješno kontrolisan ili će se razviti u ozbiljan sigurnosni problem.Naravno, ovakav stepen automatizacije otvara i nova pitanja: Kako osigurati da su odluke sistema razumljive i provjerljive? I šta ako sistem pogriješi? Zbog toga INZA Risk Management uključuje mogućnost ljudske kontrole nad svakim automatiziranim

postupkom, čime se postiže ravnoteža između efikasnosti tehnologije i stručne procjene sigurnosnog tima. Na kraju, rješenja poput INZA Risk Management više nisu opcija – ona su postala nužnost.

4. Unaprijeđen algoritam predikcije rizika: primjeri i funkcionalnosti

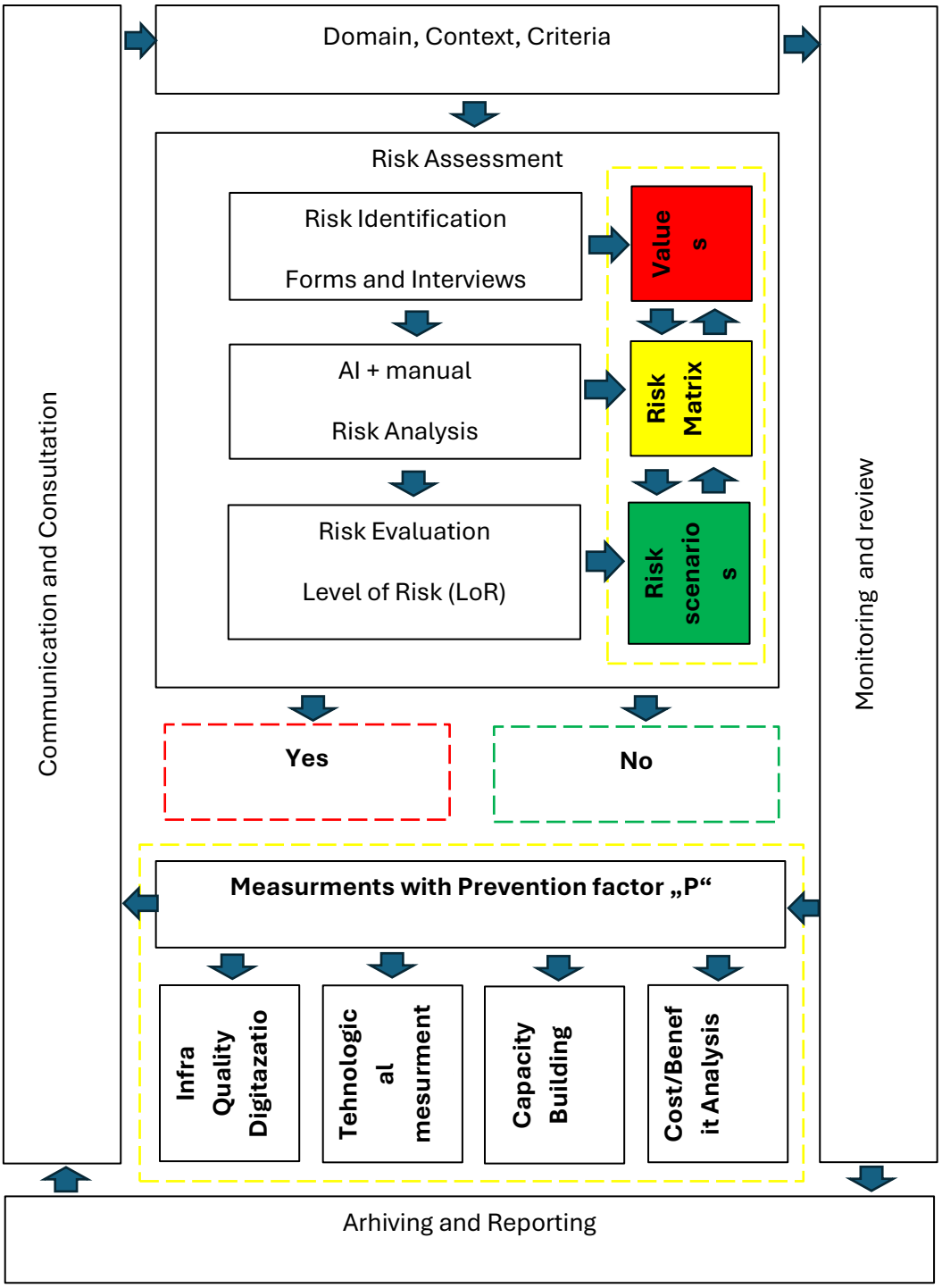
U samoj srži INZA Risk Management platforme za upravljanje rizicima nalazi se algoritam razvijen s ciljem rane detekcije sigurnosnih prijetnji u sistemima kritične infrastrukture. Za razliku od konvencionalnih pristupa koji se uglavnom oslanjaju na poznate obrasce, ovaj sistem koristi kombinaciju učenja iz podataka u realnom vremenu i analize anomalija kako bi kontinuirano prilagođavao svoje procjene i reagovao na nove situacije (Garaplija, 2022).

Jedna od njegovih ključnih prednosti jeste to što ne posmatra samo jedan izvor informacija, već istovremeno uzima u obzir različite aspekte: tehničke indikatore, način na koji je organizovana struktura kompanije i pravila pristupa, kao i samo ponašanje korisnika. U praksi to znači da sistem može prepoznati kada se neko ponaša drugačije nego inače, bilo da se radi o zaposleniku koji pokušava pristupiti osjetljivim podacima u neuobičajeno vrijeme, ili o iznenadnoj promjeni pristupnih prava.

Posebno je važan kontekst u kojem se te promjene dešavaju. Nije isto ako se administrator prijavljuje u sistem iz prostorija firme tokom radnog vremena ili ako se nepoznati korisnik prijavi s udaljene lokacije usred noći. Algoritam uzima u obzir ove razlike i, u zavisnosti od ozbiljnosti odstupanja, pokreće odgovarajuće upozorenje ili predlaže preventivne mjere.

Kako bi svoje procjene učinio što jasnijim i razumljivijim, INZA Risk Management koristi i vizuelne oznake rizika, određena boja i procenat prikazanina mapi označavaju nivo rizika, što korisnicima omogućava brz i intuitivan uvid u sigurnosnu situaciju bez potrebe da ulaze u tehničke detalje. (Garaplija, 2023)

INZA Risk Management softver za upravljanje rizicima usklađuje sajber i fizičku sigurnost povezivanjem različitih digitalnih protokola mjerenja i sigurnosnih senzora u jedinstvenu AI bazu podataka, što ne samo da ubrzava efikasnost donošenja odluka, već i razvija baze znanja za buduća istraživanja i razvoj.



Slika 2.: Unaprijeđeni algoritam za prevenciju rizika prema standardu ISO 31000, (Garaplija, 2022)

Teorija sajber-fizičkih sistema (CPS) potiče iz teorije upravljanja i inženjerstva upravljačkih sistema, te se fokusira na međusobno povezivanje fizičkih komponenti i upotrebu složenih softverskih entiteta za uspostavljanje novih mrežnih i sistemskih funkcionalnosti. Na taj način, CPS sistemi povezuju fizičke i inženjerske komponente, predstavljajući most između sajber svijeta i fizičkog svijeta.

Suprotno tome, teorija Interneta stvari (IoT) nastala je iz računarskih nauka i internet tehnologija, i prvenstveno se bavi međusobnom povezanošću, interoperabilnošću i integracijom fizičkih komponenti putem interneta. S potpunom tržišnom integracijom IoT-a u narednoj deceniji, očekuje se da će ova integracija rezultirati razvojem poput automatizacije CPS sistema putem IoT-a.

Ono što dodatno potvrđuje efikasnost algoritma INZA Risk Management sistema za upravljanje rizicima jeste način na koji se ponašao tokom testiranja u stvarnim uslovima. U više navrata, uspio je detektovati potencijalne rizike mnogo ranije nego što bi to učinio standardni sistem. Za razliku od mnogih generičkih rješenja koja se oslanjaju na unaprijed definisane šablone, INZA Risk Management je prilagođen lokalnim uslovima na terenu. Uzima u obzir specifične karakteristike tržišta, jezičkog okruženja, pravnog okvira i sigurnosnih izazova karakterističnih za određenu regiju.

Upravo ta sposobnost adaptacije čini ga posebno korisnim za kompanije i institucije širom svijeta, gdje često postoje nijanse koje strana rješenja jednostavno ne prepoznaju, što može dovesti do pogrešnih procjena i neadekvatnog odgovora.

5. Izazovi i ograničenja korporativne primjene

Integracija vještačke inteligencije u svakodnevne poslovne procese donosi brojne prednosti, ali istovremeno predstavlja i izazove, posebno kada se primjenjuje na osjetljiva područja poput procjene sigurnosnih rizika i upravljanja kritičnom infrastrukturom. Platforma INZA Risk Management, kao primjer takvog sistema, predstavlja snažan alat, ali njeno uklapanje u postojeće strukture kompanije često nije jednostavno, jer zahtijeva promjene koje se ne odnose samo na tehnologiju, već i na ljude, procese i organizacijsku kulturu.

Jedan od prvih problema koji se može pojaviti jeste pitanje spremnosti organizacije da prihvati takav sistem, budući da u mnogim okruženjima još uvijek dominira pristup u kojem se sve oslanja na ljudsku procjenu, dok automatizovani sistemi izazivaju oprečnost, naročito kada se od njih očekuje davanje preporuka.

Ako uposlenici nisu upoznati s načinom na koji algoritam funkcioniše, može se javiti osjećaj nepovjerenja, pa čak i otpora. Situacija se dodatno komplikuje ukoliko nije jasno definisano ko snosi odgovornost za odluke koje sistem donosi – da li osoba koja ga nadgleda ili tim koji ga koristi.Tehnički aspekt integracije također može predstavljati ozbiljan izazov. Iako je INZA Risk Management dizajniran da bude fleksibilan, ipak zahtijeva pristup ključnim podacima, logovima, mrežnim zapisima i autentifikacijskim protokolima. Ako su ovi sistemi zastarjeli, zatvoreni ili nepovezani, integracija može zahtijevati dodatno vrijeme i resurse, što nije uvijek lako ostvariti u kratkom roku. Posebnu dimenziju predstavlja pitanje privatnosti. Da bi algoritam mogao ispuniti ono što se od njega očekuje, mora analizirati informacije koje mogu uključivati lične podatke – aktivnosti zaposlenika, pristup određenim datotekama, vrijeme i lokaciju prijave u sistem. Bez jasno definisanih granica, postoji rizik da se sigurnost pretvori u nadzor. Zbog toga je u sistem INZA Risk Management ugrađena kontrola pristupa podacima i princip ograničene obrade; analiziraju se samo podaci koji su zaista neophodni, a svaki korak koji sistem poduzme moguće je naknadno provjeriti.

Pored tehničkih i pravnih izazova, često postoji i suptilnija, ali jednako važna prepreka: ljudski faktor. Zaposlenici mogu osjećati nelagodu zbog uvođenja AI tehnologije u njihovo radno okruženje, ponekad je doživljavajući kao prijetnju sopstvenoj poziciji. Zbog toga uspješna implementacija mora ići dalje od pukog instaliranja softvera, potrebni su prije svega edukacija, otvoren dijalog i jasno objašnjenje kako ovakvi sistemi mogu donijeti dodatnu vrijednost. Pristup „korak po korak“, u kojem se ljudi kroz praksu postepeno upoznaju sa sistemom, pokazao se kao najefikasniji način za izgradnju povjerenja.

Pitanje standardizacije i formalne validacije ovakvih sistema dodatno komplikuje njihovu širu primjenu. Iako INZA Risk Management koristi provjerene modele i samoučeće algoritme, još uvijek ne postoji univerzalan okvir koji bi precizno definisao kako se ovakvi alati testiraju, odobravaju ili certificiraju, posebno u regulisanim industrijama poput bankarstva, zdravstva ili energetike, gdje nema prostora za pogrešne procjene.Uz sve to, neophodno je imati na umu da se ovakvi sistemi moraju redovno održavati, jer vještačka inteligencija nije statična, ako se ne ažurira, brzo zastarijeva i prestaje biti korisna. Modeli moraju pratiti nove podatke, učiti iz promjena i revidirati svoja pravila kako bi ostali relevantni, što znači da organizacija mora imati ne samo dobar početni plan, već i dugoročnu podršku: tehničku, kadrovsku i stratešku.Međutim, kada postoji iskrena spremnost, jasan plan implementacije i snažna podrška rukovodstva, iskustvo pokazuje da se ovakvi sistemi mogu uspješno integrisati. U takvom okruženju, INZA Risk Management ne samo da povećava nivo sigurnosti i ubrzava odgovor na incidente, već i pomaže promjeni organizacijske svijesti ka proaktivnijem pristupu upravljanju rizicima.

6. Zakonodavstvo, profesionalna etika i odgovornost

Razvoj tehnologija koje koriste vještačku inteligenciju za upravljanje rizicima, posebno u kontekstu korporativne sigurnosti, donosi ne samo tehnička, već i pravna i etička pitanja. Kada algoritmi počnu preuzimati zadatke koje su prethodno obavljali ljudi, analizirajući ponašanje i dajući preporuke, javlja se logična zabrinutost: šta ako sistem napravi grešku? I, još važnije, ko je tada odgovoran?

Implementacija rješenja poput platforme INZA Risk Management zahtijeva da se već od samog početka uzmu u obzir zakoni koji štite lične podatke i definišu granice automatizovanog odlučivanja. U Evropi se posebna pažnja posvećuje pravilima poput Opće uredbe o zaštiti podataka (GDPR), koja jasno propisuje da korisnici imaju pravo znati na koji način se donose odluke koje ih se tiču, te da u proces odlučivanja može biti uključen čovjek, kad god je to potrebno.Sistem INZA Risk Management je izgrađen tako da svaka akcija koju inicira sistem bude zabilježena, te da se može naknadno pregledati, objasniti i ako je potrebno na kraju osporiti. Cilj nije da se AI postavi iznad ljudi, već da pomogne timu da reaguje brže i efikasnije. No, pored zakona, važno je i profesionalno poštivanje etičkih principa. Osobe koje razvijaju i koriste ovakve sisteme imaju obavezu da djeluju pošteno, da poštuju granice i da ne koriste tehnologiju u svrhe koje nisu u skladu s njenom namjenom.

Na primjer, algoritmi se ne smiju koristiti za nadzor zaposlenih izvan jasno definisanog, opravdanog i poznatog okvira, niti smiju donositi automatske zaključke o nečijem ponašanju bez dodatne provjere i konteksta. INZA Risk Management je razvijen s ciljem da podrži „odgovornu upotrebu vještačke inteligencije“, ne da zamijeni ljudsku procjenu, već da je unaprijedi, ubrza i učini informisanijom.

Odgovornost je, naravno, i dalje osjetljivo pitanje. U tradicionalnim sistemima često je jasno, ako dođe do greške, zna se ko je postupao i gdje je pogreška nastala. Kod AI sistema ta granica nije toliko jasna. Da li je odgovorna osoba koja je kreirala model? Ili ona koja ga koristi? Ili možda sam sistem, iako pravno ne postoji kao „subjekt“? Zbog toga je važno da svaka organizacija koja koristi ovakva rješenja ima jasno definisan okvir: interne procedure, pravila upravljanja rizikom i dokumentaciju koja definiše postupanje u slučaju greške.

Ključ nije u prebacivanju odgovornosti, već u tome da svi znaju kako se ponašati u skladu s jasno utvrđenim pravilima. Još jedan važan aspekt je povjerenje, jer uposleni u organizaciji moraju znati da postoji sistem koji analizira njihove aktivnosti, ali i da znaju zašto, kako i u kojoj mjeri. Transparentnost se ne postiže samo kroz regulative i pravne formulacije, već i kroz iskren dijalog unutar tima.

Zato INZA Risk Management ne nudi samo tehničke mehanizme koji osiguravaju privatnost, već i podržava kulturu u kojoj se korisnici osjećaju informisano, a ne nadgledano. U konačnici, uspjeh ovakvih rješenja neće zavisiti samo od toga koliko su pametni algoritmi, već od toga kolika je spremnost organizacija da ih koriste odgovorno.Rješenja poput INZA Risk Management mogu biti izuzetno efikasna, ali samo ako se uklapaju u širi okvir koji uključuje zakonsku regulativu, interna vrijednosna načela i snažan osjećaj etičke odgovornosti. Kada se ti elementi spoje, sistem postaje praktičan alat koji doprinosi jačanju sigurnosti i podršci u donošenju informisanih odluka.

7. Sistemski pristup i dalji razvoj

Upravljanje rizicima u sistemima kritične infrastrukture zahtijeva mnogo više od jednog softverskog rješenja ili izolovanog sigurnosnog alata, potrebna je sveobuhvatna strategija koja objedinjuje tehnologiju, procese, ljude i zakonske obaveze u funkcionalan sistem sposoban da odgovori na vremenski promjenjive izazove.Platforma INZA Risk Management razvijena je upravo s tim ciljem, kao dio šireg sigurnosnog ekosistema, spremna da se prilagodi različitim sektorima, veličinama organizacija i stepenu digitalne zrelosti. Ono što INZA Risk Management čini drugačijom jeste njen pristup koji ne posmatra procjenu rizika kao krajnji cilj, već kao početak procesa koji se stalno razvija. Svaka identificirana prijetnja pokreće lanac aktivnosti, od analize i odgovora, do naknadnog učenja i prilagođavanja.Sistem „pamti“, procjenjuje vlastite reakcije i prilagođava se promjenama u okruženju, čime se izbjegava statički model i gradi okruženje u kojem sigurnost postaje dinamičan proces.

Već se razmatra niz novih mogućnosti u okviru daljih razvojnih planova, među kojima se izdvaja sposobnost da se dostupni resursi – bilo da se radi o ljudstvu, opremi ili vremenu, automatski usmjere tamo gdje su najpotrebniji, u zavisnosti od trenutnog nivoa rizika.Također se planira uvođenje simulacija i testova koji organizacijama omogućavaju da unaprijed provjere kako bi njihov sistem reagovao u slučaju ozbiljnog napada i na taj način na vrijeme otkriju svoje ranjivosti, prije nego ih neko iskoristi.U budućnosti će INZA Risk Management biti još tjesnije povezana s fizičkom infrastrukturom, putem IoT senzora, sigurnosnih kamera i drugih uređaja, kako bi slika o potencijalnim prijetnjama bila što potpunija i dostupna u realnom vremenu.Lokalizacija također igra veoma važnu ulogu. Platforma već sada podržava rad na različitim jezicima i unutar različitih pravnih okvira, što je od posebnog značaja za organizacije koje djeluju u više zemalja ili na tržištima sa specifičnim regulatornim zahtjevima.

Pored samog softvera, posebna pažnja se posvećuje i ljudima koji s njim rade, jer nijedna tehnologija neće dati očekivane rezultate ako oni koji je koriste nisu obučeni da je pravilno interpretiraju i primjenjuju.Zato INZA Risk Management uključuje podršku kroz interaktivne vodiče, objašnjenja odluka koje sistem predlaže i preporuke za dodatnu edukaciju, jer cilj nije da se korisnik izgubi u složenosti, već da sistem bude alat koji pomaže, a ne prepreka.Kada je riječ o usklađenosti s propisima, posebno onim koji tek dolaze, INZA Risk Management već sada prati regulative koje se razvijaju unutar Evropske unije, omogućavajući korisnicima da unapređuju svoje sigurnosne prakse, a da pritom ostanu usklađeni s pravnim očekivanjima i standardima koji će tek stupiti na snagu.

U narednim fazama, INZA Risk Management će otvoriti vrata ka još širem spektru saradnje, jer će zajednički rad na razvoju i testiranju novih modela dodatno pomoći platformi da se prilagodi različitim okruženjima i složenim izazovima, ne samo u digitalnom prostoru, već i u fizičkom i društvenom kontekstu.Suština sistemskog pristupa nije u pronalasku savršenog rješenja, već u osnaživanju organizacije da stalno prilagođava svoje mehanizme zaštite. INZA Risk Management je dizajniran da upravo to omogući, ne samo kao alat koji reaguje na prijetnje, već kao rješenje koje pomaže da se iz svake situacije nešto nauči, sistem stalno unapređuje, a organizacija iz dana u dan postaje otpornija.

8. Zaključak

Danas je izuzetno važno razmišljati unaprijed, djelovati preventivno te brzo spriječiti i reagovati. Ovaj rad je pokazao da vještačka inteligencija, ukoliko se razvija promišljeno i koristi odgovorno, može imati ključnu ulogu u takvom pristupu. Platforma INZA Risk Management upravo je takav primjer, jer se njena vrijednost ogleda ne samo u tehnološkim rješenjima koja koristi, već i u načinu na koji povezuje različite izvore informacija, uči kroz vrijeme i korisnicima pruža ono što im zaista treba: jasne uvide i preporuke koje se mogu odmah primijeniti.Postoje brojni tehnički izazovi, promjene unutar organizacije i niz pravnih pitanja koja prate svaki ozbiljan pokušaj digitalne transformacije.

Međutim, ti izazovi ne predstavljaju razlog za odustajanje, naprotiv, oni su poziv da se tehnologijom upravlja odgovorno i s razumijevanjem. Jasna pravila, usklađenost sa zakonodavstvom i etički pristup nisu opcija, već neophodna osnova za stabilnu i dugoročno održivu implementaciju ovakvih rješenja.U budućnosti će INZA Risk Management nastaviti svoj razvoj ka još boljoj povezanosti s drugim sistemima, većoj transparentnosti i jednostavnijoj upotrebi. Vizija nije samo tehnološki napredan alat, već partner koji raste, uči i zajedno s organizacijom sve bolje razumije složenost sigurnosnih izazova.

Na kraju, važno je jasno naglasiti: vještačka inteligencija neće zamijeniti čovjeka u donošenju odluka, ali ga može osnažiti – može mu pomoći da bolje razumije prijetnje, brže reaguje i donosi sigurnije odluke. U tom smislu, INZA Risk Management nije samo softver, već alat koji spaja ljudsku prosudbu i digitalnu preciznost u svrhu upravljanja rizicima u sistemima kritične infrastrukture.

LITERATURA

1. Dworschak, B., Zaiser, H. (2014). „Kompetencije za sajber-fizičke sisteme u proizvodnji – prvi nalazi i scenariji“, *Procedia CIRP*, 25:345–350.

2. Garaplija, E., Prguda, S. (2023). „Pametni gradovi za smanjenje rizika od katastrofa: korištenje tehnologije i inovacija za otpornu urbanu sredinu“, *Asocijacija za upravljanje rizicima*, www.zisjournal.com

3. Garaplija, E. (2024). „3D logički model integracije između metafizike i upravljanja rizicima od katastrofa“, *Asocijacija za upravljanje rizicima*, www.zisjournal.com

4. Ni, B., Wu, F., Huang, Q. (2023). „Kada vještačka inteligencija izražava ljudske brige: paradoksalni efekti AI glasa na percepciju klimatskih rizika i namjeru za proekološkim ponašanjem“, *International Journal of Environmental Research and Public Health*, 20(4), 3772.

5. Radanliev, P., De Roure, D., Walton, R., Van Kleek, M., Anthi, E. (2020). „Vještačka inteligencija i mašinsko učenje u dinamičkoj analitici sajber rizika na ivici mreže“, *SN Applied Science*, *Springer Nature Journal*.

6. Wahlster, W., Helbig, J., Hellinger, A., Stumpf, M. A. V., Blasco, J., Galloway, H., Gestaltung, H. (2013). „Preporuke za implementaciju strateške inicijative Industrija 4.0“, *Savezno ministarstvo za obrazovanje i istraživanje*, Njemačka.

7. Uredba (EU) 2016/679 Evropskog parlamenta i Vijeća od 27. aprila 2016. o zaštiti fizičkih osoba u vezi s obradom ličnih podataka i o slobodnom kretanju takvih podataka, kojom se stavlja van snage Direktiva 95/46/EZ (Opšta uredba o zaštiti podataka – GDPR

8. ISO 31010:2019, Upravljanje rizikom – Tehnike procjene rizika, *Međunarodna organizacija za standardizaciju (ISO)*.

RISK MANAGEMENT SOFTWARE BASED ON AI AND CPS PREDICTION

DOI: *10.70329/2744-2403.2025.5.9.1*

Scientific article

Edin Garaplija [3]
Muhamed Durakovic [4]

Abstract:
This paper focuses on the use of machine learning and the use of dedicated AI databases to create solutions based on an improved algorithm for preventive risk management, and real-time risk prediction. The paper analyses the existing standard, its shortcomings and solutions for improvement, and the structure and algorithmic basis of these systems, as well as their integration into existing security architectures and platforms. The work includes the detection of threats based on anomalies and the analysis of established user behavior according to given patterns, risk assessment and proactive detection of attacks. Timely identification and management of risks are becoming key factors in corporate sustainability and security of business and information systems. Predictive analytics, based on artificial intelligence, machine learning and big data analytics, bring transformational opportunities in areas such as industry, finance, healthcare, which in the modern era are connected by cybersecurity and risk prediction that help decision makers to manage systems more efficiently and protect them. An integrative approach to harmonizing these technologies, especially considering the organizational structure and legal framework, includes issues of reliability and transparency of models, as well as accountability for automated decisions, privacy protection and compliance with legislation. The aim of the paper is to provide a comprehensive overview of technological and methodological innovations in predictive protection against cyber risks, and to identify directions for future development with a special focus on the security, ethics and reliability of AI systems.

Keywords: *Risk, AI Prediction, Cyber Security*

---

[3] Edin Garaplija, PhD in security Science, President of INZA Institute of the Risk Management
[4] Muhamed Durakovic, IT Eng., IT Development engineer of the INZA Group

1. Introduction

Risk management in critical infrastructure systems is becoming an increasingly demanding task, especially in the context of accelerated technology development, increased connectivity of the systems themselves, and the growing sophistication of cyber threats. Current approaches based on measures, which usually omit prevention at the very beginning, are no longer sufficient to respond to modern corporate security challenges. In this context, artificial intelligence (AI) and machine learning offer new perspectives and opportunities for improving existing security systems, primarily through the introduction of predictive models that enable the recognition of threats before they cause damage in time. The focus will be on how algorithms are integrated into existing processes to improve standard approaches and enable timely reactions in complex environments. In addition to technical aspects, the paper will also address broader issues that accompany the application of these technologies, from ethical and legal challenges to issues of transparency and compliance with laws and internal regulations. This dimension is crucial to ensure the responsible and long-term sustainable use of AI systems in business practice. Today's digital transformation processes significantly contribute to greater connectivity and operational efficiency, but at the same time open up space for new vulnerabilities. Attacks on information systems are increasingly based on a combination of technical failures and human factors. Therefore, modern security approaches must go beyond traditional network boundary protection and encompass a broader risk analysis in everyday business. An expanded vision of security is needed, which connects technical, organizational, and human factors into a single early warning and preventive response system. The INZA Risk Management platform was developed with this vision in mind, in response to global challenges, offering a scalable and intelligent solution that can be adapted to the specific needs of different organizations in the management process of critical infrastructures.

2. Theoretical framework

In today's business environment, where digital technologies form the foundation of almost every sector, risk management is increasingly becoming part of a broader strategy for survival and growth. Instead of reacting only after an incident has occurred, increasing emphasis is placed on timely identification of threats and adequate responses to them.

It has been argued that the spectacular advancements in cyber-physical systems (CPSs) and internet of things (IoT) technology represent the foundation for Industry 4.0 (Whalster, W., 2013)CPS theory emerged from control theory and control systems engineering and focuses on the interconnection of physical components and use of complex software entities to establish new network and

systems capabilities. CPSs thus link physical and engineered systems and bridge the cyber world with the physical world.In contrast, IoT theory emerged from computer science and Internet technologies and focuses mainly on the interconnectivity, interoperability and integration of physical components on the Internet. With full IoT market adoption over the next decade, this integration work is anticipated to lead to developments such as IoT automation of CPSs (Dworschak, B., Zaiser, H., 2014)

This is especially true for cybersecurity, where a single failure can cause serious damage, both technical and reputational. At its core, risk management involves identifying threats, assessing them, making decisions about how to respond, and monitoring changes over time. Standards such as ISO 31000 offer a useful framework, but in practice it is often shown that classic models do not always correspond to the complexity of the modern digital environment. They rely on assessments that are sometimes subjective and difficult to adapt to the speed of change. The emergence of advanced technologies such as artificial intelligence has brought significant changes to this approach. Algorithms can now analyze huge amounts of data, detect patterns that previously went unnoticed, and warn of potential problems before they develop into serious incidents. Such systems are particularly useful for identifying deviations in behavior, whether of users or devices, which may indicate errors, abuses, or security attacks. The INZA Risk Management platform was developed on these principles, where it does not function only as a risk monitoring tool but as a system that actively learns from previous experiences and adapts to new situations.

Based on real data and user behavior, the system can warn of suspicious activities much earlier than classic mechanisms would. In this way, the reaction time is shortened, and damages can be significantly reduced. In addition, the platform uses predictive analysis methods, an approach that allows useful patterns to be extracted from past events for future assessments. This includes a situation analysis, an evaluation in which preventive measures are proposed, the creation of risk scenarios, and finally a crucial cost-benefit analysis that shows how much engaging in preventive measures ultimately reduces the possibility of a breakdown, as well as how much it brings, in economic terms, in benefits for the organization itself. Ultimately, INZA Risk Management is the product of a combination of years of experience and innovation, where its strength lies in its ability to adapt to any environment, especially those who have already embarked on the path of digitalization and are looking for ways to protect their systems in a smarter and longer-term way.

3. Security systems based on artificial intelligence

The use of artificial intelligence in modern security systems is becoming an increasingly common response to the challenges posed by the protection of complex information networks. Although classic measures such as firewalls, antivirus tools, and manual access control are still used, practice shows that they often cannot keep up with the speed and unpredictability of modern attacks. Today's attacks are not easily noticeable; they often occur through subtle changes and behaviors that can pass under the radar. Therefore, attention is increasingly being directed towards systems that do not depend on predefined rules but have the ability to recognize deviations in behavior themselves.

Table 3 The applications and technologies related to artificial intelligence for CPS

Connection	SAAS	BDP, mCPS	CBM	Self-maintain
Conversion	LCM	HMI, MaC	PHM	Self-aware
	AMAT	LTTA, SDC		
Cyber (analytic solutions)	EaPS	RTD, FoM, AA, PtPM	CPS	Self-compare
Cognition	SCRM	POD, SOPS	DSS	Self-predict
	ISaDS	ACD, MLA, HPC, ISR		Self-optimise
Configuration	TaT	CoA	RCS	Self-organise
	FPR	KPI		
	AMaAC	CPPS		Self-configure

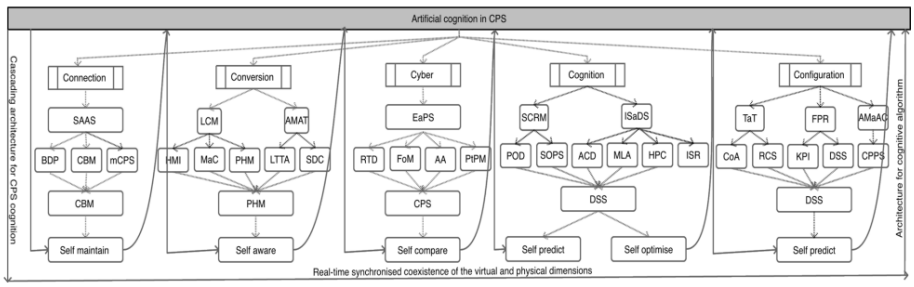


Fig. 2 Cascading framework for artificial intelligence for CPS

SN Applied Sciences
A SPRINGER NATURE journal

Fig.1.: Radanliev, P., (2020). „Artifcial intelligence and machine learning in dynamic cyber risk analytics at the edge“, SN Applied Science, Springer Nature Journal

The cascading framework in Fig. 2 presents a new way to design dynamic and automated predictive systems supported with real-time intelligence. This framework supports an assessment of the potential for adapting AI cognitive engines in data collection and analytics with dynamic real-time feedback. These engines might provide predictive intelligence on threat event frequency and the potential magnitude of resulting losses. Undoubtedly, to provide this

functionality, deep learning algorithms need to be adopted into cognitive engines to form dynamic confdence intervals and time bound ranges with real-time data. Once we have these abilities the cascading framework in Fig. 2 becomes a modern tool for risk analytics. (Radanliev, P., 2020)

Artificial intelligence algorithms analyze large amounts of data in real time and look for signs that deviate from the usual flow of activity, thus enabling them to detect threats that are not recorded in existing databases. The techniques used include various approaches, including classification, data clustering, and neural networks, which enable very precise recognition of irregularities in the system.

Advanced computer programs (AI) can quickly look through a lot of information to find and respond to potential threats, and change security methods as needed. These technologies utilize advanced algorithms to analyze large volumes of data and uncover potential risks, patterns, and anomalies. This enhancement in decision-making and resource allocation can be paralleled to the role of AI in other domains, such as climate change communication, where AI voices have shown to be as effective as human voices (Ni, B.,2023).

As part of the INZA Risk Management platform, AI is applied at multiple levels of protection. The first layer involves state analysis, where changes in usage patterns are constantly monitored in order to identify anything unusual. In addition, the system continuously monitors the behavior of all critical infrastructure components, records their “normal” operating modes, and recognizes when something deviates. When such a situation occurs, the system reacts immediately, sends a notification, and suggests steps for a preventive response. The special value of the INZA Risk Management system is reflected in its ability to connect to external data sources, such as global databases of known threats and previous accidents, and to use its own history to better understand the specifics of the environment in which it is used. This way, the system reacts not only to what it sees but also to what it knows, relying on experience combined with current data. In addition, automation plays a key role. When a risk is detected, the system immediately notifies the responsible persons and offers preventive measures, which shortens the reaction time to a minimum. It is this speed that often decides whether an incident will be successfully controlled or will develop into a serious security problem. Of course, such a degree of automation also opens up new questions: How to ensure that the system's decisions are understandable and verifiable, and what if the system makes a mistake? That is why INZA Risk Management includes the possibility of human control over each automated procedure, which achieves a balance between the efficiency of the technology and the professional assessment of the security team, and in the end, solutions like INZA Risk Management aren't more options, it's a necessity.

4. Improved risk prediction algorithm: examples and functionalities

At the core of the INZA Risk Management platform is an algorithm that was developed to help in the early detection of security threats in critical infrastructure systems. Unlike conventional approaches that mainly rely on known patterns, this system uses a combination of real-time data learning and anomaly analysis to continuously adjust its assessments and react to new situations (Garaplija, 2022).

One of its key advantages is that it does not look at just one source of information but simultaneously takes into account different aspects: technical indicators, the way the company structure is organized and access rules, and the behavior of the users themselves. In practice, this means that the system can notice when someone behaves differently than usual, whether it is an employee trying to access sensitive data at an unusual time or an unexpected change in access rights.

The context in which these changes occur is particularly important. It is not the same if an administrator logs into the system from the office premises during working hours or if an unknown user logs in from another location in the middle of the night. The algorithm takes these differences into account and, depending on the severity of the deviation, triggers an appropriate warning or offers preventive action. In order to be as clear as possible in its assessments, INZA Risk Management also uses visual risk labels; a certain color and percentage on the map show the level of risk, and in this way, people using the system quickly get an overview of the situation without having to go into technical details. (Garaplija, 2023).

Additionally, the system throws out what could happen if the observed problem is not resolved. Based on previous experiences and current analysis, the user is given three possible scenarios: realistic, most likely, and worst case. And what is more important, descriptions are written in a way that they can understand in their profession.

Great attention is also paid to preventive advice. When a threat is detected, the system suggests specific steps to be taken sometimes it is a technical intervention sometimes it is an organizational measure or employee education.

These recommendations are not random but are based on situations that have already occurred and have been successfully resolved in similar circumstances.

INZA risk management software has aligned Cyber and Physical Security by connecting various digital protocols of measurement and security sensors into a single AI database, which not only accelerates decision-making efficiency but also develops knowledge bases for future research and development.

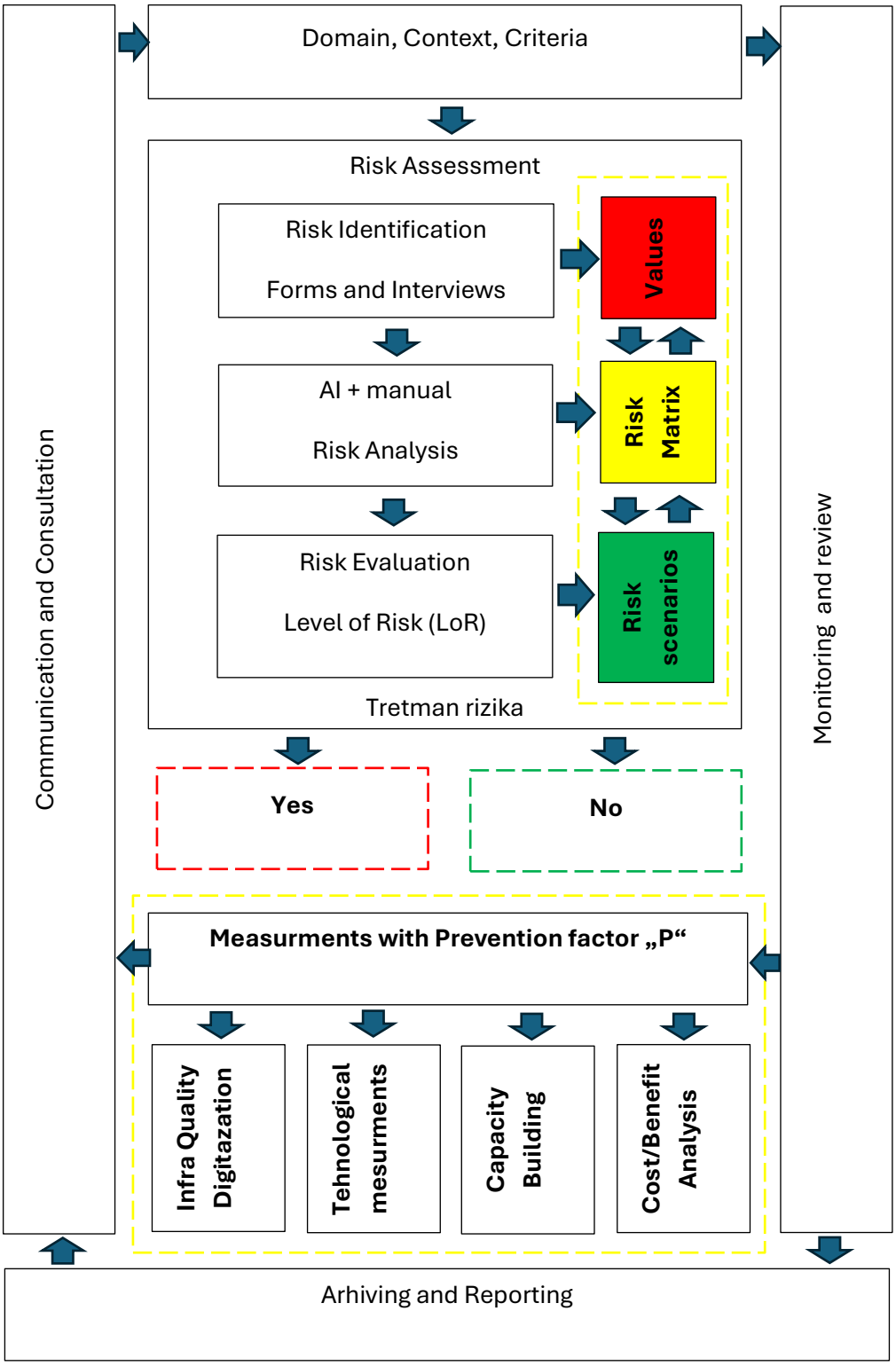


Fig.2: Improved ISO 31000 Risk Prevention Algorithm, (Garaplija, 2022)

CPS theory emerged from control theory and control systems engineering and focuses on the interconnection of physical components and use of complex software entities to establish new network and systems capabilities. CPSs thus link physical and engineered systems and bridge the cyber world with the physical world. In contrast, IoT theory emerged from computer science and Internet technologies and focuses mainly on the interconnectivity, interoperability and integration of physical components on the Internet. With full IoT market adoption over the next decade, this integration work is anticipated to lead to developments such as IoT automation of CPSs

What further confirms the efficiency of the INZA Risk Management algorithm is the way it reacted during testing in real conditions. In several cases, it managed to detect potential risks long before a standard system would have done so. Unlike many generic solutions that rely on predefined templates, INZA Risk Management is adapted to local conditions on the ground. It takes into account the specific characteristics of the market, language, legal framework, and security challenges that are characteristic of that region. It is precisely this ability to adapt that makes it particularly useful for companies and institutions around the world, where there are often nuances that foreign solutions simply do not recognize and then make incorrect assessments.

5. Challenges and limitations of corporate application

Integrating artificial intelligence into everyday business operations offers numerous advantages, but it also presents challenges, particularly when applied to sensitive domains like security risk assessment and the management of critical infrastructure. The INZA Risk Management platform, as an example of such a system, represents a powerful tool, but its inclusion in existing company structures is often not easy, as it requires changes that relate not only to technology but also to people, processes, and work culture. One of the first problems that may arise is how ready the organization is to adopt such a system, because in many environments the approach in which everything relies on human judgment still prevails, and automated systems cause skepticism, especially when they are expected to make recommendations. If employees are not familiar with how the algorithm works, a feeling of distrust and even resistance may arise, and in this way the situation is further complicated if it is not clearly defined who bears responsibility for the decisions made by the system, whether it is the person who monitors it or the team that uses it. The technical aspect of integration can also pose a serious challenge. Although INZA Risk Management is designed to be flexible, it still requires access to key data—logs, network records, and authentication protocols. If these systems are outdated, closed, or disconnected,

integration can take time and require additional resources, which is not always easy to do in the short term. A separate dimension is the issue of privacy. In order for the algorithm to do what is expected of it, it must analyze information that may include personal data—employee activities, access to certain files, and time and location of logging. Without clearly defined boundaries, there is a risk that security will turn into surveillance. That is why the INZA Risk Management system has built-in data access control and the principle of limited processing—only what is really necessary is analyzed, and every step the system takes can be subsequently verified. Beyond the technical and legal challenges, there's often a more subtle yet equally important barrier: the human factor. Employees may feel uneasy about AI being introduced into their work environment, sometimes perceiving it as a risk to their position. That's why successful implementation must go beyond simply deploying software; it also requires education, honest dialogue, and a clear explanation of how these systems can add value. A "step-by-step" approach, in which people learn the system through practice, has proven to be the most effective way to build trust. The issue of standardization and formal validation of such systems further complicates wider implementation. Although INZA Risk Management uses proven models and self-trained algorithms, there is still no universal framework that would accurately define how such tools are tested, approved, or certified, especially in regulated industries such as banking, healthcare, or energy, where there is no room for misjudgments. Added to all this is the fact that these systems must be regularly maintained, because AI is not static; if we do not update it, it quickly becomes outdated and ceases to be useful. Models must adapt to new data, learn from changes, and revise their rules to remain relevant, which means that the organization must have not only a good initial plan but also long-term support: technical, human, and strategic. However, when there is genuine willingness, a clear implementation plan, and strong leadership support, experience shows that such systems can be successfully embedded. In these environments, INZA Risk Management not only enhances security and accelerates incident response but also helps shift organizational mindsets toward a more proactive approach to risk.

6. Legislation, professional ethics and responsibility

The development of technologies that use artificial intelligence for risk management, especially in the context of corporate security, brings not only technical but also legal and ethical issues. When algorithms start taking over tasks that were previously performed by people, analyzing behavior and making recommendations, a logical concern arises: what if the system makes a mistake? And more importantly, who is responsible then? The implementation of solutions such as the INZA Risk Management platform requires that laws that protect

personal data and define the boundaries of automated decision-making be taken into account from the very beginning. In Europe, special attention is paid to rules such as the GDPR, which clearly states that users have the right to know how decisions that affect them are made and that a human can be involved in the process whenever necessary. INZA Risk Management is built so that every action initiated by the system is recorded and can be subsequently reviewed, explained, and, if necessary, challenged. The goal is not to put AI above people but to help the team react better and faster, but in addition to the law, professional ethics are also important. People who develop and use such systems have an obligation to act fairly, to respect boundaries, and not to use technology for things that are not in accordance with its purpose. For example, algorithms should not be used to monitor employees outside of a framework that is clear, justified, and known to everyone, and they should not draw automatic conclusions about someone's behavior without additional verification and context. INZA Risk Management is developed to support the "responsible use of AI"—not to replace human judgment, but to improve it and make it faster and more informed. Liability, of course, remains a sensitive issue. In traditional systems, it is often clear that if an error occurs, it is known who acted and where the mistake was made.

With AI systems, this boundary is not so clear. Is the person who created the model responsible? Or the person who uses it? Or maybe the system itself, although it does not legally exist as a "subject"? Therefore, it is important that every organization that uses such solutions has a clear framework: internal procedures, risk management rules, and documents that define how to act in the event of an error. The key lies in this, not in shifting responsibility, but in ensuring that everyone knows how to behave in accordance with clearly defined rules. Another important aspect is trust, because people working in an organization must know that there is a system that analyzes their activity, but also that they know why, how, and to what extent. Transparency is not achieved only by regulations and legal formulations but by honest conversations within the team.

INZA Risk Management therefore offers technical mechanisms that ensure privacy but also supports a culture in which users feel informed, not monitored. Ultimately, the success of such solutions will not depend only on how smart the algorithms are but on how much organizations are willing to use them responsibly. The solution, like INZA Risk Management, can be highly effective, but only when it fits within a broader framework that includes legal regulations, internal values, and a strong sense of ethical responsibility. When these elements come together, the system becomes a practical tool that helps strengthen security and support more informed decision-making.

7. System approach and further development

Risk management in critical infrastructure systems requires more than a single software solution or isolated security tool, or rather a comprehensive strategy that combines technology, processes, people, and legal obligations into a functional system that can respond to time-changing challenges. The INZA Risk Management platform was developed with this very goal in mind as part of a broader security ecosystem, ready to adapt to different sectors, sizes of organizations, and degrees of digital maturity, and what makes INZA Risk Management different is its approach that does not view risk assessment as the end goal but as the beginning of a constantly evolving process. Each identified threat triggers a chain of activities, from analysis and response to subsequent learning and adaptation. The system remembers, evaluates its own reactions, and adapts to changes in the environment, thus avoiding a static model and creating an environment in which security becomes a dynamic process.

A number of new possibilities are already being considered in further development plans, one of which is the ability to automatically direct available resources, whether it is personnel, equipment, or time, to where they are most needed, depending on the current level of risk. It is also planned to introduce simulations and tests, which allow organizations to test in advance how their system would react in the event of a serious attack and thus discover where they are vulnerable before someone else takes advantage of it. In the future, INZA Risk Management will be even more closely connected to the physical infrastructure with IOT sensors, security cameras, and other devices so that the picture of potential threats is as complete as possible and available in real time. Localization also plays a very important role: the platform already supports work in different languages and legal frameworks, which is especially important for organizations operating in multiple countries or in markets with specific requirements. In addition to the software itself, special attention is paid to the people who work with it, because no technology will produce the expected results if those who use it are not trained to interpret and apply it correctly.

That is why INZA Risk Management includes support through interactive guides, explanations of decisions proposed by the system, and recommendations for additional training, because the goal is not for the user to get lost in complexity, but for the system to be a tool that helps, not an obstacle. When it comes to regulatory compliance, especially those that are yet to come, INZA Risk Management is already keeping pace with the regulations that are developing within the European Union, thus enabling users to improve their security practices while remaining in line with legislative expectations and standards that are yet to come into force. In the following phases, INZA Risk Management will open the door to an even wider range of cooperation, as joint work on the development and

testing of new models will help the platform to further adapt to different environments and complex challenges that arise not only in the digital space, but also in the physical and social context. The essence of a systems approach is not to find the perfect solution but to teach the organization how to constantly adapt its protection mechanisms. INZA Risk Management is designed to provide exactly that, not just a tool that reacts to threats, but a solution that helps to learn something from every situation, to constantly improve the system, and to make the organization more resilient day by day.

8. Conclusion

Today, it is very important to think ahead, act preventively, and prevent and react quickly. This work has shown that artificial intelligence, if developed thoughtfully and used responsibly, can play a key role in this approach. The INZA Risk Management platform is just such an example, because its value is reflected not only in the technological solutions it uses, but also in the way it connects different sources of information, learns over time, and gives users what they really need: clear insights and recommendations that can be applied immediately.

There are numerous technical obstacles, changes in the organization, and numerous legal issues, which are part of any serious attempt at digital transformation. But these challenges are not a reason to give up; on the contrary, they are a call to manage technology responsibly and with understanding. Clear rules, legal compliance, and an ethical approach are not options but a necessary foundation for the stable and long-term implementation of such solutions. In the future, INZA Risk Management will continue to develop towards even better connectivity with other systems, greater transparency, and easier use.

The vision is not just a technologically advanced tool but a partner that grows, learns, and better understands the complexity of security challenges together with the organization. Finally, it should be clear: artificial intelligence will not replace humans in decision-making, but it can empower them; it can help them better understand what threatens them, react faster, and make safer decisions. In this sense, INZA Risk Management is not just software but a tool that combines human judgment and digital precision for management in critical infrastructure systems.

LITERATURE

1. Dworschak B, Zaiser H (2014), "Competences for cyber-physical systems in manufacturing - frst fndings and scenarios", Procedia CIRP 25:345–350

2. Garaplija, E., Prguda, S., (2023), "Smart cities for disaster risk reduction: using technology and innovation for a resilient urban environment", Assosiation of Risk Management, www.zisjournal.com

3. Garaplija, E., (2024), „3D logical model of integration between metaphysics and Disaster Risk Management, Assosiation of Risk Management, www.zisjournal.com

4. Ni, B., Wu, F., Huang, Q. (2023), „When artificial intelligence voices human concerns: The paradoxical effects of AI voice on climate risk perception and pro-environmental behavioral intention. International Journal of Environmental Research and Public Health, 20(4), 3772.

5. Petar Radanliev, David De Roure, Rob Walton, Max Van Kleek, (2020), „Eirini Anthi4, Artifcial intelligence and machine learning in dynamic cyber risk analytics at the edge"m SN Applied Science, Springer Nature Journal

6. Wahlster W, Helbig J, Hellinger A, Stumpf MAV, Blasco J, Galloway H, Gestaltung H (2013) Recommendations for implementing the strategic initiative Industrie 4.0. Federal Ministry of Education and Research

7. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR)

8. ISO 31010:2019, Risk management - Risk assessment techniques, International Standard Organisation