Marek Dźwiarek
CIOP-PIB, Warszawa

CYBER BEZPIECZEŃSTWO MASZYN W PRZEMYŚLE 4.0

CYBER SECURITY OF MACHINERY IN INDUSTRY 4.0

Streszczenie: Problem bezpieczeństwa w systemach produkcyjnych Przemysłu 4.0 ma charakter wielowymiarowy. Nowe technologie generują nowe rodzaje zagrożeń, ale jednocześnie umożliwiają budowę bardziej efektywnych systemów bezpieczeństwa. W nowoczesnych maszynach coraz większa rolę w zapewnianiu bezpieczeństwa ich operatorów odgrywają systemy sterowania. Ubocznym tego skutkiem jest pojawienie się nowych zagrożeń związanych z nieuprawnionymi ingerencjami w systemy informatyczne. Projektując takie systemy, należy pamiętać o możliwości wystąpienia defektów i uszkodzeń, które mogą spowodować powstanie zagrożeń dla operatorów maszyn. Oznacza to, że przy ocenie ryzyka należy uwzględnić także możliwość niekorzystnego oddziaływania potencjalnych ataków na integralność systemów sterowania realizujących funkcje bezpieczeństwa. Pierwszym dokumentem normalizacyjnym w którym omówiono aspekty bezpieczeństwa maszyn, na które mogą mieć wpływ ataki na bezpieczeństwo informatyczne związane z bezpośrednim lub zdalnym dostępem do systemów sterowania związanych z bezpieczeństwem i manipulowaniem nimi przez osoby w celu zamierzonego nadużycia jest przewodnik ISO/TR 22100-4:2018. Problem ochrony danych w komputerowych systemach sterowania maszynami aktualnie jest całkowicie pomijany przez ich projektantów ze względu na brak przystępnej metodyki oceny ryzyka w tym aspekcie. Opracowanie takiej metodyki znacząco usprawni proces projektowania zabezpieczeń odpowiednich do poziomu ryzyka. W artykule omówione główne zagadnienia, które wziąć pod uwagę przy uwzględnieniu oceny ryzyka cyber atakiem w procesie oceny ryzyka związanego z obsługą maszyn.

Abstract: The problem of safety in production systems of Industry 4.0 is multidimensional. New technologies generate new types of hazards, but at the same time make it possible to build more effective safety systems. In modern machines, control systems play an increasingly important role in ensuring the safety of operators. A side effect of this is the occurrence of new hazards related to unauthorized access to information systems. When designing such systems, one must take into account the possibility of faults and failures that may cause hazards for machine operators. This means that the risk assessment must also take into account the possibility of adverse effects of potential attacks on the integrity of control systems performing safety functions. The first standardization document that discusses aspects of machine safety that can be affected by IT security attacks related to direct or remote access to and manipulation of safety-related control systems by individuals for intentional misuse is ISO/TR 22100-4:2018. The problem of data protection in computer-based machine control systems is currently completely neglected by their designers due to the lack of an accessible risk assessment methodology for this aspect. The development of such a methodology will significantly improve the process of designing protections appropriate to the level of risk. The article discusses the main issues that should be taken into account considering the risk of cyber attack in the process of evaluating the risks associated with operating machinery.

Słowa kluczowe: *bezpieczeństwo maszyn, cyber bezpieczeństwo, bezpieczeństwo funkcjonalne*
Keywords: *safety of machinery, cybersecurity, functional safety*

1. Wstęp

Koncepcja Przemysłu 4.0 to nowa rzeczywistość współczesnej gospodarki, gdyż postępy w transformacji cyfrowej i rosnące wzajemne połączenia stanowią nowe wyzwania dla wielu organizacji [1]. Została początkowo zaproponowana w Niemczech w 2011 r. [2]. Jego cechy charakterystyczne to wykorzystanie systemów cyber-fizycznych (CPS), opartych na heterogenicznej integracji danych i wiedzy. Najistotniejsze komponenty Przemysłu 4.0, odróżniające od nadal jeszcze powszechnych zautomatyzowanych systemów produkcyjnych (3 rewolucja przemysłowa w lata 1980 – 1985) to [3]:

- systemy cyber-fizyczne,
- Internet Rzeczy,
- Internet Usług, i
- inteligentna fabryka.

Przemysł 4.0 obiecuje wzrost wydajności poprzez integrację cyfrowych systemów produkcji

z analizą i komunikacją wszystkich danych generowanych w inteligentnym środowisku. Komunikacja w czasie rzeczywistym, duże zbiory danych, współpraca człowiek-maszyna, teledetekcja, monitoring i sterowanie procesem, autonomiczne urządzenia i połączenia międzysystemowe stają się głównymi atutami nowoczesnego przemysłu. Jako że czwarta rewolucja przemysłowa, czyli Przemysł 4.0 staje się dominującą rzeczywistością, przyniesie nowe zmiany paradygmatu, które będą miały wpływ na zarządzanie bezpieczeństwem i higieną pracy (BHP).

Przemysł zaczyna wykorzystywać pozytywny wpływ na zdolność reagowania, autonomię i elastyczność zakładów produkcyjnych. Jednak żadna modyfikacja przemysłowego systemu produkcji nie powinna być rozważana bez szczegółowego omówienia potencjalnych skutków dla zdrowia i bezpieczeństwo pracowników. Przedsiębiorstwa, które wdrażają inteligentne fabryki, dążą do ograniczenia ryzyka związanego z planowaniem, określenia skutków, jakie nowa instalacja będzie miała dla pracowników, uniknięcia konieczności przeprojektowania sprzętu, zoptymalizowania wykorzystania zasobów, wyeliminowania marnotrawstwa oraz zwiększenia wydajności i elastyczności. Analizy te nie muszą oznaczać korzyści w zakresie w BHP, zwłaszcza w przypadku radykalnej zmiany organizacji pracy [4]. Zaawansowane procesy produkcyjne mogą generować nowe zagrożenia w zakresie BHP, ale konwencjonalne narzędzia analizy ryzyka zawodowego wydają się niezdolne do identyfikacji tych pojawiających się zagrożeń. W [5] Javed i in. stwierdzają, że w celu wykazania dopuszczalnego bezpieczeństwa operacji produkcyjnych, kwestie bezpieczeństwa są rozważane tak, aby zapewnić kompleksowe, logiczne i dające się obronić uzasadnienie bezpieczeństwa systemu produkcyjnego dla danego zastosowania w uprzednio zdefiniowanym środowisku pracy. Kaivo-Oja i in. [6] badali wpływ IoS, Big data i innych kluczowych fal technologicznych czwartej rewolucji (robotyka, sztuczna inteligencja, itp.) na praktyki zarządzania w organizacjach. Autorzy traktują te czynniki technologiczne jako sposób na wzmocnienie produkcji, ale zalecają nowe podejścia do analizy organizacyjnej w celu skuteczniejszego dostosowania swoich praktyk zarządczych, łącznie z tymi związanymi z bezpieczeństwem i higieną pracy. Ostatnio rozwój inteligentnych czujników, IoT, CPS i postępy w informatyce doprowadziły do licznych prób ich zastosowań do BHP. Podgórski i in. [7] ujawnia szeroką gamę środków ochrony osobistej, które wykorzystują te technologie. Dźwiarek w [8, 9, 10] przedstawił zastosowania systemów lokalizacji w różnych obszarach BHP.

Widzimy więc, że problem bezpieczeństwa w systemach produkcyjnych Przemysłu 4.0 ma charakter wielowymiarowy. Z jednej strony nowe technologie generują nowe rodzaje zagrożeń, ale jednocześnie umożliwiają budowę bardziej efektywnych systemów bezpieczeństwa. Prace w tym zakresie prowadzone są w wielu ośrodkach na świecie, ale wszyscy podkreślają ze są one jeszcze w fazie początkowej.

2. Bezpieczeństwo funkcjonalne systemów sterowania maszynami

W nowoczesnych maszynach coraz większa rolę w zapewnianiu bezpieczeństwa ich operatorów odgrywają systemy sterowania. Projektując takie układy, należy jednak pamiętać o możliwości wystąpienia defektów i uszkodzeń, które mogą spowodować powstanie zagrożeń dla operatorów maszyn. W [11] przedstawiono wyniki analizy wypadków spowodowanych nieprawidłowym działaniem systemów sterowania maszynami. W grupie wypadków spowodowanych niewłaściwym funkcjonowaniem systemu sterowania znacznie częściej występowały wypadki ciężkie (41%) niż wśród wypadków niezwiązanych z systemem sterowania (7%). Wskazuje to, jak istotne są kwestie związane z systemami sterowania maszyn. Następnie wypadki przeanalizowane zostały pod kątem ich przyczyn. Najczęstszą przyczyną był brak funkcji bezpieczeństwa (58%), takich jak kontrola położenia osłony lub nadzorowanie obecności w strefie niebezpiecznej. Kolejną grupę stanowiły wypadki spowodowane uszkodzeniem elementu systemu sterowania związanego z bezpieczeństwem w wyniku niewystarczającej odporności systemu na defekty. Stanowiły one 26% wszystkich wypadków. Pozostałe przyczyny, a więc błędy w definicji funkcji bezpieczeństwa (4%), błędy w oprogramowaniu systemu sterowania (6%) i brak wystarczającej odporności na oddziaływanie środowiska (klimatyczne, zaburzenia w zasilaniu w energię 6%) stanowiły znacznie mniejszy procent wszystkich wypadków. Tak więc jednym z istotnych problemów występujących przy wykorzystywaniu nowoczesnych syste-

mów sterowania maszynami jest zapewnienie pewności realizacji funkcji bezpieczeństwa przez te systemy. Ponieważ niezadziałanie tych funkcji może podnieść poziom ryzyka, projektanci związanych z bezpieczeństwem układów sterowania powinni stosować rozwiązania, które zwiększają ich odporność na uszkodzenia. Z jednej strony odporność na uszkodzenia danego układu sterowania może być podniesiona poprzez obniżenie prawdopodobieństwa pojawienia się uszkodzenia, a z drugiej strony poprzez podjęcie środków mających na celu zapewnienie, że uszkodzenie, które może się pojawić nie będzie niebezpieczne. Taką poprawę możemy osiągnąć poprzez:

- zastosowanie niezawodnych "wypróbowanych" elementów oraz „wypróbowanych" zasad bezpieczeństwa,
- rozszerzenie struktury układu – na etapie projektowania bierze się pod uwagę dodatkowe podzespoły, które mają na celu wykrywanie uszkodzeń; najczęściej są to redundancje obwodów monitorujących pracę.

Podstawowe zasady poprawy odporności układu sterowania maszyny na uszkodzenia zostały podane w następujących normach PN-EN 62061:2008 [12] i PN-EN 138491-1:2008 [13]. W normie PN-EN 62061:2008 dla każdego związanego z bezpieczeństwem układu sterowania realizującego daną funkcję bezpieczeństwa podano probabilistyczne kryteria oceny ich odporności na uszkodzenia (nazwane Poziom Nienaruszalności Bezpieczeństwa SIL). W normie ISO 13849-1 sformułowano uproszczona metodę oceny układów sterowania maszyn. Następujące parametry charakteryzują każdy układ: struktura (kategoria), średni czas pracy do uszkodzenia (MTTF), pokrycie diagnostyczne (DC), współczynnik uszkodzeń o wspólnej przyczynie (CCF). Oczekiwany poziom zapewnienia bezpieczeństwa wyznacza się ze schematu, do którego wprowadzono szacunkowe parametry oraz strukturę układu. Pozwala to na ocenę projektowanego układu w stosunkowo prosty sposób. Poziom zapewnienia bezpieczeństwa (PL) odzwierciedla odporność układu na uszkodzenia.

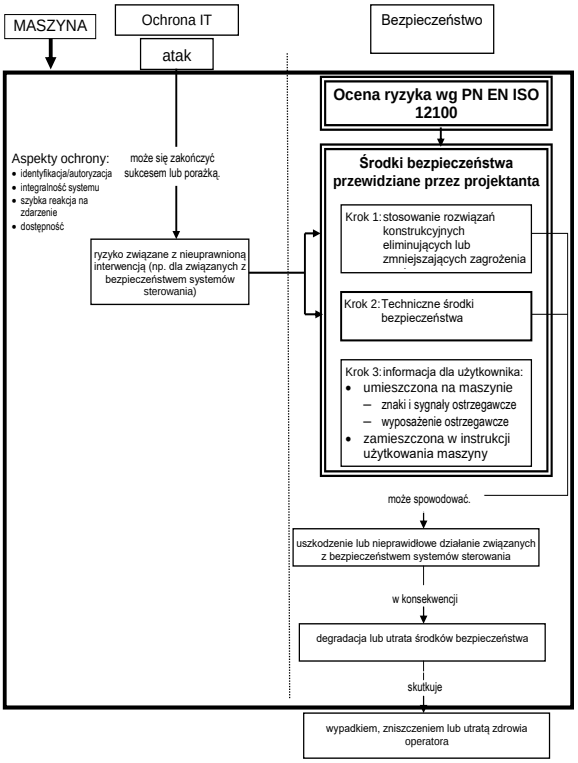
Wdrożenie w Przemyśle 4.0 systemów wytwórczych wykorzystujących Internet Rzeczy umożliwiło znaczące uelastycznienie produkcji z ukierunkowaniem na potrzeby odbiorców. Jednocześnie ubocznym tego skutkiem było pojawienie się nowych zagrożeń związanych z nieuprawnionymi ingerencjami w systemy informatyczne. Jest to szczególnie istotne w przypadku infrastruktury krytycznej, gdzie nieuprawniona ingerencja może prowadzić nawet do katastrofy przemysłowej o znaczących skutkach dla ludzi i środowiska. Dlatego też w przypadku infrastruktury krytycznej prace dotyczące zabezpieczeń przed nieuprawnioną ingerencją prowadzone są od wielu lat [14, 15]. Wraz z rozwojem przemysłowego Internetu Rzeczy Problem aspekt ten nabrał także znaczenia w przypadku systemów sterowania maszynami. Według raportu [16] w 2017 roku około 2% przemysłowych systemów sterowania podlegało próbom nieuprawnionej ingerencji.

3. Ocena ryzyka związanego z zagrożeniami powstającymi przy obsłudze maszyn w wyniku nieuprawnionej ingerencji w system sterowania

Jak wykazano wyżej, inteligentna produkcja zwiększa podatność maszyn na zagrożenia bezpieczeństwa informatycznego. Pierwszym dokumentem normalizacyjnym w którym omówiono aspekty bezpieczeństwa maszyn, na które mogą mieć wpływ ataki na bezpieczeństwo informatyczne związane z bezpośrednim lub zdalnym dostępem do systemów sterowania związanych z bezpieczeństwem i manipulowaniem nimi przez osoby w celu zamierzonego nadużycia jest przewodnik [17]. Stwierdza on, że ataki na bezpieczeństwo informatyczne coraz częściej stanowią zagrożenie dla bezpieczeństwa maszyn. Chociaż celowe nadużycia nie wchodzą w zakres normy ISO 12100 [18] i procesu oceny ryzyka, uzasadnione jest, aby również producenci maszyn brali pod uwagę takie zagrożenia.

Obecne technologie umożliwiają dostawcom maszyn zdalne monitorowanie i poprawę parametrów maszyn poprzez regulację parametrów bez konieczności przebywania w miejscu pracy maszyny. Możliwość ta zapewnia znaczne korzyści, ponieważ maszyny mogą działać bez przestojów i kosztów związanych z wezwaniem serwisu przez pracownika terenowego. Jednakże ta sama możliwość regulacji parametrów maszyny w celu poprawy jej wydajności stwarza możliwość dokonywania regulacji przez osoby o złych zamiarach lub mające zamiar popełnienia przestępstwa, co może narazić pracowników i inne osoby na niebezpieczeństwo. Na przykład, prędkość lub siła mogą zostać regulowane do niebezpiecznego poziomu, temperatura może zostać obniżona poniżej poziomu

"kill step", co spowoduje skażenie żywności, a kody błędów lub komunikaty mogą zostać usunięte lub sfałszowane. Potencjalny wpływ cyber ataków na bezpieczeństwo maszyny pokazany jest na rys. 1.



Rys. 1. Wpływ cyber bezpieczeństwa na bezpieczeństwo maszyn

Wynika z niego, że przy ocenie ryzyka związanego z obsługą maszyn należy uwzględnić także możliwość niekorzystnego oddziaływania potencjalnych ataków na integralność systemu informatycznego maszyny, a zwłaszcza systemów sterowania realizujących funkcje bezpieczeństwa. Oznacza to, że przy stosowaniu rozwiązań konstrukcyjnych eliminujących lub zmniejszających zagrożenie oraz na etapie doboru technicznych środków bezpieczeństwa należy przeprowadzić analizę ewentualnych słabych punktów w odniesieniu do ataków (zagrożeń) związanych z bezpieczeństwem informatycznym. Analiza ta powinna dać odpowiedź na pytania:

1) Czy system sterowania musi mieć możliwość połączenia z zewnętrzną siecią informatyczną?
2) Czy musi być połączony przez stale (w sposób ciągły)?
3) Czy połączenie jest monitorowane (np. za pomocą systemu wirtualnej sieci prywatnej (VPN))?
4) Czy połączenie jest konfigurowalne (np. dostęp tylko dla osób uprawnionych)?
5) Czy połączenie może być ograniczone do trybu "tylko do odczytu" (bez możliwości zmiany)?

Wzajemną korelację zasad bezpieczeństwa maszyn i ochrony systemów informatycznych pokazano w tab. 1. Jak widzimy aspekty cyber bezpieczeństwa istotnie się różnią od kwestii bezpieczeństwa maszyn. Najistotniejsze jest, że zagrożenia bezpieczeństwa informatycznego i podatności na nie wymagają współpracy i koordynacji pomiędzy dostawcami komponentów, producentem maszyn, integratorem systemów i użytkownikiem maszyn. Każdy z nich ma do odegrania rolę w zapobieganiu atakom związanym z bezpieczeństwem informatycznym na wszystkich etapach cyklu życia maszyny. Żadna ze stron nie może przypisać sobie, ani zakładać, że inna strona jest w pełni odpowiedzialna za bezpieczeństwo IT. Jednocześnie żadna ze stron nie posiada wszystkich wymaga-

Tabela 1. Wzajemna korelacja zasad bezpieczeństwa maszyn i ochrony IT

	Bezpieczeństwo maszyn	Ochrona IT (cyber bezpieczeństwo)
Cel	zapobieganie urazom, wypadkom, chorobom (unikanie szkód)	dostępność, integralność, poufność
Warunki (ryzyko, metody, środki)	przejrzyste (nie poufne)	poufne (nie udostępniane użytkownikowi maszyny)
Dynamika	raczej statyczne (zamierzone użycie, racjonalnie przewidywalne niewłaściwe użycie)	bardzo dynamiczne; ruchomy cel (celowa manipulacja, zamiar popełnienia przestępstwa)
Środki redukcji (ograniczenia ryzyka)	głównie przez producenta maszyny (przy dostarczaniu maszyny do pierwszego użycia)	przez różne podmioty (producent maszyny, integrator systemu, użytkownik maszyny, dostawca usług) w każdym momencie całego cyklu życia

nych informacji, aby skutecznie przeciwdziałać zagrożeniom i podatnościom w zakresie bezpieczeństwa IT na wszystkich etapach cyklu życia maszyny.

6. Podsumowanie

Systemy automatyki przemysłowej mogą być narażone na ataki bezpieczeństwa ze względu na to, że:

- możliwy jest dostęp do systemu sterowania, np. przeprogramowanie funkcji maszyn (w tym funkcji bezpieczeństwa);

- wzrasta "konwergencja" pomiędzy standardowymi systemami informatycznymi i przemysłowymi;

- systemy operacyjne stały się obecne w systemach wbudowanych, np. protokoły oparte na IP zastępują własnościowe protokoły sieciowe, a dane są wymieniane bezpośrednio z sieci SCADA do świata biurowego;

- zdalny dostęp od dostawców stał się standardowym sposobem obsługi i konserwacji, z podwyższonym ryzykiem cyber bezpieczeństwa dotyczącym np. nieautoryzowanego wejścia, dostępności i integralności.

- oprogramowanie jest tworzone poprzez ponowne wykorzystanie istniejących komponentów oprogramowania innych firm;

Związane z bezpieczeństwem systemy sterowania maszynami, jako część systemu automatyki przemysłowej, mogą być również narażone na ataki, które mogą skutkować utratą zdolności do utrzymania bezpiecznej eksploatacji maszyny.

Cele bezpieczeństwa funkcjonalnego uwzględniają ryzyko poprzez oszacowanie ciężkości szkody i prawdopodobieństwa jej wystąpienia: Skutki każdego zdarzenia niebezpiecznego określają wymagania dotyczące integralności bezpieczeństwa (poziom nienaruszalności bezpieczeństwa (SIL) zgodnie z IEC 62061 lub poziom zapewnienia bezpieczeństwa (PL) zgodnie z ISO 13849-1). W odniesieniu do funkcji bezpieczeństwa, zagrożenia bezpieczeństwa (wewnętrzne lub zewnętrzne) mogą mieć wpływ na integralność bezpieczeństwa i ogólną dostępność systemu.

Problem ochrony danych w komputerowych systemach sterowania maszynami aktualnie jest obecnie całkowicie pomijany przez ich projektantów ze względu na brak przystępnej metodyki oceny ryzyka w tym aspekcie. Opracowanie takiej metodyki znacząco usprawni proces projektowania zabezpieczeń odpowiednich do poziomu ryzyka. Maszyny wyposażone w systemy sterowania odpowiednio chronione przed cyberatakami będą bardziej konkurencyjne w stosunku do maszyn, dla których problem cyber bezpieczeństwa nie został uwzględniony w ocenie ryzyka.

Postęp w rozwoju informatycznych systemów sterowania powoduje, że dyrektywa 2006/42/WE w sprawie maszyn nie obejmuje w wystarczającym stopniu nowych rodzajów ryzyka wynikających z pojawiających się technologii. Można tutaj wyróżnić kilka aspektów tego problemu. Pierwszy dotyczy potencjalnych czynników ryzyka wynikających z bezpośredniej współpracy ludzi i robotów w miarę coraz bliższej współpracy między robotami współpracującymi (cobotami). Drugim źródłem potencjalnego ryzyka są maszyny podłączone do internetu. Trzeci obszar budzący obawy jest związany ze sposobem, w jaki aktualizacje oprogramowania komputerowego wpływają na „zachowanie" maszyn po ich wprowadzeniu do obrotu. Czwarta wątpliwość polega na zdolności producentów do przeprowadzenia pełnej oceny ryzyka związanego z zastosowaniami uczenia się maszyn przed wprowadzeniem produktu do obrotu (sztuczna inteligencja AI). Ponadto, jeżeli chodzi o maszyny autonomiczne i stacje nadzoru na odległość, w obecnej dyrektywie w sprawie maszyn przewidziano kierowcę lub operatora odpowiedzialnego za przemieszczanie się maszyny. Kierowca może być transportowany przez maszynę, towarzyszyć jej albo kierować nią zdalnie, jednak możliwość braku kierowcy nie jest brana pod uwagę, ani nie ma żadnych wymagań dotyczących maszyn autonomicznych.

Kolejny problem polega na tym, że aktualny wykaz maszyn wysokiego ryzyka zamieszczony w załączniku IV do dyrektywy 2006/42/WE opracowano 15 lat temu, a od tego czasu rynek bardzo się zmienił. Należało usunąć z niego maszyny, które nie są już uważane za charakteryzujące się wysokim ryzykiem, lub dopisać nowe (np. maszyny wykorzystujące systemy AI realizujące funkcje bezpieczeństwa).

Wszystkie te aspekty spowodowały, że Komisja Europejska podjęła prace nad opracowaniem rozporządzenia, które uwzględni wszystkie te aspekty i zastąpi dyrektywę 2006/42/WE. Prace

nad tym rozporządzeniem znajdują się w fazie końcowej.

7. Literatura

[1]. B. Ślusarczyk "Industry 4.0 – are we ready?". *Polish Journal of Management Studies*. 17, 3 (2018): s. 232 – 248.
[2]. B. Vogel-Heuser, D. Hess "Guest editorial Industry 4.0–prerequisites and vi- sions". *IEEE Trans. Autom. Sci. Eng*. 13 (2) (2016): s. 411–413.
[3]. M. Hermann, T. Pentek, B. Otto "Design principles for Industrie 4.0 scenarios, A Literature Review". *49th Hawaii International Conference on System Sciences (HICSS): IEEE*, (2016), s. 3928–3937.
[4]. M. Reuter, H. Oberc, at. all. "Learning factories 'Trainings as an Enabler of Proactive Workers' Participation Regarding Industrie 4.0". *Procedia Manuf.* 9 (2017): s. 354–360.
[5]. M. Javed, F. Muram, H. Hansson, S. Punnekkat "Towards dynamic safety assurance for Industry 4.0". *Journal of Systems Architecture* 114 (2021). DOI: https://doi.org/10.1016/j.sysarc.2020.101914.
[6]. J. Kaivo-Oja, P. Virtanen, H. Jalonen, J. Stenvall "The effects of the internet of things and big data to organizations and their knowledge management practices". *Lect. Notes Business Inform. Process*. 224 (2015): s. 495–513.
[7]. D. Podgórski, K. Majchrzycka, A. Dąbrowska, G. Gralewicz, M. Okrasa "Towards a conceptual framework of OSH risk management in smart working environments based on smart PPE, ambient intelligence and the Internet of Things technologies". *Int. J. Occup. Safe. Ergon*. 23, 1 (2017): s. 1–20.
[8]. M. Dźwiarek "Real Time Location Systems for monitoring safety of the machine operators". *Safety of Industrial Automated Systems 2015*. 18-20.11. 2015, Königswinter, Niemcy. ISBN 987-3-86423-163-6. s. 153 – 156.
[9]. M. Dźwiarek, T. Strawiński, T. Łempiński, M. Światowski, „The simulation of the use of personal protective equipment in investigation of Smart ID Card system efficiency", *Journal of KONBIN*. 43 (2017): s. 163 – 178.
[10]. M. Dźwiarek, T. Łempiński, M. Światowski "Effectiveness investigation of the correlation algorithms applied in a Smart ID Card system to monitor the use of PPE". in: *Safety and Reliability – Safe Societies in a Changing World*. Stein Haugen at. all (eds.) © Taylor & Francis Group, London, ISBN 978-1-351-17466-4, (2018): s.1965 – 1971.
[11]. M.Dźwiarek "An analysis of Accident Caused by Improper Functioning of Machine Control Systems". *International Journal of Occupational Safety and Ergonomics* vol. 10, no. 2, 2004 (129–136).
[12]. PN-EN 62061:2008 "Bezpieczeństwo maszyn. Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem".
[13]. PN-EN 138491-1:2008 "Bezpieczeństwo maszyn - Elementy systemów sterowania związane z bezpieczeństwem - Część 1: Ogólne zasady projektowania".
[14]. Y. Ota, at all. „Cyber incident exercise for safety protection in critical infrastructure". *Int. J. of Safety and Security Eng*., Vol. 8, No. 2 (2018) 246–257.
[15]. Barnert, T., Kosmowski, K.T. Śliwiński, M. Integrated functional safety and security analysis of the process control and protection systems with regard to uncertainty issue. *10th International Conference on Probabilistic Safety Assessment and Management 2010, PSAM 2010*; Seattle, WA; United States; June 2010.
[16]. "Threat Landscape for Industrial Automation Systems in H2 2017". Raport Kaspersky Lab ICS CERT.
[17]. ISO/TR 22100-4:2018 "Safety of machinery - Relationship with ISO 12100 - Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects".
[18]. PN – EN ISO 1200:2012 „Bezpieczeństwo maszyn - Ogólne zasady projektowania - Ocena ryzyka i zmniejszanie ryzyka". (ISO 12100:2010)

Autor

M. Dźwiarek, tel. 22 623 46 35, e-mail: madzw@ciop.pl
Centralny Instytut Ochrony Pracy – Państwowy instytut Badawczy. ul. Czerniakowska 16, 00-701 Warszawa.

Informacje dodatkowe

Publikacja opracowana na podstawie wyników V etapu programu wieloletniego „Poprawa bezpieczeństwa i warunków pracy", finansowanego w latach 2020-2022 w zakresie badań naukowych i prac rozwojowych ze środków Narodowego Centrum Badań i Rozwoju (projekt nr IIPB18 pt. Metoda analizy ryzyka prowadzonej przez projektantów maszyn z uwzględnieniem aspektów cyberbezpieczeństwa).

Koordynator programu: Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy