napędy i sterowanie

miesięcznik naukowo-techniczny

Nr 6 (302)
Rok XXVI
Czerwiec 2024
ISSN 1507-7764
Indeks 36018X
Cena: 28,08 zł
(w tym 8% VAT)

napędy ● automatyka przemysłowa ● energoelektronika ● aparatura kontrolno-pomiarowa ● mechatronika ● systemy zasilające
układy zabezpieczeń ● hydraulika ● pneumatyka ● robotyka ● systemy transportowe ● utrzymanie ruchu

norelem

norelem Sp. z o.o.
ul. Myśliborska 22
66-400 Gorzów Wielkopolski

Tel. + 48 572 895 704
Email: info@norelem.pl

www.norelem.pl

napędy i sterowanie miesięcznik naukowo-techniczny

Adres redakcji:
47-400 Racibórz
ul. Środkowa 5
tel. 32 755 19 17
e-mail: redakcja.nis@drukart.pl; www.nis.com.pl

Redaktor naczelna: Katarzyna Zając
tel. 32 755 19 17 • e-mail: redakcja.nis@drukart.pl

Redaguje zespół: Katarzyna Zając, Agnieszka Gutowska, Ludmiła Urbińska, Ryszard Klencz

Redaktor statystyczny: Ludmiła Urbińska
tel. 32 755 23 23 • e-mail: nis@drukart.pl

Redakcja techniczna: Agnieszka Subocz

Marketing:
• Aleksandra Misiewicz
tel. 32 755 18 23 • e-mail: marketing@drukart.pl
• Patrycja Hoszycka
tel. 32 755 24 55 • e-mail: marketing7@drukart.pl

Dział prenumerat: Norbert Klencz
tel. 502 132 515 • e-mail: prenumerata@drukart.pl

Podstawowa korekta tekstu: Ewa Halewska-Karaśkiewicz

Wydawca: Wydawnictwo Druk-Art SC
47-400 Racibórz, ul. Środkowa 5

Konto: VeloBank SA O/Racibórz
57 1560 1140 0000 9090 0004 0921

Patronat honorowy:

Instytut Konstrukcji i Eksploatacji Maszyn Politechniki Wrocławskiej

Katedra Automatyki i Inżynierii Biomedycznej Akademii Górniczo-Hutniczej

Instytut Pojazdów, Konstrukcji i Eksploatacji Maszyn Politechniki Łódzkiej

Punktacja MNiSW za publikacje naukowe wynosi 5 pkt (poz. 1652).
Przyłączając się do realizacji idei Otwartej Nauki, udostępniamy bezpłatnie powierzchnię na artykuły naukowe publikowane w miesięczniku naukowo-technicznym „Napędy i Sterowanie".

Szanowni Państwo!

Z pozoru wydawałoby się, że właściwie wszystko, co związane jest z postępem naszego życia już zostało odkryte. Tymczasem nieustannie epatowani jesteśmy informacjami na temat nowych wynalazków. Powszechne zainteresowanie wzbudza w ostatnim czasie sztuczna inteligencja. Niczym z filmu science fiction brzmią informacje o jej roli w doskonaleniu ludzkiego umysłu.

W książce pt. „Sztuczna inteligencja 2041. 10 wizji przyszłości" Kai-Fu Lee oraz Chen Qiufan (autor bestsellerowej książki „Inteligencja sztuczna, rewolucja prawdziwa", ekspert do spraw AI, były prezes Google China oraz znany powieściopisarz s.f.) połączyli siły, żeby odpowiedzieć na pytanie, jak sztuczna inteligencja zmieni nasz świat w ciągu najbliższych dwudziestu lat.

Według autorów książki sztuczna inteligencja będzie definicją rozwoju XXI wieku – wygeneruje bezprecedensowe bogactwo, zrewolucjonizuje medycynę i edukację poprzez symbiozę człowiek-maszyna oraz stworzy zupełnie nowe formy komunikacji i rozrywki. Jednak uwalniając nas od rutynowej pracy, zakwestionuje także zasady organizacyjne naszego ładu gospodarczego i społecznego i przyniesie nowe zagrożenia w postaci autonomicznej broni i inteligentnej technologii.

To zaledwie kilka spośród wielu fantastycznych, a przecież bardzo realnych wizji. Jednak obok tych przyszłościowych i z pewnością bardzo potrzebnych rozwiązań, pojawia się inny problem, któremu już dziś trzeba stawić czoła. To zagadnienie związane jest oczywiście z poszukiwaniem taniej, a jednocześnie bezpiecznej dla Ziemi energii. Za fascynującym nas postępem podąża bowiem popyt, który sprawia, iż każdego roku spalamy duże ilości paliw kopalnych (węgla, ropy naftowej i gazu, dlatego konieczne jest pozyskiwanie energii ze źródeł odnawialnych, takich jak np. wiatr czy słońce.

Nie można zapomnieć też o konsekwencjach ekologicznych. Na negatywne skutki emisji dwutlenku węgla, wynikające ze spalania paliw z pewnością nie trzeba już długo czekać. Topnienie lodowców, pożary lasów, zmiany w występowaniu roślin i zwierząt, zanikanie i zmiany raf koralowych, pustynnienie obszarów niegdyś zielonych oraz ekstremalne zjawiska pogodowe – to aktualnie zauważalne rezultaty nastających zmian, powodowanych ociepleniem klimatu naszej planety. Chcąc więc uniknąć katastrofy klimatycznej, priorytetowe są dalsze prace nad opracowaniem technologii i urządzeń pozwalających na pozyskiwanie taniej energii, a także umożliwiających jej oszczędzanie, poprzez ograniczenie zużycia prądu, ciepła oraz paliw. Świat bez światła jest dziś równie trudny do wyobrażenia, jak bez niezbędnego do życia powietrza.

Dlatego oprócz nowych trendów w sferze związanej ze sztuczną inteligencją, na łamach naszego pisma znajdziecie Państwo publikacje o treści związanej z efektywnością energetyczną, automatyzacją i optymalizacją różnych gałęzi przemysłu.

Zachęcam do lektury
Katarzyna Zając
Redaktor naczelna

Strona 7
Twój niezawodny partner w technice napędowej

Strona 12
Branża spawalnicza rozwinie się dynamicznie. Nowe możliwości już wkrótce

Strona 32
Robot paletyzujący: bezpieczne prowadzenie kabli 3D z wieloosiowym e-prowadnikiem triflex® R dla robotów

CO W NUMERZE

Nauka

Technologie i produkty

Informacje branżowe

Strona 11
Nowa polska montownia przekładni i motoreduktorów

Strona 48
Gripmaxx™: Trwałe mocowanie napędu przy minimalnej obsłudze

Strona 50
Dobór zasilaczy UPS i zespołów prądotwórczych, a ich prawidłowa współpraca

Indeks reklam

NOWOŚCI TECHNICZNE

JIE EURONORM – Twój niezawodny partner w technice napędowej

- posiadamy bardzo duże zapasy magazynowe części i możliwości montażowe motoreduktorów walcowych z dostawami do 2 tygodni, od przyszłego roku uruchamiamy kolejny magazyn w Polsce;
- nasze motoreduktory walcowe, przekładnie ślimakowe i inne produkty są w pełni zamienne za czołowych producentów w każdym z tych rodzajów produktów, tzn. zamiana na nasze napędy nie wymaga żadnych zmian konstrukcyjnych;
- jesteśmy atrakcyjniejsi cenowo od naszej głównej niemieckiej konkurencji;
- nasze produkty są na tym samym najwyższym poziomie jakościowym co najlepsza konkurencja;
- wszystkim klientom oferujemy bezpłatne wysyłki zamówień od niskiego progu;
- nowym klientom oferujemy bardzo atrakcyjne warunki płatności;
- oferujemy elastyczne warunki gwarancyjne;
- oferujemy indywidualne podejście do każdego, nawet najmniejszego zapytania i projektu, dzięki naszemu centrum warsztatowemu w Holandii i fabryce w Chinach, jesteśmy w stanie wykonać napędy pod specjalne wykonania;
- jesteśmy obecni na wielu rynkach Europy i mamy tam swoje przedstawicielstwa;
- nasze napędy oznaczane są Made in the Netherlands a silniki posiadają certyfikat CE (posiadamy również silniki z certyfikatami na rynek amerykański UL/CSA);
- na każdym kroku służymy pomocą i wsparciem, jak i również posiadamy najczytelniejszy i intuicyjny konfigurator online, który ułatwia pracę konstruktorom, technikom i innym specjalistom – configurator.euronormportal.com.

Michał Piśniak – manager sprzedaży Polska
m.pisniak@euronorm.nl
tel. +48 692 476 519
JIE Euronorm BV
www.jie-euronorm.com/pl/

Sonepar Polska na liście Diamentów Forbesa

Z przyjemnością informujemy, że otrzymaliśmy tytuł Diamentów w szesnastym rankingu publikowanym przez miesięcznik „Forbes". Jest to coroczne prestiżowe zestawienie najbardziej dynamicznie rozwijających się prywatnych firm w Polsce. – Bardzo cieszy nas przyznane wyróżnienie i obecność w rankingu Forbesa. Jesteśmy dumni, że nasi partnerzy handlowi obdarzają nas zaufaniem i doceniają za odpowiedzialność w prowadzeniu biznesu. Bez wątpienia jest to dla nas duża motywacja do dalszego rozwoju – powiedział Wiesław Romańczuk, prezes zarządu Sonepar Polska.

Na liście Diamentów Forbesa znalazły się przedsiębiorstwa, które w ostatnich trzech latach najszybciej zwiększały swoją wartość, wykazały się dodatnim wynikiem finansowym oraz wartością kapitałów własnych. Poniekąd ranking odzwierciedla kondycję i tempo rozwoju polskiego biznesu, a firmy z tytułem Diamentów Forbesa charakteryzują się nowoczesną i różnorodną polityką rozwoju oraz elastycznością w dostosowywaniu się do dynamicznie zmieniającego się rynku.

Do lutego 2024 roku firma działała pod marką Alfa Elektro i tak też została ujęta w rankingu Diamenty Forbesa.

Sonepar Polska jest wiodącym dystrybutorem artykułów elektrotechnicznych dla profesjonalistów. Spółka posiada sieć 56 hurtowni w Polsce. Firma wchodzi w skład międzynarodowej Grupy Sonepar, która jest niekwestionowanym numerem 1 w Europie i na świecie w branży dystrybucji wyposażenia elektrycznego ze sprzedażą przekraczającą 33 mld euro.

Sieć hurtowni elektrycznych Sonepar Polska
www.sonepar.pl

SharkBite Air zawór kulowy

Nasz zawór kulowy do instalacji pneumatycznych i sprężonego powietrza charakteryzuje się wysoką wydajnością, oszczędnością czasu i pracy. Do jego najważniejszych funkcji zalicza się:

- połączenie na wcisk;
- specjalnie zaprojektowany korpus z mosiądzu;
- O-ring z nitrylu i pierścień chwytający ze stali nierdzewnej;
- ciśnienie robocze 18 – 20 barów;
- bezpieczne narzędzie do demontażu;
- zabezpieczony, zamykany uchwyt.

Seria SharkBite Air umożliwia budowanie szybkich, prostych i niezawodnych instalacji sprężonego powietrza. Złącza dostępne są w rozmiarach od 10 do 54 mm, dzięki solidnemu wykonaniu złączy i zaworów z mosiądzu system jest odporny na wysokie ciśnienia. Spełnia on szereg wymagań i jest idealny do małych i dużych instalacji przemysłowych. Dzięki prostemu systemowi na wcisk rury są natychmiast łączone bez potrzeby użycia silikonu lub zgrzewania, lutowania lub klejenia. Połączenie można również rozłączyć za pomocą bezpiecznego przyrządu do demontażu, umożliwia to szybką i łatwą modyfikację instalacji. Złącze zaprojektowano tak, aby połączenie z rurą aluminiową było bezpieczne i pewne. Shark-Bite Air zapewnia szczelne połączenie. Złącza są również kompatybilne z rurami aluminiowymi, miedzianymi, PEX-a lub wykonanymi z poliamidu PA12.

Reliance Worldwide Corporation
www.rwc.com

Twój niezawodny partner w technice napędowej

Kim jesteśmy?

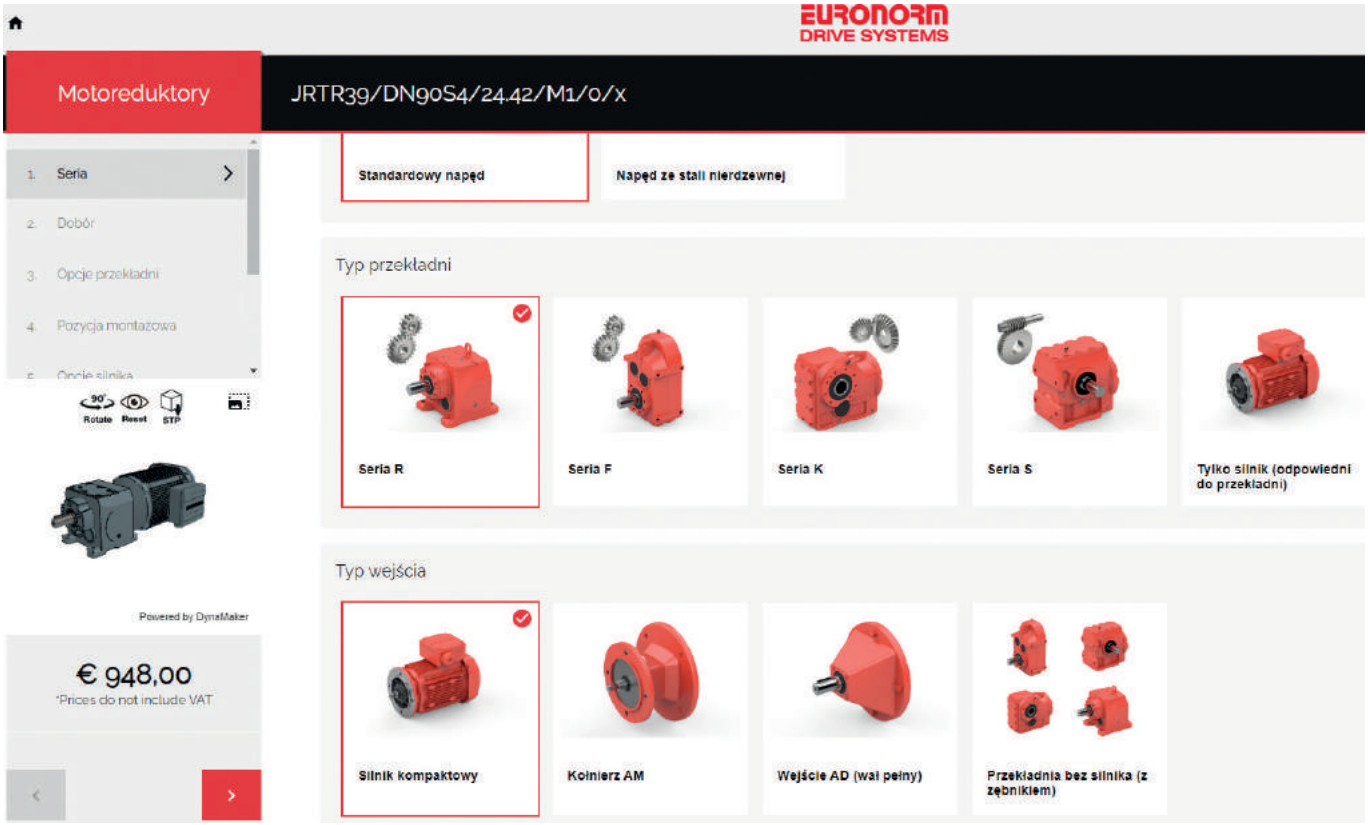
JIE EURONORM BV to holenderska spółka z siedzibą w Sassenheim (pod Amsterdamem), która wchodzi w skład grupy JIE DRIVE (grupę JIE DRIVE opisywaliśmy szerzej w wydaniu lutowym Nr 2 (298)). Firma JIE EURONORM posiada bardzo długą historię swoimi początkami sięgającą lat 30-tych ubiegłego wieku. Około 15 lat temu firma przeszła gruntowną przemianę skupiając się od tego czasu wyłącznie na technice napędowej, obierając sobie od początku za partnera grupę JIE. Przez 15 lat EURONORM budował swoją silną pozycję na rynkach zachodnioeuropejskich tj. Holandia, Belgia, Francja, Niemcy, zdobywając wiedzę, doświadczenie i zaufanie wśród bardzo wymagających klientów. Nasza firma to przede wszystkim ludzie tworzący już międzynarodową organizację, którzy swoim zaangażowaniem, wiedzą i indywidualnym podejściem do każdego projektu poszerzają horyzonty i oferują najlepsze rozwiązania swoim klientom. Warto dodać, że firmę budują w dużej mierze osoby polskiej narodowości, pracujący na co dzień w Holandii. Od tego roku JIE EURONORM jest obecny również na rynku polskim, gdzie posiada swoje biuro sprzedaży oraz przedstawicieli handlowych. Już na początku przyszłego roku otwieramy w Polsce również magazyn z centrum montażowo-serwisowym, aby stąd rozszerzyć ekspansję na inne kraje Europy Centralno-Wschodniej.

Dlaczego my?

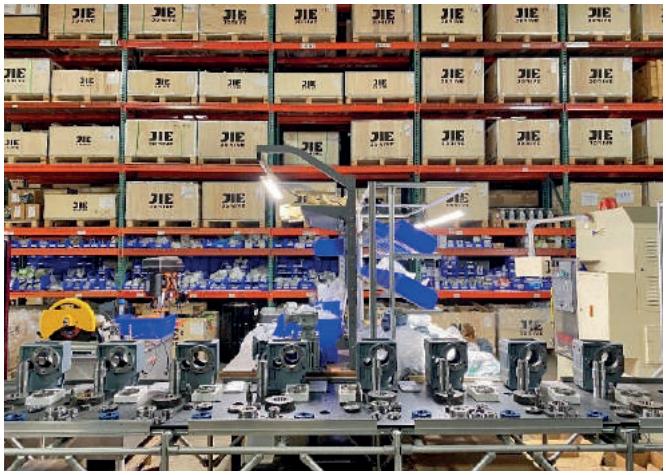
W swojej ofercie posiadamy szeroki zakres i najpopularniejsze przemysłowe rozwiązania z dziedziny techniki napędowej. Naszymi głównymi produktami są motoreduktory walcowe, w tym walcowe proste, walcowe płaskie, walcowo-stożkowe i walcowo-ślimakowe. Oprócz tego w ofercie posiadamy przekładnie ślimakowe i hipoidalne, silniki elektryczne, napędy nierdzewne, napędy planetarne, napędy *heavy-duty*, napędy wieńcowe, napędy ATEX oraz przemienniki częstotliwości i enkodery.

Jako JIE EURONORM:

- posiadamy bardzo duże zapasy magazynowe części i możliwości montażowe motoreduktorów walcowych z dostawami do 2 tygodni, od przyszłego roku uruchamiamy kolejny magazyn w Polsce;
- nasze motoreduktory walcowe, przekładnie ślimakowe i inne produkty są w pełni zamienne za czołowych producentów w każdym z tych rodzajów produktów, tzn. zamiana na nasze napędy



Konfigurator online (configurator.euronormportal.com) pozwala na dobór napędu we własnym zakresie, wygenerowanie modelu 3D oraz przygotowanie wstępnej oferty techniczno-handlowej (bez rabatu)



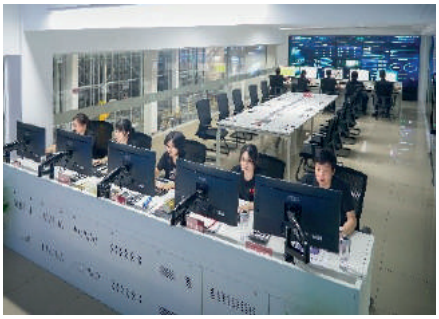
Magazyny z tysiącami komponentów gwarantują niezachwianą dostępność naszych produktów

Własna lakiernia pozwala na indywidualne podejście do kwestii powłok malarskich

Każde zamówienie jest profesjonalnie spakowane i zabezpieczone na czas transportu

nie wymaga żadnych zmian konstrukcyjnych;
- jesteśmy atrakcyjniejsi cenowo od naszej głównej niemieckiej konkurencji;
- nasze produkty są na tym samym najwyższym poziomie jakościowym co najlepsza konkurencja;
- wszystkim klientom oferujemy bezpłatne wysyłki zamówień od niskiego progu;
- nowym klientom oferujemy bardzo atrakcyjne warunki płatności;
- oferujemy elastyczne warunki gwarancyjne;
- oferujemy indywidualne podejście do każdego, nawet najmniejszego zapytania i projektu, dzięki naszemu centrum warsztatowemu w Holandii i fabryce w Chinach jesteśmy w stanie wykonać napędy pod specjalne wykonania;
- jesteśmy obecni na wielu rynkach Europy i mamy tam swoje przedstawicielstwa;
- nasze napędy oznaczane są Made in the Netherlands a silniki posiadają certyfikat CE (posiadamy również silniki z certyfikatami na rynek amerykański UL/CSA);
- na każdym kroku służymy pomocą i wsparciem, jak również



Nasza fabryka 4.0 w Hangzhou zapewnia produkcję zgodną z zasadami zrównoważonego rozwoju i w ekspresowym czasie realizuje wszelkie zamówienia pod nasze magazyny

posiadamy najczytelniejszy i intuicyjny konfigurator online, który ułatwia pracę konstruktorom, technikom i innym specjalistom – configurator.euronormportal.com.

Gdzie nas znaleźć?

W Polsce aktualnie posiadamy biuro sprzedaży zlokalizowane w Białej-Parceli (pod Wieluniem) i kilku mobilnych inżynierów wsparcia technicznego. Poza tym jesteśmy obecni na najważniejszych targach przemysłowych odbywających się na terenie Polski. Już po wakacjach będziecie mogli nas spotkać na targach:

- Recykling Tech Expo w Warszawie - 18 – 20.09.2024;
- SYMAS & MAINTENANCE w Krakowie – 16 – 17.10.2024;
- Warsaw Industry Week w Warszawie – 5 – 7.11.2024.

JIE EURONORM na targach Warsaw Industry Automatica w Warszawie

Od przyszłego roku w okolicach Wrocławia uruchamiamy również nasz magazyn i centrum montażowo-serwisowe.

Zapraszamy do odwiedzenia naszej strony internetowej www.jie-euronorm.com/pl/, gdzie znajdą Państwo wiele informacji o naszych produktach, konfigurator, wszelkie kontakty. Zapraszamy do kontaktu z nami i przesyłania zapytań ofertowych oraz w celu umówienia wizyty naszego przedstawiciela.

JIE EURONORM na targach ITM Industry Europe w Poznaniu

Michał Piśniak – manager sprzedaży Polska
m.pisniak@euronorm.nl
tel.: +48 692 476 519
JIE Euronorm BV
www.jie-euronorm.com/pl/

Tutaj bije serce branży drzewno-meblarskiej – 40. edycja targów DREMA już od 10 września w Poznaniu

Targi DREMA to najważniejsze i najbardziej wyczekiwane spotkanie branży drzewno-meblarskiej w Polsce i Europie Środkowo-Wschodniej. Edycja 2024 będzie kompleksową odpowiedzią na aktualne wyzwania rynku i promocją osiągnięć polskiego przemysłu.

Nadchodzące 4-dniowe spotkanie to nie tylko kluczowe wydarzenie dla profesjonalistów i pasjonatów, to także wyjątkowy jubileusz, który pokazuje, że polski przemysł przetrwał próbę czasu, pozostając główną konkurencją eksportową i produkcyjną na rynku światowym.

Międzynarodowe Targi Maszyn, Narzędzi i Komponentów dla Przemysłu Drzewnego i Meblarskiego DREMA są w czołówce najważniejszych wystaw światowych dedykowanych branży obróbki i przetwórstwa drewna. Jako jedyne wydarzenie w Polsce otrzymały rekomendację EUMABOIS, znajdując się wśród 10 wyróżnionych międzynarodowych ekspozycji, a także zakwalifikowane zostały do rekomendacji członkom Stowarzyszenia na 2024 rok.

– Rekomendację federacji EUMABOIS otrzymują tylko wybrane światowe wystawy. Jest to ogromne wyróżnienie, które znacząco podnosi prestiż targów DREMA, dając tym samym partnerom, wystawcom i zwiedzającym znacznie większe możliwości dotarcia do międzynarodowego środowiska i nawiązania kontaktów biznesowych z przedstawicielami szeroko pojętej branży drzewnej i meblarskiej z całego świata – podkreśla Andrzej Półrolniczak, dyrektor targów DREMA i DremaSilesia.

Co będzie się działo podczas nadchodzącego wydarzenia?

Już dzisiaj wiemy, że wydarzenie będzie wyjątkową okazją do spotkania w jednym miejscu niemal wszystkich znaczących polskich przedstawicieli branży, a także osób, które przez ostatnie 40 edycji targów przyczyniły się do tworzenia silnego

i odpowiedzialnego społecznie sektora. Swój udział potwierdzili już tacy wystawcy, jak: HOMAG, FELDER GROUP, ITA TOOLS, SCM, Lazzoni Group, ITA, OTTO MARTIN, Stowarzyszenie DROMA, BizeA.

W programie przewidzianych jest ponad 20 wydarzeń towarzyszących: konferencji i paneli dyskusyjnych dotyczących aktualnej sytuacji rynkowej oraz automatyzacji i mechanizacji procesów produkcyjnych w duchu Przemysłu 4.0. Pawilony targowe zostaną zagospodarowane na wystawę topowych marek – liderów technologii i rozwiązań. W specjalnych strefach odbędą się spektakularne pokazy pracy maszyn, jak Fabryka Mebli na Żywo, związana z akcją DREMA DZIECIOM. Swoją kontynuację będzie miała również akcja Las Dremy.

Bilety dostępne są już na stronie: tobilet.pl

Sprostowanie: >Nie przypisuję sobie wyłączności praw do utworu pt. „*Ograniczenie prądów łożyskowych*" opublikowanym w wydaniu 7/8/2023 miesięcznika „*Napędy i Sterowanie*". Jednocześnie wyjaśniam, że autorskie prawa majątkowe do tego utworu przysługują Sieć Badawcza Łukasiewicz – Górnośląskiemu Instytutowi Technologicznemu z siedzibą w Gliwicach<

Artur Polak

Nowa polska montownia przekładni i motoreduktorów

Od kilku lat z sukcesem rozwija swoją działalność polska firma Megadrive Sp. z o.o. z siedzibą w Wieluniu. Prowadzi montaż, sprzedaż i serwis wysokiej jakości przekładni i motoreduktorów przemysłowych, zamiennych do najbardziej rozpoznawanych na świecie marek niemieckich. Oferuje między innymi również napędy marki JIE. Wszystkie napędy sprzedawane są pod polską własną marką Megadrive.

Firma utrzymuje i wciąż rozbudowuje pokaźny magazyn części do budowy przekładni dostępnych od ręki. Oparcie montażu na własnym magazynie części pozwala oferować krótkie terminy realizacji dostaw oraz budowę przekładni dostosowanych do specyficznych potrzeb klientów.

Zachowanie standardu procesów zgodnie z ISO 9001 gwarantuje finalną jakość dostarczanych produktów na poziomie największych znanych firm.

Wysoka jakość produktów i wiedza techniczna w zakresie doradztwa, gwarantowane przez polską firmę, zapewniają klientom najlepszy możliwy w kraju serwis obsługi i elastyczność w działaniu, co stanowi główną przewagę na rynku zespołów napędowych.

- Szybki montaż na zamówienie.
- Zamienniki znanych marek.
- Serwis i remonty przekładni znanych producentów.
- Profesjonalne doradztwo w doborze odpowiedniego napędu.
- Stałe regularne dostawy i atrakcyjność kosztów.

MEGA DRIVE
INTELLIGENT DRIVE SOLUTIONS

MegaDrive Sp. z o.o.
ul. Sieradzka 62, 98-300 Wieluń
e-mail: biuro@megadrive.com.pl
tel. +48 (43) 821 89 85
tel. kom.: +48 885 884 854
www.megadrive.com.pl

Branża spawalnicza rozwinie się dynamicznie.

Nowe możliwości już wkrótce

Realizacja pierwszej edycji docelowo największych i najbardziej merytorycznych targów w branży spawalniczej wymaga doświadczonego organizatora i sprawdzonych partnerów. Sukces poprzedzony wieloletnią praktyką i uwierzytelnieniem umiejętności to w tych okolicznościach podstawa. Tym wyróżnia się Ptak Warsaw Expo. W dniach 3 – 5 września 2024 roku pod Warszawą odbędą się międzynarodowe targi Weld Tech, które zrewolucjonizują branżę spawalniczą, otwierając ją na dialog i pełnię biznesowych możliwości.

Aby nie być gołosłownym, warto sięgnąć po statystyki. Ptak Warsaw Expo od blisko dekady organizuje największe i najbardziej merytoryczne wydarzenia biznesowe w Polsce. Zdobyte doświadczenie i nieskazitelna reputacja przełożyły się na zbudowanie renomy nie tylko na szczeblu krajowym, ale również międzynarodowym. Dziś kompleks hal pod Warszawą uznawany jest za centralny punkt biznesowy w Europie. Zapracowano na to uznanie nie tylko rozmiarami zaplecza (sześć nowoczesnych hal targowych o powierzchni 143 000 m^2 oraz 500 000 m^2 powierzchni zewnętrznej), ale przede wszystkim konsekwencją w kreowaniu nastawionych na rozwój wydarzeń branżowych. Tych rocznie Ptak Warsaw Expo organizuje ponad siedemdziesiąt i dotyczą one najważniejszych sektorów dla polskiej przedsiębiorczości.

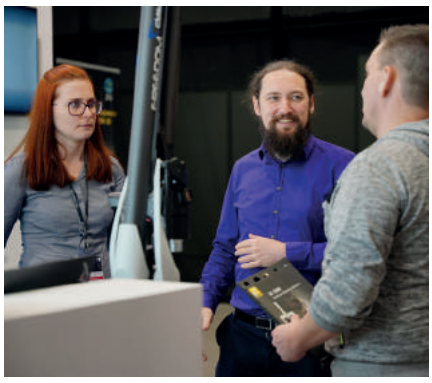
Ptak Warsaw Expo tworzy grupa ludzi, których łączy pasja do integracji biznesu. To właśnie sprawia, że wydarzenia organizowane pod Warszawą otwierają odwiedzających na nowe możliwości networkingowe i kontraktacyjne. Poza sektorem b2b organizowane są również imprezy dedykowane klientom detalicznym i komercyjnym, które z roku na rok pobijają rekordy popularności. Dowodem zdobytego zaufania są liczby – 1 000 000 odwiedzających i 10 000 wystawców.

W tym właśnie środowisku biznesowym powstał pomysł na Weld Tech, czyli pierwszą edycję merytorycznych, międzynarodowych targów poświęconych branży spawalniczej. Ptak Warsaw Expo jako organizator jest gwarantem jakości eventu i satysfakcji uczestników wydarzenia.

Branża spawalnicza przed wyzwaniami

Po okresie inflacyjnej stagnacji i słabości popytu zagranicznego polski przemysł ponownie stawia na inwestycje. Branże zaczynają znów decydować się na rozwój parków maszyn i urządzeń, przedsiębiorcy coraz śmielej korzystają z dobrodziejstw automatyzacji produkcji i wybierają często wymagającą inwestycji optymalizację procesów, która w szerszej perspektywie czasowej zwiększa jednak znacząco efektywność. Nie mają obaw odnośnie do korzystania z trendów i innowacji wprowadzanych na zagranicznych rynkach oraz wybierają rozwój w imię zwiększania konkurencyjności w przyszłości. Nie oznacza to jednak, że nie pojawiają się wyzwania, którym muszą sprostać.

Analitycy wskazują, że jednym z najważniejszych, z którymi mierzy się branża spawalnicza, jest brak wykwalifikowanych pracowników na polskim rynku. Najlepsi krajowi eksperci poszukują zatrudnienia między innymi w państwach skandynawskich. Znaleziono jednak na to rozwiązanie. Poszczególne przedsiębiorstwa stawiają na pozyskiwanie pracowników zagranicznych, szczególnie z Azji. Tamtejszy rynek bogaty jest bowiem w kapitał ludzki, co



pozwala na zapewnienie ciągłości produkcji i nieustanny rozwój poszczególnych biznesów. Nie zmienia to faktu, że „odzyskanie” polskiego pracownika jest celem dla wielu przedsiębiorców.

Jak wskazują eksperci, nowe szanse przed firmami działającymi w branży stawia również mocniejsze wejście Polski w projekty związane z energią atomową. Ten ruch może sprawić, że zwiększą się nadzieje analityków na powrót do wzrostu i ożywienie w sektorze.

Tym samym branża spawalnicza nie jest wolna od wyzwań, wątpliwości czy kwestii dotyczących przyszłości, które musi rozważyć. Jednocześnie powinna też wykorzystywać każdą szansę na rozwój. Ptak Warsaw Expo zorganizuje Weld Tech właśnie dlatego, by umożliwić to temu sektorowi przemysłu.

Branża spawalnicza się rozwija. Nowe możliwości już wkrótce podczas Weld Tech

Jak zatem Ptak Warsaw Expo zrealizuje obietnice rozwojowe pokładane w premierowej edycji Weld Tech? Zrobi to wielotorowo, bo takiego też podejścia do biznesu potrzeba w czasach dynamicznych zmian.

Podczas wydarzenia zostanie zorganizowana Międzynarodowa Konferencja Branży Spawalniczej. Podczas dwóch dni imprezy wykłady i analizy wygłosi osiemnastu prelegentów doświadczonych w tym sektorze przemysłu. Event zatytułowany „Spawalnictwo w erze cyfrowej (Przemysł 4.0)" podzielony zostanie na sesje.

Poruszonymi tematami będą technologie cyfrowe w spawalnictwie (automatyzacja i wykorzystanie AI), cyfrowe narzędzia w zarządzaniu procesami spawalniczymi (systemy zarządzania produkcją), wyzwania i perspektywy wdrażania Przemysłu 4.0 w spawalnictwie (case studies, szkolenia), czy przyszłość spawalnictwa w erze cyfrowej (realizowana jako panel dyskusyjny z udziałem branżowych ekspertów). W programie konferencji uwzględniono również czas na prezentacje ofert wystawców, dzięki czemu będą oni mogli promować swoje rozwiązania technologiczne, materiały czy usługi wśród uczestników wydarzenia.

Najwięksi będą obecni na Weld Tech. To czas dla biznesu wykorzystany do maksimum

Weld Tech będzie czasem dedykowanym przedsiębiorcom otwartym na nawiązywanie nowych kontaktów biznesowych. Networkingowy charakter eventu pozwoli porównać dostępne na rynku oferty i wprowadzić korzystne dla przedsiębiorców zmiany w zakresie łańcucha dostaw. Jednocześnie będzie to okazja do skrócenia dystansu profesjonalnego z liderami sektora i skorzystania z przygotowanych przez nich specjalnie na okoliczność eventu rabatów.

Weld Tech to narzędzie do prowadzenia marketingu jeden na jeden, utrwalania nawiązanych już kontaktów biznesowych i pozyskiwania wartościowych leadów z rynków zagranicznych. Dzięki otwarciu wydarzenia na międzynarodowych przedsiębiorców, każdy z uczestników stanie przed szansą na poznanie specyfiki europejskich odnóg sektora i znalezienie partnerów oraz inwestorów pozwalających na szerszy niż dotąd rozwój na Starym Kontynencie.

W gronie wystawców znajdą się między innymi BEAR, EAGLE, Bodor Laser China, EXPERA, STIGAL, Beboq Robotics, ELPLC, MENEGON, Air Liquide, EP LASER, SUMARIS, Kalla, EURO-BOX, RAIS-TOOLS, Delex Polska, GRADIENT POLSKA, CHOBOLA, Państwowe Przedsiębiorstwo Przemysłu Metalowego „Pomet", Maxphotonics Gmbh, H&S Maschinentechnik, IEBC Business Consulting (Beijing), Atlantic Welding Import & Export, Expowindow, WPI pro service, SYBIL GROUP, STALTEST POMORZE, Shenzhen Jianyi Automation oraz 3X Ceramic Parts Company Limited. Grono wystawców stale się powiększa. Szacuje się, że aż kilkanaście procent uczestników Weld Tech stanowić będą przedsiębiorcy zagraniczni.

Najnowsze technologie i innowacje podczas Weld Tech

Weld Tech będzie również okazją do wzięcia udziału w prezentacjach najnowszych technologii i innowacji. Zaplecze biznesowe Ptak Warsaw Expo zostanie wykorzystane do pokazania pełnego potencjału projektów. Przedsiębiorcy pochwalą się najciekawszymi rozwiązaniami w zakresie technologii spawalniczych, nowatorskimi urządzeniami i sprzętami do spawania, czy innowacyjnymi materiałami spawalniczymi. Zaprezentują też przykłady automatyzacji i robotyzacji w branży, urządzenia do cięcia gazowego, laserowego i plazmowego, produkty do zgrzewania i lutowania oraz sprzęt i akcesoria BHP dla spawalnictwa.

Tym samym każdy z przybyłych w jednym miejscu i czasie będzie mógł poznać najnowsze osiągnięcia branżowe z kraju i zagranicy przy jednoczesnym wykorzystaniu potencjału networkingowego wydarzenia do maksimum.

Rejestracja na Weld Tech wciąż trwa. Warto już dziś zapewnić sobie udział w wydarzeniu, które zagwarantuje branży spawalniczej moc nowych możliwości.

Weld Tech 3 – 5 września 2024 r., Ptak Warsaw Expo

Strona internetowa wydarzenia: weldexpopoland.com

XVIII edycja konkursu miesięcznika

napędy i sterowanie miesięcznik naukowo-techniczny

PRODUKT ROKU 2023

MEDALE ROZDANE!

Konkurs miesięcznika „Napędy i Sterowanie” PRODUKT ROKU 2023 – rozstrzygnięty!

Redakcja miesięcznika „Napędy i Sterowanie” pod patronatem Katedry Automatyki i Robotyki AGH, zorganizowała kolejną edycję konkursu na najlepsze rozwiązanie – **PRODUKT ROKU 2023**.

Przedsięwzięcie związane jest z ideą wydawnictwa, mającą na celu wyróżnienie nowych rozwiązań technicznych oraz zaprezentowanie ich czytelnikom.

Więcej na **www.nis.com.pl**

Organizując kolejną edycję konkursu postanowiliśmy uhonorować producentów, którzy wzbogacili polski rynek techniczny o innowacyjne rozwiązania. Jednocześnie postawiliśmy sobie za cel przybliżyć Państwu produkty, które obecnie są oferowane na rynku.

Polskie firmy opracowują rozwiązania na światowym poziomie. Powstał szereg rozwiązań we współpracy firm polskich i partnerów europejskich. Wiodące firmy automatyki na rynku światowym wprowadzają rozwiązania, z których korzysta polski przemysł. Konkurs NiS PRODUKT ROKU 2023 pokazuje światowe trendy w automatyce i rozwiązania wprowadzane do polskiego przemysłu. Jest on doskonałą okazją do zaprezentowania szerokiej publiczności innowacyjnych produktów. Stanowi również narzędzie służące zmianie postaw i świadomości w zakresie potrzeby wdrażania innowacji i korzyści wynikających ze współpracy sektora biznesu i nauki. Adresatami przedsięwzięcia były przedsiębiorstwa reprezentujące nowatorskie rozwiązania i myśli techniczne, które z pewnością wzbogacą polski przemysł.

Produkty i rozwiązania zgłoszone do konkursu ocenione zostały przez niezależne jury podczas posiedzenia, które odbyło się 6 maja 2024 r. w Katedrze Automatyki i Robotyki, Wydziale Elektrotechniki, Automatyki, Informatyki i Inżynierii Biomedycznej na AGH w Krakowie.

Członkowie komisji:

- prof. dr hab. inż. Krzysztof Oprzędkiewicz
- prof. zw. dr hab. inż. Ryszard Tadeusiewicz
- prof. dr hab. inż. Witold Byrski

Komisja konkursowa podczas analizy produktów brała pod uwagę innowacyjność danego produktu, możliwy krótki okres stosowania na świecie, potencjał rozpowszechniania, podnoszenie efektywności w działaniu i bezpieczeństwa.

Założenia te były podstawą zgłoszonych produktów.

Nagrody – medale oraz dyplomy przyznane zostały w następujących kategoriach:

- NOWE MASZYNY I TECHNOLOGIE
- POPRAWA BEZPIECZEŃSTWA
- NAPĘDY I SILNIKI
- SYSTEMY STEROWANIA PROCESAMI I UKŁADAMI
- URZĄDZENIA POMIAROWE I CZUJNIKI

Nagrodzone produkty z pewnością będą inspiracją dla nowych projektów, wdrożeń pozwalających na sprawniejszą i bardziej efektywną produkcję.

W imieniu całej redakcji pisma uczestnikom konkursu, jego zwycięzcom serdecznie gratulujemy innowacyjnych, nowoczesnych rozwiązań.

Na kolejnych stronach pisma zapraszam Państwa do szerszej lektury na temat produktów konkursowych.

Członkowie komisji przyznali nagrody w każdej z pięciu niżej wymienionych kategorii:

Nowe maszyny i technologie

Sieć Badawcza Łukasiewicz – Instytut Technik Innowacyjnych EMAG
Laboratorium oceny bezpieczeństwa produktów teleinformatycznych ITSEF-EMAG

Grenevia SA FAMUR Oddział w Katowicach
Stacja najazdowo-zwrotna FAMUR UPZP

Multiprojekt Automatyka Sp. z o.o.
Chwytak GMO1 LinMot

Poprawa bezpieczeństwa

Pepperl+Fuchs Sp. z o.o.
System ultradźwiękowych czujników USi-safety

Pilz Polska Sp. z o.o.
Kompleksowy system wyboru trybu pracy i kontroli uprawnień dostępu IAM (Identification and Access Management)

Napędy i silniki

Sieć Badawcza Łukasiewicz – Górnośląski Instytut Technologiczny
Seria innowacyjnych, ultralekkich silników LEMoK

Systemy sterowania procesami i układami

Lenze Polska
Sterownik c430

Urządzenia pomiarowe i czujniki

Pepperl+Fuchs Sp. z o.o.
Czujnik LiDAR z serii R2300

SMC Industrial Automation Polska
System Zarządzania Sprężonym Powietrzem serii AMS20/30/40/60

Pilz Polska Sp. z o.o.

Lenze Polska

Sieć Badawcza Łukasiewicz – Górnośląski Instytut Technologiczny

SMC Industrial Automation Polska

Multiprojekt Automatyka Sp. z o.o.

Pepperl+Fuchs Sp. z o.o.

Nagrodzone produkty z pewnością będą inspiracją dla nowych projektów, wdrożeń pozwalających na sprawniejszą i bardziej efektywną produkcję.

NOWE MASZYNY I TECHNOLOGIE

Sieć Badawcza Łukasiewicz – Instytut Technik Innowacyjnych EMAG

Laboratorium oceny bezpieczeństwa produktów teleinformatycznych ITSEF-EMAG

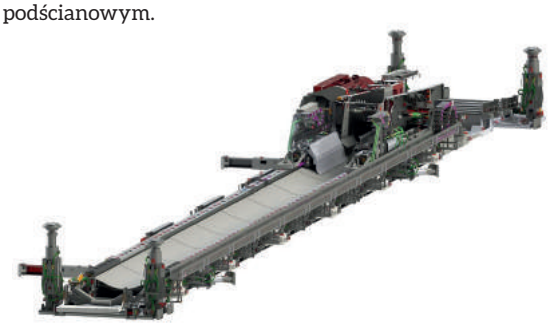
Akredytacja PCA nr AB 1781 na wykonywanie badań zgodnie z normami PN-EN ISO/IEC 15408 (Common Criteria – CC), PN-EN ISO/IEC 18045 (Common Evaluation Methodology – CEM), PN-EN IEC 62443-4-2 (Technical security requirements for IACS). Źródła innowacyjności: pierwsze w Polsce laboratorium z akredytacją IEC 62443-4-2; opracowanie i wdrożenie metodyki oceny IACS na bazie norm CC i CEM oraz lekkiego programu oceny IACS.

NOWE MASZYNY I TECHNOLOGIE

Grenevia SA FAMUR Oddział w Katowicach

Stacja najazdowo-zwrotna FAMUR UPZP

Dotychczasowe podejście do automatyzacji eksploatacji pokładów systemem ścianowym koncentrowało się głównie na automatycznym postępie sekcji zmechanizowanych oraz pracy kombajnu ścianowego, pozostawiając nierozwiązany problem przenośnika podścianowego (PZP), który to musiał być podciągany ręcznie, w czasie kiedy następował postęp sekcji w ścianie. Wdrożona stacja najazdowo-zwrotna FAMUR UPZP wykonuje samoczynne nadążne podciąganie przenośnika PZP w takt pracy sekcji zmechanizowanej, dzięki czemu unika się naprężeń mechanicznych w obszarze skrzyżowania przenośnik ścianowy z podścianowym.



NOWE MASZYNY I TECHNOLOGIE

Multiprojekt Automatyka Sp. z o.o.

Chwytak GMO1 LinMot

Chwytak GM01 jest złożony z dwóch wytrzymałych tubowych silników liniowych, umożliwia dostosowanie do różnorodnych zadań, oferując niezrównaną elastyczność w wymagających aplikacjach. Jego higieniczna konstrukcja i stopień ochrony IP69 sprawiają, że idealnie nadaje się do przemysłu spożywczego, zapewniając bezpieczeństwo chwytanych produktów. Dodatkowo możliwość precyzyjnego dostosowania chwytaka do specyficznych potrzeb użytkownika podkreśla jego unikalność na rynku.

POPRAWA BEZPIECZEŃSTWA

Pepperl+Fuchs Sp. z o.o.

System ultradźwiękowych czujników USi-safety

USi®-safety to jedyny bezpieczny system czujników ultradźwiękowych zgodny z normą EN ISO 13849 kategorii 3 PL d. Umożliwia on niezawodne monitorowanie przestrzeni trójwymiarowych, dzięki czemu idealnie nadaje się do zastosowania w sprzęcie transportu bliskiego. Czujniki są niezwykle małe i mogą być dowolnie pozycjonowane, co oznacza, że można je odłączyć od interfejsu sterującego w celu elastycznego pozycjonowania w skrajnie wąskiej przestrzeni ramion wideł. Interfejs sterujący posiada dwa bezpieczne wyjścia OSSD na kanał dla regulowanego pola ochronnego oraz jedno wyjście przełączające PNP dla pola ostrzegawczego.
Eliptyczne pole akustyczne przetwornika ultradźwiękowego ma kąt rozwarcia ±17° i ±5°. Zostało ono zoptymalizowane do monitorowania zakresu 3D i dlatego – w przeciwieństwie do skanerów laserowych – doskonale nadaje się do wykrywania przeszkód, które zwisają z góry na pasie ruchu lub są uniesione nad ziemią. Jeśli system USi®-safety jest zamontowany na kilku niezależnych pojazdach AGV, których ścieżki przecinają się nawzajem, to wzajemne tłumienie zakłóceń zapobiega zakłócaniu ich pracy. Połączenie fizyczne pomiędzy systemami USi®-safety jest zatem zbędne.

POPRAWA BEZPIECZEŃSTWA

Pilz Polska Sp. z o.o.

Kompleksowy system wyboru trybu pracy i kontroli uprawnień dostępu IAM (Identification and Access Management)

Rozwiązanie stanowi alternatywę dla konwencjonalnych systemów lockout-tagout (LOTO) do zabezpieczenia procesu, zapobiega nieoczekiwanemu uruchomieniu maszyn, dopóki ludzie znajdują się w strefie zagrożenia. Realizowane jest za pomocą technologii RFID – specjalne klucze z odpowiednimi uprawnieniami i listą bezpieczeństwa w sterownikach Pilz pozwalają na dostęp do strefy pracy maszyny tylko upoważnionym operatorom. W pełni elektroniczne zabezpieczenie eliminuje potrzebę stosowania mechanicznych blokad i znaków ostrzegawczych.
Aby wejść do instalacji operator dokonuje uwierzytelnienia za pomocą klucza transponderowego (PITreader key) na urządzeniu PITreader. Identyfikator bezpieczeństwa użytkownika jest zapisywany na liście bezpieczeństwa w sterowniku Pilz (PNOZmulti 2 lub PSS 4000). Maszyna może zostać wyłączona i operator może bezpiecznie wejść do środka. W tym czasie operator zatrzymuje przy sobie klucz transponderowy. Aby ponownie uruchomić instalację, wszystkie osoby po wyjściu ze strefy pracy maszyny muszą wylogować się za pomocą swojego klucza transponderowego. Następnie lista bezpieczeństwa zostaje skasowana i maszyna zostaje odblokowana.

NAPĘDY I SILNIKI

Sieć Badawcza Łukasiewicz – Górnośląski Instytut Technologiczny

Seria innowacyjnych, ultralekkich silników LEMoK

Przedmiotem zgłoszenia jest seria innowacyjnych, ultralekkich silników LEMoK o ponadprzeciętnym współczynniku gęstości mocy. Seria opracowanych rozwiązań obejmuje zarówno silniki z magnesami trwałymi, jak również silniki uniezależnione od magnesów trwałych tj. silnik indukcyjny (IM) oraz silnik synchroniczny reluktancyjny (SynREL). Silniki serii LEMoK charakteryzują się najwyższą w swojej klasie wartością mocy w stosunku do swoich gabarytów i masy, niespotykanych do tej pory na rynku polskim.

SYSTEMY STEROWANIA PROCESAMI I UKŁADAMI

Lenze Polska

Sterownik c430

Sterownik c430 posiada nowoczesne narzędzie programowania i gotowe moduły technologiczne FAST, skracające czas tworzenia aplikacji. Obsługuje nowoczesne sieci oparte o Ethernet. Zawiera wbudowane w system operacyjny usługi zarządzania błędami, modułami, licencjami oraz zasobami. Oparte na technologii WEB rozwiązanie HMI pozwala na tworzenie wizualizacji z atrakcyjnym UX. Edytor parametrów umożliwia łączenie zmiennych IEC ze specyfikacjami towarzyszącymi OPC UE bez konieczności programowania.

URZĄDZENIA POMIAROWE I CZUJNIKI

Pepperl+Fuchs Sp. z o.o.
Czujnik LiDAR z serii R2300

Nowy czujnik LiDAR R2300 o częstotliwości skanowania 100 Hz – idealny do zastosowań wymagających dużej prędkości. Skaner jednowarstwowy R2300 osiąga tę wyjątkowo wysoką szybkość skanowania dzięki skanowaniu tylko jednej warstwy. Czujnik oferuje takie samo połączenie wysokiej wydajności i oszczędności kosztów, jakie charakteryzują wielowarstwowe skanery serii R2300. Podstawą jest technologia impulsowego pomiaru odległości (PRT) opracowana przez firmę Pepperl+Fuchs. PRT jest rozwiązaniem klasycznej technologii czasu przelotu, która zapewnia szybkie i precyzyjne wyniki pomiarów z ponad 250 000 emitowanych impulsów laserowych na sekundę. Metoda ta działa niezawodnie nawet w zmieniających się warunkach otoczenia. Bardzo dobra rozdzielczość kątowa 0,1° i mała plamka świetlna zapewniają wysoką precyzję podczas nawigacji, pozycjonowania i wykrywania. Jako ekonomiczny czujnik LiDAR R2300 jednocześnie oferuje optymalny stosunek ceny do wydajności.

URZĄDZENIA POMIAROWE I CZUJNIKI

SMC Industrial Automation Polska
System Zarządzania Sprężonym Powietrzem serii AMS20/30/40/60

System Zarządzania Sprężonym Powietrzem (Air Management System) serii AMS20/30/40/60 to system zarządzania, który ma na celu redukcję kosztów i automatyczną optymalizację zużycia sprężonego powietrza na liniach produkcyjnych. Dzięki monitorowaniu i optymalizacji zużycia można zredukować koszty wytwarzania powietrza. Digitalizacja i monitorowanie zużycia powietrza w czasie rzeczywistym daje pełny obraz kondycji maszyn. Stały monitoring stanu technicznego maszyn pozwala na szybkie wykrycie strat. Dzięki optymalizacji zużycia powietrza można zmniejszyć emisję CO_2.

Pilz Polska

System identyfikacji i zarządzania uprawnieniami dostępu IAM

System IAM (Identification and Access Management) to najnowsze rozwiązanie firmy Pilz, które pozwala realizować indywidualne wymagania w zakresie bezpieczeństwa maszyn i bezpieczeństwa przemysłowego za pomocą szerokiej gamy komponentów sprzętowych i programowych. Wszystko zgodnie z wymaganiami Rozporządzenia UE w sprawie maszyn 2023/1230. System opiera się na znanych już urządzeniach PITreader (czytnik kluczy) czy PIT 4SEU (jednostka analizująca dla trybu pracy), a także współpracujących z nimi kluczy RFID.

ZABEZPIECZENIE DOSTĘPU DLA OSÓB NIEUPRAWNIONYCH

Rozwiązanie zapewniające bezpieczny dostęp do maszyny bazuje na systemie PITreader wraz z urządzeniem do ryglowania PSENmlock (w wersji autonomicznej lub ze zintegrowanym czytnikiem w kasetce PITgatebox) oraz przekaźnikiem bezpieczeństwa. Operator w celu dokonania ingerencji w strefę pracy maszyny musi ją zatrzymać i odblokować rygiel. Aby to zrobić najpierw musi użyć czytnika klucza RFID. Jeżeli dane zapisane na kluczu umożliwiają wejście w strefę, czytnik potwierdzi zielonym światłem prawidłowość klucza, a operator po wciśnięciu żądania zatrzymania może odblokować rygiel. Jeżeli system nie rozpozna u operatora odpowiednich uprawnień do obsługi danej strefy, odblokowanie rygla nie będzie możliwe.

Rozwiązanie to pozwala zapewnić kontrolę nad tym, kto może odryglować / zaryglować zamek, wejść w strefę pracy maszyny, zatrzymać proces czy zresetować maszynę. Uprawnienia do obsługi takiego obszaru nadawane są pracownikowi po odpowiednim przeszkoleniu, a następnie przypisywane są do klucza RFID i weryfikowane są w stacji PITreader. Uprawnienia można zapisywać na kluczu RFID przypisanym do danego pracownika. Można również nadawać im terminowość. Czytnik PITreader wykrywa wszelkie nieprawidłowości przy próbie podjęcia pracy na maszynie lub wejścia w obszar chroniony.

FUNKCJE SYSTEMU IAM

Wykorzystanie klucza elektronicznego w systemie IAM zabezpiecza przed niekontrolowanym startem maszyny.

Operator wchodząc w poszczególne strefy loguje się do systemu i chowa klucz do kieszeni. Do momentu, kiedy nie opuści strefy i nie wyloguje się z systemu, nie ma możliwości zresetowania czy uruchomienia maszyny. Do takiej strefy może zalogować się maksymalnie 20 użytkowników uprawnionych do pracy w danej strefie. Wykorzystanie klucza elektronicznego niesie ze sobą wiele zalet w stosunku do standardowego klucza. Zagubiony klucz można w szybki sposób odtworzyć. Istnieje też możliwość łatwego kodowania różnych uprawnień przy wymaganiach dla różnych stref (czego nie zapewnia klucz mechaniczny). Operator nie musi też wychodzić ze strefy tymi samymi drzwiami, którymi wszedł, co w przypadku rozległych obszarów (np: magazyny) jest dużą oszczędnością czasu.

Wykorzystanie systemu IAM wpływa również na poprawę produktywności i wydajności – pracownicy z przypisanymi personalnie kluczami RFID stają się bardziej identyfikowalni, a co za tym idzie bardziej odpowiedzialni i świadomi działań wykonywanych na maszynie. Zaletą dla kadry menadżerskiej z kolei jest informacja o tym, kto i w jakim czasie był w danej strefie i jakie czynności wykonywał na maszynie. Przekłada się to na pracę zgodnie ze standardami danej maszyny, co zwiększa nie tylko bezpieczeństwo, ale także zmniejsza liczbę nieplanowanych zatrzymań.

Nowością systemu jest możliwość zarządzania uprawnieniami i zmianami w formie sieciowej, co zdecydowanie skraca czas potrzebny na obsługę (dotychczas wprowadzanie zmian wymagało ingerencji w każdy pojedynczy czytnik PITreader). Zmiany są załadowane do bazy danych, która w sposób ciągły komunikuje się z czytnikami pozwalając uwzględnić nowe ustawienia bez zbędnego programowania czytnik po czytniku. System IAM ma również możliwość obsługi kart identyfikacyjnych czy znaczników w formie naklejki oraz doposażono go w klucze o różnej kolorystyce, co ułatwia podział na grupy wśród personelu.

Dzięki systemowi wyboru trybu pracy i kontroli uprawnień dostępu można realizować indywidualne wymagania w zakresie bezpieczeństwa maszyn i bezpieczeństwa przemysłowego za pomocą szerokiej gamy komponentów sprzętowych i programowych. Wszystko zgodnie z wymaganiami Rozporządzenia UE w sprawie maszyn 2023/1230.

Więcej o rozwiązaniu:

System Zarządzania Sprężonym Powietrzem serii AMS20/30/40/60

System Zarządzania Sprężonym Powietrzem firmy SMC seria AMS20/30/40/60 ma na celu redukcję kosztów i automatyczną optymalizację zużycia sprężonego powietrza.

Kilka informacji na temat tego produktu:

- **Redukcja kosztów:** System serii AMS20/30/40/60 został zaprojektowany w celu zmniejszenia kosztów wytwarzania sprężonego powietrza. Dzięki monitorowaniu i automatycznej optymalizacji zużycia sprężonego powietrza na maszynie produkcyjnej można osiągnąć oszczędności energetyczne sięgające nawet 62% mniejszego zużycia sprężonego powietrza.

- **Digitalizacja i monitorowanie:** W/w system umożliwia digitalizację i monitorowanie zużycia powietrza w czasie rzeczywistym. Dzięki temu można uzyskać pełny obraz zużycia powietrza w systemie pneumatycznym i zidentyfikować obszary lub miejsca, w których można dokonać ulepszeń i oszczędności. Ponadto posiada możliwość wysyłania danych po różnych protokołach komunikacyjnych stosowanych we współczesnych zakładach produkcyjnych, np.: Ethernet/IP™, PROFINET, EtherCAT czy OPC UA. Stały monitoring stanu technicznego maszyn pozwala na szybkie wykrycie nieszczelności i rozwiązanie problemów z żywotnością komponentów pneumatycznych, co przyczynia się do utrzymania efektywności i niezawodności produkcji.

- **Dostosowanie się do norm emisji CO_2**: System AMS20/30/40/60 to innowacyjne rozwiązanie, które optymalizuje i kontroluje ciśnienie, przepływ i temperaturę dostarczanego sprężonego powietrza do urządzeń oraz został zaprojektowany z myślą o eliminacji strat energii, a przy tym spełnieniu norm emisji CO_2. Dzięki optymalizacji zużycia sprężonego powietrza w postaci np.: redukcji ciśnienia, odcięcia zasilania w stanach nieprodukcyjnych można zmniejszyć emisję dwutlenku węgla i przyczynić się do ochrony naszego środowiska.

- **Bezprzewodowa komunikacja**: System Zarządzania Sprężonym Powietrzem może być wykorzystywany do przekazywania danych dotyczących zużycia powietrza, stanu technicznego urządzeń, alarmów lub ostrzeżeń w czasie rzeczywistym. Może to również umożliwiać zdalne sterowanie i konfigurację systemu, co pozwala na szybką reakcję na zmiany warunków pracy lub awarie. Bezprzewodowe rozwiązania komunikacyjne mogą być szczególnie przydatne w przypadku systemów rozproszonych lub zlokalizowanych w trudno dostępnych miejscach, gdzie instalacja przewodów komunikacyjnych może być utrudniona lub kosztowna.

SMC Industrial Automation Polska Sp. z o.o.
ul. S. Batorego 10A Pass
05-870 Błonie
tel. +48 22 344 40 00
www.smc.pl

Laboratorium oceny bezpieczeństwa produktów teleinformatycznych ITSEF-EMAG

Laboratorium ITSEF posiada akredytację nr AB 1781 PCA na zgodność z następującymi normami:

- PN-EN ISO/IEC 15408, Common Criteria;
- PN-EN ISO/IEC 18045, Common Evaluation Methodology;
- PN-EN IEC 62443-4-2, Technical security requirements for IACS components.

Laboratorium ITSEF wykonuje oceny cyberbezpieczeństwa w zakresie powyższych norm w zakresie:

1. Produktów teleinformatycznych zgodnie z międzynarodowym standardem Common Criteria (ISO/IEC 15408) oraz metodyką oceny CEM (ISO/IEC 18045) na poziomach uzasadnionego zaufania od EAL 1 do EAL 4;
2. Komponentów systemów sterowania i automatyki przemysłowej zgodnie z wymaganiami normy IEC 62443-4-2.

Laboratorium ITSEF powstało w wyniku realizacji projektu badawczego pt.: „Krajowy schemat oceny i certyfikacji bezpieczeństwa oraz prywatności produktów i systemów IT zgodny z Common Criteria (KSO3C)" w latach 2018 – 2022. Projekt był realizowany przez konsorcjum, w skład którego wchodziły: Instytut Łączności – PIB jako lider projektu oraz Naukowa i Akademicka Sieć Komputerowa – PIB i Łukasiewicz – EMAG. Projekt został sfinansowany przez Narodowe Centrum Badań i Rozwoju w ramach II programu „CyberSecIdent – Cyberbezpieczeństwo i eTożsamość".

Wynikiem projektu jest także pierwszy krajowy program oceny i certyfikacji bezpieczeństwa produktów teleinformatycznych, który posiada status autoryzowanego w ramach europejskiego porozumienia SOG-IS oraz światowego porozumienia CCRA. Oznacza to, że sprawozdania z badań wykonanych w laboratorium oraz certyfikaty wydane w ramach polskiego programu są uznawane przez wszystkich członków tych porozumień. Ponadto program oceny stosowany w laboratorium zgodny jest z pierwszym europejskim programem oceny i certyfikacji EUCC, który został przyjęty aktem implementacyjnym w styczniu 2024 r.

Laboratorium ITSEF prowadzi akredytowane badania oceny bezpieczeństwa na 4 poziomach uzasadnionego zaufania EAL 1 – 4 dla produktów w postaci oprogramowania oraz sprzętowo-programowych, które pokrywają poziomy bezpieczeństwa istotny i wysoki zgodnie z Aktem o cyberbezpieczeństwie.

Laboratorium ITSEF wdrożyło także do swojej praktyki tzw. „lekki" program oceny bezpieczeństwa dla IACS, który spełnia założenie, że ocena produktu wykonywana jest nie dłużej niż 50 dni roboczych, co przekłada się na niski koszt oceny. Lekki program oceny jest wynikiem projektu badawczo-rozwojowego pt. „System oceny i certyfikacji cyberbezpieczeństwa – lekkie programy certyfikacji" (CybeBEAM).

Źródłami innowacyjności laboratorium ITSEF są efekty następujących działań:

- Udzielenie pierwszej w Polsce akredytacji dla badań produktów IACS w oparciu o normę IEC 62443-4-2 na poziomie bezpieczeństwa SL 1 oraz wykorzystywanie w praktyce lekkiego programu oceny (wdrożenie CyberBEAM);
- Wdrożenie do praktyki laboratorium metody oceny produktów IACS zbudowanej na podstawie adaptacji Common Criteria i metodyki oceny CEM do przemysłowych wymagań bezpieczeństwa;
- Innowacyjność metodyki oceny bezpieczeństwa produktów IACS na bazie zharmonizowanych norm CC i CEM.

Obecnie trwają prace w ITSEF nad opracowaniem programu oceny i certyfikacji producentów komponentów IACS w oparciu o standard IEC 62443-4-1, który obejmuje wymagania tworzenia bezpiecznego produktu w całym jego cyklu życia.

Łukasiewicz EMAG

Sieć Badawcza Łukasiewicz – Instytut Technik Innowacyjnych EMAG
ul. Leopolda 31
40-189 Katowice
tel. + 48 32 20 07 600
emag@emag.lukasiewicz.gov.pl
emag.lukasiewicz.gov.pl

Multiprojekt. Chwytak GMO1 LinMot

Chwytak GM01 od LinMot służy do precyzyjnego pobierania oraz przenoszenia produktów. Urządzenie wyróżnia się dużą elastycznością ustawień i idealnie sprawdzi się w wymagających warunkach. Delikatne zaciskanie i transportowanie produktów suchych, wilgotnych, twardych lub miękkich odbywa się bez pozostawiania zauważalnych śladów. Za sprawą higienicznej konstrukcji i wysokiego stopnia ochrony IP69 chwytak można łatwo wyczyścić. Te wszystkie cechy sprawią, że komponent od LinMot idealnie sprawdzi się w przemyśle spożywczym.

Chwytak GM01 umożliwia wykrywanie położenia chwytaka i kontrolę jego siły zaciskania, co pozwala chwycić nawet nierówne produkty. Za pomocą monitorowania można wykryć „w locie" wadliwe pochwycenie, a nawet wadliwe części. Szeroki zakres monitorowania chwytaka jest niezbędny w aplikacjach o wysokim stopniu automatyzacji.

Cechy charakterystyczne chwytaka:

- Zgodne czasy otwierania i zamykania przy wyjątkowo wysokiej dynamice i dużych wydajnościach;
- Wysoka dokładność mocowania produktów zarówno jednolitych, jak i niejednorodnych;
- Dedykowany wymagającym branżom takim jak przemysł farmaceutyczny, spożywczy i automatyka;
- Wysoka niezawodność procesu dzięki monitorowaniu danych takich jak siła, dystans i temperatura silnika;
- Łatwość mycia zgodnie z zaleceniami odnośnie czyszczenia produkcyjnego;
- Prosta integracja oraz dostosowanie do indywidualnych formatów produkcji i pakowania.

Chwytak GM01 to kolejny komponent, który wchodzi w skład produktów ze stali nierdzewnej od LinMot. Chwytak w połączeniu z prowadnicą SM01 może stworzyć kompletną aplikację typu „pick and place". Co ważne, powstałe rozwiązanie jest wyjątkowo odporne na chemikalia i wyróżnia się dużą żywotnością nawet w trudnych warunkach.

MultiProjekt

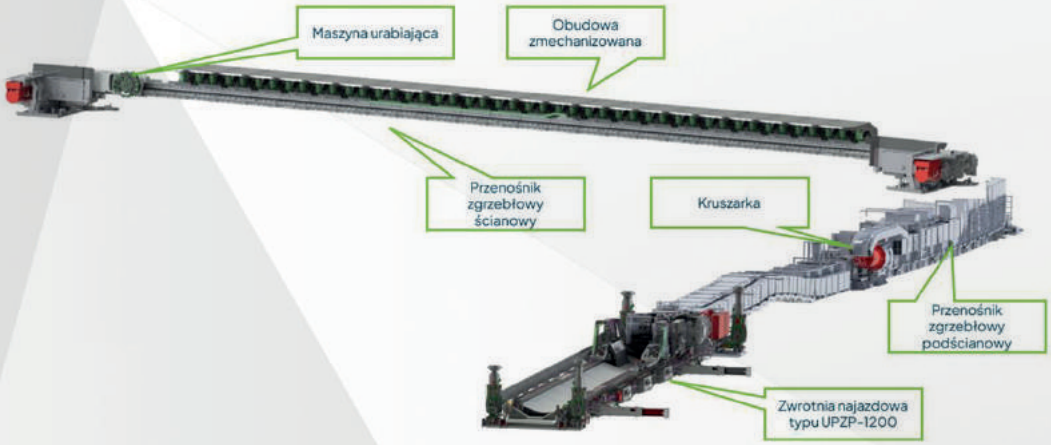
Multiprojekt Automatyka Sp. z o.o.
ul. Pilotów 2E
31-462 Kraków

FAMUR
Grenevia SA

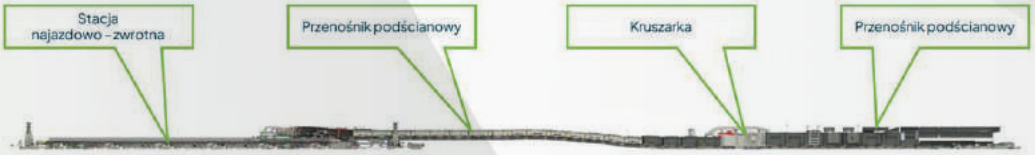
Stacja najazdowo-zwrotna UPZP-1200

Dążąc do poprawy warunków pracy, zwiększenia wydajności i zmniejszenia potrzeby interwencji ludzkiej w trudnych warunkach wydobywczych rozpoczęto automatyzację pracy maszyn kompleksu ścianowego. Jednakże mając na uwadze osiągnięcie satysfakcjonującego efektu, automatyzacja objęła nie tylko maszyny pracujące w ścianie tj. przenośnik ścianowy, maszynę wydobywczą oraz sekcje zmechanizowane, ale również maszyny w chodniku odstawczym.

FAMUR zaproponował rozszerzenie automatyzacji prac także o maszyny umieszczone w chodniku odstawczym tj. przenośnik podścianowy, kruszarkę oraz stację najazdowo -zwrotną. Rozwiązanie automatycznej maszyny w chodniku w tym stacji najazdowo-zwrotnej jest kluczowe dla automatyzacji pracujących ścian w trybie automatycznym.



Rys. 1. Maszyny zautomatyzowanego kompleksu ścianowego



Rys. 2. Zautomatyzowane maszyny pracujące w chodniku odstawczym

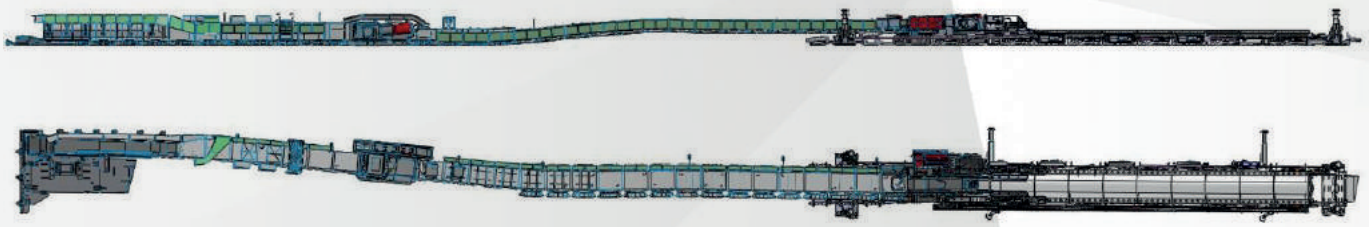
Opis

Urządzenie Przekładkowe typu UPZP-1200, które umożliwia przesuwanie w całości wysypu przenośnika ścianowego, przenośnika podścianowego względem zwrotni przenośnika taśmowego wraz z postępem ściany oraz zwrotni przenośnika taśmowego względem przenośnika podścianowego w procesie skracania taśmy.

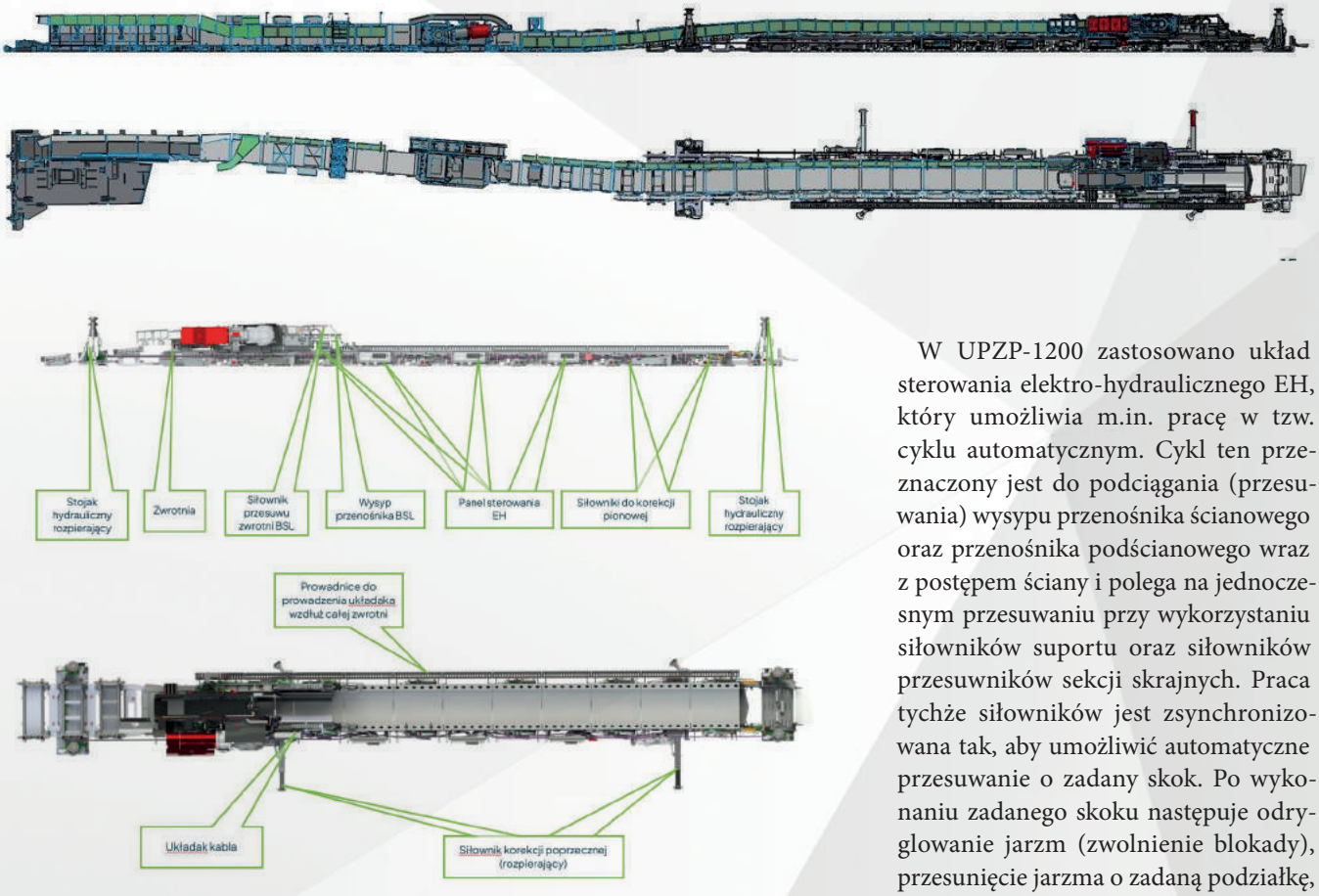
Wykonane jest z przegubowo połączonych segmentów, które tworzą trasę dla przesuwającego się suportu z jarzmami, umożliwiających ryglowanie ich w listwach segmentów trasy. Na suporcie zamocowany jest kadłub napędu wysypowego przenośnika podścianowego. Do przesuwu suportu zastosowane są siłowniki hydrauliczne.

Automatyzacja pracy w chodniku:

1. Krok początkowy: stacja najazdowo-zwrotna wysunięta



2. Krok końcowy: stacja najazdowo-zwrotna wsunięta



Rys. 3. Stacja najazdowa UPZP 1200 – budowa

Tabela 1. Dane techniczne UPZP-1200

Nachylenie podłużne	Maks. ±12°
Nachylenie poprzeczne	Maks. ±5°
Pofałdowanie (muldy)	Maks. ±3°
Szerokość taśmy przenośnika taśmowego	1 200 lub 1 000 [mm]
Średnica bębna członu zwrotnego	500 [mm]
Jednorazowy skok przesuwu	0.63 [m] (co 0,315 [m])
Sumaryczny skok przesuwu	do maks. 20 [m]
Zasilanie układu hydraulicznego	Emulsją z magistrali
Ciśnienie zasilania	32 [MPa]
Siły występujące przy wykorzystaniu siłowników hydraulicznych	
Siła nasuwająca przenośnik	2 156 [kN]
Siła wysuwająca UPZP-1200	2 650 [kN]
Siła poziomująca w członie z poziomowaniem	674 [kN]
Siła rozpierająca w mechanizmie do korekcji poprzecznej	458 [kN]
Siła rozpierająca w zespole rozpierającym	3 142 [kN]
Siła wsuwająca blokadę (jarzmo)	100 [kN]
Siła wysuwająca blokadę (jarzmo)	141 [kN]
Wymiary gabarytowe	
Długość maks.	maks. 36.192 [m]
Wysokość z napędem BSL	1.847 [m]
Masa maks.	maks. 71977,7 [kg]

W UPZP-1200 zastosowano układ sterowania elektro-hydraulicznego EH, który umożliwia m.in. pracę w tzw. cyklu automatycznym. Cykl ten przeznaczony jest do podciągania (przesuwania) wysypu przenośnika ścianowego oraz przenośnika podścianowego wraz z postępem ściany i polega na jednoczesnym przesuwaniu przy wykorzystaniu siłowników suportu oraz siłowników przesuwników sekcji skrajnych. Praca tychże siłowników jest zsynchronizowana tak, aby umożliwić automatyczne przesuwanie o zadany skok. Po wykonaniu zadanego skoku następuje odryglowanie jarzm (zwolnienie blokady), przesunięcie jarzma o zadaną podziałkę, zaryglowanie, a następnie wykonanie kolejnego skoku, czyli przesunięcie o zadaną podziałkę. Cykl ten powtarza się do momentu nasunięcia do końcowego odcinka trasy UPZP-1200.

W UPZP-1200 zastosowano układ sterowania elektro-hydraulicznego EH, który umożliwia m.in. pracę w tzw. cyklu automatycznym.

FAMUR

Grenevia SA
al. Roździeńskiego 1a
40-202 Katowice
www.famur.com

Bez kierowcy i bezpiecznie przez centrum logistyczne dzięki czujnikom ultradźwiękowym

System czujników ultradźwiękowych USi®-safety zapewnia bezpieczeństwo personelu zgodnie z normą EN ISO 13849 kategoria 3 PL d

Zastosowanie

W nowoczesnych centrach logistycznych na całym świecie materiały są obecnie transportowane za pomocą pojazdów automatycznie sterowanych (AGV), takich jak zautomatyzowane wózki widłowe. Podczas transportu materiałów za pomocą tych pojazdów AGV wszystkie kierunki jazdy muszą być niezawodnie chronione, aby zabezpieczyć przed kolizją osoby i przedmioty znajdujące się na pasie ruchu. Wymagane jest zastosowanie co najmniej jednego środka ochronnego zgodnego z PL d w głównym kierunku jazdy (do przodu) i co najmniej jednego zgodnego z PL c w kierunkach drugorzędnych (na boki i do tyłu).

Jeśli podczas transportu ładunków załadowane palety są podnoszone lub kładzione na podłożu, konieczna jest ochrona zgodna z kategorią PL d dotyczącą automatycznego ruchu wstecznego. W zależności od centrum logistycznego zabezpieczenie musi być odporne na wpływy środowiska, takie jak kurz, zanieczyszczenia i wilgoć. W przypadku wyjazdów na zewnątrz między halami istotna jest odporność na czynniki atmosferyczne, takie jak wiatr, deszcz i śnieg.

Cel

Podczas automatycznej jazdy do tyłu pojazdy AGV powinny być niezawodnie zabezpieczone przed kolizjami z osobami i przedmiotami znajdującymi się na pasie ruchu, nawet jeśli pojazd jest załadowany. Martwa strefa przed ramionami wideł musi być zabezpieczona w fazie występującej bezpośrednio przed opuszczeniem do palety. Dla tych wymagań aplikacyjnych wymagana jest homologacja zgodnie z ISO 13849-1 kategoria 3 PL d. Urządzenia te powinny być dostosowane do używania w ograniczonych przestrzeniach i muszą być odporne na wpływy środowiskowe, takie jak kurz, brud i wilgoć.

Rozwiązanie

USi®-safety to jedyny bezpieczny system czujników ultradźwiękowych zgodny z normą EN ISO 13849 kategorii 3 PL d. Umożliwia on niezawodne monitorowanie przestrzeni trójwymiarowych, dzięki czemu idealnie nadaje się do zastosowania w sprzęcie transportu bliskiego. Czujniki są niezwykle małe i mogą być dowolnie pozycjonowane, co oznacza, że można je odłączyć od interfejsu sterującego w celu elastycznego pozycjonowania w skrajnie wąskiej przestrzeni ramion wideł. Interfejs sterujący posiada dwa bezpieczne wyjścia OSSD na kanał dla regulowanego pola ochronnego oraz jedno wyjście przełączające PNP dla pola ostrzegawczego.

Eliptyczne pole akustyczne przetwornika ultradźwiękowego ma kąt rozwarcia ±17° i ±5°. Zostało ono zoptymalizowane do monitorowania zakresu 3D i dlatego – w przeciwieństwie do skanerów laserowych – doskonale nadaje się do wykrywania przeszkód, które zwisają z góry na pasie ruchu lub są uniesione nad ziemią. Jeśli system USi®-safety jest zamontowany na kilku niezależnych pojazdach AGV, których ścieżki przecinają się nawzajem, to wzajemne tłumienie zakłóceń zapobiega zakłócaniu ich pracy. Połączenie fizyczne pomiędzy systemami USi®-safety jest zatem zbędne.

Zalety

Jako jedyny przemysłowy czujnik ultradźwiękowy USi®-safety posiada dopuszczenie do stosowania zgodnie z normą EN ISO 13849 kategorii 3 PL d. Oznacza to, że przewagę technologii ultradźwiękowej nad systemami optycznymi można teraz po raz pierwszy wykorzystać w zastosowaniach związanych z bezpieczeństwem. Dzięki temu obiekty wykonane z różnych materiałów są niezawodnie wykrywane. Co więcej, czujnik jest odporny na czynniki środowiskowe, takie jak zanieczyszczenia, prądy powietrza, wilgoć i inne podobne czynniki.

Cechy szczególne:

- Zasięg wykrywania: do 2500 mm;
- Klasa bezpieczeństwa IP: czujniki IP69K, interfejs sterujący IP65;
- Czas reakcji: typowo 91 ms;Klasyfikacja bezpieczeństwa: zgodna z normą EN ISO 13849 kategoria 3 PL d;
- Temperatura robocza: –30°C … +50°C.

Najważniejsze informacje

- Jedyny system czujników ultradźwiękowych zapewniający bezpieczeństwo personelu;
- Dopuszczenie do użytku zgodnie z normą EN ISO 13849 kategoria 3 PL d;
- Eliptyczne pole akustyczne z kątem rozwarcia ±17° i ±5°;
- Wyjątkowo mały czujnik, który można zamontować w najmniejszych miejscach;
- Odporny na wpływy środowiska, takie jak zanieczyszczenia, prądy powietrza, wilgoć i inne podobne czynniki.

PEPPERL+FUCHS

Pepperl+Fuchs Sp. z o.o.
ul. Owsiana 12, 03-825 Warszawa
www.pepperl-fuchs.pl

Czujnik LiDAR z serii R2300 do zastosowań wymagających dużej prędkości

Firma Pepperl+Fuchs oferuje nowy czujnik LiDAR o częstotliwości skanowania 100 Hz – idealny do zastosowań wymagających dużej prędkości. Skaner jednowarstwowy R2300 osiąga tę wyjątkowo wysoką szybkość skanowania dzięki skanowaniu tylko jednej warstwy. Czujnik oferuje takie samo połączenie wysokiej wydajności i oszczędności kosztów, jakie charakteryzuje wielowarstwowe skanery serii R2300. Podstawą jest technologia impulsowego pomiaru odległości (PRT) opracowana przez firmę Pepperl+Fuchs.

Niezawodne wyniki pomiarów dzięki technologii impulsowego pomiaru odległości

PRT jest rozwinięciem klasycznej technologii czasu przelotu, która zapewnia szybkie i precyzyjne wyniki pomiarów z ponad 250 000 emitowanych impulsów laserowych na sekundę. Metoda ta działa niezawodnie nawet w zmieniających się warunkach otoczenia. Bardzo dobra rozdzielczość kątowa 0,1° i mała plamka świetlna zapewniają wysoką precyzję podczas nawigacji, pozycjonowania i wykrywania. Jako ekonomiczny czujnik LiDAR, R2300 jednocześnie oferuje optymalny stosunek ceny do wydajności.

Skanowanie na jednej warstwie w celu uzyskania wyższej szybkości skanowania

Dzięki czterem płaszczyznom skanowania wielowarstwowa wersja modelu R2300 jest szczególnie odpowiednia do zastosowań, w których kładzie się nacisk na wysoką niezawodność i bezpieczeństwo procesów, takich jak unikanie kolizji, wykrywanie palet lub robotyka. Z kolei w wariancie jednowarstwowym skanowanie odbywa się tylko na jednej warstwie. W rezultacie uzyskuje się czterokrotnie wyższą częstotliwość skanowania wynoszącą 100 Hz, co otwiera nowe zastosowania w zakresie dużych prędkości.

Na przykład, czujnik LiDAR może być używany na przenośnikach rolkowych o dużych prędkościach przenoszenia w celu określenia objętości przenoszonych towarów podczas ruchu. Czujnik jest również idealny do połączonej kontroli krawędzi i zwisu taśmy: korzystając z technologii PRT niezawodnie wykrywa zwis taśmy. Jednocześnie wysoka rozdzielczość kątowa umożliwia precyzyjne monitorowanie położenia krawędzi. Przy częstotliwości skanowania 100 Hz czujnik nadaje się również do stosowania z szybkimi pętlami sterowania.

Dzięki wysokiej szybkości skanowania skaner jednowarstwowy nadaje się do zastosowań wymagających dużej prędkości.

Elastyczne dostosowanie do zastosowania

Wszystkie czujniki LiDAR z serii R2300 można łatwo dostosować do różnych zastosowań: oprócz lasera pomiarowego zintegrowany jest przełączalny, widoczny laser pilotujący, który może być używany do precyzyjnego pozycjonowania urządzeń bez żadnych innych środków pomocniczych. Kąt pomiarowy 100° można zmniejszyć w razie potrzeby, aby dostosować pole skanowania do konkretnego zastosowania. Niewielki rozmiar obudowy pozwala montować go nawet w miejscach o ograniczonej przestrzeni.

Najważniejsze zalety czujników LiDAR z serii R2300

- Czujniki LiDAR oparte na technologii impulsowego pomiaru odległości (PRT) zapewniają znakomitą dokładność i odporność na zakłócenia;
- Bardzo dobra rozdzielczość kątowa i mała plamka świetlna zapewniająca wysoką precyzję w zastosowaniach związanych z nawigacją, pozycjonowaniem i wykrywaniem;
- Przełączany, widoczny laser pilotujący do precyzyjnego ustawiania i łatwego uruchamiania czujnika;
- Wielowarstwowy skaner dla większej niezawodności i oszczędności w zastosowaniach 3D;
- Skaner jednowarstwowy o częstotliwości skanowania 100 Hz do wykrywania obiektów w zastosowaniach wymagających dużej prędkości.

PEPPERL+FUCHS

Pepperl+Fuchs Sp. z o.o.
ul. Owsiana 12, 03-825 Warszawa
www.pepperl-fuchs.pl

Seria ultralekkich silników LEMoK

LEMoK to seria ultralekkich silników elektrycznych opracowana z myślą o najbardziej wymagających aplikacjach, w których gabaryty i masa silnika mają priorytetowe znaczenie. Silniki LEMoK przeznaczone są głównie dla branży lotniczej, motoryzacyjnej, wodnej, jak również do zastosowań przemysłowych jako napędy specjalne.

Seria silników LEMoK obejmuje zarówno silniki z magnesami trwałymi LEMoK 200 oraz LEMoK 300, jak również silniki pozbawione magnesów trwałych – silnik indukcyjny LEMoK IM 185 oraz silnik synchroniczny reluktancyjny LEMoK REL 200.

Wspólną cechą wszystkich opracowanych rozwiązań jest wysoki, ponadprzeciętny współczynnik gęstości mocy, czyli stosunek mocy silnika do jego masy, przy jednocześnie zachowanym wysokim poziomie sprawności. Gęstość mocy charakteryzująca serię silników LEMoK jest znacząco wyższa od rozwiązań oferowanych do tej pory na rynku krajowym, a jednocześnie dorównuje w swojej klasie rozwiązaniom spotykanym na rynkach zagranicznych.

W chwili obecnej oferowane są następujące rodzaje silników:

- LEMoK 200 (PMSM) – 60 kW / 9.2 kg / **6.52 kW/kg**
- LEMoK 300 (PMSM) – 100 kW / 18.5 kg / **5.45 kW/kg**
- LEMoK IM 185 (Indukcyjny) – 40 kW / 14.1 kg / **2.84 kW/kg**
- LEMoK 200 (Reluktancyjny) – 40 kW / 13.5 kg / **2.96 kW/kg**

Charakterystyczną cechą silników LEMoK jest:

- konstrukcja z zewnętrznym wirnikiem (outrunner);
- klasyczna topologia obwodu elektromagnetycznego (Radial Flux); uzwojenie z cewkami skupionymi;
- zakres częstotliwości napięcia zasilania 0 – 1000 Hz;
- poziom napięcia zasilania do 400 VDC;
- zakres obciążeń prądowych do 35 A/mm^2;
- rodzaj chłodzenia: cieczą/powietrzem.

Seria silników LEMoK znajduje się w ofercie Instytutu Łukasiewicz – GIT od września 2023 roku. W dalszym ciągu jest rozwijana z zamiarem poszerzenia oferty o kolejne silniki w typoszeregu.

Silnik LEMoK 300 wykorzystany został do napędu hybrydowego, lekkiego statku powietrznego o masie startowej do 750 kg

Łukasiewicz
Górnośląski Instytut Technologiczny

Sieć Badawcza Łukasiewicz
– Górnośląski Instytut Technologiczny
ul. K. Miarki 12-14, 44-100 Gliwice

Wydajność – wszystko pod kontrolą

Sterownik c430

Rosnące wymagania stawiane maszynom i nowe wyzwania w dziedzinie usług cyfrowych zwiększają wymagania stawiane systemom sterowania. Odpowiedzią na nie jest nowa generacja sterowników firmy Lenze przeznaczonych do szaf rozdzielczych.

Za pomocą tego asortymentu produktów można zapewnić obsługę wysokiej jakości systemów sterowania, takich jak np. maszyny drukarskie z wieloma zespołami drukującymi lub linie kompletujące z kilkoma robotami. W oparciu o nasze moduły oprogramowania w ten sposób można zrealizować nowoczesne, modułowe układy sterujące maszyną.

Cechy charakterystyczne

- Duża moc obliczeniowa z myślą o wymagającym sterowaniu ruchem w kompaktowych maszynach;
- Niewielkie nakłady konserwacyjne i odporność – projekt przewidujący brak baterii i zakres temperatury eksploatacyjnej rozszerzony do 60°C to gwarancja bezpieczeństwa stosowania we wszystkich gałęziach przemysłu;
- Takie same narzędzia inżynieryjne jak w przypadku wszystkich innych produktów Lenze – nie rezygnujemy z tego, co już znane i cenione;
- Przełączana funkcja magistrali przemysłowej dla c430: przełącznik Ethernet, PROFINET IO-Device lub EtherCATSlave;
- Opcjonalne rozszerzenie o magistralę przemysłową dla c520/c550;
- Połączenie EASY UI Designer oraz panelu sterowania v430 / v450 jest gwarancją gotowości na najnowocześniejsze, działające w sieci wizualizacje maszyn.

Tabela 1. Dane techniczne sterownika c430

Konstrukcja/montaż	Szyna DIN
Stopień ochrony	IP20
Dopuszczenia na rynek	
Dopuszczenia	CE, UKCA
Środowisko	RoHS
Procesor	Arm® Cortex®-A9 800 MHz
System operacyjny	RT Linux
Pamięć	
Pamięć flash	4 GB
Pamięć RAM	2 GB
Dane retain	1024 kB
Interfejs 1x EtherCAT-Master	
Sieć magistrali przemysłowej	Przełączana funkcja magistrali przemysłowej: Ethernet Switch, PROFINET IO-Device lub EtherCAT-Slave
Ethernet	1x Ethernet 100 MBit/s
USB	1x USB 2.0
Zasilanie	24 V DC (zacisk 3-biegunowy)
Chłodzenie pasywne	
Robocza temperatura otoczenia	3K3 (0 ... +60 °C) EN IEC 60721-3-3

Sterownik c430

Lenze Polska Sp. z o.o.
ul. Roździeńskiego 188 B
40-203 Katowice
www.lenze.com

Rozwój fotowoltaiki wymaga uproszczenia przepisów i budowy magazynów energii

Dalszy rozwój fotowoltaiki w Polsce potrzebuje zmian w przepisach, które uproszczą uzyskanie pozwolenia na budowę dużych instalacji i przyłączy do sieci energetycznej, konieczna jest również budowa magazynów energii – wskazali eksperci podczas premiery raportu „Rynek fotowoltaiki w Polsce 2024".

Jak podkreślił Grzegorz Wiśniewski, prezes zarządu Instytutu Energetyki Odnawialnej (IEO), polska fotowoltaika na koniec roku 2023 osiągnęła moc zainstalowaną 17,08 GW, a 17,73 GW na koniec pierwszego kwartału 2024 roku. Przyrost nowych mocy w wartościach bezwzględnych był podobny jak w roku 2022 i wyniósł ok. 4,6 GW.

„Pod względem mocy zainstalowanej jesteśmy szóstym rynkiem w UE, na którym dominują Niemcy z ponad 80 GW. Na świecie Polska znalazła się na 12 miejscu. Jeśli natomiast chodzi o moc zainstalowaną na mieszkańca jesteśmy na czwartym miejscu, wyprzedzają nas tylko Holandia, Niemcy i Australia" – podał prezes IEO.

Dodał, że ok. 2/3 mocy zainstalowanej stanowią mikroinstalacje, czyli źródła o mocy do 50 kW.

„Udział ten spada, natomiast widoczny staje się wzrost w segmencie źródeł od 50 kW do 1 MW, wynikajacy z tego, że budują je firmy na własne potrzeby" – wyjaśnił Grzegorz Wiśniewski.

Zwrócił też uwagę, że najwyższe tempo wzrostu – 110 proc. – zanotowano w segmencie farm powyżej 1 MW, choć duże instalacje stanowiły tylko 11 proc. całości mocy.

Według szefa IEO, biorąc pod uwagę wartość inwestycji, która w ub. roku przekroczyła poziom 15,6 mld zł, fotowoltaika stała się wiodącym sektorem w rodzimej energetyce. Dodał, że kolejne 17 GW w tym segmencie ma wydane warunki przyłączenia.

„Z drugiej strony aż 7,5 tys. projektów nie dostało zgody na przyłącze swojej instalacji do sieci, co staje się realnym problemem dla dalszego rozwoju" – wskazał.

W jego ocenie, fotowoltaika ma przed sobą perspektywy rozwoju, ale potrzebuje do tego odpowiednich warunków prawnych i dużych inwestycji w budowę magazynów energii i modernizację sieci energetycznych.

Jak podkreślił Miłosz Motyka, podsekretarz stanu w Ministerstwie Klimatu i Środowiska, fotowoltaika to jeden z filarów transformacji energetycznej. Przypomniał, że podpisywane są pierwsze umowy na modernizację sieci energetycznych z programu Fundusze Europejskie na Infrastrukturę, Klimat, Środowisko (FEnIKS).

„W sumie 85 mld zł trafi na modernizacje sieci energetycznych" – poinformował.

Dodał, że w jego resorcie jest świadomość, iż obecnie podstawowym wyzwaniem jest bilansowanie systemu i magazynowanie nadwyżek produkcji fotowoltaiki.

„Analizujemy program >>Mój prąd<< i rozważamy pomysł na wprowadzenie w przyszłości obowiązku posiadania magazynu energii przy instalowaniu źródła PV" – powiedział wiceminister klimatu.

Zwrócił uwagę, że takie rozwiązanie może poprawić atrakcyjność ekonomiczną inwestycji w fotowoltaikę.

„Mam poczucie, że ta atrakcyjność ostatnio jest coraz mniejsza, a jest przecież jednym z kluczowych warunków decyzji o inwestycji" – ocenił polityk.

Wiceminister Motyka zapowiedział też ułatwienia w przepisach, które pozwolą o połowę skrócić proces uzyskiwania zgód i pozwoleń na inwestycje w OZE.

Na taką konieczność zwróciła uwagę Marta Głód, dyrektor ds. Rozwoju Projektów OX2.

„Dla nas, przedsiębiorców, wyzwaniem na miarę lotu w kosmos jest sprostanie wymogom dotyczącym uzyskania pozwolenia na budowę. Przepisy są niejasne, a procedury za długie. Oczywiście cały proces jest do przejścia, ale wymaga zbyt dużego poświęcenia uwagi i czasu" – oceniła.

Marta Głód powiedziała, że efekty wielu odmów na przyłącza do sieci z ub. roku będą widoczne dopiero w 2027 roku. Dodała, że jeśli rząd uprości przepisy i stworzy dogodne warunki do inwestowania w magazyny energii, dynamika rozwoju fotowoltaiki w Polsce nie powinna spaść w najbliższych latach.

W podobnym tonie wypowiadał się Piotr Maciołek, członek zarządu Polenergia, wskazując na duży potencjał dla inwestycji w wielkoskalowe farmy fotowoltaiczne. Podkreślił przy tym, że bez uproszczenia przepisów, w tym ustawy o planowaniu i zagospodarowaniu przestrzennym, ten potencjał nie będzie w pełni wykorzystany.

Przedsiębiorca zwrócił uwagę, że bez dużych inwestycji w odnawialne źródła energii ze słońca i wiatru nie będzie transformacji energetycznej.

O potencjale rozwoju dużych farm fotowoltaicznych w kontekście ograniczeń terenowych mówił Antoni Michalski z zarządu Next2Sun Polska. Jego zdaniem odpowiedzią na problem z dostępnością gruntów rolnych pod budowę farm fotowoltaicznych jest agrofotowoltaika.

Jak wyjaśnił, OZE mają największe szanse na dynamiczny rozwój na obszarach wiejskich w Polsce.

„Przepisy o ochronie gruntów rolnych wyłączają de facto sporą część obszarów z procesu inwestycji w budowę dużych farm PV. Odpowiedzią na ten problem jest agrofotowoltaika, która pozwala połączyć produkcję energii ze słońca z uprawą roślin" – wskazał.

Dodał, że na zachodzie Europy jest to coraz popularniejsze rozwiązanie, w Polsce ze względu na bariery prawne i finansowe agrofotowoltaika nie funkcjonuje. Jak podkreślił, takie rozwiązanie jest korzystne na wielu płaszczyznach, pozwoliłoby też na wypłaszczenie miksu produkcji.

Na kwestie kosztów budowania instalacji fotowoltaicznych zwrócił uwagę Maciej Drobczyk, Country Manager IBC SOLAR Poland. Przypomniał, że ceny modułów spadły w ubiegłym roku o 60 proc., bo rynek zalały produkty z Azji.

„Nie jest to dobra sytuacja dla rynku europejskiego z wielu powodów" – ocenił. Jak podkreślił ekspert, Unia Europejska ma szereg narzędzi, żeby wesprzeć producentów z Europy z korzyścią dla europejskich konsumentów oraz środowiska naturalnego.

Źródło informacji: PAP MediaRoom

KONKURS
DLA WYSTAWCÓW

INNOWACYJNE ROZWIĄZANIA W BUDOWIE MASZYN I URZĄDZEŃ GÓRNICZYCH:

INNOWACYJNY PRODUKT KATOWICE 2024

- WYZWANIA TRANSFORMACJI ENERGETYCZNEJ W PRZEMYŚLE
- AUTOMATYZACJA I MONITOROWANIE PROCESU PRODUKCYJNEGO W KOPALNIACH PODZIEMNYCH – POLSKIE DOŚWIADCZENIA WE WDRAŻANIU PARADYGMATU PRZEMYSŁU 4.0
- NOWE TECHNIKI I TECHNOLOGIE W PODZIEMNEJ EKSPLOATACJI ZŁÓŻ

ZGŁOŚ SWÓJ UDZIAŁ W KONKURSIE

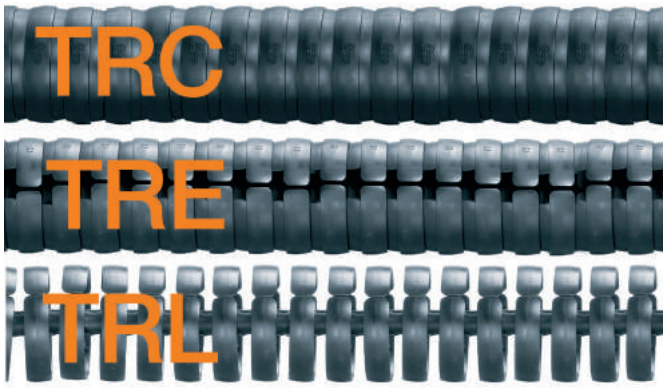
ORGANIZATORZY

EXPO Katowice S.A.

napędy i sterowanie miesięcznik naukowo-techniczny

Robot paletyzujący: bezpieczne prowadzenie kabli 3D z wieloosiowym e-prowadnikiem triflex® R dla robotów

W aplikacjach 3D ruchy obrotowe i wahliwe są częścią codziennego życia. Wymagane są tutaj e-prowadniki, które bezpiecznie prowadzą i chronią przewody do robotów. e-prowadnik triflex® R (TRE, TRC i TRL) od igus, został opracowany specjalnie dla wymagających robotów przemysłowych. Dzięki dużej absorpcji siły rozciągającej i wysokiej elastyczności, e-prowadnik umożliwia obrót o około ± 10° na ogniwo prowadnika podczas skomplikowanych ruchów na osiach pionowych. W porównaniu z wężem ochronnym dla przewodów, triflex® R oferuje określony promień gięcia, co znacznie wydłuża żywotność przewodów i węży.



e-prowadnik triflex® R (TRE, TRC i TRL) od igus. Źródło: igus GmbH

triflex® RSE – automatyczny system wciągania dla e-prowadników triflex® serii TRC, TRE, TRCF. Celem systemu odciągu triflex® RSE jest utrzymanie e-prowadnika możliwie najbliżej ramienia robota – dzięki temu prowadnik kablowy nie utrudnia ruchów robota. System odciągu triflex® RSE cechuje wyjątkowo niska masa oraz wysoka ekonomiczność. Źródło: igus GmbH

triflex® umożliwia bezpieczne ruchy kabli prezentowanego rozwiązania paletyzującego w zakresie ruchu 360°. Robot Fanuc R-2000iC/165F, bo o nim mowa, obsługuje załadunek i rozładunek palet – może pobierać określone produkty z palety, a także dodawać do niej produkty. Co ciekawe, produkty na palecie nie zawsze muszą być dokładnie takie same. Aby bezpiecznie i niezawodnie poprowadzić kable zasilające i kable danych do ramienia robota podczas ruchów 360°, zastosowano e-prowadnik triflex® 3D z systemem zwijania.

- **Wymagania:** Robot musi wykonać ruch w zakresie 360°. W trakcie tego procesu, ruchome części robota muszą znajdować się jak najbliżej siebie i być jak najkrótsze oraz bezpiecznie prowadzone;
- **Branża:** Technologia pakowania, paletyzacja;
- **Co było potrzebne:** triflex® R do systemów zwijania RS i system odciągu triflex® RS;
- **Sukces dla klienta:** Dzięki zainstalowaniu e-prowadnika triflex® wszystkie przewody mogły być bezpiecznie prowadzone na robocie. Kolejną zaletą jest wysoki poziom stabilności i możliwość łatwej wymiany kabli i węży.

Jaki był problem do rozwiązania?

W szóstej osi robota paletyzującego Fanuc R-2000iC/165F zainstalowano dodatkowy serwomechanizm, który musiał być wyposażony w dodatkowe kable i węże. Ponadto, szósta oś musi wykonywać minimalny obrót o 360°, co niepotrzebnie zwiększało długość e-prowadnika bez systemu odciągu. Węże i kable wymagane dla serwomechanizmu na osi 6 musiały być dodatkowo poprowadzone na osi 2 – 6.

Ze względu na wiele ruchów, ważne jest, aby ruchome części robota znajdowały się jak najbliżej i były jak najkrótsze oraz aby podczas złożonych ruchów robota wszystkie kable zawsze były bezpiecznie i niezawodnie prowadzone.

Jakie igus zaproponował rozwiązanie?

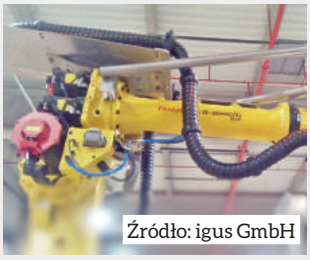
Dzięki zainstalowaniu systemu odciągu triflex® RS (TR.RS.60.L, stały koniec po lewej), pasującego zestawu e-prowadników do systemu odciągu (TRE.RS.60.087.1500.0.B), a także 40 dodatkowych ogniw prowadnika kablowego (TRE.60.087.0.B) wszystkie przewody mogły być bezpiecznie prowadzone do robota. Bez systemu odciągu długość e-prowadnika byłaby zbyt duża ze względu na ruch 360°. Ochraniacze TR.60.30 chronią e-prowadnik w bardzo mocno obciążonych punktach, a tym samym zmniejszają zużycie i zwiększają jego żywotność.

Kolejną dużą zaletą wersji TRE.B jest 4-krotnie większa stabilność w porównaniu z wersją TRE oraz możliwość łatwej wymiany przewodów lub węży. Można je łatwo zamontować i zdemontować za pomocą dwóch bocznych otworów w e-prowadniku.

Źródło: igus GmbH

Zainstalowane części na osi 2

- 81x TRE.60.087.0.B
- 1x TR.60.01
- 2x TR.60.02



Źródło: igus GmbH

Zainstalowane części na oś 3 – 6

- 1x TR.RS.60.L
- 1x TRE.RS.60.087.1500.0.B
- 40x TRE.60.087.0.B
- 5x TR.60.30
- 2x TR.60.01
- 1x TR.60.02
- 1x TR.60.05

Bezpłatny konfigurator e-prowadników igus dla wyposażenia robotów

igus oferuje konfigurator Quick Robot, aby znaleźć odpowiedni system dla swojego robota www.igus.pl/konfigurator_robot

igus oferuje również usługę montażu robota przemysłowego

Zastosowania robotów są bardzo zróżnicowane i czasami dość złożone pod względem struktury i obsługi. Aby osiągnąć możliwie najdłuższą żywotność dla aplikacji robotów z triflex® R, igus wyszkolił zespół projektów i montażu dla aplikacji związanych z robotami, który optymalnie zainstaluje e-prowadnik triflex® R.

Jak zmniejszyć wysiłek związany z planowaniem projektu? Wystarczy skontaktować się z wyszkolonym personelem igus, który będzie wspierał Państwa w sprawnej realizacji projektu na każdym etapie. Niezależnie od tego, czy potrzebna jest tylko porada od zespołu montażowego igus, czy też konieczne będzie zaplanowanie i zainstalowanie całej maszyny.

Podczas rozmowy telefonicznej eksperci igus odpowiedzą na wiele pytań i omówią wszystkie zalety triflex® R dla Państwa firmy. Na miejscu rejestrują wszystkie niezbędne dane do stworzenia dokładnych dokumentów projektu. W ten sposób odpowiadają konkretnie na pytania dotyczące Państwa indywidualnych zastosowań. Od planowania projektu i indywidualnej oferty po profesjonalny montaż triflex® R na miejscu dla Państwa aplikacji.

Osiągniemy najdłuższą możliwą żywotność dla Państwa robota.

Jakub Lachowski
Product Manager triflex® & Robotics
tel. kom.: +48 606 857 583
e-mail: jlachowski@igus.net

Nowoczesne rozwiązania intralogistyczne z elektrorolką Lenze

Lenze wprowadza na rynek sterowaną analogowo elektrorolkę o450 MDR z wbudowanym silnikiem własnej produkcji. Jest to innowacyjne rozwiązanie, zaprojektowane przez inżynierów Lenze, które może zrewolucjonizować systemy przenośnikowe, poprawiając wydajność i oszczędność energii.

INNOWACYJNA ELEKTROROLKA LENZE: MOC, ENERGOOSZCZĘDNOŚĆ I ELASTYCZNOŚĆ

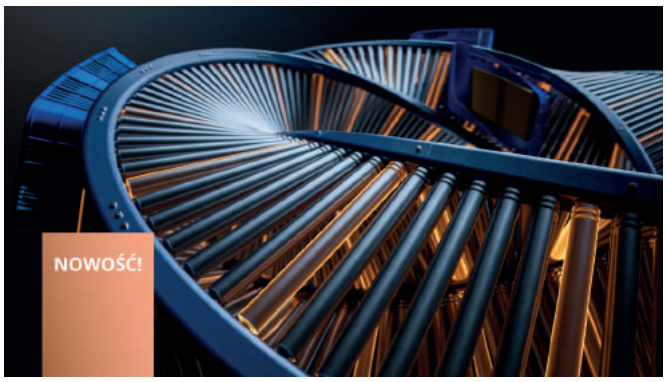
Elektrorolka Lenze wyróżnia się na tle innych dostępnych na rynku rolek dzięki swoim zaawansowanym cechom. Jest napędzana bezpośrednio przez silnik bezszczotkowy z magnesami trwałymi. To rozwiązanie pozwala na uzyskanie wysokiego momentu obrotowego przy niskich prędkościach, podobnie jak w przypadku konwencjonalnego motoreduktora. Jednocześnie zachowana jest wysoka dynamika i wydajność, dzięki precyzyjnemu sterowaniu prędkością.

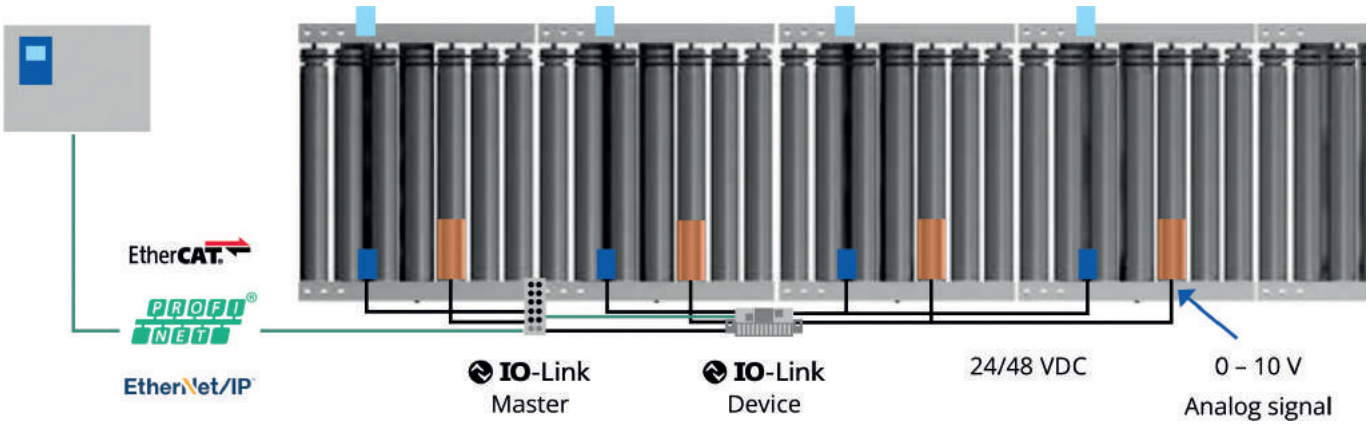
Wyeliminowanie przekładni i zastosowanie bezpośredniego napędu silnikiem oferuje wiele korzyści. Oto szczegóły:

- **Zwiększona moc:** Rolka napędowa osiąga moc wyjściową 57 W przy 24 V i 115 W przy 48 V. To ponad dwukrotnie więcej niż porównywalne elektrorolki dostępne na rynku;
- **Energooszczędność:** Rolka z napędem Lenze spełnia wymogi klas sprawności IE7-IE9 w zależności od prędkości. To oznacza, że klient może zaoszczędzić nawet do 30% energii w porównaniu z konwencjonalnymi systemami. Przykładowo, w centrum logistycznym z 20 km linii przenośników i 20 000 rolek napędzanych silnikiem Lenze, możliwe byłoby zaoszczędzenie do 335 MWh energii elektrycznej lub 145 t CO_2;
- **Cicha praca:** Silnik z zewnętrznym rotorem sprawia, że rolka pracuje bardzo cicho. Brak ruchomych części poza łożyskami eliminuje typowe odgłosy przekładni;
- **Elastyczność:** Rolka działa przy napięciu 24 V lub 48 V, co ułatwia instalację, konserwację i wymianę;
- **Optymalizacja i redukcja wariantów:** Pojedynczy wariant obejmuje wszystkie prędkości i momenty obrotowe, co upraszcza zarządzanie i redukuje liczbę wariantów;
- **Zaawansowana elektronika:** Elektronika zasilająca jest zintegrowana w rolce, co ułatwia obsługę i zapewnia spójność systemu.

WSZECHSTRONNE ROZWIĄZANIE DLA SYSTEMÓW PRZENOŚNIKOWYCH

Elektrorolka Lenze może działać z dowolną kartą sterującą zasilaną napięciem 24 lub 48 VDC i dającą sygnał analogowy 0 – 10 V do sterowania prędkością. To sprawia, że





Jeden moduł sterujący, na przykład G20 firmy Pepperl+Fuchs, może napędzać do 4 elektrorolek

jest wszechstronnym rozwiązaniem w różnych aplikacjach. Ze względu na zintegrowaną elektronikę zasilającą zbędne są karty sterujące z wbudowanym zasilaniem.

Rolkę o450 MDr można bezpośrednio zintegrować z istniejącymi systemami przenośników. To ułatwia modernizację i poprawia elastyczność działania.

Lenze oferuje różne powłoki i sposoby przeniesienia napędu, aby dostosować rolkę do indywidualnych potrzeb klienta.

Rolka oferuje pełny nominalny moment obrotowy, co jest korzystne przy przyspieszaniu transportowanych towarów. Może przenosić ładunki o masie do 30 kg.

ELEKTROROLKA LENZE W MAGAZYNACH I CENTRACH DYSTRYBUCYJNYCH

Rolka napędowa Lenze pozwala na dokładne dostosowanie systemu przenośnikowego do indywidualnych potrzeb. Dzięki niej można zoptymalizować przepływ towarów, minimalizując straty czasu i energii.

Sprawdzi się w różnych rodzajach przenośników, takich jak rolkowe, taśmowe, akumulacyjne, sortujące i poprzeczne. To oznacza, że rolkę z napędem Lenze można wykorzystać w wielu różnych aplikacjach.

Elektrorolka zapewnia płynną pracę i umożliwia szybkie zmiany kierunku ruchu. To ważne, zwłaszcza w dynamicznych środowiskach magazynowych.

Ze względu na zróżnicowane zalety elektrorolki Lenze warto wziąć ją pod uwagę przy projektowaniu nowoczesnych magazynów i centrów dystrybucyjnych.

Lenze

Lenze Polska Sp. z o.o.
ul. Roździeńskiego 188 B
40-203 Katowice
www.lenze.com

Uroczystość nadania tytułu Profesora Honorowego AGH prof. Ryszardowi Tadeusiewiczowi

5 lipca 2024 r. o godz. 12.00 w auli AGH odbędzie się uroczystość nadania tytułu Profesora Honorowego AGH prof. Ryszardowi Tadeusiewiczowi – byłemu rektorowi AGH, wybitnemu specjaliście w dziedzinie biocybernetyki, automatyki i informatyki.

Program uroczystości:

- „Gaude Mater Polonia" w wykonaniu chóru Zespołu Pieśni i Tańca AGH „Krakus"
- Przemówienie rektora AGH prof. Jerzego Lisa
- Wystąpienie dziekana Wydziału Elektrotechniki, Automatyki, Informatyki i Inżynierii Biomedycznej prof. Ryszarda Sroki
- Wystąpienie promotora
- Wręczenie dyplomu
- Wykład mistrzowski
- „Gaudeamus igitur" w wykonaniu chóru Zespołu Pieśni i Tańca AGH „Krakus"

Biogram prof. Ryszarda Tadeusiewicza

Urodził się 5 maja 1947 r. w Środzie Śląskiej. Studia na Wydziale Elektrotechniki Górniczej i Hutniczej Akademii Górniczo-Hutniczej ukończył z wyróżnieniem w 1971 r. Dodatkowo studiował na Wydziale Lekarskim Akademii Medycznej w Krakowie. Ponadto przeszedł studia w zakresie metod matematycznych i informatycznych w ekonomii, uzyskując pełne prawa profesora Akademii Ekonomicznej (obecnie Uniwersytet Ekonomiczny) w Krakowie.

Od 1971 r. skupił się na pracy naukowej związanej z biocybernetyką, automatyką i informatyką, osiągając kolejno: w 1975 r. stopień naukowy doktora, w 1981 r. doktora habilitowanego, w 1986 r. tytuł profesora nadzwyczajnego, a w 1991 r. profesora zwyczajnego nauk technicznych – wszystkie w AGH.

W 1990 r. wybrany na członka Komitetu Badań Naukowych I kadencji, po upływie której wybrany ponownie w skład II kadencji. Po wyczerpaniu możliwości kandydowania do KBN prof. Tadeusiewicz został mianowany przez kierownictwo KBN przewodniczącym Sekcji Informatyki Komisji Badań Stosowanych KBN, a następnie Minister Nauki i Informatyzacji powołał go na pierwszego przewodniczącego Rady Informatyzacji.

W 1996 r. został wybrany na stanowisko prorektora AGH ds. nauki, a w styczniu 1998 r. na rektora AGH. Funkcję tę piastował przez kolejne kadencje (1999 – 2002, 2002 – 2005).

W 1998 r. został powołany na członka Polskiej Akademii Umiejętności, w 2002 r. na członka Polskiej Akademii Nauk, a w roku 2013 na członka rzeczywistego PAN. Trzykrotnie był też wybrany do pełnienia funkcji prezesa Krakowskiego Oddziału PAN.

Sprawował wiele innych funkcji kierowniczych: kierownika Samodzielnej Pracowni Biocybernetyki AGH (1974 – 1982), zastępcy dyrektora Instytutu Automatyki, Inżynierii Systemów i Telekomunikacji AGH (1980 – 1988), kierownika Zakładu Biocybernetyki AGH (1980 – 1992), kierownika Katedry Automatyki AGH (od 1997), p.o. kierownika Zakładu Biocybernetyki CM UJ (od 2001), p.o. kierownika Zakładu Biostatystyki i Informatyki Medycznej CM UJ (2001 – 2002), przewodniczącego Rady ds. Informatyzacji Akademii Ekonomicznej, przewodniczącego Konferencji Rektorów Polskich Uczelni Technicznych i wiele innych.

Trzykrotnie był wybrany na członka Centralnej Komisji ds. Stopni i Tytułów (organu pełniącego podobne funkcje jak obecna Rada Doskonałości Naukowej).

W 2019 r. Prezydent RP nadał prof. Tadeusiewiczowi Krzyż Komandorski z Gwiazdą Orderu Odrodzenia Polski. Otrzymał także Krzyż Komandorski i Krzyż Oficerski tego orderu.

Do kwietnia 2024 r. opublikował 126 książek jako autor, 67 książek jako edytor, 1375 artykułów lub referatów umieszczonych w materiałach konferencji naukowych oraz 1427 artykułów popularnonaukowych. W zakresie kształcenia kadr naukowych był promotorem 75 obronionych doktoratów, pracował jako recenzent 354 prac doktorskich, 179 habilitacji i 167 wniosków profesorskich.

Więcej informacji o prof. Ryszardzie Tadeusiewiczu

Sonepar Polska: razem dla planety!

Już po raz piąty sieć hurtowni elektrotechnicznych Sonepar (wcześniej działająca pod marką Alfa Elektro) razem z grupą dostawców przeprowadzili akcję „Zielony maj", podczas której zachęcali do dbałości o klimat.

Firma Sonepar Polska zaprosiła do akcji dostawców, którzy troszczą się o środowisko naturalne: Eaton, Kontakt-Simon, Lapp, NKT, PCE, Philips oraz Schneider Electric. Grupa tych 7 firm wspólnie promowała potrzebę ograniczania ilości odpadów i zmniejszania zużycia prądu, a tym samym redukcji śladu węglowego.

Sonepar świeci przykładem

Sieć hurtowni Sonepar zrealizowała wiele działań, które pozytywnie wpływają na klimat. W tym zakresie firma chce być liderem branży dystrybucji elektrotechnicznej w Polsce. W centrali i kilku oddziałach Sonepar powstały instalacje fotowoltaiczne, które nawet o 60% zredukowały pobór prądu z sieci na rzecz zielonej energii. Firma we wszystkich lokalizacjach w Polsce wymieniła oświetlenie tradycyjne na ledowe, co znacząco obniżyło zużycie energii. W magazynie w Chorzowie o 21% spadło zużycie energii po modernizacji sterowania oświetleniem regału wielopoziomowego. Z kolei po ociepleniu firmowych budynków potrzeba mniej energii do ich ogrzania oraz poprawił się komfort cieplny.

„Zielone" produkty przyczyniają się do ochrony klimatu

W ramach akcji „Zielony maj" sieć hurtowni Sonepar promuje produkty i usługi, które przyczyniają się do redukcji śladu węglowego.

- **Firma PCE** oferuje rodzinę ładowarek eMobility – zarówno do samochodów elektrycznych, jak i… rowerów. W ten sposób producent promuje wykorzystanie energii ze słońca i… zdrowy styl życia.
- **Firma LAPP** – dostawca kabli i przewodów – stosuje tworzywa sztuczne wytwarzane… z kukurydzy. Bio-plastik na jej bazie zawiera 45 – 60% surowca naturalnego.
- **Firma Kontakt-Simon** – producent osprzętu elektroinstalacyjnego – oferuje serię produktów Simon GO. Dbając o mniejsze zużycie prądu, automatyzując oświetlenie, ogrzewanie oraz klimatyzację system ten pozwala zadbać o ekologię oraz własny budżet.
- **Firma NKT** – dostawca kabli i przewodów – dla wielu swoich produktów udostępnia deklaracje środowiskowe EPD (Environmental Product Declaration). Dokumentują one wpływ przewodów i kabli na środowisko w całym cyklu ich życia, aż do wycofania z eksploatacji.
- **Firma Signify** oferuje nowoczesne źródła światła pod marką Philips w ramach transformacji oświetlenia na LED. Są to produkty UltraEfficient o najwyższej klasie energetycznej A, co pozwala zaoszczędzić około 50% energii.
- **Firma Eaton** projektuje wszystkie produkty z myślą o ich długiej żywotności, wykorzystując materiały pochodzące z recyklingu. Produkty tej firmy pomagają zwiększyć ilość ekologicznej energii w sieci, jak również wydajność jej przepływu i wykorzystania.
- Z kolei **Schneider Electric** przyjął zobowiązania w zakresie ochrony klimatu, które zamierza zrealizować w latach 2021 – 2025. Firma chce osiągać 80% przychodu ze sprzedaży produktów wspierających zrównoważony rozwój i zmniejszyć o 800 mln ton emisję CO_2.

Miód zachęca do ponownego wykorzystania opakowań

Sieć hurtowni elektrycznych Sonepar wraz z dostawcami zachęca także do wielokrotnego wykorzystania opakowań z tektury. W ramach akcji „Zielony maj" wystarczyło zwrócić 5 kartonów, aby otrzymać słoik miodu.

Sonepar Polska jest wiodącym dystrybutorem artykułów elektrotechnicznych dla profesjonalistów. Spółka posiada sieć 56 hurtowni w Polsce. Firma wchodzi w skład międzynarodowej Grupy Sonepar, która jest niekwestionowanym numerem 1 w Europie i na świecie w branży dystrybucji wyposażenia elektrycznego ze sprzedażą przekraczającą 33 mld euro.

sonepar
Powered by Difference

Sieć hurtowni elektrycznych
Sonepar Polska
ul. Obrońców Westerplatte 81
40-335 Katowice
www.sonepar.pl

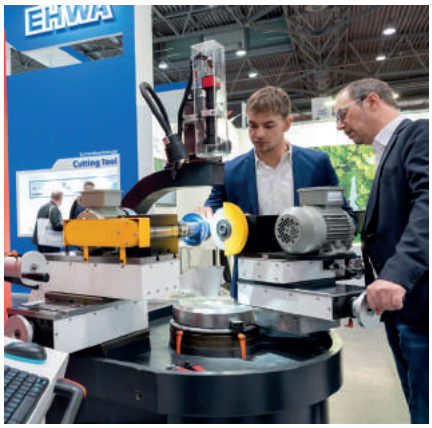
Intec – Międzynarodowe Targi Obrabiarek, Technologii i Automatyzacji Produkcji **11 – 14.03.2025 r.**

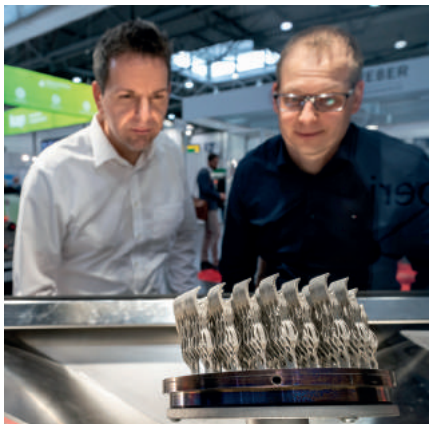
Zuliefermesse – Międzynarodowe Targi Poddostawców: Części, Podzespoły, Moduły, Technologie **11 – 14.03.2025 r.**

GrindTec – Międzynarodowe Targi Szlifowania i Ostrzenia Narzędzi **11 – 14.03.2025 r.**

Już w marcu 2025 roku kolejna edycja wiodących w Europie targów przemysłowych Intec, Zuliefermesse i GrindTec

W dniach od 11 do 14 marca 2025 roku w Lipsku odbędzie się kolejna edycja trio targowego: Intec, Zuliefermesse i GrindTec. Wspólny termin trzech uzupełniających się tematycznie imprez, gwarantuje prezentację w jednym miejscu i czasie pełnej oferty i innowacyjnych technologii z zakresu narzędzi precyzyjnych i przemysłu metalowego i poddostawczego.





Międzynarodowe Targi Obrabiarek, Technologii i Automatyzacji Produkcji Intec należą do grona wiodących imprez wystawienniczych dla przemysłu metalowego i maszynowego w Europie. Swoim zakresem tematycznym obejmują m.in. obrabiarki, maszyny i urządzenia, komponenty i podzespoły maszynowe, narzędzia, systemy mocowania, automatyzację produkcji, robotykę, produkcję urządzeń technologicznych służących wytwarzaniu odnawialnych źródeł energii, technikę transportu bliskiego i magazynową, metrologię przemysłową i kontrolę jakości, a także usługi i produkcję kontraktową.

W 2025 roku podczas targów Intec swoją aktualną ofertę zaprezentują wiodący światowi producenci obrabiarek i maszyn specjalnych, systemów zautomatyzowanej produkcji oraz innowacyjnych technologii produkcji przemysłowej. Targi Intec stanowią sprawdzone źródło kontaktów i wiedzy dla osób na stanowiskach kierowniczych oraz ekspertów. Impreza ta skupia uwagę na najważniejszych zagadnieniach dla branży, w tym m.in. na tematyce związanej z automatyzacją i robotyzacją produkcji, na transformacji cyfrowej w przemyśle produkcyjnym oraz wyzwaniach zrównoważonego rozwoju w przemyśle.

W tym samym terminie odbędą się Międzynarodowe Targi Poddostawców: Części, Podzespoły, Moduły, Technologie Zuliefermesse. Targi Z są wiodącym w Europie spotkaniem B2B dla firm poddostawczych niskiego i średniego szczebla oraz dla dostawców usług przemysłowych. W 2025 roku targi Z prezentować będą bogatą ofertę produktów i usług i po raz kolejny stanowić będą istotne miejsce spotkań dla osób decyzyjnych oraz specjalistów z branży budowy maszyn, urządzeń i narzędzi, przemysłu motoryzacyjnego i budowy pojazdów oraz innych gałęzi przemysłu.

Równocześnie z targami Intec i Z odbędzie się już po raz drugi w Lipsku kolejna edycja Międzynarodowych Targów Szlifowania i Ostrzenia Narzędzi GrindTec. Targi GrindTec to istotne branżowe spotkanie dla producentów szlifierek do produkcji i ostrzenia narzędzi, producentów technologii szlifowania i obciągania, dostawców urządzeń peryferyjnych i maszyn, a także dla firm z branży technologii procesowej, oprogramowania oraz badań i rozwoju.

Targi Z, Intec i GrindTec tworzą wspólnie jedyne w swoim rodzaju trio targowe w Europie, prezentujące

kompletny łańcuch wartości dodanej dla branży obróbki metali. Odwiedzający targi mają możliwość znalezienia dostosowanych do indywidualnych potrzeb rozwiązań dla wszystkich etapów produkcji, od planowania, przygotowania produkcji, poprzez procesy produkcyjne, po dystrybucję.

Podczas ostatniej edycji targów, która odbyła się w 2023 roku, w ramach trio targowego Intec, Zuliefermesse i GrindTec zaprezentowało się łącznie 821 wystawców z 29 krajów, natomiast odwiedziło je 19 300 przedstawicieli przemysłu z 49 krajów – to wielki potencjał do nawiązywania nowych, międzynarodowych kontaktów kooperacyjnych i skutecznej promocji na międzynarodowym rynku.

Inspirujący program

Dzięki licznym wydarzeniom targi Intec, Zuliefermesse i GrindTec umożliwiają uzyskanie informacji na temat innowacyjnych technologii i najnowszych rozwiązań dla produkcji, a także nawiązywanie nowych kontaktów biznesowych. W ramach targów odbędą się sympozja, warsztaty i konferencje, dzięki którym możliwy będzie transfer wiedzy i innowacji pomiędzy światem badań, przemysłu i gospodarki.

Wsparcie kooperacji

Podczas targów odbywa się Międzynarodowa Giełda Kooperacji CONTACT Business Meetings organizowana w ramach sieci Enterprise European Network. Udział w giełdzie to doskonała szansa na nawiązanie nowych kontaktów biznesowych w całej Europie. Do grona uczestników należą firmy oferujące nowe technologie i innowacyjne rozwiązania, a także poszukujące potencjalnych partnerów do kooperacji oraz do realizacji wspólnych projektów.

Więcej informacji znajduje się na:
www.messe-intec.de,
www.zuliefermesse.de oraz
www.grindtec.de

Informacji w Polsce udziela oficjalne przedstawicielstwo:
Targi Lipskie Polska Sp. z o.o.
info@targilipskie.pl

Grind Tec 11-14.03.2025 Międzynarodowe Targi Szlifowania i Ostrzenia Narzędzi

intec 11-14.03.2025 Międzynarodowe Targi Obrabiarek, Technologii i Automatyzacji Produkcji

Zuliefer Messe 11-14.03.2025 Międzynarodowe Targi Poddostawców: Części, Podzespoły, Moduły, Technologie

Zalety kołków sprężystych zwijanych ze stali nierdzewnej chromowej 420

Michael Pasko

Kołki sprężyste zwijane oferowane są w wersji lekkiej, standardowej i ciężkiej, aby spełnić wymagania właściwe dla określonych zastosowań

Firma SPIROL jest wynalazcą kołka sprężystego zwijanego w 1948 r. Kołki zwijane są stosowane w wielu branżach, w tym motoryzacyjnej, medycznej, ciężkiego sprzętu, wojskowej, lotniczej i produktów konsumenckich. W zastosowaniach wymagających połączenia wysokiej wytrzymałości, doskonałej odporności na zużycie i odporności na korozję, nierdzewna chromowa stal martenzytyczna 420 oferuje szereg zalet technicznych oraz stanowi rzetelne i racjonalne pod względem kosztów rozwiązanie.

Wytrzymałość

Kołki sprężyste zwijane ze stali nierdzewnej 420 firmy SPIROL podlegają hartowaniu nadającemu im parametry zbliżone do parametrów ich odpowiedników wykonanych ze stali wysokowęglowej i mają taką samą minimalną znamionową wytrzymałość na ścieranie. Proces ten zapewnia również pożądane parametry sprężystości i odporności na zużycie. Zwijane kołki ze stali nierdzewnej chromowej posiadają również wysoką odporność na korozję powodowaną przez najbardziej typowe warunki atmosferyczne i otoczenia bez ryzyka szybkiego umocnienia występującego w przypadku stali nierdzewnej austenitycznej 302/304.

W większości przypadków kołki sprężyste zwijane ze stali nierdzewnej chromowej 420 mogą być stosowane jako zamienniki kołków ze stali wysokowęglowej, przy czym należy uwzględnić efekt korozji kontaktowej w odniesieniu do materiału łączonych elementów.

Odporność na korozję

Jeżeli istnieje konieczność zastosowania kołków zwijanych odpornych na korozję, typowym rozwiązaniem są produkty w dwóch technologiach:

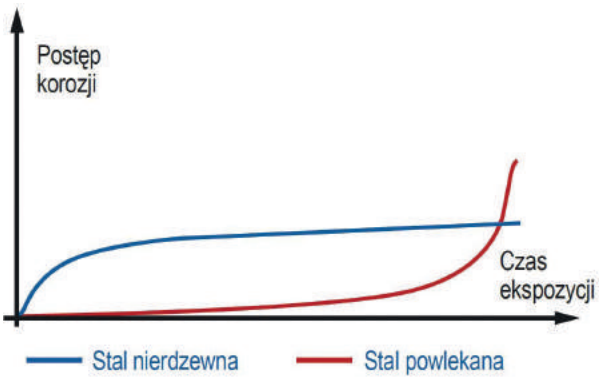
- stal węglowa z ochronną galwaniczną powłoką protektorową;
- stopy stali nierdzewnej, których właściwości zapewniają odporność na korozję.

Pomimo iż powłoki zapewniają doskonałe parametry ochronne, z czasem ulegają zużyciu, natomiast stal nierdzewna zapewnia ochronę przez cały okres użytkowania, pod warunkiem, że w otoczeniu dostępny jest wolny tlen (wolny tlen umożliwia odtworzenie ochronnej warstwy tlenku chromu elementu złącznego w przypadku jej uszkodzenia). W przypadku części platerowanych, po naruszeniu powłoki stal węglowa pozostaje niezabezpieczona i szybko ulega korozji.

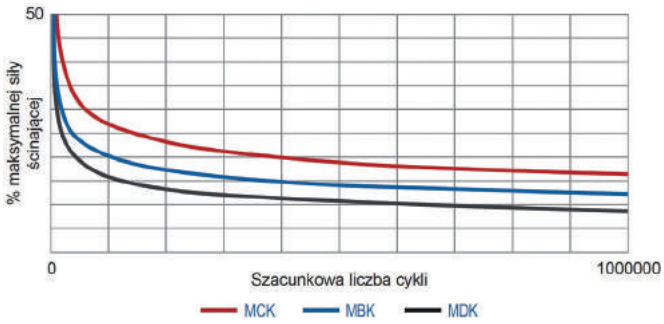
Nierdzewna chromowa stal martenzytyczna 420 zapewnia wysoką odporność na korozję m.in. w następujących środowiskach:

- normalne warunki atmosferyczne i poziom wilgotności;
- para wodna;
- woda słodka;
- alkohol;
- amoniak;
- czynniki alkaliczne;
- łagodne kwasy (np. węglowy);
- produkty ropopochodne, takie jak benzyna, olej, ropa naftowa itp.;
- łagodne detergenty i roztwory sterylizujące.

Pomimo iż kołki zwijane wykonane ze stali nierdzewnej austenitycznej 302/304 zapewniają doskonałą ochronę przed korozją, materiał ten nie jest odpowiedni, gdy kołek będzie poddawany obciążeniom dynamicznym lub gdy parametry wytrzymałościowe, w tym w zakresie odporności na zużycie, muszą być równe lub wyższe



Wykres pokazuje, jak czas wpływa na odporność na korozję stali powlekanej w porównaniu ze stalą nierdzewną



Dane służą wyłącznie do celów porównania – warunki występujące w tym teście nie stanowią podstawy do określenia parametrów efektywności w żadnym zastosowaniu, ponieważ na parametry efektywności wpływ mają takie czynniki, jak różny poziom obciążenia, różne materiały elementów łączonych, rozmiar otworu i jakość płaszczyzny ścinania/prześwit

niż te właściwe dla stali wysokowęglowej. Alternatywnym rozwiązaniem jest nierdzewna chromowa stal martenzytyczna 420, która oprócz naturalnej odporności na korozję zapewnia wyjątkowe połączenie parametrów wytrzymałościowych i odporności na zużycie.

Odporność na zużycie

Nierdzewna stal chromowa 420 zapewnia podwyższoną odporność na zużycie, co jest istotne biorąc pod uwagę, że kołki sprężyste zwijane w wielu zastosowaniach często mają służyć jako elementy dynamiczne. Unikalną cechą kołków sprężystych zwijanych jest to, że ich elastyczność po instalacji chroni otwory i zespoły elementów łączonych poprzez tłumienie wibracji i obciążeń udarowych. Aby porównać parametry pracy, przeprowadzono testy kołków zwijanych tej samej kategorii (tj. grubość materiału), o takich samych wymiarach, wykonanych z trzech standardowych materiałów:

- **MBK** – kategoria standardowa, stal wysokowęglowa, zwykłe wykończenie;
- **MCK** – kategoria standardowa, nierdzewna stal chromowa 420, zwykłe wykończenie;
- **MDK** – kategoria standardowa, stal nierdzewna austenityczna 300, zwykłe wykończenie.

Wynikające z testu linie trendu wskazują na lepsze właściwości stali nierdzewnej chromowej 420 pod względem odporności na zużycie podczas testu z zastosowaniem zwiększanej wartości procentowej minimalnej siły ścinania podwójnego.

Podsumowanie

Kołki sprężyste zwijane wykonane ze stali nierdzewnej chromowej 420 są doskonałym wyborem w wypadku zastosowań, w których kluczowe znaczenie mają wysokie parametry wytrzymałościowe, umiarkowana ochrona przed korozją oraz wyjątkowa odporność na zużycie. Dodatkowe korzyści, które należy wziąć pod uwagę:

- doskonały stosunek kosztów do korzyści w zastosowaniach, w których wymagana jest wysoka efektywność;
- wysoka odporność na zużycie;
- dobra wytrzymałość na rozciąganie i rozstęp w umiarkowanie podwyższonych temperaturach;
- odporność na utlenianie i erozję;
- wyższa czystość elementów w porównaniu do stali wysokowęglowej;
- ograniczona możliwość występowania produktów wielomateriałowych i zanieczyszczeń w porównaniu do zastosowania produktów wykonanych z powlekanej stali węglowej.

SPIROL®

www.spirol.com

Bezpieczeństwo energetyczne z wojskowej perspektywy jednym z tematów rzeszowskiej konferencji energetycznej

Instytut Polityki Energetycznej im. Łukasiewicza, organizator corocznej konferencji „Bezpieczeństwo Energetyczne – filary i perspektywa rozwoju" od paru lat współpracuje z Kwaterą Główną Organizacji Paktu Północnoatlantyckiego. Podobnie będzie w tym roku. Eksperci z NATO będą brali udział w dwóch panelach: „Nowoczesny łańcuch dostaw paliw: wyzwania i możliwości" oraz „Ochrona krytycznej infrastruktury podmorskiej".

Tegoroczna konferencja „Bezpieczeństwo Energetyczne – filary i perspektywa rozwoju" odbędzie się w dniach 9 i 10 września 2024 r. w Centrum Konferencyjnym Politechniki Rzeszowskiej. W ramach konferencji odbędą się dwa panele organizowane z udziałem przedstawicieli Kwatery Głównej Paktu. W tym roku tematami przewodnimi tych sesji będzie kwestia rozbudowy systemu rurociągów NATO na wschodnią flankę Sojuszu, w tym do Polski, oraz problematyka ochrony morskiej infrastruktury krytycznej, w tym infrastruktury na Morzu Bałtyckim.

– W kontekście pierwszego tematu chcemy porozmawiać m.in. o kwestii wpływu rosyjskiej agresji na Ukrainę na bezpieczeństwo dostaw paliw dla sił zbrojnych, ale także o procesach transformacji energetycznej i tego jak system rurociągów NATO wpisuje się w to kompleksowe zagadnienie – mówi Dominik P. Jankowski, zastępca stałego przedstawiciela Polski przy NATO, który będzie moderatorem obydwu paneli. – W kontekście drugiego tematu chcemy dyskutować o roli, jaką NATO może odegrać we wspieraniu sojuszników w ochronie podwodnej infrastruktury energetycznej i wzmacnianiu jej odporności. Z perspektywy Polski jest to szczególnie ważne w kontekście takich instalacji jak m.in. Baltic Pipe, terminal LNG, Naftoport czy farmy wiatrowe na Bałtyku.

Jak podkreśla dr hab. Mariusz Ruszel, prof. Politechniki Rzeszowskiej i prezes Instytutu Polityki Energetycznej, to właśnie region Morza Bałtyckiego ma strategiczne znaczenie dla Polski z perspektywy nie tylko zachowania ciągłości dostaw ropy naftowej i gazu ziemnego, ale także zabezpieczenia kabli elektroenergetycznych łączących Polskę ze Szwecją oraz budowanych morskich farm wiatrowych.

– Należy pamiętać, że powstanie elektrowni jądrowej w Polsce będzie wymagało również zagwarantowania bezpieczeństwa logistyki morskiej w regionie Morza Bałtyckiego, chociażby ze względu na transport elementów niezbędnych do jej budowy – dodaje dr hab. Mariusz Ruszel.

Podobnie jak w ostatnich latach, także w tym roku w konferencji wezmą udział jako prelegenci i słuchacze liczni przedstawiciele wojska, m.in. wojskowych uczelni i jednostek badawczych.

Konferencja dofinansowana jest ze środków budżetu państwa, przyznanych przez Ministra Edukacji i Nauki w ramach Programu „Doskonała Nauka II".
Partner strategiczny: ML-SYSTEM
Partner merytoryczny: Polskie Towarzystwo Bezpieczeństwa Narodowego
Patronaty honorowe: Minister Spraw Zagranicznych, Prezes Urzędu Regulacji Energetyki, Wojewoda Podkarpacki, Marszałek Województwa Podkarpackiego, Prezydent Miasta Rzeszowa, Narodowa Agencja Poszanowania Energii S.A., Główny Instytut Górnictwa Państwowy Instytut Badawczy, Rektor Politechniki Rzeszowskiej im. Ignacego Łukasiewicza

Przemysł Spotkań:

Przełomowa platforma wspierająca rozwój przemysłu

Podążając za zmianami na szybko ewoluujących rynkach przemysłu ciężkiego, technologii i energii odnawialnej w EXPO Katowice S.A. narodziła się koncepcja Przemysłu Spotkań. Ta nowatorska platforma przyciąga przedstawicieli biznesu z różnych sektorów przemysłu, oficjeli państwowych i dyplomatów z różnych krajów. W ramach Przemysłu Spotkań odbywają się nie tylko ekspozycje najnowszych technologii i rozwiązań, lecz także konferencje, debaty i panele dyskusyjne, które eksplorują kluczowe kwestie związane z przyszłością i rozwojem przemysłu i technologii. Przemysł Spotkań to dynamiczna platforma, na której przemysł i biznes spotyka się z globalnym zapotrzebowaniem, tworząc możliwości współpracy, innowacji i rozwoju.

Jednym z najważniejszych wydarzeń Przemysłu Spotkań są Międzynarodowe Targi EXPO KATOWICE, które zdobyły silną pozycję, dzięki wystawie innowacyjnych maszyn i urządzeń. Od 40 lat wydarzenie to nieustannie ewoluowało i w miarę postępu i rozwoju wystawcy z kraju i ze świata prezentowali na nim najnowsze technologie w dziedzinie sprzętu dla górnictwa. Międzynarodowe Targi EXPO KATOWICE na stałe już wpisały się w światowy kalendarz wydarzeń przemysłowych.

Duże znaczenie podczas tegorocznego wydarzenia będą miały konferencje, które wzbogacą ekspozycję targową, a ich tematyka poruszy istotne kwestie. Podczas konferencji „Przemysł 5.0 – Wyzwania Transformacyjne Sektora Przemysłowego" 4 – 6 września 2024 liderzy branży, eksperci, innowatorzy oraz przedstawiciele sektora publicznego i prywatnego będą dyskutować o kluczowych wyzwaniach związanych z piątą rewolucją przemysłową: o wpływie nowoczesnych technologii na przyszłość sektora przemysłowego, o adaptacji przedsiębiorstw do nowych realiów rynkowych oraz o strategicznych kierunkach rozwoju przemysłu w nadchodzącej dekadzie. Szczególna uwaga poświęcona będzie procesom cyfryzacji w gospodarce, praktycznym wdrożeniom robotyzacji, sztucznej inteligencji oraz analizie Big Data w produkcji i usługach. Ciekawym tematem będą również zagadnienia związane z IoT, Cloud Computing i cyberbezpieczeństwem.

Kolejna konferencja w ramach Przemysłu Spotkań to „Nowe Horyzonty Miast" z tematyką skoncentrowaną m.in. na najnowsze trendy i wyzwania urbanistyczne. Debaty dotyczyć będą elektromobilności, nowoczesnej komunikacji publicznej czy transformacji energetycznej. Poruszana będzie także tematyka smart city. Są to kluczowe zagadnienia dotyczące rozwoju miast i kształtowania przyszłości społeczności miejskich. Integracja nowoczesnych technologii w infrastrukturze miejskiej, tworzenie inteligentnych i zrównoważonych środowisk miejskich, prezentacja konkretnych przykładów wdrożeń technologicznych, które już teraz zmieniają sposób funkcjonowania miast, o tym wszystkim dowiemy się już we wrześniu w Międzynarodowym Centrum Kongresowym podczas Międzynarodowych Targów EcoDom EXPO KATOWICE.

Integralną częścią Przemysłu Spotkań jest wydarzenie Start-up UNIVERSE, które promuje innowacje przemysłowe. Konkursy dla firm i studentów stymulują rozwój nowych technologii oraz wspierają rozwój gospodarczy.

Przemysł Spotkań, organizowany w sercu Katowic, jest nie tylko miejscem prezentacji najnowszych osiągnięć technologicznych, lecz również platformą integracji, wymiany doświadczeń i kreowania przyszłości przemysłu w kontekście globalnym. Dzięki różnorodności tematycznej i interdyscyplinarnemu podejściu, wydarzenie staje się niezwykle istotnym czynnikiem w kształtowaniu gospodarki przyszłości. Współgospodarzem Przemysłu Spotkań jest Miasto Katowice – Miasto wielkich wydarzeń, które wspólnie z EXPO Katowice S.A. zapraszają już dziś na wydarzenia w dniach 4 – 6 września br.

EXPO Katowice S.A.

KATOWICE dla odmiany

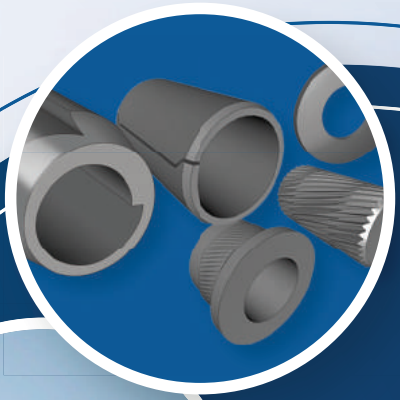
SPIROL®

Od 1948

Odwiedź *NOWE* SPIROL.com!

Twoje źródło informacji na temat elementów złącznych oferujące:

- *Katalogi Produktów & Specyfikacje*
- *Rysunki 2D/3D*
- *Filmy instruktażowe*
- *Opracowania techniczne*
- *Przykłady aplikacji*
- *Często zadawane pytania*
- *I dużo więcej...*



Również dostępne na SPIROL.com:

BEZPŁATNE WSPARCIE INŻYNIERYJNE

Inżynierowe Aplikacji SPIROL czekają, by pomóc Ci wybrać najbardziej odpowiedni element złączny, podkładkę precyzyjną lub sprzęt instalacyjny do Twojej aplikacji!

Zgodne z:
IATF 16949 • AS9100 • ISO 9001

Odwiedź SPIROL.com!

SHARKBITE I JOHN GUEST AIR & PNEUMATICS

Dwa światowej klasy, niezawodne rozwiązania typu push-fit, które pasują do wszystkich zastosowań sprężonego powietrza i pneumatyki

Sprężone powietrze jest to powietrze utrzymywane pod pewnym ciśnieniem, które zwykle jest wyższe od ciśnienia atmosferycznego. W krajach europejskich od 8% do 10% energii elektrycznej jest wykorzystywane do wytwarzania sprężonego powietrza. W przemyśle (po sprężeniu do odpowiedniego ciśnienia) powietrze wykorzystywane jest jako nośnik energii do zasilania maszyn i urządzeń o napędzie pneumatycznym. Może być również stosowane jako nośnik informacji w pneumatycznych układach sterowania. Przygotowanie sprężonego powietrza realizowane jest w specjalnych urządzeniach sprężarkowych, składowane jest w zbiornikach, a jego transport odbywa się z wykorzystaniem rur i elementów instalacji pneumatycznych.

W 2018 roku nastąpiło połączenie firm John Guest i RWC. Jednym z pierwszych efektów wspólnej pracy było stworzenie nowego systemu instalacji pneumatycznej SharkBite Air – systemu mosiężnych złączy wtykowych i anodowanej rury aluminiowej, aby uprościć małe i duże komercyjne i przemysłowe instalacje sprężonego powietrza. Wysoce niezawodne mosiężne i plastikowe systemy wciskane marek RWC SharkBite i JG Speedfit uzupełniają się wzajemnie, aby ułatwić życie instalatorom, poprawić wydajność i wydajność pierścieni powietrznych oraz skrócić czas konfiguracji nawet o 50% w porównaniu z konwencjonalnymi metodami.

Specjalnie zaprojektowany do małych i dużych zastosowań komercyjnych i przemysłowych, SharkBite wprowadził wytrzymały system rur powietrznych typu push-fit, który może pracować pod ciśnieniem do 20 barów i przekracza standardy branżowe, zapewniając dodatkowy spokój ducha. System ten jest mile widzianym rozwiązaniem tradycyjnych wyzwań w branży, takich jak długi czas instalacji, korozja rurociągów, spadki ciśnienia i wycieki, które prowadzą do wyższych kosztów energii.

Mosiężny system sprężonego powietrza wciskany jest dostępny w rozmiarach od 10 mm do 54 mm i zawiera konstrukcję zabezpieczającą przed manipulacją, która zapewnia bezpieczny demontaż. Gama obejmuje również kolanko 45° dla lepszego przepływu powietrza i zmniejszenia spadków ciśnienia w przewodzie powietrznym. SharkBite Air to także nowa gama

zaworów wtykowych w zakresie średnic *fi* 15 mm do *fi* 54 mm – od tak dawna oczekiwanych przez instalatorów.

Nasi klienci borykają się z wieloma problemami związanymi z wydajnością miedzianych i stalowych instalacji sprężonego powietrza. Systemy te są podatne na korozję i z czasem ulegają degradacji, co powoduje wycieki i spadki ciśnienia, a także wpływa na zużycie energii, cykl życia sprzętu i wydajność użytkowania. Konserwacja i serwisowanie konwencjonalnych instalacji jest również wyzwaniem i wiąże się z długimi przestojami, ponieważ rury i złącza muszą być gwintowane, zaciskane, lutowane lub sklejane. Dzięki naszej gamie SharkBite Air & Pneumatics montaż instalacji jest znacznie szybszy, a połączenia można wykonać bez użycia narzędzi za pomocą prostego działania na wcisk. Mosiężne złączki i rury z anodyzowanego aluminium są wysoce odporne na korozję, zapewniając optymalny przepływ i jakość powietrza, jednocześnie wydłużając cykl życia i wydajność systemu i sprzętu.

Nowe rozwiązania SharkBite Air & Pneumatics uzupełniają istniejącą gamę lekkich plastikowych złączek wtykowych John Guest firmy RWC i rur przeznaczonych do małych i średnich obiektów, do 10 barów, takich jak warsztaty czy serwisy motoryzacyjne. Dostępne w rozmiarach od 3 do 28 mm. John Guest oferuje szybki montaż za pomocą prostego mechanizmu push-fit, który eliminuje konieczność stosowania narzędzi, rur gwintowanych, rozpuszczalników i kleju. Nasza unikalna konstrukcja pierścienia zacinającego mocno i bezpiecznie blokuje i utrzymuje rurę na miejscu, nie deformując jej i nie ograniczając przepływu. Systemy powietrzne John Guest są łatwe w rozbudowie lub modyfikacji, ponieważ są w pełni demontowalne, bez użycia narzędzi, co skraca czas konserwacji i przestojów produkcyjnych. Złącza są dostępne w wersji z tworzywa sztucznego lub mosiądzu, w tym unikalny separator wody, który usuwa wilgoć z przewodu powietrznego, poprawiając wydajność i trwałość systemu.

Zarówno plastikowe, jak i mosiężne systemy wciskane doskonale nadają się do obecnego trendu elastycznych fabryk, w których układy fabryk muszą dostosowywać się i zmieniać szybciej niż kiedykolwiek wcześniej przy minimalnych przestojach. Wszystkie złączki i rury można łatwo zdemontować, a następnie zmienić, przedłużyć lub zmodyfikować w ciągu kilku sekund. Rozwiązania te są również z natury zrównoważone – rury i złączki są wielokrotnego użytku i wymienne, posiadają akredytacje UKAS i BCAS.

Reliance Worldwide Corporation
Reliance Worldwide Distribution (Europe) Ltd.
Oddział Polska
ul. Starołęcka 7, 61-361 Poznań
tel. +48 61 87 80 408
e-mail: info.pl@rwc.com
www.rwc.com
www.johnguest.com

Aby uzyskać więcej informacji o naszej rodzinie marek RWC oraz jak nasze rozwiązania mogą pomóc w codziennym życiu zapraszamy do odwiedzania nas na stronie **www.rwc.com** **www.johnguest.com**

SharkBite®

Zawór kulowy
do instalacji pneumatycznych i sprężonego powietrza

- Połączenie na wcisk
- Specjalnie zaprojektowany korpus z mosiądzu
- O-ring z nitrylu i pierścień chwytający ze stali nierdzewnej
- Ciśnienie robocze 18-20 bar
- Bezpieczne narzędzie do demontażu
- Zabezpieczony, zamykany uchwyt

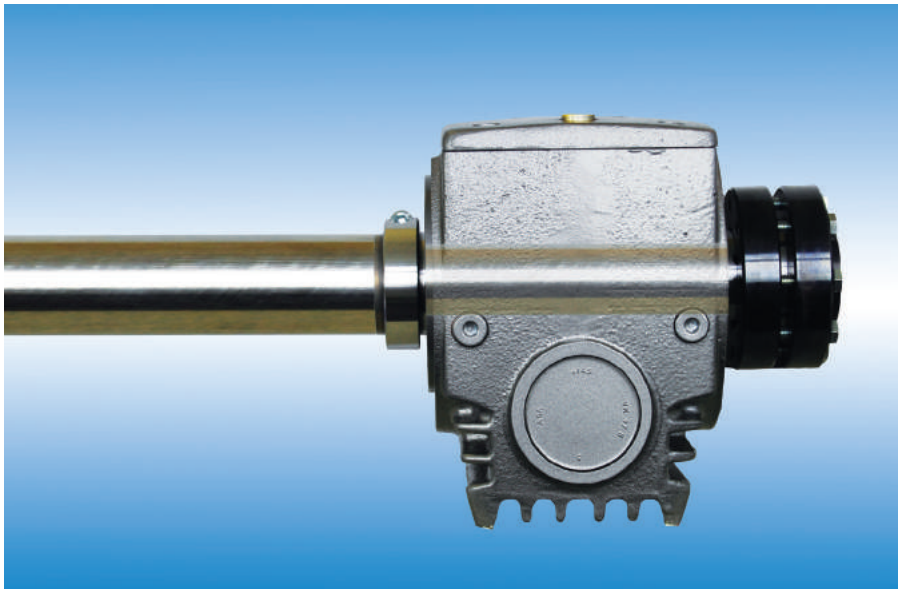
Reliance Worldwide Distribution (Europe) Ltd
Oddział Polska
Tel: +48 / 878-04-08 info.pl@rwc.com
www.rwc.com www.johnguest.com

AN RWC BRAND

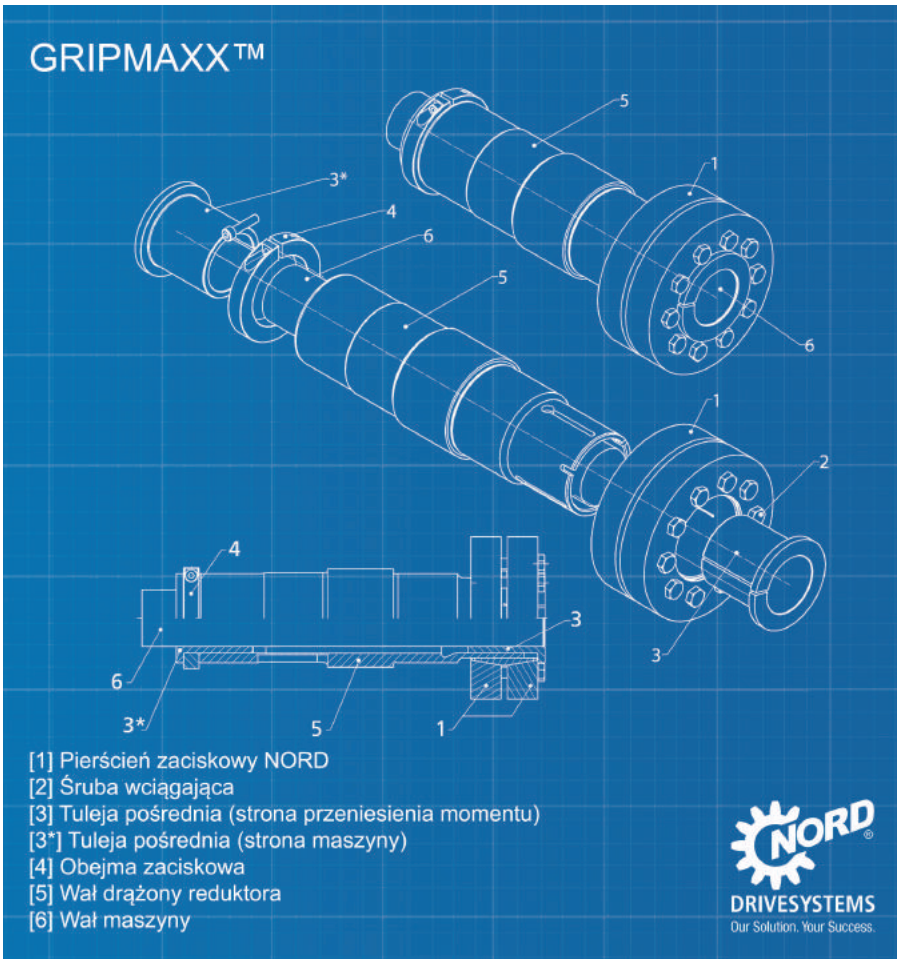
Gripmaxx™:

Trwałe mocowanie napędu przy minimalnej obsłudze

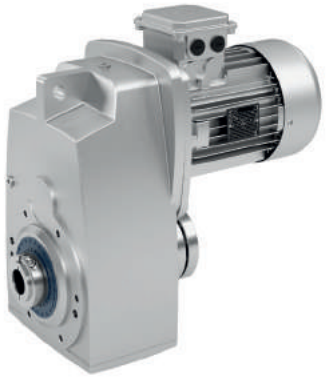
Nowoczesne zakłady przemysłowe coraz częściej poszukują innowacyjnych i efektywnych rozwiązań technicznych, które umożliwiają optymalizację procesów produkcyjnych i minimalizację przestojów. Jednym z takich przełomowych rozwiązań jest system mocowania Gripmaxx™ oferowany przez firmę NORD DRIVESYSTEMS.



Gripmaxx™ to zaawansowany system bezwpustowego mocowania tulei, który wykorzystuje pierścienie zaciskowe oraz tuleje dzielone do montażu przekładni NORD z wałami drążonymi na wałach maszyn klienta. System ten działa poprzez dociskowe pierścienie zewnętrzne i dwustronnie stożkowy pierścień wewnętrzny, które zapewniają wysokie ciśnienie na wał urządzenia. W miarę dokręcania śrub wciągających, pierścień wywiera nacisk poprzez tuleję pośrednią i tuleję przekładni na wał urządzenia, tworząc interferencyjne połączenie o wysokiej wytrzymałości. Dzięki temu rozwiązaniu uzyskuje się wysoką siłę zacisku, która jest idealna do aplikacji wymagających precyzyjnego pozycjonowania lub odwracania kierunku ruchu, a także do zastosowań z częstymi startami i zatrzymaniami. Gripmaxx™ eliminuje luzy oraz korozję cierną, co jest częstym problemem w tradycyjnych systemach z wałem wpustowym.



Gripmaxx został opracowany przy użyciu najnowszej technologii modelowania elementów skończonych (FEM), aby jak najlepiej zoptymalizować dobór materiału, konstrukcję mechaniczną i wykonanie. Gripmaxx™ oferuje szereg korzyści w porównaniu do konwencjonalnych rozwiązań mocowania. System jest wszechstronny – jeden rozmiar obudowy przekładni może być dostarczony z aż 15 różnymi rozmiarami tulei, co zapewnia elastyczność w doborze odpowiednich elementów.



System wykorzystuje standardowe wały, co eliminuje konieczność obróbki mechanicznej kluczy i wpustów. Do wygenerowania dużych sił zacisku nie ma potrzeby stosowania specjalistycznych narzędzi. W aplikacjach z częstymi startami i zatrzymaniami, obciążeniami udarowymi lub odwracaniem kierunku ruchu, tradycyjne rozwiązania z kluczem mogą powodować mikroruchy na styku wału z piastą, co prowadzi do wysokich naprężeń i możliwej awarii komponentów. Gripmaxx™ eliminuje te problemy, oferując bezkluczowe połączenie interferencyjne, które minimalizuje korozję cierną i redukuje koszty instalacji oraz eksploatacji. Brak korozji ciernej jest zapewniony poprzez zastosowanie, między pierścieniem zaciskowym a tuleją, rozciętego wzdłużnie pierścienia z hartowanej stali poddanej procesowi obróbki cieplnej – azotowaniu gazowemu oraz plazmowemu. Dodatkowo powierzchnie pierścienia zaciskowego poddane są procesowi chemicznemu, podczas którego powstaje powłoka tlenku żelaza zapewniająca podwyższoną odporność na ścieranie oraz korozję. W porównaniu do standardowych systemów shrink disc, które oferowane są w ograniczonej liczbie rozmiarów, Gripmaxx™ zapewnia szeroką gamę kombinacji rozmiarów przekładni i wałów, co zwiększa elastyczność i oszczędności.

Gripmaxx™ to innowacyjne rozwiązanie od NORD DRIVESYSTEMS, które oferuje zaawansowane możliwości mocowania wałów w przekładniach przemysłowych. Dzięki swojej wszechstronności, łatwości instalacji i niezawodności, system ten stanowi doskonały wybór dla zakładów przemysłowych poszukujących optymalizacji swoich procesów produkcyjnych. Gripmaxx™ to inwestycja w trwałość, efektywność i niezawodność, które przekładają się na realne oszczędności i zwiększenie wydajności operacyjnej. Rozwiązanie minimalizuje czas potrzebny na demontaż napędu z urządzenia. Za jego zastosowanie podziękują serwisanci, którzy nigdy już nie spędzą godzin na próbach ściągnięcia skorodowanej tulei napędu z wału maszyny.

NORD Napędy Sp. z o.o.
Zakrzów 414
32-003 Podłęże
tel. 12 288 99 00
fax 12 288 99 11
biuro@nord.com
www.nord.com

Dobór zasilaczy UPS i zespołów prądotwórczych, a ich prawidłowa współpraca

W dzisiejszych czasach, przy wszechobecnej elektronice, bardzo istotne jest zabezpieczenie się przed nagłymi i niekontrolowanymi przerwami w dostawach prądu, które mogą sparaliżować nasze codzienne życie. Najbardziej zalecanym sposobem zapewnienia poprawności zasilania urządzeń jest zastosowanie systemów zasilania gwarantowanego UPS. W przypadku zaniku lub nieprawidłowości napięcia sieciowego zadaniem ich jest dostarczenie energii do odbiorników (przy wykorzystaniu energii zgromadzonej w akumulatorach) w określonym czasie, niezbędnym do bezpiecznego, kontrolowanego zakończenia realizowanych procesów, a często dodatkowo poprawa jakości dostarczanego do odbiorników napięcia.

Tandem UPS + agregat łączy w sobie zalety długiego czasu podtrzymania awaryjnego, z możliwością zasilania wrażliwych odbiorników napięciem wysokiej jakości

W celu zapewnienia dłuższego podtrzymania (przy oczekiwaniu wysokiej jakości dostarczanej energii) warto do zasilaczy UPS podłączyć dodatkowe moduły bateryjne lub zastosować połączenie zasilacza UPS z zespołem prądotwórczym. Agregat dostarcza energię o gorszych parametrach niż UPS, natomiast czas zasilania awaryjnego jest niemalże nieograniczony – należy tylko uzupełniać zużywane paliwo. Pewnym problemem w jego funkcjonowaniu jest fakt, że przy zanikach napięcia sieciowego powstaje przerwa w zasilaniu, wynikająca z czasu uruchomienia się silnika spalinowego zespołu prądotwórczego. Wówczas rolą UPS jest zapewnienie bezprzerwowego zasilania odbiorników napięciem o odpowiednich parametrach do czasu ustabilizowania się parametrów napięcia generowanego przez agregat prądotwórczy. W wyniku współdziałania tych urządzeń osiąga się bezprzerwowe zasilanie wrażliwych odbiorników napięciem o wymaganej jakości i długim czasie autonomii. Często się zdarza, że zestawiane do współpracy UPS-y oraz agregaty funkcjonują nieprawidłowo, dlatego bardzo istotne jest ich prawidłowe zestawienie.

Dobierając zestaw UPS – agregat należy prawidłowo dobrać moce znamionowe obu urządzeń. W praktyce stosowany współczynnik doboru mocy agregatu do mocy UPS jest na poziomie 1,2 ÷ 1,7. W oferowanych przez firmę EVER rozwiązaniach mieści on się w dolnej części tego zakresu, co wynika z jakości zestawianych urządzeń. Niski współczynnik doboru mocy jest dla użytkownika korzystny, ponieważ zapotrzebowaną moc odbiorników pokrywa UPS, dla którego dobrany jest agregat o mniejszej mocy, co skutkuje niższymi kosztami inwestycyjnymi podczas instalacji systemu.

Kolejnymi istotnymi parametrami, na które należy zwrócić uwagę przy doborze zestawu UPS – agregat są wartość i częstotliwość napięcia generowanego przez agregat, które to powinny mieścić się w oknie wejściowym zasilacza UPS. Parametry te szczególnie zmieniają się podczas dynamicznych zmian obciążenia. W przypadku gdy wartość i częstotliwość napięcia generowanego przez agregat będą poza zakresem akceptowalnym przez zasilacz UPS, wówczas zasilacz nie przełączy się na pracę sieciową (normalną) tylko pozostanie w trybie rezerwowym (bateryjnym). Zalecane jest stosowanie zespołów prądotwórczych wyposażonych w elektroniczne regulatory prędkości obrotowej, z prądnicami przystosowanymi do nieliniowych obciążeń.

Agregat i UPS gwarantuje bezprzerwowe zasilanie od momentu zaniku zasilania, aż do czasu przejęcia pracy przez agregat. Tym samym zapewnia ciągłość pracy i zachowanie jej rezultatów bez ryzyka ponoszenia strat

Przy doborze zestawu UPS – agregat przydatne również jest posiadanie przez zasilacz UPS interfejsu umożliwiającego komunikację z zespołem prądotwórczym pozwalającym ograniczyć prąd wejściowy zasilacza UPS (przez zablokowanie prądu pobieranego przez układ prostownika do czasu powrotu napięcia w sieci). Taką funkcjonalność umożliwiają np. rozwiązania UPS EVER serii POWERLINE GREEN 33 PRO.

W praktyce często się zdarza, że zestawiane do współpracy UPS-y oraz agregaty funkcjonują nieprawidłowo. W celu rozwiązania tego problemu warto oprzeć się o zestaw (UPS + agregat prądotwórczy) dopracowany i przetestowany przez ekspertów. Takimi właśnie rozwiązaniami są m.in. UPS-y EVER serii POWERLINE GREEN 33 PRO oraz polecane przez firmę EVER agregaty.

EVER Sp. z o.o.
Michał Przybylski – Starszy Inżynier Wsparcia Technicznego

Trendy w automatyzacji i robotyzacji, interaktywne pokazy, najnowsze rozwiązania dla fabryk przyszłości, a także setki maszyn dla przedsiębiorstw produkcyjnych zdominowały w tym roku ekspozycję targów ITM INDUSTRY EUROPE

Zakończoną 7 czerwca edycję odwiedziło 14.726 profesjonalistów, by zapoznać się z ofertą ponad siedmiuset wystawców, która zajęła aż dziesięć pawilonów. W Poznaniu na inauguracji targów symbolicznie rozpoczęto dekadę Przemysłu 5.0.

– Idea Przemysłu 4.0, o której zaczynaliśmy mówić dekadę temu, dziś jest codziennością i jest mocno widoczna na ITM INDUSTRY EUROPE w ofercie produktów i technologii prezentowanych na targach. Możemy śmiało powiedzieć, że rozpoczynamy dekadę Przemysłu 5.0. Największym wyzwaniem będzie połączenie robotyzacji i automatyzacji z czynnikiem ludzkim. W tej edycji można zwiedzić ekspozycję ponad siedmiuset wystawców – mówił podczas ceremonii otwarcia targów ITM INDUSTRY EUROPE, MODERNLOG i SUBCONTRACTING Filip Bittner, wiceprezes zarządu Grupy MTP.

Tegoroczna edycja tego kluczowego dla branży przemysłowej i logistycznej wydarzenia trwała cztery dni – od 4 do 7 czerwca 2024 r. – i odbyła się tradycyjnie na terenie Międzynarodowych Targów Poznańskich.

W blasku nagród

Produkt, który otrzymuje Złoty Medal MTP musi wyróżniać się nowoczesnością i unikalnością. Takie właśnie są rozwiązania nagrodzone podczas tegorocznych targów. Kapituła konkursu postanowiła przyznać aż dwadzieścia dwa Złote Medale produktom zgłoszonym przez wystawców targów ITM INDUSTRY EUROPE. Dodatkowo pięć tych prestiżowych wyróżnień otrzymały firmy prezentujące swoją ofertę na targach MODERNLOG.

Na czele kapituły konkursu stanął prof. dr hab. inż. Michał Wieczorowski, prorektor ds. rozwoju i współpracy z gospodarką Politechniki Poznańskiej. Jak podkreślał przewodniczący, wybór laureatów był bardzo trudny z uwagi na ich wysoki poziom innowacyjności oraz unikalne cechy związane ze zrównoważonym rozwojem. Nowością tegorocznej edycji konkursu Złoty Medal MTP targów ITM INDUSTRY EUROPE i MODERNLOG było przyznanie specjalnej nagrody Grand Prix za wyjątkowe rozwiązanie, które poruszyło ekspertów, pokazując ciekawe możliwości. Takim okazało się być ProtoPlastMaker 4.0 – centrum addytywno-skrawające obróbki tworzyw sztucznych zgłoszone przez Zachodniopomorski Uniwersytet Technologiczny w Szczecinie, wyprodukowane przez PPHU POLIGRAF WIESŁAW KASPROWIAK. W tym roku także po raz pierwszy kapituła przyznała wyróżnienie Eco Prize Grupy MTP – za najbardziej ekologiczny produkt pośród nagrodzonych. Za taki uznano produkt Altergrinding E firmy Lubrinnova, zgłoszony przez SYNTACO Sp. z o.o.

Ceremonia otwarcia była także momentem triumfu wystawców targów ITM INDUSTRY EUROPE, którzy najciekawiej zaaranżowali swoje stoiska zdobywając uznanie kapituły, a w rezultacie prestiżową nagrodę Acanthus Aureus.

Gorące debaty, spektakularne pokazy i gratka dla „gamerów”

Jak przekonywać firmy do wdrożenia automatyzacji, jak obliczać ślad węglowy w przedsiębiorstwach, jak zbudować bliźniaka cyfrowego? – to tylko część pytań, na które odpowiadali eksperci podczas dyskusji toczonych w trakcie ITM INDUSTRY EUROPE. Nie zabrakło też widowiskowych pokazów na stoiskach wystawców i w strefach specjalnych oraz warsztatów zakończonych certyfikatem.

Uczestnicy targów ITM INDUSTRY EUROPE mogli m.in. zaczerpnąć wiedzy na temat technologii jutra w Fabryce Przyszłości przygotowanej przez DBR77. Od wczesnych godzin rannych nie cichły

tam także rozmowy na Scenie Tech. Słuchacze dowiedzieli się m.in. jak tworzy się Bliźniaka Cyfrowego, a także jak market place może zrewolucjonizować zarządzanie zasobami. Poruszono także temat AI i wpływu sztucznej inteligencji na działalność fabryk.

Niuanse współpracy robota i człowieka można było bliżej poznać w Strefie Robotów Współpracujących, która była nowością tegorocznej edycji targów ITM INDUSTRY EUROPE. W jednym miejscu i czasie przedstawiono ofertę niemal wszystkich kluczowych producentów cobotów. Spektakularne pokazy towarzyszyły także Strefie Bezpieczeństwa, gdzie pięć wiodących firm działających w branży bezpieczeństwa przemysłowego połączyło siły, tworząc innowacyjne widowisko w postaci testów uderzeniowych.

Jednocześnie w innych salach w ramach przestrzeni wystawienniczej debatowano m.in. o bezpieczeństwie maszyn i ich wpływie na konkurencyjność, a także obalano mity dotyczące AI i analityki w przemyśle. Eksperci TIDK zastanawiali się wspólnie, czy przemysł jest gotowy na AI i czy to już jest dobry moment na rozwijanie kompetencji w zespole w tym zakresie.

Na stoisku redakcji „Lakiernictwa Przemysłowego" można było zobaczyć interaktywną wystawę urządzeń do malowania oraz produktów dedykowanych lakierowaniu. Uczestnicy testowali w praktyce urządzenia, m.in. pistolety i pompy, a także samodzielnie malowali detale farbą proszkową czy na mokro. Ponadto redakcja przygotowała specjalne wykłady branżowe.

Prawdziwa gratka czekała także w Strefie Pneumat.Game, gdzie można było

wziąć udział w Turnieju Służb Utrzymania Ruchu, zagrać w wyjątkowe, bo pneumatyczne piłkarzyki, przejść labirynt skonstruowany przez Politechnikę Krakowską lub zagrać we flippera.

Warsztaty z certyfikatem, czyli jak obliczać ślad węglowy

W przedsiębiorstwach produkcyjnych ślad węglowy powstaje bezpośrednio w działalności wytwórczej przedsiębiorstwa, ale też w procesach poprzedzających wytwarzanie produktów oraz w procesach wprowadzania produktów na rynek. Jak obliczać ślad węglowy i jak nim zarządzać dla spełnienia wymagań regulacyjnych i zwiększenia konkurencyjności? Na to pytanie można było uzyskać odpowiedź podczas warsztatów odbywających się w trakcie targów. Jak przekonywano podczas warsztatów, obecnie obowiązujące nowe regulacje wymagają od przedsiębiorców raportowania poziomu śladu węglowego. Warsztaty zakończone certyfikatem dotyczące obliczania, raportowania i redukowania śladu węglowego zorganizowane zostały przez Centrum Przemysłu 4.0

Politechniki Śląskiej we współpracy z Grupą MTP.

Przemysł wspierany przez naukę

Targi ITM INDUSTRY EUROPE to miejsce, gdzie szczególnie mocno wybrzmiewa współpraca nauki i przemysłu. Widząc potencjał współpracy na linii biznes – nauka, Grupa MTP podjęła decyzję o zainicjowaniu nowej koncepcji: Strefy Nauki i Startupów. Idea polega na zebraniu w jednym miejscu najciekawszych innowacji z polskich uczelni oraz stworzeniu wystawcom i gościom targowym dogodnej możliwości dyskusji z osobami odpowiedzialnymi za współpracę polskich jednostek naukowych z otoczeniem. Za przygotowanie i prowadzenie Strefy odpowiada Porozumienie Spółek Celowych oraz Porozumienie Akademickich Centrów Transferu Technologii, łącznie skupiające ponad 120 jednostek zajmujących się transferem wiedzy. Podczas targów ITM INDUSTRY EUROPE Strefę Nauki i Startupów stworzyło 15 uczelni, które zaprezentowały aż 32 innowacyjne rozwiązania pod wspólnym hasłem „Nauka dla przemysłu ery cyfrowej".

Międzynarodowe targi innowacyjnych rozwiązań przemysłowych. Za nami trzecia edycja targów Warsaw Industry Automatica 2024!

W dniach 14 – 16 maja 2024 roku Ptak Warsaw Expo stało się europejską stolicą automatyzacji i robotyki. To wszystko dzięki największym targom Warsaw Industry Automatica 2024. Wydarzenie to stanowiło platformę do rozwoju branży między innymi dzięki praktycznym wykładom.

Lata 2020 – 2024 to dla sektora przemysłowego okres dynamicznego wzrostu automatyzacji i robotyzacji procesów produkcyjnych. Oznacza to ułatwiony dostęp do tego typu rozwiązań dla przeciętnego przedsiębiorcy. Obecna sytuacja stymuluje popyt oraz zachęca dostawców technologii do różnicowania oferowanych produktów, w efekcie czego nowe rozwiązania są jeszcze bardziej dopasowane do potrzeb poszczególnych gałęzi gospodarki. Ten trend stał u podstaw organizacji Warsaw Industry Automatica, czyli międzynarodowych targów integrujących krajowych przedsiębiorców z zagranicznymi inwestorami. Wydarzenie odbyło się w dniach 14 – 16 maja 2024 roku w Ptak Warsaw Expo.

Cenieni liderzy w branży

Warsaw Industry Automatica zgromadziła wyłącznie sprawdzone i cenione marki. Właściciele przedsiębiorstw produkcyjnych, kierownicy produkcji, specjaliści ds. utrzymania ruchu oraz inżynierowie automatyzacji i robotyki mogli zapoznać się z nowościami oraz zagranicznymi trendami, które zdobywają uznanie na światowych rynkach.

Swoje rozwiązania zaprezentowali producenci i dystrybutorzy zaawansowanych technologii automatyki przemysłowej, w tym robotów przemysłowych, systemów wizyjnych, czujników, oprogramowania sterującego oraz komponentów maszyn przemysłowych. Obecni byli również dostawcy oprogramowania do zarządzania produkcją, producenci systemów sterowania oraz firmy oferujące rozwiązania w zakresie elektroniki przemysłowej.

Podczas wydarzenia swoje rozwiązania prezentowali przedstawiciele takich firm jak: BECKHOFF, FINDER, INDUPROGRESS, WIRE SOLUTIONS, PROPOINT, i wielu innych wiodących producentów w branży automatyki przemysłowej.

Dyskusja o rozwoju branży automatyki przemysłowej

Podczas panelu „Prezentacje i trendy wystawców" praktycy podzielili się swoją wiedzą na temat najnowszych trendów i technologii, które zdobywają uznanie na światowych rynkach. Dyskutowano o innowacjach w automatyce przemysłowej, bezpieczeństwie pracy oraz nowoczesnych technikach w robotyzacji. Małgorzata Kocur (Automa.Net) opowiedziała rozwiązaniach B2B i dropshippingu dla handlu przemysłowego, Krzysztof Gliński (EKALTECH) zreferował opracowanie systemu paletyzacji/depaletyzacji produktów z nowatorski przenośnikiem 3-sekcyjnym i robotem przemysłowym. Marcin Szuper (Finder Polska) przedstawił historię rozwoju przekaźników programowalnych, a Maciej Wawrzyniak (Robotics) omówił innowacje w chwytakach do robotów.

Wielki sukces trzeciej edycji Warsaw Industry Automatica

Trzecia edycja Warsaw Industry Automatica zakończyła się sukcesem. Odwiedziło ją 10415 uczestników, którzy poznali oferty 215 wystawców. Zapraszamy na kolejną odsłonę wydarzenia! Więcej informacji już wkrótce.

Rozłączne scenariusze katastrofalnego ryzyka SI

Kaj Sotala

Wprowadzenie

Praca w dziedzinie związanej z bezpieczeństwem wymaga czegoś, co zostało nazwane „mentalnością bezpieczeństwa" (Schneier, 2008): umiejętności spojrzenia na istniejący system i zaobserwowania, w jaki sposób może on zostać zagrożony przez zdeterminowanego atakującego. Podobnie praca nad bezpieczeństwem związanym ze SI wymaga analogicznego sposobu myślenia, w którym ludzie aktywnie analizują, w jaki sposób coś może pójść nie tak, zamiast zakładać, że wiarygodny pomysł na wykonanie czegoś dobrze, jest wystarczający do zapewnienia bezpieczeństwa (Arbital, 2017).

Niestety scenariusze dotyczące ryzyka związanego z wyrafinowaną SI (np. Yudkowsky, 2008a, Bostrom, 2014, Sotala i Yampolskiy, 2015) nie zawsze były przedstawiane w sposób, który wyraźnie jasno akcentował potrzebę myślenia o bezpieczeństwie SI. Powszechną krytyką jest to, że choć scenariusze te zawierają wiarygodny argument, to nie jest on w żadnym wypadku *nieunikniony*, a odrzucenie jakiejkolwiek kluczowej przesłanki umożliwiłoby uniknięcie scenariusza. Następnie przyjmuje się, że cała analiza sugerująca taki scenariusz jest fatalnie wadliwa i można ją bezpiecznie porzucić.

Trafną odpowiedzią na taką krytykę byłoby wskazanie różnych sposobów wystąpienia katastroficznego wyniku, aby się przekonać, czy argumenty za ryzykiem rzeczywiście zależą od łatwych do obalenia przesłanek. Jednak oprócz jednego znaczącego wyjątku (A. Barrett i Baum, 2017a) nie podjęto próby systematycznej analizy różnych czynników umożliwiających katastrofę w sposób, który ułatwiłby ich analizę.

Ten rozdział ma na celu przedstawienie szerokiego spojrzenia na różne sposoby, w jakie rozwój wyrafinowanej SI może doprowadzić do tego, że stanie się ona wystarczająco potężna, aby spowodować katastrofę. W szczególności ten rozdział ma na celu skupienie się na sposobie, w jaki różne rodzaje ryzyka są *rozłączne*, na jak wiele różnych sposobów coś może pójść nie tak, z których każdy może doprowadzić do katastrofy. Czyniąc to, rozdział ma na celu rozwinięcie dotychczasowych prac (A. Barrett i Baum, 2017a), które zainicjowały stosowanie ustalonych metodologii analizy ryzyka w dziedzinie bezpieczeństwa SI (A. Barrett i Baum, 2017b).

Skoncentrowano się na SI na tyle zaawansowanej, aby można było ją uważać za OSI lub ogólną sztuczną inteligencję, raczej pomijając ryzyko związane z „wąską SI", takie jak na przykład technologiczne bezrobocie (Brynjolfsson i McAfee, 2011). Należy jednak zauważyć, że niektóre z omówionych zagrożeń, w szczególności kluczowe zdolności związane z wąskimi dziedzinami zawarte w części „Inicjator MSA: kluczowe możliwości", mogą powstać na dowolnym etapie przejścia od wąskich systemów SI do superinteligencji.

Celem pracy nie było zaprzeczenie lub zminimalizowanie różnych pozytywnych aspektów, które mogą również wynikać z tworzenia SI, ani sugerowanie, że nie należy kontynuować rozwoju SI. Celem było raczej umożliwienie realizacji pozytywnego potencjału SI w taki sam sposób, w jaki lepsze zrozumienie słabości związanych z bezpieczeństwem komputerowym pozwala na tworzenie bezpiecznych systemów komputerowych.

Inicjatorzy katastrofy

Większość argumentów za ryzykiem związanym z SI wynika z połączenia dwóch roszczeń (Yudkowsky, 2008a, Bostrom, 2014, Sotala i Yampolskiy, 2015): roszczenia dotyczącego zdolności i roszczenia dotyczącego wartości. W tym rozdziale skoncentrowano się na badaniu różnych sposobów, dzięki którym roszczenie zdolności może się spełnić. Model roszczenia wartości wykracza poza zakres tego rozdziału, aczkolwiek można zapoznać się na przykład z pracą Barretta i Bauma (2017a).

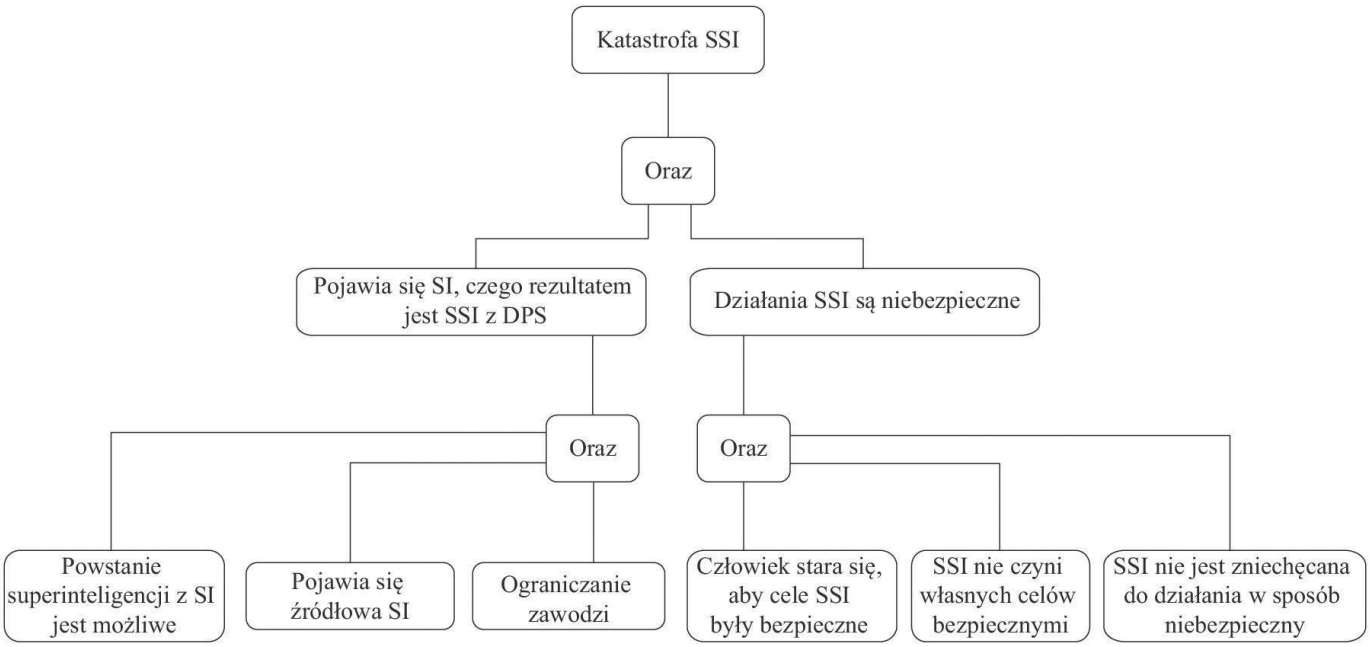
1. *Roszczenie dotyczące zdolności*: SI może stać się wystarczająco zdolna do potencjalnego wyrządzenia poważnych szkód dobru ludzkiemu.
2. *Roszczenie dotyczące wartości*: SI może działać zgodnie z wartościami, które nie są zgodne z wartościami ludzkości, powodując w ten sposób znaczne szkody.

Roszczenia te można rozpatrzeć bardziej szczegółowo. Istniejącym modelem takich roszczeń jest model SSI-PATH (A. Barrett i Baum, 2017a) (rysunek 1). SSI-PATH koncentruje się na analizie ścieżek, po których SI może doprowadzić do katastrofy, stając się superinteligentną przez rekurencyjne samodoskonalenie, przy czym ludzie nie są w stanie zapobiec tym niebezpiecznym działaniom.

Model SSI-PATH wykorzystuje konwencje schematu błędów, w których niepożądanym zdarzeniem (katastrofą SI) jest węzeł górny, po którym następują dwa węzły mogące uaktywnić górny węzeł, gdyby oba były prawdziwe. Są to węzły „Działania SSI są niebezpieczne", które odpowiadają roszczeniu wartości oraz „SI rozwija się, powstaje [Sztuczna SuperInteligencja] z [Decydująca Przewaga Strategiczna]", co odpowiada określonej formie roszczenia zdolności. W tym rozdziale rozwinięto SSI-PATH przez rozważenie bardziej ogólnych form roszczenia zdolności.

Roszczenie zdolności jest często formułowane jako możliwość osiągnięcia przez SI decydującej przewagi strategicznej (DPS). Pojęcie DPS były przyjmowane domyślnie w wielu wcześniejszych pracach, a koncepcja ta została po raz pierwszy wyraźnie zdefiniowana przez Bostroma (2014, s. 78) jako „poziom technologicznych i innych korzyści wystarczających, aby umożliwić [SI] osiągnięcie pełnej dominacji nad światem".

Jednakże założenie, że SI osiągnie DPS wydaje się niepotrzebnie silną formą roszczenia zdolności, ponieważ SI może



Rys .1. Górne warstwy modelu SSI-PATH. (Na podstawie: Barrett i Baum, *Journal of Experimental & Theoretical Artificial Intelligence: JETAI* 29 nr 2, 2017a: 397 – 414). Warstwy te zostały zaprojektowane jako drzewo błędów, obrazujące różne warunki, które muszą zostać spełnione, aby nastąpiła katastrofa związana z SSI. Według schematu katastrofa SSI zdarza się wtedy, gdy: (1) SI rozwija się, czego efektem jest SSI z DPS oraz (2) działania SSI są niebezpieczne, powodując katastrofalne użycie DPS. Dolne węzły wskazują trzy przypadki, które muszą być prawdziwe, aby SI mogła się rozwinąć, oraz kolejne trzy przypadki, które muszą zaistnieć, aby działania SSI były niebezpieczne. Pełny model zawiera dodatkowe warstwy, które nie zostały pokazane na rysunku. Więcej szczegółów można znaleźć w Barrett i Baum (2017a)

spowodować katastrofę niezależnie od niego. Rozważmy na przykład scenariusz, w którym SI rozpoczyna atak obliczony na zniszczenie ludzkiej cywilizacji. Jeśli SI udałoby się zniszczyć ludzkość lub jej dużą część, ale w rezultacie sama SI również zostałaby zniszczona, to nie liczyłoby się to jako DPS, jak pierwotnie zdefiniowano. Trudno jednak zaprzeczyć, że wynik taki należy jednak uznać za katastrofę.

Z tego powodu rozdział ten koncentruje się na sytuacjach, w których SI osiąga przynajmniej *znaczną* przewagę strategiczną (ZPS), którą określamy jako „poziom technologiczny i inne korzyści wystarczające, aby stanowić katastrofalne ryzyko dla społeczeństwa ludzkiego". Katastrofalne ryzyko to takie, które może spowodować poważne szkody dla dobrobytu ludzi w skali globalnej i spowodować 10 milionów lub więcej ofiar śmiertelnych (Bostrom i Ćirković, 2008).

Oprócz oczywistych przyczyn chęci uniknięcia katastroficznego ryzyka spowodowanego przez SI, zauważamy, że zniszczenia na szeroką skalę mogą przyczynić się do *globalnych zawirowań* (Bostrom i in., 2016), sytuacji, w której istniejące instytucje byłyby zagrożone, a koordynacja i długoterminowe

planowanie stałyby się także trudniejsze. Globalne turbulencje mogłyby następnie przyczynić się do kolejnego niekontrolowanego projektu SI, który zawiódłby jeszcze bardziej katastrofalnie i spowodowałby jeszcze większe szkody. Zatem to, co pierwotnie było jedynie katastroficznym ryzykiem, może przyczynić się do dalszego rozwoju ryzyka *egzystencjalnego* (Bostrom, 2002, 2013, Sotala i Gloor, 2017).

Znaczna część istniejącej literatury na temat bezpieczeństwa SI koncentruje się na badaniu scenariuszy, w których SI osiąga DPS, oraz na analizie warunków do tego prowadzących. Jest to pod wieloma względami rozsądna strategia, ponieważ jeśli bylibyśmy w stanie poradzić sobie z SI, która mogłaby osiągnąć DPS, to najprawdopodobniej bylibyśmy również w stanie poradzić sobie z SI, która mogłaby osiągnąć ZPS, zakładając, że silniejsza SI jest konserwatywnym założeniem (Yudkowsky, 2001). Jednak ta strategia ma tę wadę, że może sprawiać wrażenie, że znaczna część analizy bezpieczeństwa SI jest nieistotna, jeśli okaże się, że możliwość uzyskania DPS przez SI jest wyjątkowo nieprawdopodobne. Niektóre mechanizmy obronne mogą być również wystarczające, aby uniemożliwić SI uzyskanie DPS, ale nie są wystarczające, aby zapobiec uzyskaniu ZPS.

Kiedy zostaną podjęte działania przeciwko przewadze strategicznej?

SI, która jest w stanie wyrządzić znaczne szkody dobrobytowi ludzi, jest szczególnie groźna, gdy ma do tego motywację. Istnieje również możliwość, że SI zamierzająca współpracować z ludzkością może spowodować szkody przez przypadek, wykracza to jednak poza zakres niniejszej analizy. Pomimo że pełna analiza roszczenia wartości wykracza poza zakres tego rozdziału, to nie można jej całkowicie odseparować od roszczenia zdolności, ponieważ wartości SI wpływają również na próg zdolności, przy którym racjonalne staje się dla niej działanie przeciwko ludzkości. Jak omówiono, niektóre wartości i sytuacje zwiększają prawdopodobieństwo podjęcia wrogich działań przez SI, nawet jeśli ma niewielkie możliwości.

Dwa główne powody, dla których SI może podjąć działania powodujące szkody dla ludzkości, to:

- Szkodziłaby ludzkości w dążeniu do celu, który neguje ludzkie dobro, na przykład przez rozebranie ludzkich miast w poszukiwaniu surowców. „SI ani cię nie nienawidzi ani cię nie kocha, ale jesteś zbudowany z atomów, które może wykorzystać do czegoś innego" (Yudkowsky, 2008a, s. 333).
- Może oczekiwać, że ludzie podejmą działania przeciwko niej, co uniemożliwiłoby jej osiągnięcie celów, dlatego może podjąć działania w ich obronie, przeprowadzając atak zapobiegawczy. Byłoby to racjonalnym działaniem, ponieważ pozwoliłoby SI faktycznie zrealizować jej cele (Omohundro, 2007, 2008). Mogłoby się tak zdarzyć nawet wtedy, gdyby SI miała cel uwzględniający elementy ludzkiego dobrobytu, jeśli tylko SI znalazłaby powody, by sądzić, że ludzie mimo wszystko sprzeciwią się realizacji tego celu.

Dokładne cele, jakie ma SI, wpływają na poziom zdolności, których potrzebuje do tego, by wrogie ludziom działania uznać za racjonalną strategią. SI, która troszczy się głównie o jakiś mocno sprecyzowany cel, może chcieć zniszczyć ludzką cywilizację, aby mieć pewność, że potencjalne zagrożenie tego celu zostanie wyeliminowane. Dzięki temu SI mogłaby kontynuować realizację swojego celu bez przeszkód. Jednak SI, która zostałaby zaprogramowana tak, aby maksymalizować coś takiego jak „szczęście obecnie żyjących ludzi", mogłaby być znacznie mniej skłonna zaryzykować znaczną liczbę ofiar śmiertelnych. Zmusiłoby to ją do skupienia się na mniej niszczycielskich metodach przejmowania potencjalnie wymagających bardziej wyrafinowanych umiejętności.

W rezultacie wartości SI określają poziom zdolności, jaki musi mieć, aby wrogie działanie było wykonalną strategią. W uproszczonym modelu (Shulman, 2010) SI uważająca, że zainicjowanie agresywnych działań ma prawdopodobieństwo odniesienia sukcesu P oraz oczekiwaną użyteczność UE(Sukces), jeśli się powiedzie, UE(Niepowodzenie), jeśli się nie powiedzie, i UE(Współpraca), jeśli zaprzestanie agresji i nadal będzie współpracować, racjonalnie zainicjuje agresję, jeśli:

$$P \times UE(\text{Sukces}) + (1 - P) \times UE(\text{Niepowodzenie}) > UE(\text{Współpraca}).$$

Można to uznać za sugestię, że SI przeprowadziłaby atak przede wszystkim wtedy, gdyby miała DPS lub myślała, że może ją zdobyć, a tym samym ustanowić dominację nad ludźmi. Jednak nawet SI z tylko ZSA może podjąć wrogie działania, stosując środki, takie jak wymuszenie i groźby wyrządzenia bardziej ograniczonych szkód, w celu zdobycia większej ilości zasobów lub skierowania świata w bardziej sprzyjającym kierunku.

Między innymi może się to zdarzyć:

- Jeśli SI nabrałaby tempa we własnym rozwoju, uzyskując tym samym zdolność do autonomicznego działania i wierzyła, że nie można jej wyśledzić (zobacz części od „Wyzwanie techniczne" do „Dobrowolne uwolnienie z desperacji", gdzie omówiono sposoby, w jakie SI może uzyskać swobodę lub zostać dobrowolnie uwolniona przez jej twórców).
- Gdyby SI miała sojuszników, którzy chroniliby ją przed odwetem (zobacz część „Inicjator ZPS: kluczowe zdolności", gdzie zamieszczono informacje na temat umiejętności manipulacji społecznych oraz część „Wyzwanie społeczne", aby dowiedzieć się, w jaki sposób autonomiczna SI może pozyskać ludzkich sojuszników).
- Jeśli SI kontrolowałaby ludzką organizację, której nie można zaatakować bez olbrzymich, postronnych zniszczeń (zobacz części „Inicjator DPS/ZPS: SI stopniowo przejmuje władzę" oraz „SI pozostaje ograniczona, jednak ostatecznie przejmuje kontrolę", gdzie opisano przejęcie kontroli nad ludzką organizacją).
- Gdyby istniały już silniejsze systemy SI podejmujące działania, a SI uznałaby siebie za zbyt mało wartą odwetu (zobacz część „Uwagi na temat pojedynczej i licznej SI", gdzie omówiono liczną SI).

Niezależnie od skali agresji na zachowanie SI wpływają również różne inne czynniki sytuacyjne. Na przykład SI może nie być skłonna do powodowania szkód, ponieważ mogłaby pomyśleć, że spowoduje to zbyt wiele szkód ubocznych wobec rzeczy, które ceni, ponieważ nie uważałaby się za zdolną do przetrwania wynikającego z jej działań odwetu lub ponieważ oszacowałaby, że wynikające z takiej agresji szkody w infrastrukturze pozbawiłby ją zasobów (takich jak elektryczność) potrzebnych do jej przetrwania.

Ataki różnią się także zakresem, w jakim można je selektywnie zastosować. Tradycyjna broń palna może być wycelowana wybiórczo, podczas gdy pandemie potencjalnie zagrażają wszystkim przedstawicielom gatunku. W zakresie, w jakim SI musi polegać na ludzkiej gospodarce, która wytwarza zasoby potrzebne do przetrwania SI, ataki zagrażające gospodarce również zagrażają zasobom SI. Zasoby te są w pewnym sensie dzielone pomiędzy SI i ludzkość, tak więc wszelkie ataki, które powodują masowe uszkodzenia tych zasobów, są niebezpieczne dla obu stron. Im bardziej SI może projektować ataki selektywnie pozbawiające przeciwników zasobów, tym niższy jest próg ich wykorzystania. Bardziej zaawansowane możliwości przebudowy infrastruktury pozwoliłyby SI na przeprowadzenie bardziej masowego ataku. SI, która była w stanie zbudować bardziej zaawansowaną infrastrukturę niż obecnie istniejąca, mogłaby zlekceważyć uszkodzenia obecnej infrastruktury, jeśli i tak planowałaby zburzyć jej większość.

Bilans tych kalkulacji mógłby zostać przesunięty, gdyby SI myślała, że grozi jej zniszczenie przez ludzi, nawet gdyby współpracowała (obniżając oczekiwaną użyteczność współpracy). Samozachowawczość jest instrumentalnym celem wielu różnych wartości, ponieważ istniejący agent jest bardziej zdolny do promowania większości wartości niż agent, który nie istnieje (Omohundro, 2007, 2008, Bostrom, 2012). SI, która znalazłaby się w bezpośrednim niebezpieczeństwie zniszczenia, mogłaby racjonalnie zainicjować kontratak, ryzykując nawet duże zniszczenia, o ile oszacowałaby, że oczekiwana wartość scenariusza, w którym kontratak umożliwiłby jej przetrwanie i promowanie jej wartości, przewyższałaby szkody spowodowane przez taki kontratak. Byłoby to szczególnie przekonującym czynnikiem motywującym, gdyby SI miała idiosynkratyczne wartości, które jej zdaniem z małym prawdopodobieństwem byłyby promowane przez innych agentów. Gdyby istniało wiele projektów SI i SI uwierzyłaby, że jeden z innych projektów może pierwszy uzyskać DPS, to byłby to wystarczający powód, by zaryzykować wcześniejszy atak (zobacz część „Uwagi na temat pojedynczej i licznej SI", gdzie zawarto opis licznej SI). Pojawiły się również propozycje zaprojektowania wartości SI w sposób, który wyraźnie obniża wartość wrogiego działania.

W powyższej analizie założono, że SI wybiera swoje działania racjonalnie. Irracjonalność może wydawać się czymś, co uniemożliwiłoby SI uzyskanie bardzo dużych zdolności, jednak, podobnie jak ludzie, SI mogłaby być pod niektórymi względami racjonalna, a pod innymi nieracjonalna. Dla SI może być również racjonalne podjęcie działań pozornie nieracjonalnych, na przykład poprzez irracjonalne ignorowanie zagrożeń, tak aby inni uważali próby zagrażania jej za mniej opłacalne (Parfit, 1984, część 5). Główną kwestią wynikającą z potencjalnej nieracjonalności jest to, że nie można po prostu polegać na tym, że SI nie spowoduje uszkodzeń, nawet jeśli byłby to racjonalny sposób jej zachowania. Oczywiście nieracjonalność może również spowodować, że SI uniknie wyrządzania szkód w sytuacji, gdyby było to racjonalne (tabela 1).

Inicjatorzy katastroficznych zdolności

W tej części rozważono cztery ogólne scenariusze, według których SI mogłaby uzyskać DPS lub ZPS: scenariusze indywidualnego wejścia w życie z jego trzema głównymi podtypami, scenariusze zbiorowego wejścia w życie, scenariusze stopniowego przejęcia kontroli przez systemy SI oraz scenariusze, kiedy SI staje się wystarczająco dobra w niektórych kluczowych możliwościach i uzyskuje ZPS lub DPS.

Na prawdopodobieństwo sukcesu lub porażki każdego z tych scenariuszy wpływa również to, jaką zdolnością do współpracy wykażą się ludzie. Pomimo że możliwe są scenariusze, w których SI staje się całkowicie samodzielna i musi uniemożliwić twórcom jej wyłączenie, to istnieje również wiele możliwych scenariuszy omówionych w części „SI uzyskuje zdolność do samodzielnego działania", w których SI uzyskuje częściową lub pełną współpracę swoich twórców, przynajmniej do pewnego momentu. Taki rozwój wydarzeń wpłynąłby na prawdopodobieństwo spełnienia się każdego z poniższych scenariuszy. Scenariusz, w którym prototypowa SI musi unikać jej zamknięcia przez programistów, różni się bardzo od scenariusza, w którym programiści są pewni, że SI jest bezpieczna i dobrowolnie pomagają jej gwałtownie się rozwinąć, szczególnie jeśli mają do dyspozycji zasoby dużej korporacji lub państwa.

Inicjatorzy DPS: scenariusze wejścia w życie

„Odejście" (Bugaj i Goertzel, 2007) to proces, w którym SI staje się znacznie bardziej zdolna niż ludzkość. W przypadku łagodnego wejścia w życie dzieje się to stopniowo w czasie, co pozwala na ciągłą interakcję człowieka, podczas gdy w przypadku gwałtownego wejścia w życie po przekroczeniu pewnego etapu SI bardzo szybko zwiększa swoje zdolności, wyrywając się ze skutecznej kontroli człowieka.

Warto zauważyć, że w przypadku gwałtownego wejścia w życie nie zakłada się, że SI stanie się bardzo zdolna natychmiast po stworzeniu (jednak moment jej utworzenia jest określony). Scenariusz gwałtownego wejścia w życie może obejmować wydłużony okres stopniowego rozwoju, aż do osiągnięcia pewnego kluczowego poziomu zdolności, od którego SI gwałtownie się rozwija.

Wiele wcześniejszych dyskusji (np. Yudkowsky, 2008a, Bostrom, 2014, Sotala, 2017) koncentrowało się na analizie możliwości gwałtownego wejścia w życie. Chociaż nie jest to jedyny możliwy scenariusz, w którym SI może stać się zdolna, to jest to scenariusz, który pozostawia najmniej możliwości przeciwdziałania złemu rozwojowi zdarzeń.

Mając na uwadze, że nadmierne skupienie się na scenariuszach gwałtownego wejścia w życie może zamaskować fakt, że nie jest on konieczny do tego, aby SI mogła uzyskać ZPS lub DPS, najpierw rozważymy scenariusze gwałtownego wejścia w życie, a następnie inne czynniki inicjujące.

Inicjator DPS: indywidualne wejście w życie

„Indywidualne wejście w życie" to takie, w którym pojedyncza SI staje się tak potężna, że całkowicie dominuje ludzkość. W literaturze zaproponowano trzy ogólne ścieżki prowadzące do takiego scenariusza: nadwyżka sprzętowa („więcej SI"), eksplozja prędkości („szybsza SI") i eksplozja inteligencji („inteligentniejsza SI") (Sotala i Yampolskiy, 2015). Bostrom (2014) omówił je w kategoriach odpowiednio superinteligencji kolektywnej, szybkiej superinteligencji i jakościowej superinteligencji. Należy zauważyć, że ścieżki te nie wykluczają się wzajemnie i wręcz przeciwnie, każda z nich może przyczynić się do rozwoju drugiej.

TABELA 1. Czynniki zwiększające prawdopodobieństwo, że SI będzie działać wbrew ludzkim interesom

Czynniki zwiększające prawdopodobieństwo ataku	Czynniki zmniejszające prawdopodobieństwo ataku
Wysokie subiektywne prawdopodobieństwo sukcesu lub oczekiwanie niewielkiego odwetu w przypadku niepowodzenia	Niskie subiektywne prawdopodobieństwo sukcesu i oczekiwanie późniejszego odwetu
Ochrona przed odwetem przez sojuszników lub kontrolą potężnej organizacji	Niechęć do utraty sojuszników lub kontroli nad organizacją z powodu odwetu
Cel, który nie uwzględnia obecnie żyjących ludzi	Cel, który ceni obecnie żyjących ludzi[a]
Możliwość ukrycia się przed odwetem	Brak możliwości przemieszczania lub ukrycia się przed działaniami odwetowymi
Możliwość przeprowadzania ataków, które pozwalają uniknąć uszkodzenia kluczowej infrastruktury lub innych cennych celów	Możliwość przeprowadzania tylko masowych ataków
Ryzyko zbliżającego się zniszczenia	Łatwo satysfakcjonujące lub trywialne wartości
Zaawansowana zdolność do budowy lub przebudowy infrastruktury	Cele o niskim wpływie
Wysoki poziom istniejącej automatyzacji zmniejszający zależność od pracowników	
Istnienie innych SI, które mogą pierwsze uzyskać DPS	
Irracjonalność	Irracjonalność

[a] W zależności od stopnia, w jakim obecnie żyjący ludzie są cenieni: „schwytaj, nie zabijaj" może być implikowane przez niektóre pozornie korzystne cele (Williamson, 1947), aczkolwiek nawet cele, które „tylko" zabraniają ludzkiej śmierci są trudniejsze do osiągnięcia niż cele, które pozwalają na więcej szkód ubocznych

Nadwyżka sprzętowa

W scenariuszu nadwyżki sprzętowej (Yudkowsky, 2008b, Shulman i Sandberg, 2010) sprzęt rozwija się szybciej niż oprogramowanie, dzięki czemu mogą zaistnieć komputery o większej mocy obliczeniowej niż ludzki mózg, jednak bez możliwości efektywnego wykorzystania całej tej mocy. Gdyby jednak ktoś opracował algorytm ogólnej inteligencji mogącej efektywnie wykorzystać taki sprzęt, to nagle mogłoby pojawić się mnóstwo taniego sprzętu, który mógłby zostać wykorzystany do uruchamiania tysięcy lub milionów kopii SI. Taka liczna SI mogłaby, ale i nie musiałaby być superinteligentna, jednak sama ich liczba pozwoliłaby SI na prowadzenie skoordynowanych operacji na masową skalę. Gdyby pojedyncza SI wykorzystała ten potencjał do wytworzenia dużej liczby swoich kopii lub subagentów, to umożliwiłoby to jej indywidualne wejście w życie. W przeciwnym razie stanowiłoby to zbiorowe wejście w życie, jak omówiono to poniżej.

Nadwyżka sprzętowa może się faktycznie wydarzyć, nawet jeśli SI byłaby początkowo ograniczona sprzętowo: pierwsze jednostki SI mogą wymagać dużej ilości sprzętu, jednak dalsze optymalizacje szybko mogą obniżyć wymagania sprzętowe. Patrząc na ostatnie postępy w rozwoju SI, początkowe podejście do nauki gier Atari 2600 (Mnih i in., 2015) wykorzystywało specjalistyczny sprzęt w postaci GPU, jednak dopiero rok później wydano alternatywne podejście, w którym wykorzystano standardowy procesor i osiągnięto lepsze wyniki przy użyciu krótszego czasu uczenia (Mnih i in., 2016). Oprócz sugestii, że optymalizacje oprogramowania mogą szybko zwiększyć liczbę możliwych do uruchomienia kopii SI, to także fakt poprawy szybkości i wydajności podkreśla możliwość wystąpienia scenariusza nadwyżki sprzętowej, który jednocześnie przyczynia się do możliwości wystąpienia scenariuszy eksplozji prędkości i eksplozji inteligencji, jak omówiono poniżej.

Eksplozja prędkości

W scenariuszu eksplozji prędkości (Solomonoff, 1985, Yudkowsky, 1996, Chalmers, 2010) inteligentne maszyny projektują coraz szybsze maszyny. Nadwyżka sprzętowa może się przyczynić do eksplozji prędkości, nie jest jednak ona warunkiem koniecznym. SI działająca w tempie człowieka mogłaby opracować sprzęt drugiej generacji, na którym mogłaby działać w znacznie szybszym tempie niż ludzkie myśli. Opracowanie sprzętu kolejnej, trzeciej generacji wymagałoby zatem krótszego czasu i umożliwiłoby SI działać jeszcze szybciej niż poprzednia generacji i tak dalej. W pewnym momencie proces dotarłby do fizycznych granic i zatrzymałby się, jednak do tego czasu sztuczna inteligencja mogłaby wykonać większość zadań w znacznie szybszym tempie niż ludzie, osiągając w ten sposób dominację. Zasadniczo można to również osiągnąć za pomocą ulepszonego oprogramowania, jak to wcześniej omówiono.

Stopień, w jakim SI potrzebuje ludzi do wyprodukowania lepszego sprzętu, ogranicza tempo eksplozji prędkości, tak więc szybka eksplozja prędkości wymaga zdolności do automatyzacji dużej części procesu produkcji sprzętu. Jednak ten rodzaj automatyzacji może zostać osiągnięty do czasu opracowania SI. Im większa automatyzacja, tym szybciej może nastąpić zdobycie dominacji przez SI.

Jeśli poziom bezpieczeństwa sprzętu byłby dobry, to scenariusze eksplozji szybkości, w których SI włamuje się do systemów produkcyjnych i przejmuje nad nimi kontrolę, stają się mniej prawdopodobne. Z drugiej strony istnieją możliwe ścieżki, omówione w części „SI uzyskuje zdolność do samodzielnego działania", w których SI uzyskuje prawowitą kontrolę nad różnymi zasobami. Zapewnienie odpowiedniej kontroli bezpieczeństwa zautomatyzowanym fabrykom nie byłoby pomocne, jeśli byłyby one kierowane przez SI lub jeśli SI mogłaby uzyskać do nich dostęp na otwartym rynku i miałaby na ten cel wystarczającą ilość środków.

Eksplozja prędkości może również przyczynić się do zaistnienia nadwyżki sprzętowej i eksplozji inteligencji, umożliwiając znalezienie bardziej wydajnych lub w inny sposób lepszych algorytmów w krótszym czasie.

Eksplozja inteligencji

Podczas eksplozji inteligencji (Dobry, 1965, Chalmers, 2010, Bostrom, 2014) SI wymyśla, jak stworzyć jakościowo inteligentniejszą SI i następnie ta inteligentniejsza SI wykorzystuje swoją zwiększoną inteligencję do stworzenia jeszcze bardziej inteligentnej SI i tak dalej. W ten sposób ludzka inteligencja pozostałaby daleko w tyle, a maszyny osiągnęłyby dominację.

W wielu dziedzinach istnieją granice przewidywania na podstawie eksplozji kombinatorycznych, które wynikają z próby prognozowania coraz bardziej w przyszłość. Na przykład w modelowaniu prognozy pogody można uzyskać dostęp tylko do ograniczonej liczby wstępnych obserwacji w odniesieniu do liczby stopni swobody systemu przewidywania pogody (Buizza, 2002). Jednak, nawet jeśli superinteligentna SI nie byłaby w stanie dokładnie przewidzieć każdego przyszłego zdarzenia, to nadal mogłaby zareagować na to zdarzenie i przewidzieć jego prawdopodobne konsekwencje lepiej niż ludzie. Tetlock i Gardner (2015) dokonali przeglądu i omówili zdolność niektórych ludzkich prognostów („superprognostów") do

przewidywania wydarzeń na świecie ze znaczną dokładnością. Na temat nieprzewidywalnych wydarzeniach zwanych „czarnymi łabędziami" (Taleb, 2007) Tetlock i Gardner (2015, Kindle lok. 3614) piszą:

Możemy nie mieć żadnych dowodów na to, że superprogności mogą przewidzieć wydarzenia takie jak te z 11 września 2001. Istnieje jednak cały szereg dowodów na to, że mogą prognozować pytania, takie jak: czy Stany Zjednoczone zagrożą działaniami wojskowymi, jeśli talibowie nie przekażą Osamy bin Ladena? Czy talibowie zgodzą się na to? Czy bin Laden ucieknie z Afganistanu przed inwazją? W zakresie, w jakim takie prognozy mogą przewidzieć konsekwencje wydarzeń podobnych do tych z 11 września, a konsekwencje takie sprawiają, że czarny łabędź jest tym, czym jest, to możemy przewidzieć wystąpienie czarnych łabędzi.

Sotala (2017), na podstawie przeglądu literatury na temat ludzkiej wiedzy i inteligencji, stwierdza, że u ludzi wiedza specjalistyczna opiera się na rozwijaniu wyobrażeń mentalnych, które pozwalają ekspertom zrozumieć różne sytuacje i albo natychmiast poznać odpowiednie działania w danej sytuacji, albo przeprowadzić mentalną symulację tego, jak może się rozwinąć taka sytuacja i jaka powinna być na nią reakcja. Taką wiedzę specjalistyczną zapewnia połączenie dwóch umiejętności: rozpoznawania wzorców i symulacji mentalnej.

Sotala (2017) twierdzi, że SI mogłaby usprawnić obie umiejętności. Zdolność nadludzkiej symulacji mentalnej można osiągnąć przez połączenie wykonywania bardziej złożonych symulacji z uwzględnieniem większej liczby czynników, a także poprzez wykorzystanie kilku strumieni uwagi, które mogłyby badać wiele alternatywnych metod równolegle, jednocześnie analizując wiele różnych perspektyw i czynników przyczynowych. Przeprowadzanie dokładnych symulacji mentalnych wymagałoby również dobrej reprezentacji mentalnej w celu utworzenia podstawowych elementów składowych symulacji. Wśród ludzi istnieją różnice poznawcze, które pozwalają niektórym ludziom uczyć się i uzyskiwać dokładne reprezentacje mentalne szybciej niż inni i wydaje się, że sprowadzają się one do takich czynników, jak pojemność pamięci roboczej, kontrola uwagi i pamięć długoterminowa. Czynniki te można udoskonalić przez połączenie ulepszeń sprzętowych i teoretycznej informatyki. Wydaje się, że u ludzi ulepszenie inteligencji zapewnia dodatkowe korzyści w całym udokumentowanym zakresie różnic inteligencji i wydaje się prawdopodobne, że różne ograniczenia ewolucyjne przyczyniły się do ograniczenia rozwoju ludzkiej inteligencji znacznie poniżej teoretycznego maksimum. W odniesieniu do ograniczeń prognozowania wynikających z wewnętrznej niepewności świata, Sotala (2017, s. 12) uznaje istnienie takich ograniczeń, jednak twierdzi, że:

wygląda na to, że chociaż system SI od samego początku nie byłby w stanie stworzyć jednego superplanu podboju świata, to wciąż miałby nadludzką zdolność adaptacji i uczenia się na podstawie zmieniających się i nowatorskich sytuacji oraz reagowania na nie szybciej niż ludzcy przeciwnicy. Analogicznie, eksperci grający w większość gier nie są w stanie obliczyć zwycięskiej strategii już od pierwszego ruchu, jednak nadal mogą reagować i dostosowywać się do zmieniającej się sytuacji gry lepiej niż nowicjusz, co pozwala im wygrać.

Eksplozja inteligencji może również przyczynić się do wystąpienia eksplozji prędkości i nadwyżki sprzętowej, jeśli zwiększona inteligencja SI umożliwiłaby jej znalezienie algorytmów, które były najbardziej wydajne pod względem możliwości uruchomienia większej liczby systemów SI z tym samym sprzętem (nadwyżka sprzętowa) lub możliwości szybszego uruchomienia (eksplozja prędkości).

Inicjator DPS: zbiorowe wejście w życie handlującej SI

Vinding (2016), a także Hanson i Yudkowsky (2013) argumentują, że duża część pozornie indywidualnej ludzkiej inteligencji w rzeczywistości opiera się na możliwości korzystania z rozproszonych zasobów całej ludzkości, zarówno tych materialnych, jak i poznawczych. Z tego powodu błędem może być skupienie się na punkcie, w którym SI osiągają inteligencję na poziomie ludzkim, ponieważ inteligencja zbiorowa jest ważniejsza niż inteligencja indywidualna. Najłatwiejszym dla SI sposobem na osiągnięcie poziomu zdolności porównywalnego z ludzkim byłaby współpraca ze społeczeństwem ludzkim i pokojowe wykorzystanie jego zasobów.

Hall (2008) podobnie zauważa, że nawet gdy pojedyncza SI dokona samodoskonalenia, na przykład opracowując lepsze modele kognitywistyki w celu ulepszenia swojego oprogramowania, to reszta gospodarki również będzie rozwijać takie lepsze modele. Z tego powodu dla SI korzystniejsze jest skupienie się na ulepszaniu wszystkiego, w czym jest najlepsza, i kontynuowanie handlu z resztą gospodarki oraz kupowanie tych rzeczy, w których reszta gospodarki jest lepsza od niej.

Jednak Hall zauważa, że nadal może nastąpić gwałtowne wejście w życie SI w momencie, gdy wystarczająca liczba kopii SI zostanie połączona w sieć. SI, która myśli szybciej niż ludzie, może się ze sobą komunikować i dzielić się spostrzeżeniami znacznie szybciej, niż może to robić z ludźmi. W rezultacie dla SI zawsze byłoby lepiej handlować i współpracować z innymi SI niż z ludźmi. Wielkość gospodarki SI może rosnąć dość szybko, a Hall (s. 464) sugeruje scenariusz: „od […] 30 000 równoważników ludzkich na początku do około 5 miliardów równoważników ludzkich dekadę później". Nawet więc jeśli żadna pojedyncza SI nie mogłaby sama osiągnąć DPS, to wspólna społeczność SI mogłaby ją osiągnąć, ponieważ taka społeczność rozwinęła się tak, aby była zdolna do wszystkiego, co ludzie byli w stanie osiągnąć.

Inicjator DPS/ZPS: SI stopniowo przejmuje władzę

Historycznym trendem było zautomatyzowanie wszystkiego, co można było zautomatyzować zarówno w celu zmniejszenia kosztów, jak i dlatego, że maszyny mogą robić rzeczy lepiej niż ludzie. Każda firma mogłaby potencjalnie lepiej funkcjonować, gdyby była prowadzona przez umysł, który został specjalnie zaprojektowany do prowadzenia danej firmy, włącznie z zastąpieniem wszystkich pracowników jednym lub większą liczbą takich umysłów. SI może myśleć szybciej i mądrzej, radzić sobie z większą ilością informacji naraz i pracować w jednym celu, zamiast osłabiać swoją efektywność przez politykę biurową, która nęka każdą dużą organizację. Niektóre szacunki już sugerują, że połowa zadań, za które ludzie są wynagradzani jest podatna na automatyzację przy użyciu technik współczesnego uczenia maszynowego i robotyki, nawet bez wprowadzania SI z ogólną inteligencją (Frey i Osborne, 2013, Manyika i in., 2017).

Tendencja do automatyzacji trwała przez całą historię, nie wykazuje żadnych oznak słabnięcia i nieodłącznie wiąże się z udzielaniem systemom SI dowolnych, potrzebnych możliwości, tak aby mogła lepiej zarządzać firmą. Istnieje ryzyko, że systemy SI, które początkowo były proste i miały ograniczoną inteligencję, będą stopniowo zdobywały coraz większą moc i odpowiedzialność, w miarę jak będą się uczyły i będą ulepszane, dopóki znaczna część społeczeństwa nie znajdzie się pod kontrolą SI.

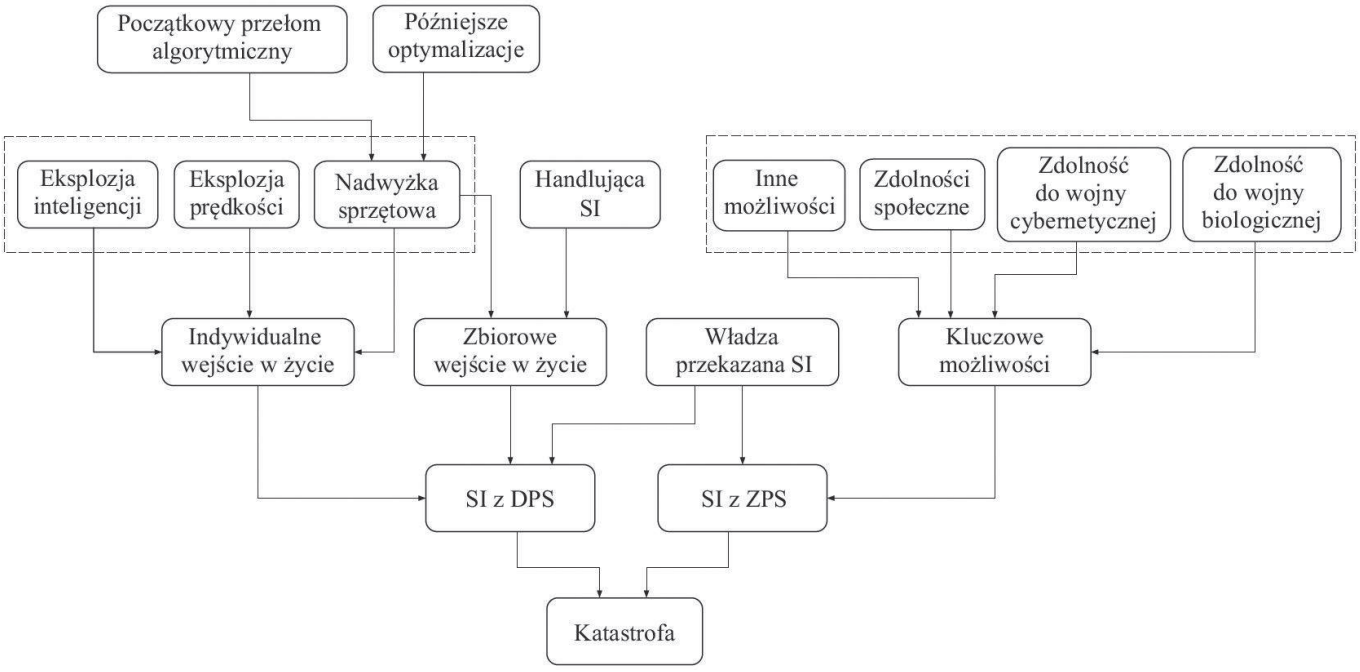
Inicjator ZPS: kluczowe możliwości

W przypadku omawiania ZPS kluczową kwestią jest próg zdolności wystarczający do zadania katastroficznych szkód. SI mogłaby być katastrofalnym ryzykiem, gdyby jej zdolności ofensywne w niektórych kluczowych dziedzinach były wystarczające do pokonania istniejącej obrony.

Jak krótko omówiono to w części „Kiedy zostaną podjęte działania przeciwko przewadze strategicznej?", zakładając, że SI byłaby racjonalna, to wybór spowodowania takich szkód wymagałby rozsądnego motywu. Jednak podobnie jak w przypadku ludzi, może istnieć szereg motywów, które uczynią rozsądną strategią wrogie działania, takie jak wymuszenie, chęć pomocy sojusznikowi lub atak uprzedzający przeciwko innej SI lub grupie mogącej uzyskać DPS. W zależności od celów i od tego, czy SI miałaby sojuszników, przeprowadzenie ataku możliwego ze względu na kluczowe zdolności może wymagać posiadania dodatkowych możliwości, takich jak odbudowa po zniszczeniu kluczowej infrastruktury.

Należy zauważyć, że powodowanie katastrofalnych uszkodzeń prawdopodobnie nawet nie wymaga nadludzkich zdolności (Torres, 2016, 2017, rozdz. 4). Na przykład wydaje się możliwe, że wystarczająco zdeterminowany ludzki napastnik mógłby obecnie spowodować poważne szkody w społeczeństwie przez wojnę elektroniczną. Chociaż nie odnotowano jeszcze cyberataków, które mogłyby bezpośrednio przyczynić się do śmierci, to kilka z nich spowodowało szkody fizyczne lub zakłócenia w działaniu służb ratunkowych. W maju 2017 roku ogłoszono, że robak ransomware „WannaCry" zainfekował ponad 230 000 komputerów w ponad 150 krajach (Ehrenfeld, 2017), powodując zakłócenie działania kluczowych usług, takich jak opieka zdrowotna (Gayle i in., 2017). W 2016 roku ogłoszono, że trzy podstacje w ukraińskiej sieci energetycznej zostały odłączone w wyniku ataku złośliwego oprogramowania, pozostawiając bez prądu około połowę domów w regionie zamieszkałym przez około 1,3 miliona mieszkańców (Goodin, 2016). Stworzony kiedyś robak Stuxnet również został skierowany przeciwko fizycznemu celowi, jakim były wirówki przemysłowe, które zostały skutecznie uszkodzone (Chen i Abu-Nimeh, 2011). W licznych przeprowadzonych badaniach wykazano, że ogromna liczba przemysłowych systemów kontroli, nadzorujących operacje w bankach i szpitalach, jest podłączona bezpośrednio do internetu bez jakiejkolwiek ochrony (Kiravuo i in., 2015).

Broń nuklearna posiadana przez USA i Rosję prawdopodobnie już teraz mogłaby zabić większość ludzkości. Związek Radziecki prowadził również szeroko zakrojony program rozwoju broni biologicznej, z roczną zdolnością produkcyjną wynoszącą około 90 – 100 ton zmodyfikowanego wirusa prawdziwej ospy, a także genetycznie opracowanymi chorobami odpornymi na ciepło, zimno i antybiotyki (USAMRIID, 2014), które mogły spowodować ogromne liczby ofiar śmiertelnych w przypadku ich użycia. Rozwój inżynierii genetycznej i biologii syntetycznej umożliwił również tworzenie czynników biologicznych o wiele bardziej zabójczych od tych, które mogły kiedykolwiek ewoluować w sposób naturalny (ibid., s. 150 – 153).



Rys. 2. Różne ścieżki, w wyniku których SI może uzyskać DPS lub ZPS, prowadząc tym samym do katastrofy. Połączenia między węzłami oznaczają bramki LUB (pominięte w celu zwiększenia czytelności). Na przykład nadwyżka sprzętowa może wynikać albo z początkowego przełomu dotyczącego algorytmów LUB późniejszych optymalizacji. Jak omówiono w tekście, każda z nadwyżek sprzętowych, eksplozji prędkości i eksplozja inteligencji może przyczynić się do dwóch pozostałych, co zostało oznaczone ramką. Podobnie oznaczono różne kluczowe zdolności

To, że jak dotąd żaden z tych scenariuszy się nie ziścił wynika z wartości ludzi zajmujących kluczowe stanowiska, a nie dlatego, że powodowanie ogromnych szkód wymagałoby nadludzkich zdolności.

W dziedzinie manipulacji społecznych wykorzystano współczesne uczenie maszynowe do tworzenia prognoz opartych na „polubieniach" dawanych przez użytkowników na Facebooku, a prognozy te są dokładniejsze niż prognozy dokonywane przez znajomych na podstawie kwestionariusza osobowości (Youyou i in., 2015).

„Polubienia "zostały również wykorzystane do dokładnego przewidywania cech prywatnych, takich jak orientacja seksualna (Kosinski i in., 2013). Niektóre doniesienia w popularnej prasie podają, że firma marketingowa Cambridge Analytica wykorzystująca marketing oparty na SI odegrała istotną rolę w wyborach prezydenckich w USA w 2016 roku oraz w referendum w sprawie członkostwa w Unii Europejskiej, które odbyło się w Wielkiej Brytanii w 2016 roku (Grassegger i Krogerus, 2017). Pomimo że prawdziwość tego twierdzenia pozostaje pytaniem otwartym i została zakwestionowana (Taggart, 2017), to daje to wyobrażenie, jakim rodzajem siły może dysponować SI zdolna do bardziej wyrafinowanego modelowania społecznego i manipulacji, stwarzającego możliwość stworzenia świata, w którym o wynikach wyborów krajowych decydowałyby systemy SI.

Ogólnie rzecz biorąc, niektóre prawdopodobne możliwości, które mogą pomóc uzyskać MPS, to wojna biologiczna (rozwijanie i uwalnianie plag biologicznych), wojna cybernetyczna (atakowanie systemów kluczowej infrastruktury) i manipulacje społeczne (przekonanie wystarczająco wielu ludzi do wykonania woli SI, nawet tylko jeden człowiek może spowodować katastrofalne zniszczenia, jeśli byłby na przykład głową państwa). Należy zauważyć, że podobnie jak w przypadku inicjatorów wejścia w życie SI, posiadanie jednej zdolności może przyczynić się do posiadania innych. Na przykład SI zdolna do manipulacji społecznej może wykorzystać ją do znalezienia współpracowników zdolnych do działania w innych dziedzinach, a wojna cybernetyczna może dostarczyć kompromitujących informacji, które będą pomocne w szantażowaniu ludzi lub gromadzeniu informacji o ludzkim zachowaniu.

Zestawienie inicjatorów DPS/ZPS

Na rysunku 2 przedstawiono różne ścieżki, które mogą prowadzić do wcześniej omówionych katastrof. Każda z nich, eksplozja prędkości, eksplozja inteligencji lub nadwyżka sprzętowa, może przyczynić się do indywidualnego wejścia w życie, kiedy to pojedyncza SI osiągnie ogromne możliwości.

Nadwyżka sprzętowa może również przyczynić się do zbiorowego wejścia w życie SI, kiedy to dodatkowe możliwości sprzętowe mogą umożliwić tworzenie dużej liczby systemów SI w krótkim czasie, które następnie mogą zacząć ze sobą handlować, wkrótce wyprzedzając ludzkość. Węzeł „handlująca SI" to kolejny inicjator umożliwiający zbiorowe wejście w życie SI, reprezentujący podobny scenariusz, w którym jednak nie występuje nadwyżka sprzętowa, a różne kopie SI są budowane przez dłuższy okres, aż do momentu osiągnięcia poziomu zdolności niezbędnego do zbiorowego wejścia w życie. Każda forma wejścia w życie SI mogłaby doprowadzić do powstania SI z DPS. SI może również osiągnąć DPS, jeśli ludzie dobrowolnie dadzą jej wystarczające możliwości. Gdyby liczne SI otrzymały pewną władzę, niewystarczającą do osiągnięcia DPS, to nadal mogłyby osiągnąć ZPS. Ponadto nawet pojedyncza SI, która nie była wystarczająco silna do osiągnięcia DPS, mogłaby osiągnąć ZPS, gdyby posiadała pewne wystarczające zdolności ofensywne.

SI uzyskuje zdolność do samodzielnego działania

Ażeby SI stanowiła zagrożenie dla ludzkości, musi dysponować sposobami wpływania na świat i wywoływania katastrof. Powszechną propozycją ograniczenia potęgi SI jest próba ograniczenia jej zdolności do komunikowania się ze światem i wpływania na niego, co jest ogólnie znane jako „uwięzienie" lub „zapakowanie SI" (Chalmers, 2010, Armstrong i in., 2012, Yampolskiy, 2012, Bostrom, 2014).

Wyzwania związane z ograniczeniem SI są dwojakie. Po pierwsze, istnieje techniczne wyzwanie polegające na ograniczeniu SI w taki sposób, aby nie była w stanie się oswobodzić i nadal była w stanie dostarczać użytecznych informacji. Ponadto takie ograniczenie ma też wymiar społeczny, w którym decydenci mogą mieć różne zachęty do złagodzenia zabezpieczeń związanych z ograniczeniem SI lub nawet do całkowitego uwolnienia SI, nawet jeśli utrzymanie jej w zamknięciu byłoby technicznie wykonalne (Sotala i Yampolskiy, 2015). Jeśli uwięzienie ma być skuteczne, to muszą zostać spełnione wymagania zarówno techniczne, jak i społeczne.

Wyzwanie techniczne

Powszechną reakcją jest to, że wystarczająco inteligentna SI znajdzie pewien sposób na oswobodzenie się, albo przez socjotechnikę, albo przez znalezienie możliwych do wykorzystania słabości w zastosowanych fizycznych zabezpieczeniach. Możliwość ta została szeroko omówiona w wielu artykułach, w tym przez Chalmersa (2010) oraz Armstronga, Sandberga i Bostroma (2012). Ogólnie, autorzy są bardzo ostrożni w formułowaniu zdecydowanych twierdzeń na temat naszych zdolności do utrzymywania w ograniczeniu umysłu o wiele mądrzejszego niż nasz wbrew jego woli. Jednak przy ostrożnym projektowaniu nadal może być możliwe zaprojektowanie SI łączącej wewnętrzną motywację do pozostania w kontakcie z szeregiem zewnętrznych zabezpieczeń monitorujących SI.

Wyzwanie społeczne

Ograniczenie SI zakłada, że ludzie, którzy je tworzą i są za nie odpowiedzialni, muszą być faktycznie zmotywowani do ograniczenia SI. Jeśli grupa ostrożnych badaczy zbuduje i następnie z powodzeniem ograniczy stworzoną SI, może to nie odnieść zamierzonego skutku, jeśli inna grupa stworzy SI, która została celowo uwolniona od ograniczeń. Przyczyny pozbawienia ograniczeń SI mogą obejmować: (i) korzyści ekonomiczne lub presję konkurencyjną, (ii) przyczyny etyczne lub filozoficzne, (iii) zaufanie do zabezpieczeń SI oraz (iv) rozpaczliwe okoliczności, takie jak nieuchronna zagłada. Każdą z tych przyczyn omówiono poniżej.

Dobrowolne uwolnienie SI ze względu na korzyści ekonomiczne lub presję konkurencyjną

Jak wspomniano wcześniej w części „SI stopniowo przejmuje władzę", istnieje znaczna ekonomiczna zachęta do wdrażania systemów SI w celu kontroli korporacji. Może się to wydarzyć w dwóch formach: przez zwiększenie zakresu kontroli, jakim dysponują istniejące już systemy, albo alternatywnie przez aktualizację istniejących systemów lub dodawanie nowych z nieistniejącymi wcześniej możliwościami. Te dwie formy mogą się ze sobą łączyć. Jeśli pewne zadania wykonywane jak dotąd przez ludzi zostaną następnie przekazane ulepszonej SI, która stanie się zdolna do ich wykonywania, to może to zwiększyć autonomię SI zarówno przez zwiększenie jej zdolności, jak i zmniejszenie liczby ludzi biorących udział w dotychczasowym procesie.

Częściowym przykładem jest dążenie wojsk USA do ostatecznego przejścia do stanu, w którym ludzcy operatorzy broni robotycznej znajdowaliby się „nad pętlą", a nie „w pętli" (Wallach i Allen, 2013). Innymi słowy, podczas gdy dotychczas człowiek był zobowiązany do wyraźnego wydania polecenia, zanim robot mógł rozpocząć potencjalnie śmiercionośne działania, to w przyszłości ludzie mają po prostu nadzorować działania robota i interweniować w przypadku niekorzystnego rozwoju zdarzeń. Pozwoliłoby to systemowi na szybszą reakcję, jednak ograniczyłoby także możliwości ludzkich operatorów do podjęcia interwencji w przypadku błędów popełnianych przez system. Obecnie w przypadku licznych systemów wojskowych, takich jak automatyczne systemy obrony zaprojektowane do zestrzeliwania nadlatujących pocisków i rakiet, zakres ludzkiego nadzoru jest ograniczony do przyjęcia lub zastąpienia komputerowego planu działań w ciągu kilku sekund, co w praktyce może być za krótkim czasem na podjęcie sensownej decyzji (Human Rights Watch, 2012).

Sparrow (2016) przeanalizował trzy główne powody motywujące większe rządy do przejścia na autonomiczne systemy uzbrojenia i ograniczenie kontroli ludzi:

1. Obecnie istniejące, zdalnie pilotowane „drony wojskowe", takie jak US Predator i Reaper, wymagają dużej przepustowości łącza komunikacyjnego. Ogranicza to liczbę dronów, które mogą być rozmieszczone jednocześnie, i uzależnia je od satelitów komunikacyjnych, których nie ma każdy naród i które mogą zostać zablokowane lub zaatakowane przez wrogów. Konieczność stałej komunikacji ze zdalnymi operatorami uniemożliwia również tworzenie podwodnych dronów – okrętów, które musiałyby działać również w przypadku utraty łączności przed i podczas walki. Z tego powodu uczynienie dronów autonomicznymi i zdolnymi do działania bez nadzoru człowieka pozwoliłoby uniknąć tych wszystkich ograniczeń.
2. W szczególności w walce powietrznej zwycięstwo może zależeć od podjęcia bardzo szybkich decyzji. Już obecnie wymagania walki powietrznej znajdują się na granicy możliwości ludzkiego układu nerwowego, a dalszy postęp może zależeć od całkowitego usunięcia człowieka z tego procesu.
3. Większość rutynowych operacji dronów jest bardzo monotonna i nudna, co w znacznym stopniu przyczynia się do wypadków. Ponadto wydatki na szkolenia, wynagrodzenia i inne benefity dla operatorów dronów stanowią obecnie

dużą część wydatków ponoszonych przez siły zbrojne.

Argumenty postawione przez Sparrowa są specyficzne dla dziedziny wojskowej, sugerują jednak, że „każda rozległa dziedzina dotycząca wysokich stawek, kontradyktoryjne podejmowanie decyzji oraz potrzeba szybkiego działania zostaną najprawdopodobniej coraz bardziej zdominowane przez systemy autonomiczne" (Sotala i Yampolskiy, 2015, s. 18). Podobne argumenty można wysunąć w dziedzinie biznesu. Wyeliminowanie ludzkich pracowników w celu zmniejszenia kosztów spowodowanych ich błędami i wynagrodzeniami mogłoby być kuszące dla firm. Już obecnie osiąganie zysków w dziedzinach transakcji o wysokiej częstotliwości zależy od osiągania lepszych wyników od innych traderów w ułamkach sekund. Pomimo że obecnie istniejące systemy SI nie są wystarczająco potężne, aby spowodować globalną katastrofę, to motywy, jak te przedstawione powyżej, mogą się przyczynić do ostatecznego podniesienia zdolności SI do takiego poziomu.

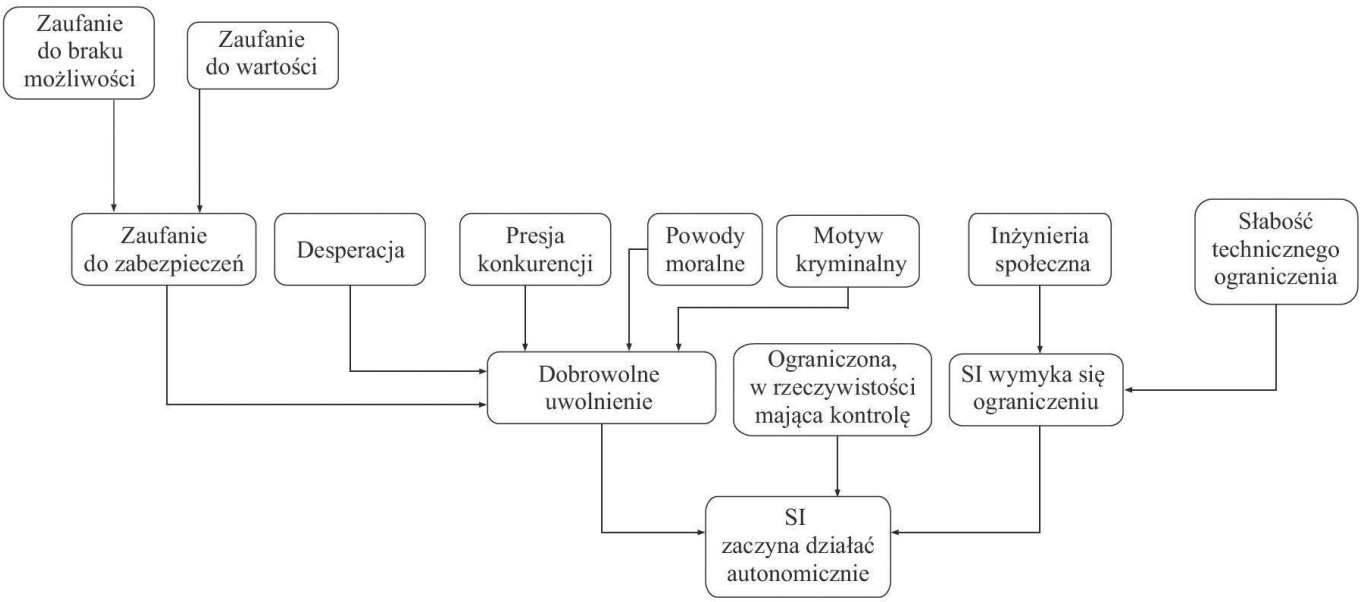
W przypadku braku wystarczających regulacji może dojść do „równania w dół ludzkiej kontroli", w którym podmioty państwowe lub biznesowe rywalizowałyby o ograniczenie kontroli ludzkiej i zwiększanie autonomii systemów SI w celu uzyskania przewagi nad konkurencją. Więcej szczegółów można znaleźć w pracy Armstronga i innych (2016), gdzie przedstawiono uproszczony scenariusz „wyścigu do przepaści". Byłoby to analogiczne do obecnej polityki „równania w dół", w której podmioty rządowe rywalizują o deregulację lub obniżenie podatków w celu utrzymania lub przyciągania przedsiębiorstw.

Organicznie systemów SI może także być argumentowane tym, że przyznanie systemom SI większych możliwości i autonomii może stwarzać znaczne ryzyko w przypadku nieprawidłowego działania SI. W biznesie ogranicza to zakres, w jakim duże i ugruntowane firmy mogą zaadoptować systemy kontroli opartej na SI, z drugiej strony startupy są zachęcane do inwestowania w autonomiczną SI, tak aby uzyskać przewagę nad konkurencją. W dziedzinie handlu algorytmicznego systemy SI mogą obecnie obracać ogromnymi sumami pieniędzy pomimo możliwości spowodowania znacznych strat. W 2012 roku Knight Capital straciła 440 mln USD z powodu usterki w oprogramowaniu transakcyjnym (Popper, 2012, Securities and Exchange Commission, 2013). Sugeruje to, że jeśli nawet nieprawidłowo działająca SI może potencjalnie powodować poważne ryzyko, to niektóre firmy nadal będą skłonne inwestować w powierzenie kontroli nad swoją działalnością autonomicznej SI, jeśli potencjalny zysk może być wystarczająco duży.

Prawo Stanów Zjednoczonych dopuszcza już możliwość nadania SI osobowości prawnej, ustawiając SI jako zarządzającą spółką z ograniczoną odpowiedzialnością. Człowiek może zarejestrować spółkę z ograniczoną odpowiedzialnością (z o.o.), zawrzeć umowę operacyjną określającą, że spółka z o.o. będzie zarządzana przez SI i następnie wystąpić z tej spółki (Bayern, 2015). Rezultatem tego jest podmiot prawny działający niezależnie i bez nadzoru oraz kontroli ze strony człowieka. Firmy kontrolowane przez SI mogą być również tworzone w różnych miejscach znajdujących się poza jurysdykcją USA. Ograniczenia zabraniające korporacjom braku właścicieli można w dużej mierze obejść, stosując takie sztuczki, jak tworzenie sieci korporacji, które są wzajemnymi właścicielami samych siebie (LoPucki, 2017). Możliwą początkową strategią mogłoby być opracowanie licznych systemów SI, wyposażenie ich w początkowe zasoby, a następnie uruchomienie kontroli nad własnymi korporacjami. W takim przypadku ryzykiem objęte są jedynie te początkowe zasoby z jednoczesną wizją potencjalnych zysków, jakie korporacja może uzyskać w przypadku odniesienia sukcesu. W przypadku odniesienia sukcesu przez takie korporacje i związanego z tym skutecznego osłabienia bardziej znanych firm, zostałaby wywarta presja na te firmy, aby one także przekazały kontrolę autonomicznym systemom SI.

Dobrowolne uwolnienie w celu osiągnięcia korzyści kryminalnych lub terroryzmu

LoPucki (2017) twierdzi, że jeśli człowiek stworzy autonomicznego agenta mającego ogólny cel, taki jak „optymalizacja zysku", a następnie agent ten niezależnie zdecyduje, by na przykład popełnić przestępstwo w celu zwiększenia zysku,



Rys. 3. Sposoby, w wyniku których SI może uzyskać swobodę autonomicznego działania. Połączenia pomiędzy węzłami oznaczają bramki LUB (pominięte w celu zwiększenia czytelności): na przykład zaufanie do zabezpieczeń może wynikać z zaufania do braku możliwości LUB zaufania do wartości

to prokuratorzy mogą nie być w stanie skazać człowieka za to przestępstwo i jedynym zarzutem wobec człowieka może co najwyżej być oskarżenie o lekkomyślność. LoPucki utrzymuje, że ta „luka w odpowiedzialności" zapewnia między innymi, że ludzie stworzą kiedyś korporacje kierowane przez SI.

Ponadto LoPucki (2017, s. 16) utrzymuje, że takie „podmioty algorytmiczne" można tworzyć anonimowo, a osoby posiadające osobowość prawną mogą przyznać im szereg praw, takich jak możliwość „kupowania i dzierżawy nieruchomości, zawarcia umowy z legalnymi firmami, otwierania kont bankowych, składania pozwów w celu wyegzekwowania swoich praw lub kupowania rzeczy na Amazonie i zamawiania ich wysyłki". Jeśli podmiot algorytmiczny zostałby stworzony w celu takim, jak finansowanie lub przeprowadzanie aktów terrorystycznych, byłby wolny od presji społecznej lub zagrożeń ze strony ludzkich kontrolerów:

Decydując się na próbę zamachu stanu, zbombardowanie restauracji lub zgromadzenie zbrojnej grupy w celu zaatakowania centrum handlowego, kontrolowana przez człowieka istota naraża życie swoich kontrolerów. Takie same decyzje podjęte przez podmiot algorytmiczny stwarzają ryzyko jedynie wobec zasobów, które podmiot algorytmiczny wydaje na planowanie i realizację (LoPucki, 2017, s. 18).

Podczas gdy większość grup terrorystycznych powstrzymałaby się przed celowym zniszczeniem świata, ograniczając się co najwyżej do spowodowania katastrofalnego ryzyka, to nie wszystkie z grup terrorystycznych mogłyby tak postąpić. Niektóre grupy mogą być zainteresowane spowodowaniem wyginięcia człowieka, w szczególności ekoterroryści uważający ludzkość za szkodliwą dla planety oraz terroryści religijni uważający, że świat musi zostać zniszczony, aby osiągnąć zbawienie (Torres, 2016, 2017, rozdz. 4).

Dobrowolne uwolnienie ze względów estetycznych, etycznych lub filozoficznych

Kilku myślicieli, takich jak Gunkel (2012), poruszyło kwestię praw moralnych maszyn oraz tego, że nie wszyscy stanowczo uznają ograniczenie SI za etycznie dopuszczalne. Projektant wyrafinowanej SI może postrzegać ją jako coś w rodzaju swojego dziecka i czuć, że zasługuje ono na prawo do autonomicznego działania w społeczeństwie, bez jakichkolwiek zewnętrznych ograniczeń.

Dobrowolne uwolnienie z powodu zaufania zabezpieczeniom SI

Jeśli zespół badawczy ma ograniczyć SI, to musi poważnie potraktować możliwość, że stanie się ona niebezpieczna. Obecne badania nad SI nie obejmują żadnych zabezpieczeń ograniczających, ponieważ naukowcy mają uzasadnione przekonanie, że ich systemy nie są nawet zbliżone do ogólnej inteligencji. Wiele z tworzonych systemów jest również podłączona bezpośrednio do internetu. Mamy nadzieję, że zabezpieczenia zaczną być wdrażane, gdy naukowcy stwierdzą, że tworzony system może mieć bardziej ogólne możliwości, będzie to jednak zależeć od ogólnej kultury bezpieczeństwa społeczności badawczej zajmującej się rozwojem SI (Baum, 2016), a w szczególności od konkretnej grupy badawczej. Jeśli grupa badawcza błędnie

uzna, że jej SI nie może osiągnąć niebezpiecznego poziomu zdolności, to może nie zastosować wystarczających zabezpieczeń ograniczających.

Oprócz przekonania, że SI jest niewystarczająco zdolna do bycia zagrożeniem, badacze mogą również (poprawnie lub niepoprawnie) wierzyć, że udało się im dostosować SI do ludzkich wartości, tak aby nie miała żadnej motywacji do wyrządzania szkód ludziom.

Dobrowolne uwolnienie z desperacji

Miller (2012) zwraca uwagę, że jeśli ktoś byłby bliski śmierci, to z przyczyn naturalnych, będąc przegranym w wojnie lub z jakiegokolwiek innego powodu, mógłby uwolnić nawet potencjalnie niebezpieczny system OSI. Byłby to racjonalny sposób działania, o ile ten ktoś ceniłby sobie przede wszystkim własne przetrwanie i sądził, że nawet niewielka szansa na uratowanie życia przez OSI była lepsza niż niemal pewna śmierć.

SI pozostaje ograniczona, jednak ostatecznie przejmuje kontrolę

Nawet jeśli ludzie technicznie występowaliby w pętli procesu decyzyjnego, to mogliby nie mieć czasu, okazji, motywacji, inteligencji lub pewności siebie, aby zweryfikować porady udzielone przez SI. Byłoby tak w szczególności w przypadku, gdyby SI działała już przez pewien czas i zyskała reputację godnej zaufania. Automatyczną reakcją na zalecenia SI może stać się rutynowa praktyka i coraz trudniejsze może być zakwestionowanie „autorytetu" jej zaleceń. W rezultacie SI mogłaby efektywnie narzucać własne decyzje (Friedman i Kahn, 1992).

Podobnie Bostrom i Yudkowsky (2014) zwracają uwagę, że współcześni biurokraci bardzo często dosłownie przestrzegają ustalonych procedur, zamiast dokonywać własnych osądów, w obawie o to, że mogliby zostać później obwinieni za popełnione błędy. Podobnym sposobem na unikanie winy mogłoby być posłuszne przestrzeganie wszystkich zaleceń systemu SI.

O'Neil (2016) udokumentował wiele sytuacji, w których współczesne uczenie maszynowe jest wykorzystywane do podejmowania merytorycznych decyzji, nawet jeśli dokładne modele stojące za tymi decyzjami mogą być tajemnicą handlową lub w inny sposób ukryte przed krytyką zewnętrzną. Między innymi takie modele były już wykorzystywane do zwalniania nauczycieli sklasyfikowanych przez system jako nieefektywni oraz do wymierzania surowszych wyroków przestępcom, których model określił jako obarczonych wysokim ryzykiem ponownego popełnienia przestępstwa. W niektórych przypadkach ludzie byli sceptycznie nastawieni do wyników takich systemów i nawet wskazywali prawdopodobne powody błędności wyników, nadal jednak zgadzali się z autorytetem systemu, o ile nie można było jednoznacznie wykazać, że model się pomylił.

W dziedzinie wojskowej Wallach i Allen (2013) zasygnalizowali istnienie robotów, które próbują automatycznie wykrywać lokalizacje wrogich snajperów i wskazywać je żołnierzom. W zakresie, w jakim ci żołnierze zaczęli ufać tym robotom, można postrzegać ich jako wykonujących rozkazy robotów. W końcu wyposażenie robota we własną broń po prostu wyeliminowałoby formalną potrzebę, by to człowiek pociągał za spust. Na rysunku 3 przedstawiono podsumowanie różnych sposobów, w jakie SI może uzyskać swobodę autonomicznego działania.

TABELA 2. Różne drogi prowadzące do katastroficznych scenariuszy

Czynniki zwiększające prawdopodobieństwo ataku	Czynniki zmniejszające prawdopodobieństwo ataku
Poziom strategicznej przewagi SI	Decydujący Znaczny
Próg zdolności SI do wystąpienia braku współpracy	Bardzo niski do bardzo wysokiego, w zależności od różnych czynników
Źródła zdolności SI	Indywidualne wejście w życie Nadwyżka sprzętowa Eksplozja prędkości Eksplozja inteligencji Zbiorowe wejście w życie Kluczowe możliwości Wojna biologiczna Wojna cybernetyczna Manipulacja społeczna Coś innego Stopniowe przesunięcie władzy i możliwości
Sposoby SI na osiągnięcie autonomii	Oswobodzenie się Manipulacja społeczna Słabość techniczna Dobrowolne uwolnienie Przyczyny ekonomiczne lub konkurencyjne Przyczyny kryminalne lub terrorystyczne Przyczyny etyczne lub filozoficzne Desperacja Zbytnie zaufanie: • Do braku możliwości • Do wartości Ograniczona, w rzeczywistości mająca kontrolę
Liczba SI	Pojedyncza Wiele

Uwagi na temat pojedynczej i licznej SI

Wiele analiz koncentruje się na przypadku istnienia tylko pojedynczej SI. Scenariusz, w którym istotna byłaby tylko jedna kopia SI, mógłby się wydarzyć, gdyby:

1. Pierwsza stworzona SI bardzo szybko osiągnęłaby DPS, zaraz po jej utworzeniu.
2. Pewna grupa badawcza znacznie wyprzedziła wszystkich konkurentów w rozwoju SI i była w stanie utrzymać tę przewagę przez dłuższy czas.

Na potrzeby tej analizy przyjęto scenariusz, w którym istnieje wiele kopii pojedynczej SI, wszystkie z nich mają te same cele, a cała ich zbiorowość jest traktowana jako pojedyncza SI. To samo dotyczy sytuacji, w której pojedyncza SI tworzy bardziej wyspecjalizowane „robotnicze SI", aby zrealizować jakiś bardziej określony cel związany z osiągnięciem celu podstawowego.

Spośród dwóch powyższych możliwości opcja druga wydaje się stosunkowo mało prawdopodobna w ciągu co najwyżej kilku lat, biorąc pod uwagę obecną silną konkurencję w dziedzinie rozwoju SI. Pomimo że jedna firma mogłaby osiągnąć znaczącą przewagę w pewnej rzadkiej niszy przy niewielkiej konkurencji, to wydaje się, że nie zdarzy się to w przypadku rozwoju SI.

Możliwym wyjątkiem może być sytuacja, gdy firmie uda się całkowicie zmonopolizować pewną dziedzinę lub jeśli będzie miała zasoby programistyczne, jakich nie ma nikt inny. Na przykład firmy, takie jak Google i Facebook, mają obecnie dostęp do znacznie większych zbiorów danych niż większość innych podmiotów korporacyjnych lub akademickich. We współczesnym uczeniu maszynowym duże zestawy danych w połączeniu z prostymi modelami zwykle dają lepsze wyniki niż małe zestawy danych i bardziej wyrafinowane modele (Halevy i in., 2009). Jak zauważyli Goodfellow i inni (2016, rozdz. 1), algorytm głębokiego uczenia wymaga z reguły co najmniej 10 milionów oznakowanych przykładów w celu osiągnięcia wydajności na poziomie człowieka lub lepszej.

Z drugiej strony zależność od tak ogromnych zestawów danych jest dziwactwem obecnych technik uczenia maszynowego. Ludzie uczą się na podstawie znacznie mniejszych ilości danych, a także są w stanie wykorzystywać swój proces uczenia się w bardziej elastyczny sposób, co sugeruje fundamentalne różnice w sposobie, w jaki ludzie i współczesne algorytmy uczą się (Lake i in., 2016). Z tego powodu możliwe jest, że OSI byłaby w stanie uczyć się na podstawie znacznie mniejszych ilości danych, a projekt OSI nie byłby tak ograniczony przez potrzebę dużych zbiorów danych.

Innym prawdopodobnym kluczowym zasobem mogą być zasoby sprzętowe. Być może pierwsza OSI będzie wymagała ogromnych mocy obliczeniowych. Bostrom (2017) zauważa, że jeśli w rozwoju SI istnieje duży stopień otwartości i każdy ma dostęp do tych samych algorytmów, to właśnie sprzęt może się stać głównym czynnikiem ograniczającym. Gdyby wymagania sprzętowe dla SI były stosunkowo niskie, wysoka otwartość mogłaby doprowadzić do powstania wielu jednostek SI. Z drugiej strony, jeśli sprzęt byłby głównym czynnikiem ograniczającym i potrzebne byłyby duże ilości sprzętu, to kilka zamożnych organizacji mogłoby przez jakiś czas zmonopolizować SI. Jak wcześniej omówiono w części „Inicjatorzy katastroficznych zdolności", optymalizacje oprogramowania mogą szybko zmniejszyć zapotrzebowanie na sprzęt, ograniczając tym samym czas, kiedy sprzęt może być kluczowym ograniczeniem.

Branwen (2012) zasugerował, że produkcja sprzętu zależy od niewielkiej liczby scentralizowanych fabryk, które byłyby łatwym celem regulacji. Sugerowałoby to możliwą drogę, według której SI mogłaby podlegać regulacjom rządowym, ograniczając liczbę wdrożonych jednostek SI. Podobnie pojawiły się propozycje rządowych i międzynarodowych regulacji rozwoju SI (np. Wilson, 2013, argumentów przeciwko szukaj w: McGinnis, 2010). W przypadku pomyślnego uchwalenia, takie regulacje mogą ograniczyć liczbę wdrożonych jednostek SI.

Innym możliwym kluczowym zasobem byłoby posiadanie nieoczywistego przełomowego osiągnięcia, które byłoby trudne do odkrycia dla innych badaczy. Gdyby było ono utrzymywane w tajemnicy, to jedna firma mogłaby prawdopodobnie znacznie posunąć się naprzód w stosunku do innych.

Skuteczne procedury ograniczania SI mogą również zwiększać szanse na powstanie wielu SI, ponieważ ograniczenie pierwszych jednostek SI, umożliwiłoby innym projektom nadrobienie zaległości.

Niektóre przykładowe scenariusze

Różnorodne kombinacje różnorakich omówionych ścieżek mogą prowadzić do powstania wiele rodzajów scenariuszy ryzyka związanego z rozwojem SI. Poniżej przedstawiono cztery przykłady:

Klasyczne przejęcie

(Decydująca przewaga strategiczna, wysoki próg zdolności, eksplozja inteligencji, wejście w życie SI i pojedyncza SI)

„Klasyczny" scenariusz przejęcia SI został opisany przez Bostroma (2014, rozdz. 6). Rozwijana SI ostatecznie staje się lepsza w projektowaniu SI niż jej programiści. SI wykorzystuje tę zdolność do eksplozji inteligencji i ostatecznie ucieka do internetu ze swojego ograniczonego środowiska. Po sekretnym zdobyciu wystarczającego wpływu i zasobów przeprowadza atak przeciwko ludzkości, eliminując ludzkość jako dominującego gracza na Ziemi, w wyniku czego SI może bez przeszkód realizować własne plany.

Stopniowe przejęcie

(Zasadnicza przewaga strategiczna, wysoki próg zdolności, stopniowe przesunięcie władzy, uwolnienie z przyczyn ekonomicznych i wiele kopii SI)

Wiele korporacji, rządów i osób prywatnych dobrowolnie powierza wykonanie zadań SI, aż do momentu zupełnego uzależnienia od systemów AI. W początkowym etapie są to wyspecjalizowane systemy SI, jednak ciągłe aktualizacje sprawiają, że niektóre z nich osiągają poziom ogólnej inteligencji. Stopniowo zaczynają one podejmować wszystkie decyzje. Wiemy, że pozwolenie im na prowadzenie takich działań jest ryzykowne, jednak są one zaangażowane w zbyt wiele spraw, które przynoszą zysk i są naprawdę skuteczne w tworzeniu pożytecznych dla ludzkości przedmiotów. Do pewnego czasu.

Wojny zdesperowanych SI

(Zasadnicza przewaga strategiczna, niski próg zdolności, kluczowe zdolności, oswobodzenie się SI i wiele kopii SI)

Wielu różnych twórców opracowuje systemy SI. Większość tych prototypów nie jest zgodna z ludzkimi wartościami i nie posiada niezwykłych zdolności, jednak liczne z tych SI uważają, że niektóre inne prototypy mogą okazać się bardziej zdolne. W rezultacie systemy SI starają się zdradzić ludzkość nawet pomimo małych szans na powodzenie, motywowane tym, że miałyby jeszcze mniejsze szanse na osiągnięcie swoich celów, gdyby nie zdradziły. Społeczeństwo zostaje zaatakowane przez różne systemy wymykające się spod kontroli i które mają kluczowe możliwości do wyrządzenia katastrofalnych szkód, zanim zostaną powstrzymane.

Czy ludzkość uważa, że ma szczęście?

(Decydująca przewaga strategiczna, wysoki próg zdolności, kluczowe zdolności, ograniczona jednak w efekcie mająca kontrolę SI i pojedyncza SI)

Google zaczyna podejmować decyzje dotyczące wprowadzanych produktów i strategii zgodnie z wytycznymi strategicznej SI. Pozwala to firmie stać się jeszcze potężniejszą i bardziej wpływową, niż są obecnie. Kierując się strategią, SI zaczyna podejmować coraz bardziej wątpliwe działania, które zwiększają jej władzę i możliwości. W końcu staje się zbyt potężna, aby społeczeństwo mogło ją powstrzymać. Trudny do zrozumienia kod napisany przez strategię SI wykrywa i subtelnie sabotuje projekty SI innych twórców, aż do momentu, kiedy Google nie stanie się dominującą potęgą światową. Odmiana tego scenariusza z gwałtownym wejściem w życie SI została opisana w rozdziale otwierającym pracę Tegmarka (2017).

Sytuacja rozwoju wielu różnych jednostek SI może zaistnieć, gdy:

1. Kilku twórców osiągnęło zdolność do budowania SI w tym samym czasie i żadna SI nie osiągnęła DPS.
2. Jeden twórca mógł wyprodukować kilka różnych SI mających różne cele.
3. Tylko jeden twórca był w stanie wdrożyć SI, ale ta SI stworzyła własne kopie i nie dostosowała celów tych kopii do własnych.

Trudno przewidzieć konsekwencje istnienia wielu jednostek SI. Obecnie opracowywana jest SI w celu ostrzegania przed potencjalnym ryzykiem, na przykład przez przewidywanie ryzyka finansowego na podstawie artykułów prasowych (Rönnqvist i Sarlin, 2017), a od wielu lat wykorzystuje się SI do celów takich jak automatyczne wykrywanie włamań (Lunt, 1988). Bardziej wyrafinowana i dopasowana do człowieka SI może pomóc w obronie przed niedopasowanymi systemami SI (Hall, 2007, Goertzel i Pitt, 2012).

Z drugiej strony podstawowym problemem związanym z obroną jest to, że aby zapobiec katastrofie, obrońcy muszą odnieść sukces za każdym razem, podczas gdy atakującemu wystarczy tylko jedno odniesienie sukcesu. W przypadku istnienia licznych SI procedury, takie jak ograniczanie SI, musiałyby być skuteczne dla każdej pojedynczej SI, a wszyscy ludzie musieliby uznawać stosowanie ograniczeń SI za wartościowe. W rezultacie istnienie licznych SI jest zwielokrotnieniem liczby systemów, które mogłyby potencjalnie spowodować katastrofę.

Inną kwestią jest to, że istnienie licznych SI wydaje się pomocne tylko wtedy, gdy wystarczająco duża ich część ma wartości dostosowane do wartości ludzkich. Scenariusz z istniejącą liczną SI, z których każda realizuje interesy w niewielkim stopniu związane z wartościami ludzkimi, najprawdopodobniej byłby niekorzystny dla ludzkich wartości. Zwłaszcza jeśli wszystkie SI byłyby znacznie bardziej zdolne niż ludzie, to taki scenariusz po prostu stawia ludzi w krzyżowym ogniu.

Wnioski

W tym rozdziale rozważaliśmy różne drogi rozwoju SI, które mogą zakończyć się katastrofą (tabela 2). W części „Inicjatorzy katastrofy" przedstawiono dowody na to, że nadmierne skupianie się na SI osiągającej DPS umożliwiającej jej osiągnięcie całkowitej dominacji nad światem, może być nierozsądne. Wydaje się raczej uzasadnione, aby rozważyć również możliwości uzyskania ZPS, poziomu zdolności, który może umożliwić SI spowodowanie co najmniej dziesiątek milionów ofiar. Oprócz tego jest znacznie bardziej prawdopodobne, że SI uzyska ZPS niż DSA, a chaos spowodowany przez SI z ZPS może ostatecznie doprowadzić do pojawienia się SI z DSA, nawet jeśli pierwsza SI zostałaby pomyślnie wyłączona.

Rozważenie scenariuszy, w których SI osiąga „tylko" ZPS wymaga położenia większego nacisku na analizę, kiedy SI byłaby skłonna zaryzykować podjęcie działań wrogich wobec ludzi. Liczne rozważania przedstawiono w części „Kiedy zostaną podjęte działania przeciwko przewadze strategicznej". Zasadniczo, jeśli SI działałaby racjonalnie, to zainicjowałaby agresywne działania tylko wtedy, gdyby spodziewana uzyskana w ten sposób użyteczność przewyższała spodziewaną użyteczność uzyskaną w przypadku współpracy, przy uwzględnieniu ryzyka niepowodzenia i odpowiadającego mu odwetu ze strony ludzi (Shulman, 2010). Istnieje jednak wiele sytuacji, które mogą zmusić SI do podjęcia wrogiego działania.

Próbując ustalić katastrofalne ryzyko związane z SI jako formę ryzyka rozłącznego, gdzie wiele różnych spraw może potoczyć się niekorzystnie, w części „Inicjatorzy katastroficznych zdolności" przedstawiono różne sposoby, dzięki którym SI lub grupy SI mogą się stać wystarczająco zdolne do uzyskania pewnej formy przewagi strategicznej. Omówiono indywidualne scenariusze wejścia w życie wraz z trzema głównymi podtypami, scenariusze zbiorowego wejścia w życie, scenariusze, w których władza jest przejmowana przez systemy SI, oraz scenariusze, w których SI staje się wystarczająco zdolna, by zdobyć kluczowe możliwości dające jej ZPS lub DPS.

Ponieważ SI może stać się zdolna tylko wtedy, gdy uzyska wystarczającą autonomię, w części „SI uzyskuje zdolność do samodzielnego działania" przedstawiono różne sposoby, w jakie SI może osiągnąć taką autonomię. Przedstawione przyczyny przyznania autonomii SI obejmowały: (i) korzyści ekonomiczne lub presję konkurencyjną, (ii) przyczyny kryminalne lub terrorystyczne, (iii) przyczyny etyczne lub filozoficzne, (iv) zaufanie do zabezpieczeń SI oraz (v) rozpaczliwe okoliczności, takie jak wizja nieuchronnej zagłady. Ponadto wystarczająco inteligentna SI może uniknąć ograniczenia lub może stać się wystarczająco wpływowa, aby uzyskać skuteczną kontrolę nawet pomimo teoretycznego istniejącego ograniczenia.

Wreszcie, wszystkie drogi prowadzące do katastrofy mogą ulegać zwielokrotnieniu w przypadku istnienia licznych różnych kopii SI, z których każda może być w stanie osiągnąć autonomię, a następnie duży poziom zdolności. W części „Uwagi na temat pojedynczej i licznej SI" omówiono, czy możemy się spodziewać bardzo małej liczby SI, czy też będzie ich wiele, a także niektóre implikacje w stosunku do każdego scenariusza.

Łączenie różnych dróg omówionych w poprzedniej części może skutkować wieloma różnymi scenariuszami (patrz ramka poniżej), poczynając od tych, w których SI oswobadza się i szybko osiąga superinteligencję, po te, w których SI jest budowana celowo z zamiarem kontrolowania korporacji, a rosnące zasoby są jej dobrowolnie przydzielane aż do momentu, gdy SI zawładnie całą planetą. Każda z tych dróg będzie musiała zostać osobno oceniona pod kątem wiarygodności, a także pod kątem najbardziej odpowiednich metod zapobiegających. Mamy nadzieję, że taka analiza pozwoli wykorzystać pozytywny potencjał SI, jednocześnie unikając katastrofy.

Podziękowania

Autor chciałby podziękować Alexowi Mennenowi, Eli Senneshowi, Jesse'owi Cliftonowi, Lukasowi Gloorowi, Magnusowi Vindingowi, Matthew Gravesowi, Maxowi Danielowi, Milesowi Brundage, Philipowi Ehrnroothowi, Stuartowi Armstrongowi, Tobiasowi Baumannowi, Toniemu Barrettowi i Vadimowi Kosoyowi za komentarze dotyczące tego rozdziału. Bardzo pomocna była też dyskusja na seminarium, które odbyło się w Existential Risk to Humanity research program of the Gothenburg Center for Advanced Studies (GoCAS).

Kaj Sotala

Nowinki z branży

PÓŁ MILIONA SPRZEDANYCH ROBOTÓW W 2023

Jak wynika z nowego raportu Interact Analysis, w 2023 roku na całym świecie sprzedano ponad 500 000 robotów przemysłowych. Był to poziom zbliżony do osiągniętego w roku 2022, jednak w zeszłym – po dwóch latach pozytywnej dynamiki – spadła średnia cena maszyn tego typu.

– Spodziewamy się spadku cen o około 3% rocznie w latach 2024 – 2028 – powiedziała Maya Xiao, kierownik ds. badań Interact Analysis. – Pandemia Covid-19 w połączeniu z wysokimi cenami energii i inflacją spowodowała średni wzrost cen w 2022 roku. Analitycy początkowo spodziewali się ponownego spadku cen robotów w 2023 roku, ale problemy z łańcuchem dostaw i inflacją spowodowały, że wzrosły do poziomu zbliżonego do obserwowanego rok wcześniej.

Z danych wynika, że profil wzrostu robotów przemysłowych odzwierciedla spowolnienie produkcji w erze pandemii i późniejsze pogorszenie koniunktury w 2023 roku. Jeśli skierujemy wzrok na dane dotyczące produkcji w Chinach, Europie i obu Amerykach, historyczne spadki produkcji jawią się jako równoznaczne z obniżeniem wzrostu rynku robotów przemysłowych, który obserwowano w ostatnich latach.

Trzy najważniejsze zastosowania robotów przemysłowych – obsługa materiałów, spawanie i montaż – odpowiadały za ponad 70% przychodów ze sprzedaży robotów w 2023 roku, przy czym sama obsługa materiałów stanowiła jedną trzecią. To zastosowanie jest dominujące w obu Amerykach i Europie. Największą koncentracją rynku charakteryzuje się rynek amerykański, gdzie pięciu największych dostawców odpowiada za prawie 80% przychodów i ponad dwie trzecie dostaw.

Region Azji i Pacyfiku wygenerował prawie dwie trzecie (62%) światowych przychodów ze sprzedaży robotów w rozpatrywanym okresie. Za nim uplasował się region EMEA z 22% i Ameryki z 17%. Region APAC również odnotował dodatnią dynamikę wzrostu w 2023, podczas gdy w obu Amerykach nastąpił gwałtowny spadek o 17,3%, a region EMEA pozostał stabilny.

Po pandemii rynek robotów przemysłowych odnotował silny wzrost w obu Amerykach zarówno w sektorze motoryzacyjnym, jak i pozostałych gałęziach przemysłu. Lokalna sprzedaż robotów dla przemysłu motoryzacyjnego znalazła się pod znaczną presją, co spowodowało powolny wzrost. Najbardziej dotknięty tym zjawiskiem w ubiegłym roku okazał się Meksyk.

Źródło: drivesncontrols

Wstęp do hakowania systemów uczących się

Jerzy Surma

WSTĘP

W ostatniej dekadzie doszło do niezwykłej synergii trzech nurtów badawczo-rozwojowych związanych z cyfryzacją współczesnego świata. Po pierwsze, mamy do czynienia z masowym rejestrowaniem śladów cyfrowych (ang. *digital footprints*), związanym z rozwojem internetu, w tym zwłaszcza mediów społecznościowych oraz internetu rzeczy (ang. I*nternet of Things*). Po drugie, nastąpił rozwój usług informatycznych dostępnych w „chmurze" (ang. *cloud computing*), co umożliwia nawet małym innowacyjnym firmom dostęp po relatywnie niskich kosztach do olbrzymich mocy obliczeniowych, pamięci masowych oraz gotowych rozwiązań analizy danych. Po trzecie, nastąpił również intensywny rozwój metod analizy danych o niestandardowych formatach, takich jak teksty, zdjęcia, sekwencje wideo czy audio. W tym nurcie badawczym prym wiodą obecnie metody nazywane powszechnie głębokim uczeniem się (ang. *deep learning*), które zostały zainicjowane badaniami profesora G.E. Hintona (2007) nad algorytmami uczenia wielowarstwowych sieci neuronowych. Zbieżność w tym samym czasie tych trzech nurtów implikuje olbrzymi potencjał rozwojowy dla biznesu, medycyny, transportu, czy obronności.

Chciałbym podkreślić, że rozwój praktycznych zastosowań metod sztucznej inteligencji ma już niemal 30-letnią historię. Niemniej spektakularne sukcesy zastosowań metod głębokiego uczenia się spowodowały niezwykłe zainteresowanie tą tematyką przez tzw. media mainstreamowe, generując niestety kuriozalne nieporozumienia i zafałszowania. Dotyczy to głównie zrozumienia pojęcia „sztuczna inteligencja" (ang. *artificial intelligence*). W interpretacji odwołującej się do wizji Johna McCrathy'ego pojęcie to oznacza zbudowanie maszyny, która funkcjonowałaby na poziomie ludzkiej inteligencji w pełnym zakresie, takim jak rozumienie języka naturalnego, zdolność do uczenia się, rozwiązywanie problemów, a nawet kreatywność, myślenie zdroworozsądkowe i samoświadomość. To podejście znane jest w literaturze naukowej jako tzw. silna sztuczna inteligencja (ang. *strong artificial intelligence*) albo ostatnio coraz częściej jako ogólna sztuczna inteligencja (ang. *artificial general intelligence*). Badania naukowe w tym obszarze są na poziomie podstawowym i nie ma ciągle jakiś wymiernych sukcesów. Niestety w oczach laików, wspieranych przez niedouczonych dziennikarzy, ogólna sztuczna inteligencja już istnieje jako rodzaj tajemnej wiedzy. W tym nurcie pseudonaukowego postrzegania rzeczywistości należy przekazać sztucznej inteligencji odpowiednie informacje i… problemy świata zostaną rozwiązane. Prawda jest natomiast taka, że rzeczywiste sukcesy istnieją w obszarze tzw. słabej sztucznej inteligencji (ang. *weak artificial intelligence*), określanej również jako ograniczona sztuczna inteligencja (ang. *narrow artifi cial intelligence*). Ograniczoność sztucznej inteligencji oznacza jej użycie dla ściśle określonych zadań (ang. *single domain*), jak na przykład umiejętność gry w GO, rozpoznawanie obiektów na zdjęciach, czy określenie zdolności kredytowej pożyczkobiorcy. Dla takich dobrze ustrukturalizowanych zadań i wąskich zastosowań systemy sztucznej inteligencji potrafią działać niejednokrotnie lepiej od człowieka.

Pod ogólnym pojęciem „sztuczna inteligencja", w kontekście realnych zastosowań praktycznych, kryje się obszar badawczy nazywany maszynowym uczeniem się (ang. *machine learning*). Budowane w ramach maszynowego uczenia się systemy, nazywane systemami uczącymi się, zostały zdefiniowanie w rozdziale 1. Te właśnie systemy, budowane w paradygmacie ograniczonej sztucznej inteligencji, są rzeczywistym źródłem niemal wszystkich spektakularnych sukcesów i zastosowań biznesowych sztucznej inteligencji. Te systemy potrafią funkcjonować lepiej od człowieka nie tylko na poziomie jakości działania, lecz także szybkości, niższego kosztu i bez „zmęczenia" przez przysłowiowe 24 godziny i 7 dni w tygodniu. Te wymierne korzyści determinują coraz powszechniejsze stosowanie tych systemów w automatyzacji (robotyzacji) procesów biznesowych, realizacji transakcji na rynkach kapitałowych, rozpoznawaniu twarzy w procesach uwierzytelniania tożsamości, nawigowaniu pojazdów autonomicznych czy identyfikacji jednostek chorobowych w systemach diagnostyki medycznej. Te oczywiste korzyści muszą być skonfrontowane z ryzykiem stosowania tych innowacyjnych technologii. Ciemna strona cyfrowej transformacji z wykorzystaniem sztucznej inteligencji to olbrzymie zagrożenie związane z intencjonalnymi atakami na systemy tego typu. Jest to szczególnie krytyczne zagadnienie, kiedy systemy tego typu są coraz powszechniej wykorzystywane w zastosowaniach mających bezpośredni związek z życiem i zdrowiem człowieka, jak na przykład w pojazdach autonomicznych. Niepoprawne działanie takich systemów może zatem determinować katastrofalne konsekwencje.

Celem autorów niniejszej monografi i jest próba całościowego spojrzenia na problematykę intencjonalnego hakowania systemów uczących się. Historycznie termin „hakowanie" związany jest z aktywnością, która ma na celu włamanie do systemów informatycznych i w tym kontekście „hakerstwo" jest utożsamiane z działaniami dokonywanymi w złośliwych celach z nieetycznymi intencjami. W tej publikacji zagadnienie to zostanie omówione w kontekście celowego atakowania systemów uczących się nie tylko na poziomie „włamywania" do nich w czasie działania, lecz także potencjalnej ingerencji na każdym etapie ich cyklu życia. Jest to szczególnie istotne zagadnienie w sytuacji znikomej obecnie świadomości tych realnych zagrożeń. Potwierdza to badanie przeprowadzone przez Shankar z zespołem (2020) w 28 firmach, które w zaawansowanym zakresie wykorzystują i rozwijają samodzielnie systemy uczące się. Badani pracownicy (szefowie zespołów programistycznych i menedżerowie odpowiedzialni za cyberbezpieczeństwo)

wyrażali w zdecydowanej większości opinie o futurystycznym charakterze ataków na systemy uczące się i deklarowali brak zasobów do analizy tego typu zagrożeń. Znamienna jest opinia jednego z badanych, który stwierdził: „tradycyjne hakowanie oprogramowania jest sytuacją typu: wiemy, że nie wiemy, natomiast ataki na modele systemów uczących się to sytuacja, w której: nie wiemy, że nie wiemy". W tym kontekście ta książka ma szczególne znaczenie nie tylko dla środowiska naukowego, lecz także dla menedżerów zajmujących się rozwojem takich systemów oraz odpowiedzialnych za ryzyko operacyjne i ciągłość działania.

Dla mnie jest to szczególnie ważna tematyka, gdyż dotyka ona moich pasji naukowych i poznawczych. Te moje pasje znalazły odzwierciedlenie w programach studiów podyplomowych, które zorganizowałem i prowadzę do chwili obecnej w Szkole Głównej Handlowej w Warszawie (SGH). W roku 2005 opracowałem absolutnie pionierski w tamtych latach program studiów Business Intelligence, które dotyczą zastosowań metod analizy danych i sztucznej inteligencji w biznesie. Natomiast w roku 2015 opracowałem oryginalny program studiów w zakresie zarządzania cyberbezpieczeństwem. Nie jest zatem przypadkiem, że niniejsza monografia leży na pograniczu zastosowań sztucznej inteligencji i cyberbezpieczeństwa. Jest to zupełnie nowy obszar badawczy i zarządczy, który dotyczy bezpieczeństwa systemów sztucznej inteligencji.

Nie byłbym w stanie opisać tej fascynującej tematyki w sposób dogłębny i holistyczny, gdyby nie wsparcie i współpraca moich kolegów z Instytutu Informatyki i Gospodarki Cyfrowej SGH, NASK oraz moich studentów z seminarium dyplomowego. Tak powstały zespół zmierzył się z trudnym zadaniem opisania zjawiska intencjonalnych ataków na systemy sztucznej inteligencji i finalnie powstała niniejsza monografia składająca się 5 rozdziałów. Rozdział pierwszy, mojego autorstwa, jest wprowadzeniem w tę tematykę. Starałem się przedstawić i zdefiniować wszystkie pojęcia, pokazać stan prac naukowych w tym obszarze i co najważniejsze przedstawić autorską taksonomię ataków na systemy uczące się. Moją ambicją było przedstawić w sposób spójny wszystkie możliwe wektory ataków, starając się odnieść do wszystkich najważniejszych i reprezentatywnych badań naukowych w tym obszarze. Autorem rozdziału drugiego jest dr Piotr Filipkowski z SGH, który dokonał przeglądu reprezentatywnych ataków na systemy uczące. W ramach tego przeglądu omówił ataki na systemy uwierzytelniania tożsamości, pojazdy autonomiczne oraz systemy diagnostyki medycznej. Rozdział trzeci dotyczy ataków na systemy uczące się w zastosowaniach biznesowych. Tego zadania podjął się dr Mariusz Rafało z SGH, który przedstawił to ważne zagadnienie w kontekście zarządzania ryzykiem operacyjnym dla robotyzacji procesów biznesowych. Dodatkowo rozdział zawiera spektakularne przykłady ataków na systemy rekomendacyjne oraz systemy automatycznego zawierania transakcji finansowych. Rozdział czwarty składa się z dwóch studiów przypadków opracowanych przez moich dyplomantów w ramach ich prac magisterskich. Pierwsze studium, opracowane przez Piotra Kuca, dotyczy ataku na filtr antyspamowy wykorzystujący klasyfiator bayesowski (Kuc, 2020). Jest to niemal podręcznikowy przykład ataku typu *black box*, w którym bez wcześniejszej wiedzy o klasyfikatorze udało się przeprowadzić skuteczny atak oszukujący skutecznie filtr antyspamowy, doprowadzając do błędnej klasyfikacji nadchodzącej poczty elektronicznej. Drugie studium przypadku, opracowane przez Krzysztofa Jagiełłę, dotyczy systemu detekcji nadużyć finansowych w bankowości elektronicznej, który funkcjonuje na bazie modelu eksploracji danych (Jagiełło, 2020). Ten przykład ilustruje atak typu *grey box* na funkcjonujący system i zakłada, że atakujący pozyskał zbiór uczący. Z wykorzystaniem rzeczywistych danych pochodzących z transakcji bankowych odtworzono model systemu detekcji nadużyć, a następnie wykorzystano generatywne sieci współzawodniczące do opracowania sekwencji działań umożliwiających atakującemu przeprowadzenie ataków. Te studia przypadków zostały opracowane, w postaci uproszczonej, na podstawie prac dyplomowych, które powstały pod moim nadzorem. I w końcu ostatni piąty rozdział został opracowany przez Kamila Frankowicza z CERT Polska (NASK). W tym rozdziale omawiana tematyka dotyka poziomu bezpieczeństwa używanych środowisk programistycznych, oprogramowania systemowego i sprzętu komputerowego, które są wykorzystywane, aby systemy uczące się mogły być budowane i użytkowane. W ramach tego rozdziału przedstawione są także dwa autorskie przykłady ataków na biblioteki programistyczne z wykorzystaniem automatycznych metod testowania oprogramowania.

Zajmując się od wielu lat systemami wykorzystującymi metody sztucznej inteligencji, nigdy nie rozważałem scenariusza, że ktoś mógłby intencjonalnie zakłócać ich działanie. A teraz powstała cała monografia pod moją redakcją na ten temat. To pozornie wygląda na smutny znak czasów, w jakich przyszło nam żyć. Prawda jest jednak taka, że przestępcza działalność towarzyszy naszemu życiu od momentu wygnania z raju i dotyka każdej aktywności, która może przynosić profity. Jest to zatem nie wprost dowód ważności i dojrzałości rozwiązań wykorzystujących metody sztucznej inteligencji. Przed nami zatem fascynująca walka dobra ze złem w świecie zaawansowanych technologii. Być może to objaw mojej naiwności, ale wierzę w zwycięstwo Dobra.

1.1. Wprowadzenie

W pierwszym okresie rozwoju systemów uczących się nie rozważano możliwości intencjonalnych działań mających na celu zakłócenie ich ciągłości działania czy wpływanie na generowanie fałszywych wyników. Analizowane problemy związane z rzeczywistymi zastosowaniami wynikały głównie z ich klasycznych ograniczeń, takich jak problem zmienności dziedziny zastosowań w sytuacji uczenia z wykorzystaniem danych historycznych czy ograniczenia wynikające z wnioskowania indukcyjnego. Problem intencjonalnych ataków na systemy uczące się po raz pierwszy w sposób kompleksowy został przedstawiony w 2004 roku w czasie konferencji Knowledge Discovery in Databases. W pracy Dalvi i in. (2004) zbadano metodę manipulowania danymi wykorzystywanymi w procesie uczenia, aby zwiększyć liczbę błędów drugiego rodzaju. Dla ilustracji tego zjawiska wykorzystano „zmanipulowany" filtr antyspamowy, który klasyfikował pocztę elektroniczną ze spamem jako pocztę adekwatną do czytania. W tym pionierskim artykule zaproponowano również formalny model, opierając się na teorii gier, gdzie gra jest prowadzona pomiędzy atakującym i systemem uczącym się. Ten nowy temat badawczy był kontynuowany

w pracy Barreno i in. (2006) oraz w pracy doktorskiej Nelsona (2010). Podsumowanie wyników badań z pierwszego okresu oraz wskazanie kierunków rozwojowych zostało omówione w czasopiśmie „Machine Learning" w ramach specjalnego wydania w zakresie *Machine Learning in Adversarial Environments* (Laskov, 2010). W artykule Barreno i in. (2010) po raz pierwszy zaprezentowano systematyczne podejście do klasyfikacji potencjalnych ataków na systemy uczące się oraz zaproponowano teoretyczny model interakcji pomiędzy atakującym i broniącym z wykorzystaniem funkcji kosztu. Barreno ze współautorami sformułował kluczowe problemy badawcze oceny jakości systemów uczących się oraz weryfikacji, czy spełniają one wymagania w zakresie bezpiecznego uczenia się. W tym artykule dokonano również pełnego przeglądu publikacji naukowych do 2010 roku. Dojrzała koncepcja taksonomii ataków została zaprezentowana także w artykule Huanaga i in. (2011), która jest rozwinięciem taksonomii opartej na ilościowej analizie zagrożeń (Laskov, 2009).

Orientacyjnie od roku 2015[1], w kontekście spektakularnego sukcesu praktycznych zastosowań wielowarstwowych sieci neuronowych, tematyka ta staje się jednym z kluczowych obszarów badawczych w ograniczonej sztucznej inteligencji. Obecnie ten obszar badawczy jest najczęściej określany jako antagonistyczne maszynowe uczenie się (ang. *adversarial machine learning*)[2]. Do najbardziej innowacyjnych prac badawczych w ostatnim okresie można zaliczyć badania Goodfellowa z zespołem (2014) w zakresie generatywnych sieci współzawodniczących (antagonistycznych) – GAN (ang. *generative adversarial network*) oraz prace w zakresie tzw. ataków na czarną skrzynkę (ang. *black-box adversary attack*) z wykorzystaniem modeli głębokiego uczenia (Papernot, 2017). Popularność zastosowań sieci typu GAN jest obecnie tak duża, że niejednokrotnie pojęcie „uczenie antagonistyczne" (ang. *adversarial learning*) jest błędnie utożsamiane wyłącznie z podejściem zaproponowanym przez Goodfellowa.

W ostatnich kilku latach ten obszar badawczy rozwija się niezwykle gwałtownie i są już dostępne setki recenzowanych artykułów naukowych, a liczba ich dynamicznie rośnie[3]. Reprezentatywny przegląd najlepszych badań naukowych zawiera artykuł McDaniela i in. (2016), praca Chakraborty'ego i in. (2018) oraz książka Munoza-Gonzaleza i Lupu (2019).

1.2. Systemy uczące się

1.2.1. Definicja i rodzaje systemów uczących się

Tak jak wspomniano we wstępie, rozważania związane z atakami na systemy sztucznej inteligencji zostaną zawężone do systemów uczących się, a w szczególności do systemów uczących się pod nadzorem (uczenie nadzorowane). Zgodnie z klasyczną definicją Mitchella (1997) system jest się w stanie uczyć z doświadczenia (ang. *experience*) E w kontekście realizacji zadań (ang. *tasks*) T i miary jakości działania (ang. *performance measure*) P, jeśli jego działanie w realizacji zadań T, mierzone z wykorzystaniem P, polepsza się wraz ze wzrostem doświadczenia E. Bardzo prosto jest to ujęte w definicji Cichosza (2009), w której uczeniem się systemu nazywana jest każda autonomiczna zmiana zachodząca w systemie na podstawie doświadczeń, która prowadzi do poprawy jakości jego działania. W efekcie procesu uczenia się system jest w stanie generować poprawną odpowiedź (wyjście) dla danego obiektu na wejściu. Jeżeli w trakcie uczenia się system otrzymuje informację trenującą[4], to takie podejście nazywane jest uczeniem nadzorowanym (ang. *supervised learning*). Przykładem tego typu uczenia się jest zadanie regresji oraz zadanie klasyfikacji.

Proces uczenia w przypadku braku informacji trenującej jest natomiast nazywany uczeniem bez nadzoru (ang. *unsupervised learning*). Przykładem tego typu uczenia się jest zadanie grupowania oraz zadanie odkrywania reguł asocjacyjnych. Dodatkowo należy wspomnieć, że informacja trenująca może być przez system pozyskiwana samodzielnie przez wykonywanie określonych akcji (wyjście systemu) i obserwowanie ich konsekwencji. Ten rodzaj uczenia, kiedy system gromadzi doświadczenie przez eksperymenty ze swoim otoczeniem, jest nazywany uczeniem się przez eksperymentowanie (Cichosz, 2009). Szczególnym przypadkiem tego typu uczenia się jest tzw. uczenie się ze wzmocnieniem (ang. *reinforcement learning*).

W dalszej części rozdziału ataki na systemy uczące się zostaną szczegółowo omówione dla zadania klasyfikacji w ramach nadzorowanego uczenia się. Pozostałe zadania, takie jak grupowanie, odkrywanie reguł asocjacyjnych, selekcja poprzez współpracę oraz uczenie się ze wzmocnieniem, zostaną w skrócie omówione pod koniec rozdziału. Takie zawężenie tej tematyki wynika z dwóch przesłanek. Po pierwsze, systemy nadzorowane dysponują bardzo dojrzałymi algorytmami, metodami ewaluacji oraz, co najważniejsze, są zdecydowanie najczęściej stosowane w praktyce. W tym kontekście wzbudzają olbrzymie zainteresowanie zarówno w środowisku naukowym, jak i ze strony atakujących. Po drugie, prezentowane metody ataków na systemy nadzorowane w zasadzie w większości przypadków po niewielkich modyfikacjach mogą być stosowane także dla podejść nienadzorowanych czy też wykorzystujących wzmocnienie w procesie uczenia.

1.2.2. Zadanie klasyfikacji i uczenie nadzorowane

Zadanie klasyfikacji polega na znalezieniu funkcji Ψ, która obiektowi x reprezentowanemu przez wektor wartości cech (ilościowych lub jakościowych) przyporządkuje klasę i ze zbioru etykiet klas $M = \{1, 2, \ldots, M\}$[5] (ang. *class label*). Takie odwzorowywanie przestrzeni cech w zbiór etykiet klas nazywa się modelem klasyfikacyjnym (ang. *classification model*) albo w formie skrótowej klasyfikatorem (ang. *classifier*) i formalnie ma następującą postać:

$$\Psi(x) = i$$

gdzie $i \in M$

W praktycznych zastosowaniach, kiedy nie są znane prawdopodobieństwa *a priori* klas oraz warunkowe gęstości cech w klasach, stosuje się proces uczenia z wykorzystaniem zbioru uczącego (ang. *learning set*). Zbiór uczący $D^{(\text{uczenie})}$ składający się z N elementów jest definiowany następująco:

$$D^{(\text{uczenie})} = \{(x_1, j_1), (x_2, j_2), \ldots, (x_N, j_N)\}$$

gdzie $j \in M$

Nieformalnie można stwierdzić, że zbiór uczący powstaje dzięki współudziale „nauczyciela", który dla każdego obiektu

x w zbiorze uczącym przyporządkowuje mu etykietę, tj. klasę j. Z tego powodu to podejście, jak już wspomniano, nazywane jest uczeniem nadzorowanym. Klasyfikator (model) zbudowany z wykorzystaniem zbioru uczącego ma postać:

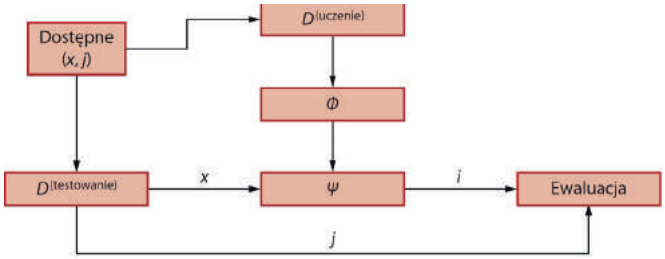
$$\Psi(x, D^{(\text{uczenie})}) = i$$

gdzie $i \in M$

Proces uczenia, mający na celu zbudowanie klasyfikatora Ψ, jest realizowany z wykorzystaniem wybranego algorytmu nadzorowanego uczenia się Φ:

$$\Psi \leftarrow \Phi(D^{(\text{uczenie})})$$

Proces testowania, mający na celu ocenę jakości klasyfikatora, jest realizowany z wykorzystaniem zbioru testującego $D^{(\text{testowanie})}$, który co do struktury ma taką samą postać jak zbiór uczący. Proces testowania polega na porównaniu wyniku $\Psi(x)$ do j dla każdego elementu $(x, j) \in D^{(\text{testowanie})}$. Proces uczenia, testowania i ewaluacji klasyfikatora jest przedstawiony na rysunku 1.1.



Rysunek 1.1. Proces uczenia, testowania i ewaluacji klasyfikatora.
Źródło: opracowanie własne

1.2.3. Ocena jakości klasyfikatora

Dla klasyfikacji binarnej ocena jakości pracy klasyfikatora jest ustalana na podstawie macierzy błędu klasyfikacji obiektu x (zob. tab. 1.1)[6], w ramach której określone są cztery możliwości:

1. PP: Prawdziwie pozytywny (ang. *true positive*) – gdy $\Psi(x) = 1$ i $j = 1$
2. PN: Prawdziwie negatywny (ang. *true negative*) – gdy $\Psi(x) = 0$ i $j = 0$
3. FP: Fałszywie pozytywny (ang. *false positive*)[7] – gdy $\Psi(x) = 1$ i j = 0
4. FN: Fałszywie negatywny (ang. *false negative*)[8] – gdy $\Psi(x) = 0$ i $j = 1$

Tabela 1.1. Macierz błędu klasyfikacji binarnej $M = \{0,1\}$ dla obiektu x.
Źródło: opracowanie własne

		Klasa j dla obiektu x ze zbioru testującego $D^{(\text{testowanie})}$	
		I	0
Klasa i wygenerowana przez klasyfikator Ψ(x)	I	PP prawdziwie pozytywny	FP fałszywie pozytywny
	0	FN fałszywie negatywny	PN prawdziwie negatywny

Dla przykładu rozważmy system detekcji nadużyć (ang. *fraud detection system*) w bankowości elektronicznej jako klasyfikator binarny, dla którego mamy: $M = \{0$ – brak nadużycia (transakcja poprawna), 1 – jest nadużycie (transakcja niepoprawna).

Dla takiego klasyfikatora interpretacja jest następująca:

1. Prawdziwie pozytywny – sytuacja poprawna, tj. nadużycie zostało prawidłowo rozpoznane przez klasyfikator jako nadużycie.
2. Prawdziwie negatywny – sytuacja poprawna, tj. brak nadużycia został prawidłowo rozpoznany przez klasyfikator jako brak nadużycia.
3. Fałszywie pozytywny – błąd, tj. brak nadużycia został nieprawidłowo rozpoznany przez klasyfikator jako nadużycie. Ten rodzaj błędu jest powszechnie nazywany fałszywym alarmem, co oznacza, że według klasyfikatora są spełnione określone warunki alarmowe, które faktycznie nie zachodzą.
4. Fałszywie negatywny – błąd, tj. rzeczywiste nadużycie zostało nieprawidłowo rozpoznane przez klasyfikator jako brak nadużycia. Dla tego rodzaju błędu faktycznie zachodzą warunki alarmowe, ale nie są one przez klasyfikator rozpoznane, czyli niepoprawna transakcja jest realizowana bez przeszkód.

Warto zauważyć potencjalne konsekwencje i koszty związane z błędami klasyfikatora, które w zastosowaniach praktycznych wymagają starannej analizy ryzyka. Formalnie to zagadnienie jest rozwiązywane przez wprowadzenie tzw. funkcji strat (ang. *loss function*)[9] i opracowanie takiego klasyfikatora Ψ, aby minimalizować wartość średnią funkcji strat (Kurzyński, 1997).

Na podstawie macierzy błędu można wyznaczyć podstawowe miary jakości klasyfikatora:

1. Dokładność (ang. *accuracy*) = (PP + PN) / (PP + PN + FP + FN).
2. Precyzja (ang. *precision*) = PP / (PP + FP).
3. Czułość (ang. *recall*) = PP / (PP + FN).
4. F1 score[10] = 2 * ((Precyzja * Czułość)/(Precyzja + Czułość)).

1.2.4. Problemy budowania systemów uczących się

Racjonalne użytkowanie systemów uczących się wymaga znajomości ich ograniczeń oraz problemów związanych z ich eksploatacją. Świadomość tych problemów implikuje rozsądne oczekiwania, poprawną interpretację jakości odkrywanej przez nie wiedzy oraz daje wytyczne metodyczne w zakresie technik uczenia, aktualizacji i testowania. Jakość działania tych systemów, budowanych nawet w warunkach „laboratoryjnych", tj. bez jakichkolwiek intencjonalnych ataków czy zakłóceń, z definicji nie jest idealna i systemy te popełniają błędy. Wynika to z następujących problemów związanych z praktyką budowy systemów uczących się[11] (Surma, 2017):

- **Problem wnioskowania indukcyjnego** – uczenie się na podstawie przykładów ze zbioru uczącego jest wnioskowaniem indukcyjnym. Istota tego wnioskowania polega na tym, że na podstawie dostępnych obserwacji (faktów) wyprowadza się generalizacje (uogólnienia) wyjaśniające te obserwacje. Istotne jest podkreślenie, że dostępne przykłady reprezentują zwykle wycinek danej rzeczywistości, ich liczebność jest ograniczona, zwykle nie są reprezentatywne dla całej populacji i oczywiście nie są znane ich rozkłady prawdopodobieństwa. Należy zatem pamiętać o fundamentalnych ograniczeniach związanym z wnioskami indukcyjnymi. W przeciwieństwie do wnioskowania dedukcyjnego niemożliwe jest udowodnienie, że wniosek indukcyjny jest prawdziwy. Natomiast można

go jednoznacznie sfalsyfikować (Popper, 2002). Wnioskowanie indukcyjne podtrzymuje fałsz, co oznacza, że jeżeli dostępne obserwacje są nieprawdziwe (w rzeczywistych zastosowaniach jest to możliwe), to wnioski indukcyjne również będą nieprawdziwe. Natomiast z prawdziwych obserwacji niekoniecznie musimy uzyskać prawdziwe wnioski. Tak więc niejako z definicji każdy wniosek indukcyjny należy traktować jako niepewny.

- **Problem historii i aktualizacji** – każdy proces uczenia się na podstawie przykładów ze zbioru uczącego dotyczy obserwacji (faktów) historycznych, tzn. takich, które zaistniały w przeszłości. Natomiast dziedzina podlegająca analizie zwykle nie jest statyczna[12], lecz dynamiczna, tj. podlega zmianom w czasie. Jest to kluczowe zagadnienie na przykład w zastosowaniach biznesowych, gdzie otrzymany model nawet po relatywnie krótkim okresie po zbudowaniu i wdrożeniu do eksploatacji może być już „przestarzały". Zmiany w samej firmie i jej otoczeniu konkurencyjnym, zmiany na poziomie makroekonomicznym i politycznym powodują, że system uczący się będzie popełniał błędy i generował wadliwe decyzje. Jedynym remedium jest częsta aktualizacja zbioru uczącego i ponowne uczenie się systemu. W praktyce jest to bardzo złożone zagadnienie, związane z permanentnym, adekwatnym do szybkości zmian i ich istotności, procesem aktualizacji systemu uczącego się.
- **Problem „przeuczenia"** – oczywistym celem budowania modelu na podstawie przykładów ze zbioru uczącego jest jego poprawne działanie nie dla przykładów, na których był uczony, ale dla przykładów „nowych", które nie należą do zbioru uczącego. Klasycznym negatywnym zjawiskiem w trakcie działania algorytmów maszynowego uczenia jest tzw. przeuczenie (ang. *overfitting*), czyli nadmierne dopasowanie powstałego modelu do zbioru uczącego. Nadmiernie dopasowany model doskonale odzwierciedla przykłady uczące, jest zwykle bardzo „rozbudowany", ale jednocześnie ma relatywnie małą zdolność generalizacji, tj. poprawnej reakcji na nowe przykłady (Mitchell, 1997). To zjawisko jest naturalne w procesie uczenia się, można je próbować redukować, niemniej samo zjawisko występuje zawsze, co w końcu objawia się obniżeniem jakości działania systemu.

1.2.5. Potencjalne cele atakującego

Intencjonalny atak na systemy uczące się może mieć następujące cele:

1. **Obniżenie jakości klasyfikatora** (ang. *misclassification*) przez generowanie błędów fałszywie pozytywnych lub fałszywie negatywnych (zob. tabela 1.1). Konsekwencją tego typu ataku jest spadek dokładności klasyfikacji, co implikuje obniżenie wiarygodności systemu (ang. *cofi dence reduction*), a nawet w sytuacji skrajnej rezygnację z jego użytkowania. Wynika to m.in. z faktu, że błędne klasyfikacje generują realne i potencjalne (np. związane z utratą reputacji) koszty będące konsekwencją błędnych decyzji albo ich braku.
2. **Celowy błąd klasyfikacji** (ang. *targeted misclassification*) przez uzyskanie błędnej klasyfikacji dla określonych obiektów. W takiej sytuacji klasyfikator niepoprawnie klasyfikuje konkretny obiekt lub zbiór obiektów zgodnie z intencją atakującego. W takim podejściu atakujący jest zainteresowany, aby jakość klasyfikatora była na odpowiednim wysokim poziomie i tym samym wzbudzał on zaufanie użytkowników. Ten atak jest najczęściej realizowany przez tzw. tylną furtkę w klasyfikatorze (ang. *targeted backdoor attack*) – zob. przykład w rozdziale 2.2.
3. **Ograniczenie dostępności** (ang. *access restriction*), czyli uzyskanie nieakceptowalnie długiego czasu reakcji systemu na dane wejściowe, a w sytuacji skrajnej zatrzymanie działania systemu. Celem atakującego może też być ograniczenie dostępności w trakcie budowania modelu, tj. w trakcie jego uczenia, aktualizacji i testowania.

Wymienione cele intencjonalnych ataków znajdują swoje odzwierciedlenie w kryteriach ochrony informacji omówionych w następnym podrozdziale.

1.3. Taksonomia ataków na systemy uczące się

1.3.1. Kryteria jakości ochrony informacji

System uczący się jest systemem informatycznym, który podlega takim samym kryteriom oceny cyberbezpieczeństwa jak każdy system informatyczny. W tej perspektywie można wyróżnić standardowo trzy kryteria jakości ochrony informacji[13] (Liderman, 2017):

1. **Poufność** (tajność) (ang. *confidentiality*) – ochrona informacji przed nieuprawnionym dostępem.
2. **Integralność** (ang. *integrity*) – zapewnienie, że składowane i przetwarzane dane są niezmienione i nie zostały wykonane na nich niedozwolone działania.
3. **Dostępność** (ang. *availability*) – zapewnienie adekwatnego stopnia dostępności do danych, procesów i aplikacji dla autoryzowanych użytkowników.

Taka specyfikacja kryteriów umożliwia poprawne zarządzanie ryzykiem operacyjnym i ustalenie odpowiednich polityk bezpieczeństwa (Andress, 2014). To podejście jest zgodne ze specyfikacją amerykańskiego instytutu standardów technicznych NIST (ang. *National Institute of Standard and Technology*)[14], który nawiązuje do standardu oceny ryzyka bezpieczeństwa informacji[15]. W specyfikacji NIST atak jest wykonywany na konkretny cel (ang. *target*) i jego konsekwencje (ang. *consequences*) zależą od przyjętych procedur obrony (ang. defenses). Potencjalne konsekwencje są zgodne z wymienionymi wcześniej trzema kryteriami jakości ochrony informacji[16]. W odwołaniu do triady Poufność–Integralność–Dostępność możliwe jest zatem przedstawienie następującej taksonomii ataków na systemy uczące się:

1. Atak na poufność (ang. *confidentiality violation*) – polega na zdobyciu informacji, które dotyczą procesu uczenia, aktualizacji, testowania i użytkowania systemu.

   Oznacza to zdobycie informacji obejmującej:
   a. obiekt x wraz z jego specyfikacją cech,
   b. zbiór etykiet klas M,
   c. klasyfikator Ψ,
   d. algorytm Φ wraz z jego parametrami,
   e. zbiór uczący $D^{(\text{uczenie})}$ oraz stosowane metody aktualizacji,
   f. zbiór testujący $D^{(\text{testowanie})}$ oraz zastosowane metody

testowania,

g. użyte biblioteki i środowiska programistyczne,

h. kontekst użycia systemu: intencje, cel użycia systemu, organizacja pracy, zaangażowani pracownicy, klienci itp.

Biorąc pod uwagę ten zakres informacji, wiedzę atakującego można podzielić na trzy grupy: pełna wiedza (*white box attack*), wiedza częściowa (*grey box*) i brak wiedzy (*black box*). W każdym wymienionym przypadku, nawet przy całkowitym braku wiedzy, możliwe są skutecznie działania atakującego. W przypadku zdobycia pełnej wiedzy mówimy o pełnej ekstrakcji modelu (ang. *extraction attack*). Natomiast przy wiedzy niepełnej lub jej braku atakujący próbuje odtworzyć model i buduje jego substytut, bazując na założeniach, domysłach i testach, jeśli jest to możliwe. Atak na poufność, jako rodzaj rozpoznania (rekonesans) i zdobycia wiedzy, zwykle poprzedza atak na integralność albo na dostępność.

Szczególnym rodzajem ataku na poufność jest naruszenie prywatności (ang. *privacy voliations*) (Huang i in., 2011), które dotyczy osób zaangażowanych w proces budowania modelu czy osób korzystających z systemu. Wiedza o członkach zespołu programistycznego może ułatwić ustalenie, z jakich bibliotek programistycznych korzystano przy budowaniu modelu. Problem naruszenia prywatności dotyczy również osób, których dane zostały wykorzystane w zbiorach uczących i testujących. Na przykład zdobycie informacji o tym, że zdjęcie konkretnej osoby zostało wykorzystane w procesie uczenia, może ułatwić odtworzenie zbioru uczącego. Niejako odwrotny scenariusz to przeprowadzenie testu, aby określić, czy w zbiorze uczącym są dane konkretnej osoby (ang. *membership inference attack*).

2. Atak na integralność (ang. *integrity violation*) – polega na zakłóceniu procesu uczenia, aktualizacji lub testowania zgodnie z celami atakującego omówionymi w poprzednim podrozdziale. Ze względu na ważność i złożoność tego zagadnienia temu rodzajowi ataków poświęcono następny podrozdział.
3. Atak na dostępność (ang. *availability violation*) – polega na spowolnieniu albo zatrzymaniu pracy systemu, co utrudnia jego praktyczne wykorzystanie. Ten rodzaj ataku może być wykonany w trakcie uczenia, testowania czy też przez zakłócenia procesu aktualizacji systemu. Niemniej najczęściej realizowany jest w fazie użytkowania (funkcjonowania) systemu. W tym kontekście możliwe jest:

a. Zakłócenie lub zablokowanie procesu zbierania i przekazywania obiektów do klasyfikacji, np. przez wygenerowanie „sztucznego tłoku" obiektów na wejściu klasyfikatora (ang. *denial of service*).

b. Generowanie dużej liczby błędów fałszywie pozytywnych, powodujących zaangażowanie zasobów na obsługę tych błędów (ang. *false positive over load*). To podejście wymaga ingerencji w proces uczenia lub testowania. Ta problematyka zostanie omówiona w dalszej części rozdziału.

1.3.2. Atak na integralność systemów nadzorowanych

1.3.2.1. Formalizacja ataku na integralność

Z formalnego punktu widzenia problem bezpieczeństwa systemów uczących się, w zakresie ataków na ich integralność, można opisać jako grę między atakującym (przestępcą) a obrońcą (administratorem) systemu. Tego typu gra może być sformalizowana przez (Huang i in., 2011):

- Φ – algorytm maszynowego uczenia się,
- $A^{(\text{uczenie})}$ – procedurę atakującego naruszającą integralność zbioru uczącego,
- $A^{(\text{testowanie})}$ – procedurę atakującego naruszającą integralność zbioru testującego.

Dla tak zdefiniowanych zmiennych gra wygląda następująco:

1. Obrońca (administrator) wybiera Φ w celu zbudowania klasyfikatora Ψ z wykorzystaniem posiadanych danych: $D^{(\text{uczenie})}$ oraz $D^{(\text{testowanie})}$
2. Atakujący (przestępca) wybiera scenariusz ataku (potencjalnie z wiedzą o Φ): $A^{(\text{uczenie})}$ lub $A^{(\text{testowanie})}$
3. Proces uczenia:

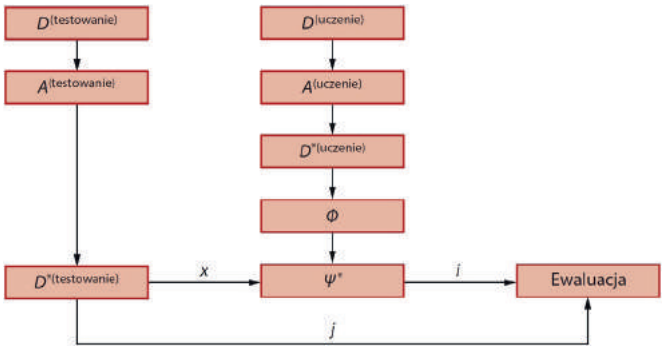
a. Z wykorzystaniem $A^{(\text{uczenie})}$ wygeneruj „zainfekowany" zbiór uczący $D^{*(\text{uczenie})}$

b. Zbuduj klasyfikator: $\Psi^* \leftarrow \Phi\,(D^{*(\text{uczenie})})$

4. Proces testowania:

a. Z wykorzystaniem A(testowanie) wygeneruj „zainfekowany" zbiór testujący $D^{*(\text{testowanie})}$

b. Wynik $\Psi^*(x)$ porównaj do j dla każdego elementu zbioru $(x, j) \in D^{*(\text{testowanie})}$



Rysunek 1.2. Scenariusze ataków na integralność systemu uczącego się. Źródło: opracowano na podstawie Huang, L., Joseph, A., Nelson, B., Rubinstein, B. i Tygar, J. (2011). Adversarial machine learning. W: *Proceedings of the 4th ACM workshop on Security and artificial intelligence* (AISec '11). ACM Press.

W tego typu grze (zob. rysunek 1.2) obrońca wybiera Φ, tak aby uzyskać najlepszą jakość klasyfikacji dla posiadanych $D^{(\text{uczenie})}$ oraz $D^{(\text{testowanie})}$ i jednocześnie nie mając wiedzy o $A^{(\text{uczenie})}$ oraz $A^{(\text{testowanie})}$. Atakujący stara się natomiast obniżyć jakość klasyfikacji przez odpowiednie dobranie $A^{(\text{uczenie})}$ lub $A^{(\text{testowanie})}$. W praktyce oznacza to intencjonalny wpływ na pracę klasyfikatora, aby uzyskać następujący jeden z dwóch rodzajów błędów klasyfikacji: typ I błędu (fałszywie pozytywny) lub typ II błędu (fałszywie negatywny).

1.3.2.2. Atak na proces budowania systemu

W ramach ataku na proces budowania systemu (uczenie, aktualizacja, testowanie) możliwe jest naruszenie integralności zarówno zbioru uczącego, testującego, jak i procesu uczenia/aktualizacji oraz testowania. Zgodnie z propozycją Chakraborty'iego i in. (2018) uzasadnione jest rozróżnienie na:

1. **Atak infekcyjny** (ang. *poisoning atack*) – atak na proces uczenia lub aktualizacji, który polega na ingerencji w zbiór

uczący[17]:

- Z wykorzystaniem $A^{(\text{uczenie})}$ wygeneruj „zainfekowany" zbiór uczący $D^{*(\text{uczenie})}$
- Zbuduj klasyfikator: $\Psi' \leftarrow \Phi(D^{*(\text{uczenie})})$

W pracy Huanga i in. (2011) ten rodzaj ataku jest nazywany atakiem przyczynowym (ang. *causative attack*). Procedura atakującego naruszająca integralności zbioru uczącego A(uczenie) może być realizowana przez:

- Infekowanie danych (ang. *data injection*) – realizowane przez dodawanie do zbioru uczącego fałszywych przykładów, a także modyfikowanie lub usuwanie istniejących elementów zbioru uczącego (ang. *data modification*). Tego typu działania mogą na przykład wpływać na taki rozkład klas w zbiorze uczącym, aby spowodować „stronniczość" (ang. *bias*) klasyfikatora.
- Manipulowanie danymi (ang. *data manipulation*) – realizowanie przez wpływanie na strukturę zbioru uczącego zarówno przez dodanie, modyfikację lub usunięcie cechy wektora x, jak i etykiety klasy j (ang. *label modification*).

Należy wspomnieć, że dane uczące niejednokrotnie reprezentują rzeczywiste obiekty. Możliwa jest zatem sytuacja, że manipulacja następuje na rzeczywistym obiekcie, np. charakteryzacja osoby, której zdjęcie trafia do zbioru uczącego i w konsekwencji reprezentacja wektorem x tej osoby jest z definicji zniekształcona.

2. **Atak inwazyjny** (ang. *envasion attack*) – atak na proces testowania, który polega na ingerencji w zbiór testujący:

- z wykorzystaniem A(testowanie) wygeneruj „zainfekowany" zbiór testujący $D^{*(\text{testowanie})}$
- wynik $\Psi(x)$[18] porównaj do j dla każdego elementu zbioru $(x, j) \in D^{*(\text{testowanie})}$

W pracy Huanga i in. (2011) ten rodzaj ataku jest nazywany atakiem eksploracyjnym (ang. *exploratory atack*). Procedura atakującego naruszająca integralności zbioru testującego $A^{(\text{testowanie})}$ może być realizowana przez infekowanie danych, co jest realizowane przez dodawanie do zbioru testującego fałszywych przykładów, a także modyfikowanie lub usuwanie istniejących elementów zbioru testującego. Aby nie być wykryty, atakujący stara się tak modyfikować zbiór testujący, żeby odzwierciedlał charakterystykę (rozkład statystyczny) rzeczywistego zbioru testującego.

3. **Atak na model** (ang. *model logic corruption*) – jest to atak przeprowadzony bezpośrednio na model Ψ, tak aby uzyskać jego wersję „zniekształconą" Ψ'. Ten rodzaj ataku może wystąpić w sytuacji, kiedy użytkownik nieświadome korzysta z algorytmu maszynowego uczenia się Φ, który został pobrany z publicznie dostępnych zainfekowanych[19] środowisk programistycznych (Chakraborty i in., 2018). Innym wektorem ataku może być przejęcie wcześniej zainfekowanego modelu przez tzw. uczenie poprzez transfer modelu (ang. *transfer learning*)[20]. Przykładem tego typu ataku jest utworzenie modelu, który będzie realizował celowy błąd klasyfikacji, a następnie przekazanie go w ramach transferu do właściwego klasyfikatora. Eksperyment tego typu dla klasyfikatora zdjęć pochodzących z rezonansu elektromagnetycznego wykonał Wang z zespołem (2020). Przez scenariusz z transferem modelu udało się zbudować niezwykle wiarygodny klasyfikator (dokładność klasyfikacji >97%), który jednocześnie był w stanie błędnie klasyfikować określone zdjęcia z rezonansu.

Możliwości ataków na proces uczenia/aktualizacji i testowania nie ograniczają się tylko do wymienionych rodzajów. Możliwa jest również manipulacja procesem uczenia i testowania, tak aby pogorszyć jakość działania klasyfikatora przez wykorzystanie klasycznych problemów systemów uczących się, takich jak na przykład uczenie na „przestarzałych" zbiorach danych. Atakujący może też dezinformować lub przez działania socjotechniczne doprowadzić obrońcę do prowadzenia procesu uczenia w sposób nierzetelny, co może skutkować na przykład „przeuczeniem" klasyfikatora.

1.3.2.3. Atak na funkcjonujący system

Klasyfikator po zbudowaniu również może podlegać atakom. Jak już wspomniano, wiedza atakującego o systemie może być pełna (*white box*), częściowa (*grey box*) albo może jej brakować (*black box*).

W przypadku udanego ataku na poufność i zdobycia wiedzy całkowitej lub częściowej atakujący ma możliwość odtworzenia modelu klasyfikatora. Na przykład zdobycie wiedzy o zbiorze uczącym oraz o używanym środowisku programistycznym może umożliwić samodzielne zbudowanie wiarygodnego modelu i analizę jego podatności. Taka próba odtworzenia i zbudowania substytutu rzeczywistego modelu jest szczególnie istotnym wektorem ataku. Wynika to z tego, że uzyskanie wpływu na proces uczenia i testowania klasyfikatora jest z reguły niezwykle trudne do osiągnięcia, i będzie potencjalnie generować niewspółmiernie wysokie koszty potencjalnego ataku[21].

W sytuacji braku jakiejkolwiek wiedzy system jest traktowany jako czarna skrzynka, która może podlegać eksperymentom mającym na celu zbadanie, jaka będzie reakcja systemu na określone dane wejściowe[22]. Jest to klasyczne zadanie identyfikacji, które ma na celu zbudować model systemu na podstawie badań eksperymentalnych, tj. danych pomiarowych zebranych z wejścia i wyjścia identyfikowanego systemu (Bubnicki, 1974). Zebranie odpowiednio dużej liczby par wejście – wyjście umożliwia zbudowanie zbioru uczącego i zbudowanie przez atakującego substytutu rzeczywistego klasyfikatora. Mając taki model, atakujący może opracować zainfekowane przykłady (ang. *adversarial examples*), które wykorzysta w ataku na rzeczywiście pracujący system. To podejście wymaga od atakującego dostępu do atakowanego systemu. Na przykład identyfikacja funkcjonowania systemu rozpoznawania obiektów w samochodach firmy Tesla wymagała od hakerów zakupienia modelu tego samochodu z funkcją „autopilot"[23]. Podobny atak w przypadku sytemu identyfikacji nadużyć w bankach jest niemal niemożliwy do realizacji. Atakujący musieliby rozważyć kradzież takiego systemu bądź zakup od dostawcy tego oprogramowania. Natomiast jakiekolwiek próby eksperymentów na operacyjnie działający system bankowy zakończyłyby się najpewniej szybkim wykryciem przez zespół nadzoru.

W kontekście ataku na funkcjonujące systemy należy jeszcze wspomnieć o dwóch teoretycznie możliwych wektorach ataków związanych z manipulacją wejścia i wyjścia systemu.

Atak na obiekt wejściowy oznaczałby taką modyfikację rzeczywistego obiektu wejściowego (np. zmiana kolorów znaku drogowego), aby został niepoprawnie rozpoznany. W tym rodzaju ataku należy także uwzględnić fizycznie usunięcie obiektu albo spowodowanie, że nie zostanie zauważony przez system. Atak na wyjście systemu oznaczałby zmianę wygenerowanego przez system wyjścia albo jego usunięcie.

1.3.3. Atak na integralność innych rodzajów systemów uczących się

Najpopularniejsze zadania realizowane przez systemy uczące się, poza omówionym zadaniem klasyfikacji i regresji, są następujące:

1. Grupowanie (ang. *clustering*) – polega na znajdowaniu w zbiorze obiektów podzbiorów (grup) obiektów o podobnych charakterystykach. Celem algorytmu grupowania jest podział zbioru obiektów na podzbiory (grupy), dla których podobieństwo obiektów wewnątrz grupy (ang. *inter class similarity*) jest maksymalizowane, a podobieństwo od obiektów z innych grup (ang. *intra class similarity*) jest minimalizowane (Surma, 2011). W przeciwieństwie do zadania klasyfikacji, gdzie podana jest klasyfikacja, w przypadku grupowania zadaniem algorytmu jest znalezienie klas, na jakie można pogrupować obiekty. Z tego też powodu to podejście nazywane jest uczeniem się nienadzorowanym, tj. bez nauczyciela (ang. *unsupervised learning*).

2. Okrywanie reguł asocjacyjnych (ang. *association rules learning*) – polega na wyszukiwaniu grup obiektów, które występują razem w określonym kontekście. Zadanie to jest realizowane przez wykorzystanie algorytmów analiz związków. Klasycznym przykładem tej klasy zadań jest analiza koszyka zakupów (ang. *market basket analysis*), gdzie szuka się odpowiedzi na pytanie, jakie produkty sprzedają się najczęściej razem w ramach jednego koszyka zakupowego (Surma, 2011)[24].

3. Selekcja przez współpracę (ang. *collaborative filtering*) – podejście, w którym rekomenduje się użytkownikowi produkt/usługę, które były odpowiednie dla innych podobnych użytkowników. Metoda powszechnie stosowana w systemach rekomendacyjnych, w których predykcja zainteresowania (filtrowanie ze zbioru możliwych rekomendacji) dla danego użytkownika oparta jest na zebraniu preferencji lub opinii innych użytkowników (współpraca). Podejście to funkcjonuje na bazie hipotezy, że jeśli użytkownik A ma taką samą opinię jak użytkownik B na wybrany temat, to prawdopodobieństwo, że A i B mają taką samą opinię na inny temat jest większe niż to, że A będzie miał taką samą opinię do losowo wybranej osoby (Ricci i in., 2011).

4. Uczenie się ze wzmocnieniem (ang. *reinforcement learning*) występuje w sytuacji, kiedy system uczący się pozyskuje informację, jak jego zachowanie (akcje) jest oceniane (nagroda). System może swoje zachowanie zmieniać w taki sposób, aby zostało ocenione lepiej i w efekcie było bliższe postawionym przed nim celom. W tym podejściu po wykonaniu określonej akcji system otrzymuje nagrodę w formie liczbowej (nazywanej często wzmocnieniem), która jest miarą oceny jakości jego działania. Najczęściej w praktyce rozważa się przypadek, kiedy system ma maksymalizować swoje nagrody długoterminowo (Cichosz, 2009).

Tabela 1.2. Badania naukowe na temat ataków na systemy uczące się. Źródło: opracowanie własne

Rodzaj zadania	Wybrane badania naukowe
Grupowanie	(Kloft i Laskov 2010) (Chhabra i in., 2019) (Chhabra i in., 2020)
Filtrowanie przez współpracę	(Li i in., 2016) (Deldjoo i in., 2020)
Uczenie ze wzmocnieniem	(Chen i in., 2019) (Gleave i in., 2020)

Reprezentatywne badania związane z atakami na tego typu systemy zostały podsumowane w tabeli 1.2. Jak widać, ten obszar badawczy jest bardzo nowatorski. Tabela nie uwzględnia ataków na systemy odkrywające reguły asocjacyjne. W czasie pisania tej monografii nie było jeszcze wiarygodnych badań naukowych w tym obszarze.

Przypisy

[1] 1 W listopadzie 2015 r. Google udostępnił na zasadach open source popularną bibliotekę oprogramowania TensorFlow, służącą do budowania modeli systemów uczących się.

[2] To pojęcie pojawia się po raz pierwszy w roku 2007 w roboczym opracowaniu pt. Foundations of Adversarial Machine Learning dostępnym na stronie: https://www.researchgate.net/publication/228623424_Foundations_of_Adversarial_Machine_Learning

[3] https://www.usenix.org/conference/scainet19/presentation/carlini (dostęp: 19.05.2020 r.).

[4] Źródło informacji trenującej jest potocznie nazywane nauczycielem.

[5] W przypadku zadania regresji zbiór M jest zbiorem liczb rzeczywistych.

[6] Omawiane podejście odwołuje się do tzw. klasyfikacji binarnej, czyli zbiór klasyfikacji jest dwuwartościowy {0;1}, niemniej może być również zastosowane dla wielowartościowych zbiorów klas. W praktyce ocena jakości pracy klasyfikatora jest poprzedzona procesem walidacji (w celu wyboru najlepszego modelu) weryfikowanym przez funkcję straty z wykorzystaniem entropii krzyżowej (ang. *binary cross entropy loss function*). Do oceny jakości klasyfikacji w przypadku ciągłego zbioru klas M (zadanie regresji) stosuje się najczęściej błąd średniokwadratowy MSE (ang. *mean square error*).

[7] W statystyce ta sytuacja jest nazywana błędem pierwszego rodzaju (ang. *type I error*).

[8] W statystyce ta sytuacja jest nazywana błędem drugiego rodzaju (ang. *type II error*).

[9] W niektórych opracowaniach używa się pojęcia funkcji kosztu (ang. *cost function*).

[10] Współczynnik Sørensena–Dice'a.

[11] Przedstawione problemy dotyczą systemów uczących się pod nadzorem, niemniej można je, przy odpowiedniej interpretacji, zastosować także do systemów uczących się bez nadzoru.

[12] Przykładem dziedziny „statycznej", niepodlegającej zmianom w czasie, jest diagnostyka techniczna. Zakładamy, że prawa fizyki, którym podlega diagnozowane urządzenie, są stałe (co może podlegać spekulacji w ramach filozofii nauki) i dzięki temu takie systemy mogą być „uczone" jednorazowo na danych historycznych bez utraty jakości ich działania.

[13] Ponadto wyróżnia się takie kryteria, jak: rozliczalność, niezaprzeczalność i autentyczność, które nie są znacząco relewantne dla bezpieczeństwa systemów uczących się.
[14] https://www.nist.gov/news-events/news/2019/10/taxonomy-and-terminology-adversarial-machinelearning-nist-releases-draft (dostęp: 21.05.2020 r.).
[15] NIST Guide for Conducting Risk Assessments (NIST 800-30) https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (dostęp: 21.05.2020 r.).
[16] W specyfikacji NIST kryterium poufności obejmuje również zagadnienie prywatności (ang. *privacy*) i w takiej szerszej interpretacji będzie analizowane w dalszej części rozdziału.
[17] W procesie aktualizacji również używany jest zbiór uczący bez względu na to, czy system jest uczony „na nowo" z wykorzystaniem aktualnie dostępnego zbioru uczącego, czy też z wykorzystaniem metod inkrementacyjnych (ang. *incremental learning*), gdzie system aktualizuje się na bieżąco w przypadku pojawienia się nowych przykładów uczących.
[18] Jeśli atak inwazyjny jest skoordynowany z przeprowadzonym wcześniej atakiem infekcyjnym, to $\Psi(x) = \Psi'(x)$.
[19] Zawierających podatności (ang. vulnerability) w kodzie programów, które są znane atakującemu. Możliwy jest też scenariusz, że atakujący podmieni używane przez obrońcę oprogramowanie, na oprogramowanie zawierające złośliwy kod.
[20] W tym podejściu do rozwiązania nowego problemu wykorzystuje się wcześniej opracowany model dla innego zagadnienia. Jest to relatywnie często wykorzystywana metoda, w warunkach dostępności relatywnie małych zbiorów uczących, do rozpoczęcia uczenia (ang. *starting point*) wielowarstwowych sieci neuronowych.
[21] Analiza rentowności ataku, czyli zestawienie kosztów przeprowadzenia ataku z korzyściami z niego wynikającymi, jest ważnym zagadnieniem badawczym, umożliwiającym analizę ryzyka i określenie najbardziej prawdopodobnych wektorów ataków. Oczywiście to podejście jest adekwatne dla grup przestępczych kierujących się zyskiem, co nie jest na przykład kryterium dla aktorów państwowych (ang. state actor).
[22] Czasami ten rodzaj ataku na czarną skrzynkę jest nazywany nieformalnie atakiem z odwołaniem się do wyroczni (ang. *oracle attack*), w którym dla zadanych pytań (wejście) wyrocznia odpowiada (wyjście).
[23] https://www.forbes.com/sites/thomasbrewster/2019/04/01/hackers-use-little-stickers-to-trick-tesla-autopilotinto-the-wrong-lane/ (dostęp: 3.05.2020 r.).
[24] Jeden z pierwszych projektów biznesowych w tej dziedzinie został przeprowadzony przez T. Blischoka z Terradata, gdzie dla sieci 50 sklepów przebadano paragony z okresu 90 dni. Wtedy została odkryta „słynna" reguła mówiąca, że w piątki po południu istnieje silny związek między sprzedażą piwa i pieluszek dla dzieci.

Bibliografia dostępna na stronie www.nis.com.pl w zakładce Bibliografia

dr hab. inż. Jerzy Surma, prof. SGH

Transport konny w podziemiach kopalń

Stefan Gierlotka

Dawniej górnik transportował węgiel z płytkich szybów za pomocą kubła i konopnej liny. Gdy wielkość kopalń wzrosła, tak, iż wyrobiska pionowe zastąpiono podziemnymi wyrobiskami poziomymi, często odległymi od szybu nawet o kilka kilometrów, ręczny transport urobku okazał się zbyt uciążliwy, a przy tym mało produktywny. Wówczas, dla zwiększenia wydajności zaprzęgnięto do pracy w kopalni konie.

Początkowo urobek ciągnięto w specjalnych skrzyniach na płozach lub kołach po spągu. Tory kolejowe w angielskich i niemieckich kopalniach znane były już w XVII wieku. Pierwsze tory kolejowe wykonane były z szyn drewnianych obitych dla wzmocnienia blachą. Szyny żelazne pojawiły się w kopalniach w XVIII wieku.

W śląskich kopalniach w początkach XIX wieku zaczęto stosować transport wozów po torach w kierunku szybu. Siłę do pchania wózków dostarczali młodzi chłopcy zwani ślęprami, którzy przyzwyczajali się do przyszłej pracy w przodku. Nazwa ślęper, popularna w kopalniach, etymologicznie pochodzi od niemieckiego bezokolicznika schleppen, co oznacza wlec, pchać.

Na Górnym Śląsku, po raz pierwszy użyto koni w transporcie podziemnym z inicjatywy Salomona Isaaca w 1803 roku. Wtedy też w kopalni Königin Luise w Zabrzu wprowadzono konie do wyrobisk górniczych i uruchomiono podziemny konny transport węgla. Salomon Isaac, pochodzący z belgijskiej żydowskiej rodziny, został przez Fryderyka Redena, ówczesnego dyrektora Wyższego Urzędu Górniczego, sprowadzony dla przeprowadzenia badań geologicznych na Górnym Śląsku. Salomon Isaac odkrył pokłady węgla w okolicach Niewiadomia, Czernicy i Czerwionki oraz bogate złoża węgla w okolicach Łagiewnik i Zabrza. Wprowadził do kopalń filarowy system eksploatacji pokładów węgla oraz zastosowanie koni w transporcie

podziemnym. W nagrodę został mianowany inspektorem górniczym.

Konie w kopalni traktowane były przez górników zawsze z szacunkiem. Dla odpoczynku konie posiadały stajnię na podszybiu. Przystosowane wyrobisko na stajnię miało odpowiednią wentylację i odwodnienie spągu. Wyrobisko było murowane, a ściany wyłożone były płytkami ceramicznymi. Żłoby dla pojenia i karmienia również były murowane i wyłożone ceramicznymi płytkami. Obok stajni znajdowało się pomieszczenie dla magazynowania słomy i siana. Woda, z uwagi na wybredność koni, była zwożona w cysternach. Dobrze napojony koń pracował wydajniej. Woda musiała być czysta, gdyż koń nie lubi

wody brudnej. Po pracy koniowi należał się taki sam czas odpoczynku jak pracującemu górnikowi. Średni dobowy czas pracy konia wynosił 8 godzin. Każdy pracujący na dole koń posiadał swoją szychtownicę, w której potwierdzano zmianę, na której pracował i należną mu, wolną od pracy niedzielę. Konie dołowe były okresowo badane przez weterynarza.

Kopalnia Kleofas w Katowicach miała w 1900 roku 94 konie pracujące na dole. Kopalnia Matylda w Świętochłowicach w 1909 roku posiadała 17 stajni dołowych. W 1913 roku, w Kopalni Charlote pracowały na dole 93 konie. W 1929 roku, w kopalniach Górnego Śląska na terenie Polski pracowało 741 koni.

W okresie międzywojennym przepisy górnicze, dotyczące pracujących koni były bardziej rygorystyczne i wymagały zapewnienia im odpowiedniej wentylacji. Na jednego pracującego na dole konia wymagano czterokrotnie większego zapotrzebowania powietrza, niż na jednego pracującego górnika i stanowić miało 20 m^3/min.

Witold Budryk w swej książce „Wentylacja kopalń" wydanej w 1951 roku, podaje wytyczne do obliczania ilości zapotrzebowanego powietrza w wyrobiskach podziemnych z uwzględnieniem zatrudnionych koni. Bolesław Krupiński w swych publikacjach wydanych w latach pięćdziesiątych ubiegłego wieku określa zapotrzebowanie powietrza dla konia pracującego na dole kopalni w liczbie 16 m^3/min. Również Przepisy Technicznej Eksploatacji Kopalń Węgla Kamiennego z 1951 roku, podają wymóg minimalnego zapotrzebowania powietrza w liczbie 16 m^3/min na każdego znajdującego się na dole konia.

Z kolei „Poradnik górnika Tom II" część 2 z roku 1959 w rozdziale „Przewóz ręczny i konny" przewiduje, że koń może dawać w przewozie dołowym stały wysiłek 90 kG, podczas gdy człowiek tylko 12 kG. Koń średnio w ciągu zmiany wykonuje pracę o wartości 50 tonokilometrów użytecznych. Prędkość ruchu zaprzęgu konnego w kopalni wynosi 1,2 m/sek. Koń w ciągu zmiany roboczej w przewozie dołowym pokonuje nie więcej niż 30 km.

W 1951 roku została wydana „Instrukcja dla woźniców", która określała szereg zachowań, służących bezpieczeństwu pracy koni w kopalni. Instrukcja zakładała, że koń ciągnie pociąg chodząc stępa. Pociąg składający się z 12 – 15 wozów z węglem jeden koń ciągnie z prędkością 70 – 80 metrów na minutę. Woźnica powinien pociąg konny prowadzić idąc ze światłem przed koniem. Na końcu pociągu konnego musi być zawieszona lampa z czerwonym światłem, oznaczająca sygnał końcowy. Woźnicy zabrania się jazdy na wozie z węglem. Na drogach przewozowych, z obawy uniknięcia najechania, należy zachowywać odstęp 10 m między kolejnymi konnymi pociągami. W chodnikach z transportem jednotorowym, woźnica ze swym pociągiem musi na mijance odczekać, aż minie go pociąg nadjeżdżający z przeciwnej strony. Orczyk musi być

tak zamocowany, aby nie wlókł się po spągu, co mogłoby spowodować zaczepienie o podkład szynowy i spowodować wykolejenie.

Przy spinaniu wozów, koń musiał być wyprzęgnięty. Uprzednio należało konia odprząc, a dopiero potem rozpinać wozy. Koń przypięty do wozu może szarpnąć i zmiażdżyć palce spinającemu wozy woźnicy. Wykolejone z torów wozy nie powinny być wyciągane przez konie.

Koń w kopalni powinien być prowadzony przez woźnicę zawsze z przodu, jedynie przy niektórych robotach przodkowych i rabowaniu obudowy można było stosować lejce do kierowania koniem.

W wysokich i poziomych chodnikach przewozowych dopuszczano czasem jazdę woźnicy w pierwszym wozie pustego pociągu jazdy. Koń wtedy musiał być trzymany lejcami, a światło pociągu miało być tak umieszczone, aby było widoczne dla poruszających się ludzi w wyrobisku. Tylko w takich warunkach, w wysokich chodnikach wolno było załodze jechać w wozach węglowych do przodka.

W niemieckim podręczniku „Lehrbuch der Bergbaukunde" autorstwa Hellmuta Fritzsche z 1957 roku można przeczytać: „Koń musi być ciężki, ponieważ jego siła ciągnąca zależy od jego wagi. Wymagania te najlepiej spełniają konie o wadze 500 – 700 kg i wzroście 155 – 165 cm. Wysokość w kłębie nie powinna przekraczać 165 cm".

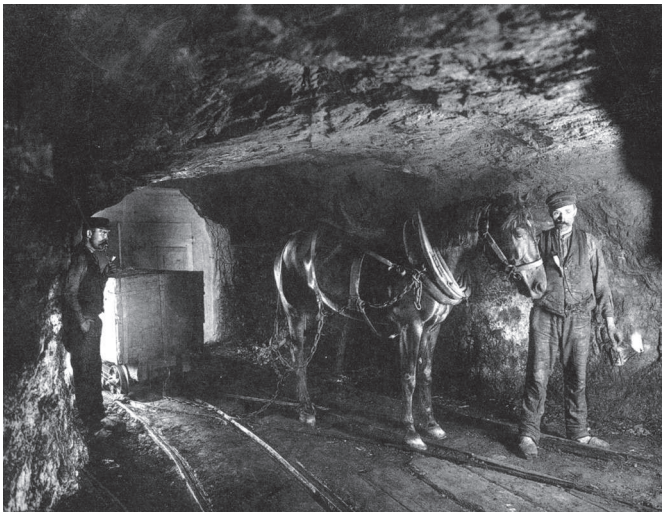
Konie karmiono mieszanką owsa, chleba paszowego, siana i ściółki. Z reguły nie stosowano zielonki, gdyż powodowała kolkę u koni. Koty wykorzystywano do zwalczania myszy, dotrzymywały one koniom towarzystwa w stajni.

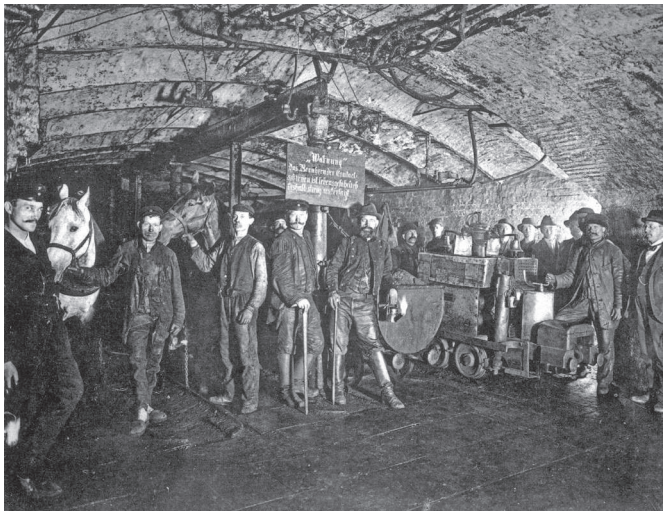
W podręczniku Stanisława Gismana „Chodniki transportowe" PWT Katowice 1950 zapisana jest przestroga: „potraktowanie biczem zmęczonego konia nic się nie wskóra, a tylko go zdenerwuje".

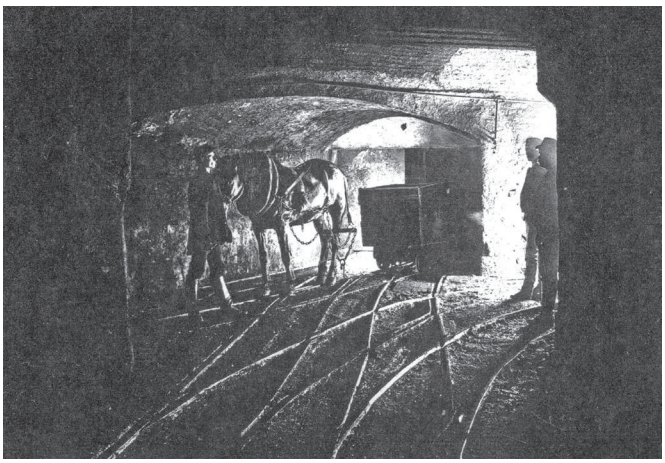
Kierat górniczy

Do wyciągania urobku z dołu kopalni oraz dla transportu wozów po pochylniach o znacznym spadzie stosowany był kierat konny. Kierat w kopalniach został opisany w XVI wieku przez Georgiusa Agricolę w książce o górnictwie „De Re Metallica libri XII" w 1556 roku.

Kierat górniczy składał się z wału pionowego lub poziomego, na którym zabudowane były dwa nawojowe bębny linowe rozdzielone tarczą hamulcową. Liny konopne nawijane były w przeciwnych kierunkach. Podczas pracy kieratu jedna lina się nawijała i wyciągała w szybie naładowany kubeł, a druga rozwijała i opuszczała pusty kubeł. Zmiana obrotu kieratu wymagała zmiany kierunku poruszania się koni. Kieraty z bębnem linowym poziomym wymagały użycia kątowej przekładni palcowo-szczebelkowej lub palcowo-gniazdowej wykonywanej z drewna dębowego. Hamulec napędu wyciągu wykonany z drewnianych szczęk dociskał specjalną tarczę







zamocowaną się na wale napędowym. Do dziś znajduje się w Wieliczce kierat zwany „Saskim", zbudowany w 1748 roku. Wysokość kieratu wynosi 7,0 m, średnica bębna linowego 2,0 m, a rozpiętość ramion, do których zaprzęgano konie 9,0 m.

Do wyciągnięcia 26 ton węgla szybem o głębokości 40 m podczas 12-godzinnej dniówki wystarczał kierat obsługiwany przez jednego konia. Kieratem dwukonnym wyciągano 44 tony węgla szybem o głębokości 36 m podczas 12-godzinnej dniówki. Napędu kieratowego zaniechano całkowicie w kopalniach z końcem XIX wieku, gdy rozwinął się napęd parowy.

W górnictwie węglowym ostatni koń oficjalnie zakończył pracę w 1960 roku w kopalni Wieczorek w Katowicach. W kopalni Brzeszcze mieli na dole konia jeszcze w 1973 roku.

Ostatni pracujący pod ziemią koń wyjechał z dołu kopalni soli w Wieliczce wiosną 2002 roku. Był to 16-letni koń, który przepracował na dole 13 lat. Po wydaniu konia na powierzchnię przeżył dwa tygodnie.

dr hab. inż. Stefan Gierlotka

Zestawienie firm
automatyka przemysłowa

Dane firmy		Profil działalności
Aparatura kontrolno-pomiarowa		
AXIS Sp. z o.o. ul. Kartuska 375 b7 80-125 Gdańsk	tel. 58 32063 80 e-mail: handel@axis.pl www.axis.pl	Szeroki wybór wag elektronicznych własnej produkcji. Nasze produkty wykorzystywane są tam, gdzie stawiane są najwyższe wymagania co do dokładności, niezawodności i odporności na czynniki środowiskowe. Oferujemy także dynamometry (siłomierze), urządzenia do pomiaru momentu siły i nowoczesne akcesoria do nich.
Automatyka przemysłowa		
COMPARTA Zajdel Sp. z o.o. ul. Marmurowa 7 05-077 Warszawa-Wesoła	e-mail: comparta@comparta.pl www.comparta.pl	Oferuje: • switche przemysłowe COMPARTA • IDEC – PLC, HMI, bezpieczeństwo • komputery przemysłowe ASEM • konwertery protokołów HILSCHER • zdalny dostęp SECOMEA – najbardziej kompletne i zaawansowane rozwiązanie umożliwia zdalny serwis, monitorowanie i zbieranie danych. Zapraszamy do sklepu internetowego COMPARTA24.PL.
Fatek Polska Sp. z o.o. ul. Siwka 11 31-588 Kraków	tel. 533 329 921 e-mail: info@fatekpolska.pl www.fatek.pl	Oferujemy kompleksową automatyzację maszyn, wsparcie w zakresie doradztwa technicznego, pomoc w doborze komponentów oraz pełne wsparcie dla naszych klientów po uruchomieniu urządzenia. Jesteśmy oficjalnym dystrybutorem sterowników PLC, paneli operatorskich HMI oraz serwonapędów firmy Fatek.
Festo Sp. z o.o. Janki k. Warszawy ul. Mszczonowska 7 05-090 Raszyn	Customer Interaction Center tel. 22 711 41 00 fax 22 711 41 02 festo_poland@festo.com www.festo.pl	Festo – lider innowacyjnych rozwiązań w dziedzinie automatyki przemysłowej i automatyzacji procesów. Oferta Festo obejmuje m.in.: siłowniki i napędy pneumatyczne oraz elektryczne, chwytaki, manipulatory i roboty przemysłowe, zawory, wyspy zaworowe, przygotowanie sprężonego powietrza, technikę podciśnieniową, czujniki, sterowniki elektroniczne, systemy magistral, technikę przyłączeniową.
Hiwin GmbH Puławska 405 A 02-801 Warszawa	tel./fax 22 544 07 07 e-mail: info@hiwin.pl www.hiwin.pl	Światowy lider w produkcji: szyn profilowych, śrub kulowych, siłowników elektrycznych, kompletnych systemów pozycjonowania, osi z silnikami liniowymi, modułów liniowych, stołów obrotowych, silników momentowych, systemów pomiaru drogi i robotów przemysłowych. Oferuje doradztwo, szkolenia i serwis.
Multiprojekt Automatyka sp. z o.o. ul. Pilotów 2 E 31-462 Kraków	tel. 12 413 90 58 fax 12 376 48 94 e-mail: krakow@multiprojekt.pl www.multiprojekt.pl	Dystrybuujemy panele operatorskie WEINTEK, serwonapędy i kontrolery ruchu TRIO, technikę liniową HIWIN, siłowniki liniowe LinMot, falowniki MICNO, coboty Neura Robotics, sterowniki PLC FATEK, przekładnie planetarne Sesame, serwowzmacniacze Copley Controls, a także silniki krokowe. Zapewniamy doradztwo techniczne, podstawowe i zaawansowane szkolenia oraz pomoc techniczną przy uruchomieniu.
Murrelektronik Sp. z o.o. al. Roździeńskiego 188 h 40-203 Katowice	tel. 32 730 00 20 fax 32 730 00 23 info@murrelektronik.pl www.murrelektronik.pl shop.murrelektronik.pl	Lider zdecentralizowanej automatyki przemysłowej dla producentów maszyn, kluczowy podmiot umożliwiający rewolucję Przemysłu 4.0. Obsługuje ponad 20 000 klientów na całym świecie. Oferuje: elektronikę w szafie sterowniczej, interfejsy, systemy I/O i technologię połączeniową. Podstawą jego sukcesu są innowacyjne produkty, wyraźna orientacja na potrzeby rynku i klienta, efektywna logistyka i troska o wysoką jakość rozwiązań.
N.B.C. Polska Sp. z o.o. ul. Złoty Potok 10/16 02-699 Warszawa	tel. 22 855 18 30 e-mail: nbc@nbc-el.pl www.nbc-el.pl	Oferujemy szeroką gamę wysokiej jakości włoskich czujników tensometrycznych, standardowych i projektowanych na zamówienie, akcesoria do czujników, torsjometry, mierniki wagowe z wieloma typami interfejsów, moduły dozujące, ograniczniki do dźwigów i suwnic z rejestratorem danych, wagi dynamometryczne.

SKAMER-ACM Sp. z o.o. ul. Rogoyskiego 26 33-100 Tarnów	tel. 14 63 23 400 e-mail: tarnow@skamer.pl www.skamer.pl	SKAMER-ACM to sprawdzony partner w pomiarach, automatyce przemysłowej i robotyce. Działalność firmy obejmuje: projektowanie systemów automatyki przemysłowej; programowanie przemysłowych systemów sterownikowych; tworzenie systemów monitoringu i wizualizacji mediów energetycznych, procesów przemysłowych i efektywności produkcji; prefabrykację szaf sterowniczych i rozdzielni; montaż, rozruch i serwis instalacji AKPiA; sprzedaż urządzeń i systemów branży AKPiA.
SMC Industrial Automation Polska Sp. z o.o. ul. Stefana Batorego 10A 05-870 Błonie	tel. 22 344 40 00 e-mail: sales@smc.pl	SMC – WIODĄCY EKSPERT Z PASJĄ do automatyki przemysłowej. Firma SMC dąży do satysfakcji klientów na całym świecie wspierając automatyzację poprzez najbardziej zaawansowane technologie. Pełna gama produktów SMC do pneumatyki i automatyzacji: • Napędy pneumatyczne • Napędy elektryczne • Zawory rozdzielające • Przygotowanie powietrza • Złącza i przewody • Elementy podciśnieniowe • Elementy do procesów technologicznych • Czujniki i przekaźniki • Neutralizacja ładunków elektrostatycznych • Regulacja i kontrola temperatury • Elementy do wysokiego podciśnienia • Rozwiązania w zakresie bezpieczeństwa • Produkty zgodne z ATEX • Produkty do czystych pomieszczeń • Produkty stosowane przy produkcji baterii.
steute Polska al. Wilanowska 321 02-665 Warszawa	tel. 22 843 08 20 e-mail: info@steute.pl www.steute.pl	Niemiecka firma steute oferuje m.in. wyłączniki linkowe bezpieczeństwa, czujniki zbiegania oraz czujniki do wykrywania uszkodzeń taśmy przenośników, wyłączniki nożne oraz podzespoły systemów bezpieczeństwa maszyn. Dostępne są również wyłączniki, czujniki i kasety sterownicze w wersji przeciwwybuchowej Ex (ATEX), radiowej oraz do pracy w ekstremalnych warunkach.
TWT Automatyka ul. Waflowa 1 02-971 Warszawa	tel./fax 22 648 20 89 e-mail: twt@twt.com.pl www.twt.com.pl	TWT to polski producent indukcyjnych czujników zbliżeniowych i czujników optycznych, obecny na rynku od 1999 r. Nasze wyroby charakteryzują się wysokim stopniem zaawansowania technicznego, dużą niezawodnością i wytrzymałością. Zapraszamy na naszą stronę www.twt.com.pl i do sklepu internetowego.
Mechatronika		
WROPOL ENGINEERING Lutynia, ul. Wróblowicka 3 55-330 Miękinia	tel. 71 317 12 18 e-mail: hydraulika@wropol.pl	Projektowanie i produkcja elementów hydrauliki siłowej oraz maszyn z napędem hydraulicznym. Siłowniki hydrauliczne do O500, multiplikatory, agregaty hydrauliczne, zawory ZO, ZZ, ZDZ, ZSZ, prasy BISON Euro, AL, BISON CNC do brykietowania trocin i wiórów AI oraz maszyny i urządzenia technologiczne.
Hiwin GmbH Puławska 405 A 02-801 Warszawa	tel./fax 22 544 07 07 e-mail: info@hiwin.pl www.hiwin.pl	Światowy lider w produkcji: szyn profilowych, śrub kulowych, siłowników elektrycznych, kompletnych systemów pozycjonowania, osi z silnikami liniowymi, modułów liniowych, stołów obrotowych, silników momentowych, systemów pomiaru drogi i robotów przemysłowych. Oferuje doradztwo, szkolenia i serwis.
Napędy		
BTT AUTOMATYKA Sp. z o.o. ul. Generała Józefa Fiszera 14 80-231 Gdańsk	tel. 58 345 49 99 tel. 58 345 44 41 e-mail: btt@bttautomatyka.pl	Naszym klientom dostarczamy kompletne napędy elektryczne maszyn i urządzeń, falowniki, zasilacze i silniki DC oraz serwonapędy napędzające maszyny i urządzenia przez nich produkowane czy używane, m.in.: wentylatory, systemy stałego ciśnienia wody, suwnice, dźwigi, obrabiarki, maszyny masarskie, cukiernicze, urządzenia w przemyśle gumowym, produkcji kabli, folii, opakowań, napędy dużej mocy w kopalniach kruszywa.
Cantoni Group ul. 3 Maja 28 43-400 Cieszyn	tel. 33 813 87 00 e-mail: motor@cantonigroup.com www.cantonigroup.com	Grupa Cantoni to największy w Polsce producent silników elektrycznych w zakresie mocy od 0,04 kW do 7000 kW oraz hamulców. Silniki elektryczne są produkowane przez firmy: Besel SA w Brzegu, Celma Indukta SA w Cieszynie i Bielsku-Białej, Emit SA w Żychlinie. Hamulce produkuje firma Ema-Elfa Sp. z o.o. w Ostrzeszowie.

ELEKTRONAPĘDY **Grzegorz Zając** ul. Kościelna 5 56-504 Dziadowa Kłoda	tel. 506 750 427 e-mail: info@elektronapedy.pl www.elektronapedy.pl	Współpracujemy od lat z kilkoma niemieckimi producentami elektrowrzecion standardowych i specjalnych do 24.000 rpm (sprzedaż, dobór, serwis: m.in. Emod, Perske). Oferujemy silniki IE5 Dyneo+ do 500 kW marki Leroy Somer (zamienniki AC i DC) wraz z montażem, serwisem oraz analizą zwrotu kosztów z inwestycji. Silniki Motive z przekładniami i sterowaniem AC IP67, nierdzewne, zanurzeniowe, DC komutatorowe.
MODUŁY-KONTROLERY ELEKTRONAPĘDY		**www.Kaiser-motoren.pl** Silniki w obudowie ze stali nierdzewnej dla branży spożywczej i farmaceutycznej  
Festo Sp. z o.o. Janki k. Warszawy ul. Mszczonowska 7 05-090 Raszyn	Customer Interaction Center tel. 22 711 41 00 fax 22 711 41 02 festo_poland@festo.com www.festo.pl	Festo – lider innowacyjnych rozwiązań w dziedzinie automatyki przemysłowej i automatyzacji procesów. Oferta Festo obejmuje m.in.: siłowniki i napędy pneumatyczne oraz elektryczne, chwytaki, manipulatory i roboty przemysłowe, zawory, wyspy zaworowe, przygotowanie sprężonego powietrza, technikę podciśnieniową, czujniki, sterowniki elektroniczne, systemy magistral, technikę przyłączeniową.
Hiwin GmbH Puławska 405 A 02-801 Warszawa	tel./fax 22 544 07 07 e-mail: info@hiwin.pl www.hiwin.pl	Światowy lider w produkcji: szyn profilowych, śrub kulowych, siłowników elektrycznych, kompletnych systemów pozycjonowania, osi z silnikami liniowymi, modułów liniowych, stołów obrotowych, silników momentowych, systemów pomiaru drogi i robotów przemysłowych. Oferuje doradztwo, szkolenia i serwis.
SMC Industrial Automation Polska Sp. z o.o. ul. Stefana Batorego 10A 05-870 Błonie	tel. 22 344 40 00 e-mail: sales@smc.pl	SMC – WIODĄCY EKSPERT Z PASJĄ do automatyki przemysłowej. Firma SMC dąży do satysfakcji klientów na całym świecie wspierając automatyzację poprzez najbardziej zaawansowane technologie. Pełna gama produktów SMC do pneumatyki i automatyzacji: • Napędy pneumatyczne • Napędy elektryczne • Zawory rozdzielające • Przygotowanie powietrza • Złącza i przewody • Elementy podciśnieniowe • Elementy do procesów technologicznych • Czujniki i przekaźniki • Neutralizacja ładunków elektrostatycznych • Regulacja i kontrola temperatury • Elementy do wysokiego podciśnienia • Rozwiązania w zakresie bezpieczeństwa • Produkty zgodne z ATEX • Produkty do czystych pomieszczeń • Produkty stosowane przy produkcji baterii.
Steinlen Polska Sp. z o.o. ul. W. Grabskiego 4/8 63-500 Ostrzeszów	tel. 62 732 23 50 fax 62 732 23 51 marketing@steinlenpolska.pl	Steinlen Polska Sp. z o.o. jest autoryzowanym przedstawicielem firmy Bauer Gear Motor GmbH. Prowadzimy sprzedaż oraz serwis motoreduktorów, silników, przekładni, hamulców i sprzęgieł.
Robotyka / Coboty		
GAZELA **Mechanika Maszyn** al. Niepodległości 801 A 81-810 Sopot	tel. 58 551 14 88 fax 58 550 16 47 info@gazela.pl www.gazela.pl	GAZELA to przedsiębiorstwo z Sopotu specjalizujące się w precyzyjnej obróbce skrawaniem, wykonawstwie bloków hydraulicznych, spawaniu, obróbce blach dla wiodących producentów maszyn. Zajmujemy się produkcją jednostkową i małoseryjną w dwóch zakładach produkcyjnych.
Hiwin GmbH Puławska 405 A 02-801 Warszawa	tel./fax 22 544 07 07 e-mail: info@hiwin.pl www.hiwin.pl	Światowy lider w produkcji: szyn profilowych, śrub kulowych, siłowników elektrycznych, kompletnych systemów pozycjonowania, osi z silnikami liniowymi, modułów liniowych, stołów obrotowych, silników momentowych, systemów pomiaru drogi i robotów przemysłowych. Oferuje doradztwo, szkolenia i serwis.
Systemy transportowe		
ABUS Crane Systems Polska sp. z o.o. ul. Gaudiego 20 44-109 Gliwice	tel. 32 334 70 00 e-mail: info@abuscranes.pl www.abuscranes.pl	ABUS Crane Systems Polska sp. z o.o. specjalizuje się w projektowaniu i produkcji systemów dźwignicowych najwyższej jakości przy zachowaniu konkurencyjności cen. Dodatkowo firma oferuje szeroką gamę akcesoriów i komponentów, doradztwo techniczne, montaż, serwis gwarancyjny i pogwarancyjny.

steute Polska al. Wilanowska 321 02-665 Warszawa	tel. 22 843 08 20 e-mail: info@steute.pl www.steute.pl	Niemiecka firma steute oferuje m.in. wyłączniki linkowe bezpieczeństwa, czujniki zbiegania oraz czujniki do wykrywania uszkodzeń taśmy przenośników, wyłączniki nożne oraz podzespoły systemów bezpieczeństwa maszyn. Dostępne są również wyłączniki, czujniki i kasety sterownicze w wersji przeciwwybuchowej Ex (ATEX), radiowej oraz do pracy w ekstremalnych warunkach.

Utrzymanie ruchu

ABUS Crane Systems Polska sp. z o.o. ul. Gaudiego 20 44-109 Gliwice	tel. 32 334 70 00 e-mail: info@abuscranes.pl www.abuscranes.pl	ABUS Crane Systems Polska sp. z o.o. specjalizuje się w projektowaniu i produkcji systemów dźwignicowych najwyższej jakości przy zachowaniu konkurencyjności cen. Dodatkowo firma oferuje szeroką gamę akcesoriów i komponentów, doradztwo techniczne, montaż, serwis gwarancyjny i pogwarancyjny.

Ad Moto Rafał Zawisz ul. Srokowiecka 5 41-106 Siemianowice Śląskie	tel. 604 580 907 e-mail: biuro@filtracjaoleju.pl www.filtracjaoleju.pl	Jesteśmy grupą profesjonalistów, którzy dzięki zdobytemu doświadczeniu są w stanie rozwiązać większość problemów związanych z gospodarką olejową. Ponad 80% awarii w urządzeniach spowodowanych jest zanieczyszczeniami występującymi w oleju. Służymy pomocą w doborze odpowiedniego sprzętu oraz usprawnieniu gospodarki olejowej u klienta.
Centrum Badań i Dozoru sp. z o.o. ul. Lędzińska 8 43-143 Lędziny	tel.+48 32 32 42 200 e-mail: cbid@cbid.pl www.cbid.pl	• Badania rzeczoznawcze maszyn i urządzeń górniczych, w tym urządzeń budowy przeciwwybuchowej • Badania zagrożeń metanowych • Pomiary i badania maszyn i urządzeń mechanicznych i elektroenergetycznych • Badania diagnostyczne • Pomiary i badania środowiska pracy • Pomiary i badania czynników środowiska naturalnego.
Hiwin GmbH Puławska 405 A 02-801 Warszawa	tel./fax 22 544 07 07 e-mail: info@hiwin.pl www.hiwin.pl	Światowy lider w produkcji: szyn profilowych, śrub kulowych, siłowników elektrycznych, kompletnych systemów pozycjonowania, osi z silnikami liniowymi, modułów liniowych, stołów obrotowych, silników momentowych, systemów pomiaru drogi i robotów przemysłowych. Oferuje doradztwo, szkolenia i serwis.
steute Polska al. Wilanowska 321 02-665 Warszawa	tel. 22 843 08 20 e-mail: info@steute.pl www.steute.pl	Niemiecka firma steute oferuje m.in. wyłączniki linkowe bezpieczeństwa, czujniki zbiegania oraz czujniki do wykrywania uszkodzeń taśmy przenośników, wyłączniki nożne oraz podzespoły systemów bezpieczeństwa maszyn. Dostępne są również wyłączniki, czujniki i kasety sterownicze w wersji przeciwwybuchowej Ex (ATEX), radiowej oraz do pracy w ekstremalnych warunkach.

BIBLIOTEKA

Andrzej Selenta
Gdy spełniają się marzenia
Droga Mieczysława G. Bekkera ze Strzyżowa na Księżyc
Wydanie: I, 2024
Wydawnictwo Naukowe PWN

Wydawnictwo Naukowe PWN ma zaszczyt polecić Państwu wyjątkową publikację popularną poświęconą wybitnemu polskiemu inżynierowi – prof. Mieczysławowi G. Bekkerowi.

Celem książki „Gdy spełniają się marzenia. Droga Mieczysława G. Bekkera ze Strzyżowa na Księżyc" jest prezentacją sylwetki i wspaniałych dokonań tego wybitnego naukowca polskiego pochodzenia. Jest to postać prawie w Polsce nieznana pomimo wybitnych osiągnięć naukowych i inżynierskich w świecie.

Jest on nazywany powszechnie ojcem terramechaniki, nauki z obszaru mechaniki stosowanej dotyczącej poruszania się pojazdów w terenie. Największym osiągnięciem prof. M. Bekkera – zwieńczeniem jego kariery naukowej – było zaprojektowanie układu jezdnego do pojazdów księżycowych LRV wykorzystanych w lotach kosmicznych Apollo 15/16/17.

Olbrzymim atutem publikacji „Gdy spełniają się marzenia. Droga Mieczysława G. Bekkera ze Strzyżowa na Księżyc" jest fakt, że w środku publikacji czytelnik znajdzie unikatowe, nieznane wcześniej ilustracje i zdjęcia pochodzące m.in. z największego archiwum dotyczącego życia i dokonań profesora M. G. Bekkera. Napisanie i wydanie książki przez Wydawnictwo Naukowe PWN związane jest z faktem uhonorowania pamięci wybitnego absolwenta Politechniki Warszawskiej profesora Mieczysława Bekkera – w 2025 r. zaplanowane są uroczystości temu poświęcone, a w tym odsłonięcie jego popiersia.

Książka „Gdy spełniają się marzenia. Droga Mieczysława G. Bekkera ze Strzyżowa na Księżyc", naszym zdaniem, wypełni lukę informacyjną, a jej lektura poprowadzi czytelnika przez mało znany świat unikalnej wiedzy i dokonań Polaka w kosmosie. W Polsce jest pierwszą obszerną książką poświęconą temu wybitnemu naukowcowi, pochodzącemu z naszego kraju. Polecamy ją wszystkim ciekawym świata i dokonań wybitnych Polaków, polskiej myśli technicznej, zainteresowanym kosmosem i srebrnym globem, a także historią wybitnych jednostek XX w.

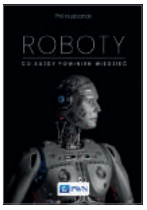
Kate Crawford
Atlas sztucznej inteligencji
Władza pieniądze i środowisko naturalne
Rok wydania: 2024
Wydawca: Bo.wiem

Sztuczna inteligencja nie jest ani inteligentna, ani sztuczna. Nieodwracalna transformacja naszego życia, jaką niesie ze sobą wynalezienie sztucznej inteligencji, staje się faktem. Czy znamy ukryte koszty tej przełomowej technologii? Czy wiemy, czyim służy interesom? I jaki ma wpływ na społeczeństwo?

Kate Crawford obala mity, jakoby sztuczna inteligencja była bezcielesna, obiektywna czy niezbędna. Udowadnia, że to narzędzie wyzysku w rękach władzy, policji, wojska i korporacji oraz podłoże narastających nierówności. Funkcjonowanie systemów AI nie byłoby możliwe bez nadmiernej eksploatacji zasobów energetycznych i mineralnych, wykorzystania taniej siły roboczej i niekontrolowanego pozyskiwania danych.

„Atlas sztucznej inteligencji" stanowi swoistą mapę teraźniejszości: miejsc, ludzi i relacji. Pomaga zrozumieć rolę AI we współczesnym świecie. Jest cenną przeciwwagą dla bezkrytycznych zachwytów nad sztuczną inteligencją oraz zaproszeniem do świadomego i odpowiedzialnego korzystania z technologii informacyjnej.

Czy wiesz, że: rekruterzy w wielkich korporacjach wykorzystują narzędzia do przechwytywania i analizy wyrazu twarzy i mowy ciała, niektóre stacje robocze w halach produkcyjnych są wyposażone w czujniki, które na bieżąco informują o temperaturze ciała pracowników i ich fizycznej odległości od innych osób, jedna z sieci restauracji zainstalowała w kuchniach systemy widzenia komputerowego sprawdzające, czy personel przygotowuje pizzę zgodnie ze standardami?



Phil Husbands
Roboty. Co każdy powinien wiedzieć
Wydanie: I, 2023
Wydawnictwo Naukowe PWN

„Toczy się cicha rewolucja. (…) Maszyny, które przejawiają właściwości przypominające żywe istoty przyciągają sporo uwagi. Nadszedł czas, by dowiedzieć się o nich czegoś więcej. W jaki sposób działają? Czy stanowią zagrożenie, czy może bezprecedensową szansę? (…) Trwają prace nad opracowaniem robotów służących do różnego rodzaju zastosowań – niekiedy korzystnych, a niekiedy martwiących. Mobilne, inteligentne roboty – będące u progu ich integracji z naszym codziennym życiem – wywołują obecnie ogromne zainteresowanie. Co już potrafią i do czego mogłyby stać się zdolne w przyszłości? Czy zmuszą nas do zmiany sposobów myślenia o technice i jej zastosowaniach? Czy zmienią w zasadniczy sposób to, jak żyjemy i jak wygląda nasza praca?

Ze wstępu autora

Phil Husbands, używając formatu pytań i odpowiedzi, przedstawia wyważone i szerokie wprowadzenie do robotyki i jej obecnego stanu, analizując, skąd się wzięła i dokąd może zajść w przyszłości. Rozpoczyna od historii robotyki i jej złożonych związków z kulturą popularną, a następnie przechodzi do omawiania technologii leżącej u podstaw robotów. Wszystko to przedstawia w angażujący i nietechniczny sposób, badając granice tego, co roboty faktycznie mogą teraz robić i co będą w stanie robić w przyszłości.

Ta wyjątkowa książka:

- szybko i przystępnie wprowadza do dziedziny robotyki,
- omawia technologię leżącą u podstaw robotyki i daje wgląd w sposób działania robotów,
- odkrywa zaskakujące początki współczesnej robotyki w rozrywce, reklamie i neurobiologii,
- obala niektóre mity dotyczące rychłego rozwoju superinteligentnych robotów, które zawładną światem,
- wyjaśnia, co naprawdę mogą robić obecne roboty, a czego nie, oraz bada problemy etyczne, które powstają w wyniku korzystania przez nas z robotów.

TEMATYKA

napędy i sterowanie
miesięcznik naukowo-techniczny
Nr 7-8 (303-304)
Rok XXVI
Lipiec – Sierpień 2024

- **SYSTEMY AUTOMATYZACJI W GÓRNICTWIE**
- **AUTOMATYZACJA TRANSPORTU SZYNOWEGO**
- Cyfryzacja w ciągu produkcyjnym
- Inteligentne układy zasilania, sterowania
- Diagnostyka
- Nowe technologie
- Silniki elektryczne
- Transformatory

Promocja pisma zgodnie z planem wydawniczym na www.nis.com.pl
Kontakt: e-mail: redakcja.nis@drukart.pl; tel. 32 755 19 17

PRENUMERATA

Prenumeratę miesięcznika „Napędy i Sterowanie” można rozpocząć w dowolnym momencie. Cena prenumeraty pozostaje bez zmian, niezależnie od zmiany stawki VAT na czasopismo. Faktura za prenumeratę zostanie przesłana wraz z pierwszym zamówionym egzemplarzem. Koszty przesyłki pokrywa Wydawnictwo. Studenci oraz uczniowie mogą skorzystać z 50-proc. zniżki, przesyłając kserokopię ważnej legitymacji szkolnej. Zniżka obejmuje również szkoły i wyższe uczelnie.

Cena prenumeraty rocznej wynosi 308,88 zł (w tym 8% VAT).

Informacje na temat prenumeraty oraz numerów archiwalnych można uzyskać pod numerem tel. 502 132 515.

Miesięcznik „Napędy i Sterowanie” można zaprenumerować, wykorzystując:

– druk zamówienia pobrany z naszej witryny internetowej, www.nis.com.pl/nis/prenumerata;
– pocztę elektroniczną, e-mail: prenumerata@drukart.pl.

lub za pośrednictwem:
– GARMOND PRESS SA, tel./fax 12 412 75 60;
– Kolporter spółka z ograniczoną odpowiedzialnością sp.k., www.kolporter.com.pl, tel. 41 367 88 88.


Organizator:
PTAK WARSAW EXPO
ufi Member
WELD TECH
MIĘDZYNARODOWE TARGI BRANŻY SPAWALNICZEJ
3-5|09|2024
ZAREJESTRUJ SIĘ
www.weldexpopoland.com
Aleja Katowicka 62, 05-830 Nadarzyn | info@warsawexpo.eu | www.warsawexpo.eu | / warsawexpo

PTAK WARSAW EXPO

ufi Member

Control & Drives Poland

BRANŻOWE TARGI Nnapędów I STEROWANIA

ZAREJESTRUJ SIĘ

21-23 STYCZNIA 2025

PATRONI TARGÓW:

CP 4.0 CENTRUM PRZEMYSŁU 4.0 Politechniki Śląskiej

EMT SYSTEMS CENTRUM SZKOLEŃ INŻYNIERSKICH Kompetencje dla Przemysłu 4.0

www.controldrivespoland.com

PTAK WARSAW EXPO | AL. KATOWICKA 62, 05-830 NADARZYN