Bezpieczeństwo maszyn. **Od Dyrektywy maszynowej do Rozporządzenia 2023/1230 poprzez cyfrową weryfikację**

Mariusz Jabłoński

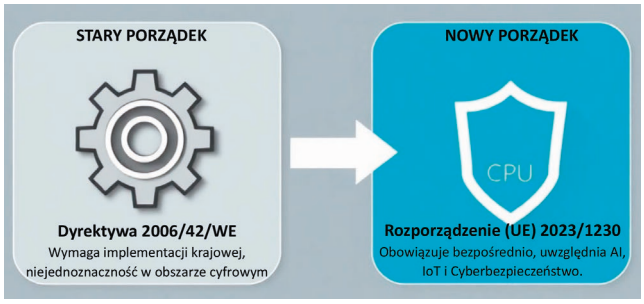
W Europie bezpieczeństwo maszyn przemysłowych opiera się na tzw. „podejściu nowym", które dzieli wymagania pod względem wymagań prawnych (dyrektywy/rozporządzenia) oraz specyfikacje techniczne (normy). Obecnie znajdujemy się w kluczowym okresie przejściowym między dotychczasową dyrektywą a nowym rozporządzeniem UE. Używane pojęcie „Nowe podejście" w Europie ma dwa wymiary: historyczno-prawny oraz technologiczny, związany z najnowszą reformą przepisów. Zasady te określają „wymagania zasadnicze", które musi spełnić każda maszyna wprowadzana na rynek. W artykule ograniczymy się głównie do analizy przepisów prawnych:

- Dyrektywa Maszynowa 2006/42/WE: Obecnie obowiązujący akt prawny. Dotyczy projektowania, budowy oraz wprowadzania maszyn do obrotu.
- Rozporządzenie Maszynowe (UE) 2023/1230: Nowy akt prawny, który zastąpi dyrektywę 20 stycznia 2027 roku. W przeciwieństwie do dyrektywy, rozporządzenie obowiązuje bezpośrednio (bez konieczności wdrażania do polskiego prawa przez ustawy). Wprowadza nowe wymogi dotyczące cyberbezpieczeństwa, sztucznej inteligencji (AI) oraz maszyn autonomicznych. Definiuje tzw. istotną modyfikację, czyli modernizację maszyny, która wymaga ponownej oceny zgodności.

1. Model legislacyjny – „Nowe Podejście" z 1985 r.

W sensie prawnym termin ten odnosi się do metody tworzenia przepisów UE, która polega na tym, że:

- Dyrektywy (przepisy prawa) określają jedynie zasadnicze wymagania dotyczące bezpieczeństwa i ochrony zdrowia (np. „w celu zapewnienia, że maszyna jest bezpieczna, powinny być spełnione zasadnicze wymagania w zakresie ochrony zdrowia i bezpieczeństwa") [1].



Rys. 1. Przejście z Dyrektywy na Rozporządzenie to krok w stronę ujednolicenia standardów bezpieczeństwa cyfrowego w całej Unii Europejskiej [12]

- Normy zharmonizowane (techniczne szczegóły, np. „jak konkretnie zbudować osłonę") są opcjonalne, ale ich zastosowanie daje tzw. domniemanie zgodności z prawem.
- Daje to producentom elastyczność – mogą stosować nowatorskie rozwiązania techniczne, o ile udowodnią, że spełniają one ogólne wymogi bezpieczeństwa.

2. Transformacja z Dyrektywy maszynowej na Rozporządzenie

Przez niemal dwie dekady fundamentem bezpieczeństwa w europejskim przemyśle była Dyrektywa Maszynowa 2006/42/WE. Jednak postępująca cyfryzacja, rozwój Internetu Rzeczy (IoT) oraz Sztucznej Inteligencji sprawiły, że ramy te stały się niewystarczające. Warto zaznaczyć, że nie została jednoznacznie określona procedura modernizacji maszyn i nie ma w aktualnych przepisach definicji: modernizacji, modyfikacji, zmian wprowadzanych na maszynach oraz jednoznacznych kryteriów kwalifikacji tych zmian [2].

Tabela 1. Porównanie kluczowych aspektów [12]

Cecha	Dyrektywa 2006/42/WE	Rozporządzenie 2023/1230
Definicja istotnej zmiany	Brak (tylko wytyczne)	Jest (prawnie wiążąca)
Zmiany w oprogramowaniu	Pomijane milczeniem	Wprost uwzględnione
Cyberbezpieczeństwo	Brak wymogów	Obowiązkowe przy modernizacji
Kto jest producentem?	Często niejasne	Każdy, kto dokona „istotnej modyfikacji"

Tabela 2. Porównanie ewolucji podejść do bezpieczeństwa maszyn [12]

Cecha	Dotychczasowa Dyrektywa (2006/42/WE)	Nowe Rozporządzenie (2023/1230)
Status prawny	Wymaga wdrożenia do prawa krajowego	Obowiązuje bezpośrednio (jednolicie)
Główny fokus	Bezpieczeństwo mechaniczne/fizyczne	Bezpieczeństwo fizyczne + cyfrowe
Nowoczesne technologie	Brak jasnych reguł dla AI/IoT	Pełna integracja z wymogami AI i cyber
Instrukcje	Zasadniczo papierowe	Preferowane cyfrowe

Odpowiedzią jest Rozporządzenie 2023/1230 z dnia 14 czerwca 2023 r. Kluczową różnicą jest zmiana formy prawnej – rozporządzenie nie wymaga implementacji do prawa krajowego, co eliminuje różnice w interpretacji między państwami członkowskimi. Nowe podejście kładzie szczególny nacisk na cyberbezpieczeństwo systemów sterowania, bezpieczeństwo maszyn autonomicznych i mobilnych oraz po raz pierwszy wprowadza definicję „istotnej modyfikacji". Podaje również kryteria na podstawie których będzie można przeprowadzić kwalifikację wprowadzanych zmian, a dzięki temu umożliwi podjęcie decyzji, czy modyfikacja była istotna czy nie [2]. Przejście z Dyrektywy 2006/42/WE na Rozporządzenie (UE) 2023/1230 odbędzie się 20 stycznia 2027 r. – data pełnego obowiązywania [3].

3. Obecna zmiana – Rozporządzenie Maszynowe 2023/1230

Obecnie termin „nowe podejście" często odnosi się do zastąpienia dotychczasowej Dyrektywy Maszynowej 2006/42/WE przez Rozporządzenie (UE) 2023/1230, które zacznie w pełni obowiązywać w 2027 roku [2]. Kluczowe zmiany to:

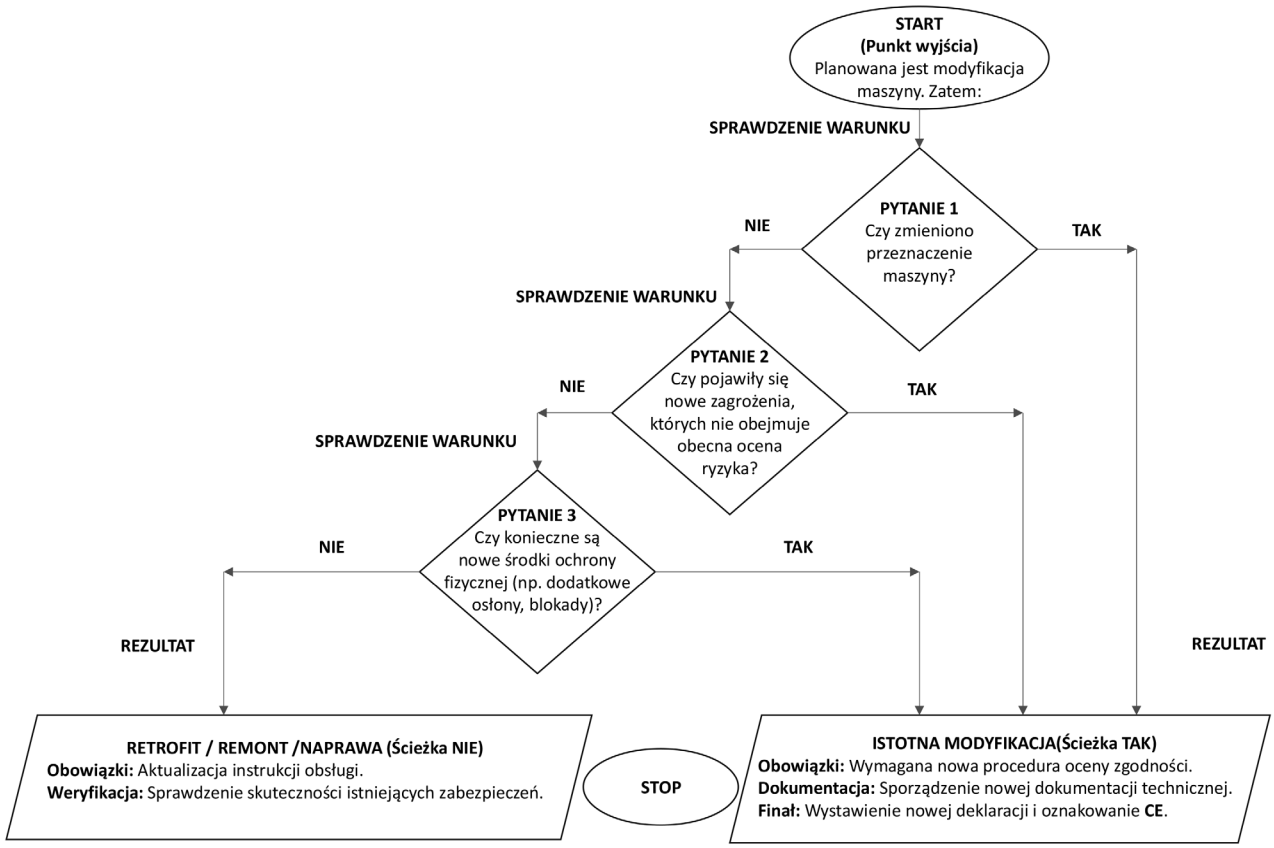
- Cyberbezpieczeństwo: Maszyny muszą być zaprojektowane tak, aby zewnętrzne ataki hakerskie nie mogły doprowadzić do niebezpiecznych sytuacji (np. nagłego uruchomienia).
- Sztuczna Inteligencja (AI): Nowe przepisy regulują bezpieczeństwo maszyn, które same „uczą się" zachowań, co wymaga nowej analizy ryzyka.
- Modyfikacje maszyn: Wprowadzono pojęcie „istotnej modyfikacji" – podmioty modernizujące stare maszyny mogą stać się ich „producentami" w świetle prawa i muszą przeprowadzić nową ocenę zgodności.
- Dokumentacja cyfrowa: Producenci mogą dostarczać instrukcje obsługi w formie cyfrowej (np. kod QR na maszynie), zamiast grubych papierowych tomów.
- Ujednolicenie prawa: Jako rozporządzenie, nowe przepisy będą obowiązywać bezpośrednio w całej UE, bez różnic w interpretacji przez poszczególne państwa.

Zauważamy, że wpływ rozwiązań cyfrowych wymusił umieszczenie w rozporządzeniu, w definicji maszyny, wzmianki o oprogramowaniu. Również element bezpieczeństwa został rozszerzony o elementy cyfrowe, co oznacza, że oprogramowanie może też pełnić funkcje bezpieczeństwa. W załącznikach, oprócz zmiany podziału maszyn o zwiększonym ryzyku w stosunku do dyrektywy dodano maszyny i elementy bezpieczeństwa samozmieniające, czyli takie które są wyposażone w funkcje uczenia maszynowego lub AI [2, 4].

Rozporządzenie (UE) 2023/1230 ustanawia ramy prawne dotyczące wprowadzania do obrotu w Unii Europejskiej bezpiecznych maszyn i obejmuje nowe zagrożenia związane z powstającymi technologiami. Cytując, w rozporządzeniu podano, że stosuje się go do maszyn i następujących produktów powiązanych: a) wyposażenia wymiennego; b) elementów bezpieczeństwa; c) osprzętu do podnoszenia; d) łańcuchów, lin i pasów; e) odłączalnych urządzeń do mechanicznego przenoszenia napędu. Niniejsze rozporządzenie stosuje się również do maszyn nieukończonych, a maszyny i produkty powiązane, wymienione powyżej oraz maszyny nieukończone zwane są łącznie „produktami objętymi zakresem stosowania niniejszego rozporządzenia". Oprócz maszyn przemysłowych i do użytku dla konsumentów, obejmuje również niewielkie pojazdy do użytku osobistego i lekkie pojazdy elektryczne, takie jak skutery i rowery, ponieważ są one popularne, a mogą być niebezpieczne dla użytkowników z punktu widzenia bezpieczeństwa technicznego lub przemysłowego. Gwarantuje pewność prawa poprzez doprecyzowanie zakresu stosowania tego aktu [2, 5]. Zatem kto według Rozporządzenia (UE) 2023/1230 będzie odpowiedzialny za zgodność maszyn z przepisami? Odpowiedzialność będzie spoczywać na: producentach, którzy projektują, wytwarzają i wprowadzają maszyny na rynek, importerach, którzy sprowadzają maszyny spoza UE, dystrybutorach, którzy udostępniają maszyny na rynku, użytkownikach maszyn, którzy mają utrzymywać maszyny w stanie, w jakim zostały wprowadzone do obrotu [2, 6]. Zauważamy zatem, że nowe przepisy nie dotyczą tylko producentów maszyn. Będą one również bezpośrednio dotyczyły innych podmiotów wprowadzających modyfikacje w maszynach: pracodawców modernizujących własne maszyny, integratorów wykonujących modyfikacje dla klientów, firm zewnętrznych świadczących usługi modernizacji, producentów maszyn wykonujących aktualizacje swoich produktów [2, 3]. Rozporządzenie wprowadza także obowiązek przeprowadzania oceny zgodności przez osobę trzecią w odniesieniu do sześciu kategorii maszyn „wysokiego ryzyka". Informacje na temat bezpieczeństwa będą musiały być przekazywane z każdym produktem, a domyślnie stosowane będą instrukcje w formacie cyfrowym. Informacje w wersji papierowej nadal będą udostępniane na prośbę klientów [2, 5].

4. Modernizacja vs Istotna Modyfikacja – granica odpowiedzialności

Dla użytkowników maszyn w Polsce kluczowym wyzwaniem jest rozróżnienie między zwykłym remontem



Rys. 2. Ścieżka decyzyjna określająca status prawny modyfikowanej maszyny zgodnie z wytycznymi Rozporządzenia 2023/1230 [12]

(utrzymaniem stanu pierwotnego) a modyfikacją [3]. Nowe rozporządzenie wprowadza definicję „istotnej modyfikacji". Mamy z nią do czynienia, gdy zmiana w maszynie:

- Wprowadza nowe zagrożenia lub zwiększa istniejące ryzyka.
- Wymaga zastosowania fizycznych środków ochronnych, których montaż narusza stateczność lub strukturę maszyny.
- Zmienia przeznaczenie maszyny.

Problem jaki się pojawia, to odpowiedź na pytanie: Kiedy użytkownik staje się producentem?

W praktyce, jeśli remont lub naprawa polega na wymianie starego sterownika PLC na nowy, ale bez zmiany logiki bezpieczeństwa i parametrów pracy – pozostajemy w obszarze remontu lub retrofitu. Jeśli jednak w ramach modernizacji zmieniamy parametry pracy linii produkcyjnej, zwiększamy prędkość linii lub dodajemy ramię robota w strefie, która wcześniej była obsługiwana manualnie, to dokonujemy istotnej modyfikacji. W takim przypadku podmiot dokonujący zmian staje się producentem i musi przeprowadzić pełną procedurę oceny zgodności (CE). Do oceny charakteru zmian można również zastosować ekspercką praktykę. Tutaj z pomocą przychodzą firmy specjalizujące się w zakresie rozwiązań i bezpieczeństwa maszyn oraz PIP i CIOP, które w opracowaniach sugerują zastosowanie prostego algorytmu oceny zmian, pozwalającego udokumentować, czy modyfikacja ma charakter istotny. Zgodnie z wytycznymi Rozporządzenia 2023/1230 opracowaliśmy prostą ścieżkę decyzyjną określającą status prawny modyfikowanej maszyny – rys. 2.

Podsumowując, Rozporządzenie (UE) 2023/1230 (tzw. Rozporządzenie Maszynowe), które w pełni zastąpi Dyrektywę 2006/42/WE od 20 stycznia 2027 roku, po raz pierwszy wprowadza prawną definicję „istotnej modyfikacji". To kluczowy termin, który wyznacza granicę między zwykłą modernizacją a przejęciem roli producenta.

Kiedy modernizacja staje się istotna? Zgodnie z Artykułem 3 pkt. 16 Rozporządzenia (UE) 2023/1230 – *Artykułem 3 pkt 16 Rozporządzenia 2023/1230*, modyfikacja jest uznana za istotną, gdy spełnione są łącznie trzy warunki:

1. Sposób dokonania: zmiana jest fizyczna lub cyfrowa (np. zmiana oprogramowania sterującego).
2. Brak przewidywalności: zmiana nie była przewidziana ani zaplanowana przez pierwotnego producenta.
3. Wpływ na bezpieczeństwo: zmiana tworzy nowe zagrożenie lub zwiększa istniejące ryzyko, co wymaga: dodania osłon lub urządzeń ochronnych wymagających modyfikacji układu sterowania, lub zastosowania dodatkowych środków ochronnych dla zapewnienia stabilności lub wytrzymałości mechanicznej.

5. Skutki prawne i podział odpowiedzialności – przykład wymiany napędów elektrycznych z jednoczesnym zwiększeniem prędkości linii o 10%

Generalnie, zmiana dotyczyć będzie również zakresu obowiązków osoby dokonującej modyfikacji. Rozporządzenie (UE) 2023/1230 – *Rozporządzenie (UE) 2023/1230* wprowadza zasadę proporcjonalności:

5.1. Nowy status „Producenta”

Osoba (fizyczna lub prawna) dokonująca istotnej modyfikacji staje się producentem w rozumieniu przepisów i przejmuje pełną odpowiedzialność za bezpieczeństwo. To może stanowić najbardziej ryzykowny punkt całego procesu modernizacji. Zgodnie z Rozporządzeniem 2023/1230, w momencie dokonania „istotnej modyfikacji” (którą np. będzie wymiana napędów elektrycznych i zmiana parametrów linii, wpływająca na drogę hamowania), następuje automatyczne przeniesienie statusu prawnego, co może stanowić pułapkę statusu producenta. Jeśli pracownicy utrzymania ruchu sami wymieniają te napędy i podkręcają prędkość bez formalnego procesu oceny, to: ta firma staje się producentem w świetle prawa, ta firma przejmuje odpowiedzialność karną za wszelkie wady konstrukcyjne maszyny (nawet te pierwotne, jeśli modyfikacja miała na nie wpływ). Następuje utrata gwarancji i wsparcie pierwotnego producenta.

Zatem, co należy zrobić i jak poprawnie przekazać status producenta integratorowi? W celu, aby zewnętrzny integrator, zgodnie z zamierzeniem zlecenia, stał się „producentem modyfikacji”, proces powinien wyglądać następująco:

- Nazewnictwo w umowie – Najprościej używać sformułowań typu – „Dokonanie istotnej modyfikacji maszyny w rozumieniu Rozporządzenia (UE) 2023/1230”.
- Tabliczka znamionowa – integrator jako nowy producent powinien: umieścić na maszynie dodatkową tabliczkę znamionową (obok starej), podać tam swoją nazwę, adres oraz rok dokonania modyfikacji, oznakować maszynę (lub jej zmodyfikowaną część) znakiem CE.
- Dokumentacja techniczna (Artykuł 10) – Integrator ma obowiązek sporządzić dokumentację techniczną, ale nie musi oddawać jej nam w całości, gdyż to może stanowić know-how i być objęte tajemnicą handlową. Nowy producent, powinien jednak: przechowywać dokumentację przez 10 lat, udostępnić na wezwanie dokumentację organom nadzoru rynku (np. PIP), przekazać dokumentację w formie instrukcji oraz w zakresie wprowadzonych zmian wraz z nową Deklaracją Zgodności UE. Gdzie zatem kończy się odpowiedzialność integratora? W omawianym przypadku (zwiększenie prędkości linii 10% oraz skanery), odpowiedzialność integratora jako producenta obejmuje: prawidłowy dobór silników i falowników, poprawne przeliczenie drogi hamowania, gwarancję, że skanery i kurtyny zdążą zatrzymać linię przy nowej prędkości – pomiary czasu dobiegu. Natomiast odpowiedzialność użytkownika (pracodawcy) zaczyna się tam, gdzie kończy się montaż: szkolenie pracowników z nowych parametrów pracy, codzienna kontrola stanu linii, czy skanery nie są zabrudzone/przestawione. Ważna wskazówka: Jeśli za kilka lat dojdzie do wypadku z powodu awarii hamulców przy wyższej prędkości linii, wtedy Deklaracja Zgodności dla wykonanej modyfikacji będzie niezbędna. Jeśli użytkownik (właściciel) maszyny nie będzie w jej posiadaniu, twierdząc, że „integrator wymienił silniki”, to odpowiedzialnym za wprowadzenie niebezpiecznej maszyny do obrotu będzie jej użytkownik – właściciel zakładu.

5.2. Ograniczony zakres oceny

W przeciwieństwie do starej dyrektywy, nowa ocena zgodności może dotyczyć wyłącznie części maszyny, która uległa modyfikacji, pod warunkiem, że zmiana nie wpływa na bezpieczeństwo całej maszyny lub zespołu maszyn (Art. 18). zgodności może dotyczyć wyłącznie części maszyny, która uległa modyfikacji, pod warunkiem, że zmiana nie wpływa na bezpieczeństwo całej maszyny lub zespołu maszyn (Art. 18). To jedno z najważniejszych ułatwień w Rozporządzeniu 2023/1230, które rozwiązuje problem „zatwierdzania całej fabryki” z powodu zmiany jednego silnika. W starej dyrektywie (2006/42/WE) granice odpowiedzialności przy modernizacji były szarą strefą – często interpretowano to tak, że modyfikujący bierze na siebie całą maszynę. Zgodnie z nowymi przepisami, integrator nie musi certyfikować całej linii od nowa, jeśli potrafi wykazać, że: modyfikacja jest odizolowana, zmiana parametrów (szybkość) wpływa tylko na konkretny moduł, zabezpieczenia reszty linii nadal działają poprawnie. Art. 18 zawiera bezpiecznik: ocenę można ograniczyć, pod warunkiem, że zmiana nie pogarsza bezpieczeństwa pozostałych części. Zatem kiedy NIE można ograniczyć oceny tylko do nowej części? Jeśli wyższa prędkość powoduje, że produkty z części linii wpadają do kolejnej maszyny z siłą, na którą tamta nie jest przygotowana lub jeśli zwiększone wibracje z nowych napędów wpływają na stabilność ramy całej maszyny lub jeśli zmiana logiki sterowania w zmienionym module blokuje sygnał E-STOP (wyłącznik awaryjny) dla reszty linii. Aby skorzystać z dobrodziejstwa Art. 18 i nie „analizować” całej linii, integrator w swojej dokumentacji musi zawrzeć Analizę Wpływu Zmian:

- Opisać zakres zmian: „Ocena zgodności dotyczy wyłącznie modułu napędowego nr X i powiązanych funkcji bezpieczeństwa”,
- Uzasadnić brak wpływu zmian: „Wzrost prędkości o 10% nie wpływa na stabilność mechaniczną pozostałych sekcji linii (sekcje Y i Z)”,
- Dokonać weryfikacji połączeń maszyn: Dowód, że połączenia (mechaniczne i elektryczne) między modyfikowaną częścią a resztą są nadal bezpieczne.

Przykładowo, przy 10% wzroście prędkości najczęstszym problemem będzie droga hamowania. Jeśli nowa droga hamowania mieści się w granicach, w których właściwie reagują obecne skanery – można ograniczyć ocenę. Jeśli jednak z tego powodu musimy przesunąć wygrodzenia na całej linii – zakres oceny musi zostać rozszerzony. Art. 18 stanowi swoistą ulgę dla integratora, ale korzyść dla właściciela maszyny, gdyż koszt modernizacji powinien być niższy, skoro nie płacimy za badanie elementów, których nie dotykano. W tym miejscu należy upewnić się, czy integrator potwierdził, czy zamierza wystawić deklarację na całą maszynę, czy tylko na wykonany „zakres modyfikacji”?

5.3. Wyłączenie dla użytkowników nieprofesjonalnych

Osoba modyfikująca maszynę na własny, nieprofesjonalny użytek, nie jest uznawana za producenta. Ten zapis

Tabela 3. Przykłady w praktyce kwalifikacji charakteru zmian w maszynie [12]

Typ zmiany	Kwalifikacja	Konsekwencja
Wymiana silnika na identyczny lub o tych samych parametrach	Modernizacja (zwykła)	Brak konieczności nowej certyfikacji CE
Zmiana oprogramowania zmieniająca logikę bezpieczeństwa (np. prędkość reakcji)	Istotna modyfikacja	Konieczna nowa ocena zgodności i znak CE
Dołożenie robota do starej maszyny, co wymaga nowych kurtyn świetlnych	Istotna modyfikacja	Modyfikujący staje się producentem nowej całości
Dodanie osłony stałej, która nie wymaga zmiany w sterowaniu	Modernizacja (zwykła)	Aktualizacja dokumentacji zakładowej

Rys. 3. Dobiegometr Safetyman DT3 wraz z zestawem pomiarowym firmy HHB Electronic [7]

dotyczący użytkowników nieprofesjonalnych w Rozporządzeniu 2023/1230 może być często mylnie interpretowany jako „wolna amerykanka" dla majsterkowiczów. W rzeczywistości ma on bardzo wąskie zastosowanie i nie dotyczy firm (pracodawców). Wyłączenie to odnosi się wyłącznie do osób fizycznych, które: modyfikują maszynę na własny użytek, działają poza swoją działalnością gospodarczą lub zawodową (użytek domowy, hobby). Przykładem może być rolnik-hobbysta przerabiający własną kosiarkę do użytku w prywatnym ogrodzie (o ile nie świadczy nią usług).

Według Rozporządzenia 2023/1230, jeśli zwiększenie prędkości linii wymaga: przestawienia kurtyn świetlnych lub wygrodzeń (bo droga hamowania się wydłużyła), czy też zmiany logiki w sterowniku bezpieczeństwa (Safety PLC), to jest to Istotna Modyfikacja. W takim przypadku integrator musi nadać nowe oznakowanie CE dla objętego zmianą zakresu. Generalnie, jeśli modyfikacja wymusza ingerencję w system sterowania bezpieczeństwem (Safety PLC) lub dodanie nowych zabezpieczeń fizycznych dla nowych zagrożeń, przekraczamy granicę i przejmujemy odpowiedzialność jako producent.

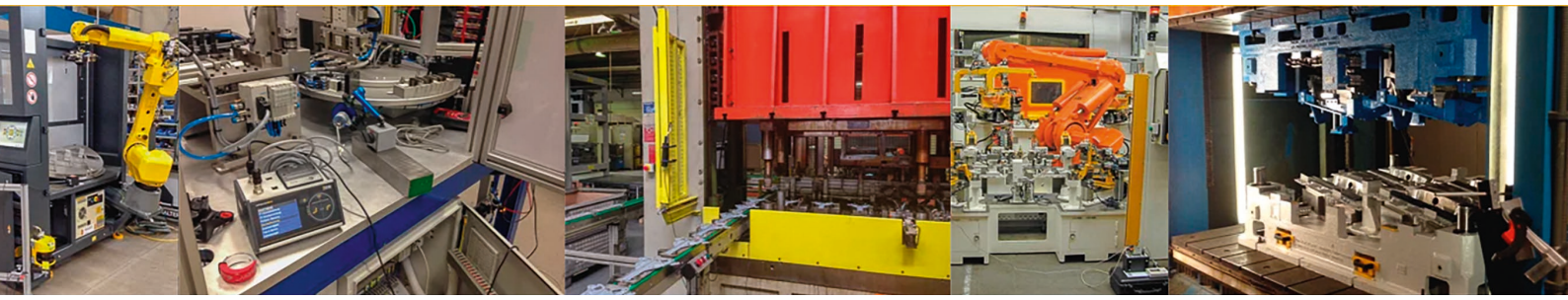
Również, jeśli planujemy zwiększenie prędkości linii produkcyjnej o np. 10% wraz z wymianą napędów (silniki, falowniki), przy istniejących systemach optoelektronicznych (skanery, kurtyny), to najprawdopodobniej zostanie to zakwalifikowane jako istotna modyfikacja. Na jakie kluczowe punkty, musimy zwrócić uwagę – kluczowe zagrożenie to czas zatrzymania maszyny. Większa masa napędowa i wyższa prędkość to większa energia kinetyczna. Nawet tylko 10% wzrostu prędkości może wydłużyć drogę hamowania powyżej bezpiecznego limitu. W tym celu, między innymi, musimy wykonać pomiary czasu dobiegu dobiegometrem posiadającym aktualne Świadectwo Kalibracji, [7].

Generalnie należy wykonać weryfikację i pomiary:

- Pomiary dobiegu: Integrator musi wykonać nowe pomiary czasu zatrzymania (stop time measurements).
- Lokalizacja czujników: Jeśli czas zatrzymania wzrośnie, kurtyny i skanery mogą okazać się zamontowane zbyt blisko strefy niebezpiecznej (zgodnie z normą EN ISO 13855).
- Skanery laserowe: Może być konieczna rekonfiguracja stref ostrzegawczych i ochronnych (poszerzenie pól widzenia skanera).

Dobiegometr SafetyMan DT3 firmy HHB Electronic to nowoczesne, mobilne urządzenie pomiarowe oferowane przez, służące do precyzyjnego wyznaczania czasu i drogi zatrzymania elementów niebezpiecznych maszyn. Model ten zastąpił starszą wersję DT2 na początku 2025 roku, wprowadzając m.in. możliwość bezprzewodowej łączności z urządzeniami mobilnymi. Kluczowe funkcje urządzenia SafetyMan DT3, [7]:

- Pomiary parametrów fizycznych: Rejestrowanie rzeczywistego czasu zatrzymania (t), drogi hamowania (s) oraz prędkości (v) maszyny.
- Obliczanie odległości bezpieczeństwa: Automatyczne wyznaczanie minimalnego dystansu (S) montażu urządzeń ochronnych (np. kurtyn świetlnych) zgodnie z normą PN-EN ISO 13855 oraz ANSI.
- Analiza graficzna: Generowanie krzywych hamowania, które pozwalają na szczegółową interpretację procesu zatrzymywania się napędów.



Rys. 4. Przykłady wykonania pomiarów dobiegu maszyn za pomocą dobiegometru Safetyman DT3 firmy HHB Electronic, [7]

- Dokumentacja i raportowanie: Tworzenie profesjonalnych protokołów pomiarowych (PDF), które stanowią dowód zgodności dla audytów BHP i kontroli Państwowej Inspekcji Pracy (PIP).

Urządzenie wykorzystuje aktywator (np. maszyny Auto-Hand), który automatycznie inicjuje zatrzymanie maszyny poprzez naruszenie bariery ochronnej (skanery laserowe, kurtyny) lub wpięcie w obwód E-Stop. Pozwala to na przeprowadzenie testów bez konieczności ingerencji w połączenia elektryczne.

Wracając do omawianego przykładu, podsumowując, w omawianym przykładzie wymiany silników i falowników, z jednoczesnym zwiększeniem prędkości linii produkcyjnej o 10%:

a) Aby nie zostać uznanym za „nowego producenta maszyny", co wiąże się z przejęciem pełnej odpowiedzialności cywilnej oraz karnej, zewnętrzny integrator musi dostarczyć komplet dokumentów potwierdzających, że „wprowadza zmianę do obrotu". Obowiązki integratora – musi dostarczyć:

- Nową deklarację zgodności: Dla zmodyfikowanego podsystemu napędowego i sterowania – wystawionej na zmodyfikowaną część maszyny lub na całość (jeśli zmiana była istotna).
- Weryfikację Performance Level (PL): Potwierdzenie, że nowe falowniki (z funkcjami typu STO, SS1) oraz silniki współpracują z systemem bezpieczeństwa na poziomie nie niższym niż dotychczasowy.
- Obliczenia wytrzymałościowe: Potwierdzenie, że konstrukcja mechaniczna maszyny (ramy, przekładnie) wytrzyma zwiększone obciążenia dynamiczne przy starcie i hamowaniu.
- Nowej lub zaktualizowanej Oceny Ryzyka – dokumentującej, że wyższa prędkość została przeanalizowana pod kątem bezpieczeństwa.
- Protokołów z pomiarów dobiegu – kluczowe przy zwiększeniu prędkości; integrator musi udowodnić, że obecne zabezpieczenia (np. kurtyny) są wystarczająco daleko, by zatrzymać maszynę przed kontaktem z operatorem.
- Instrukcji stanowiskowej (aneks) – opisującej nowe zasady obsługi przy zmienionych parametrach.
- Dokumentacji technicznej zmian – schematy elektryczne i algorytmy sterowania (jeśli uległy zmianie).

Pojęcia prac modernizacyjnych i retrofitycznych, to w nowym rozporządzeniu obszar, w którym przepisy stały się znacznie precyzyjniejsze, wprowadzając pojęcie „istotnej modyfikacji". Kiedy modernizacja staje się „produkcją"? Jeśli zmieniamy działanie maszyny, jej wydajność lub sposób sterowania w sposób, który generuje nowe ryzyka (lub zwiększa stare), dokonujesz istotnej modyfikacji. Nowa ocena zgodności: W takim przypadku modernizujący przejmuje obowiązki producenta. Musi wystawić nową Deklarację Zgodności UE i nadać nowe oznakowanie CE. Zasada proporcjonalności: Nie zawsze musimy recertyfikować całą linię. Jeśli zmiana dotyczy tylko jednego modułu i nie wpływa na resztę, ocena może ograniczyć się do zmienionej części. Bezpieczeństwo cyfrowe przy „retrofittingu": Dodając do starej maszyny moduł zdalnego dostępu (np. do serwisu), musimy zadbać o to, aby to nowe połączenie nie naruszało dotychczasowego bezpieczeństwa fizycznego.

Należy pamiętać, że wyłączenie dla użytkowników nieprofesjonalnych, jeśli modyfikacja odbywać się będzie w zakładzie produkcyjnym, warsztacie lub firmie usługowej, nie ma zastosowania, ponieważ:

- Status pracodawcy: Firma podlega pod dyrektywy dotyczące bezpieczeństwa pracy (w Polsce m.in. Minimalne Wymagania BHP – Rozporządzenie MPiPS).
- Działalność zawodowa: Każda maszyna używana w procesie zarobkowym musi spełniać wymogi bezpieczeństwa, aby chronić pracowników.
- Definicja „nieprofesjonalna": Rozporządzenie wyraźnie oddziela konsumenta od podmiotu gospodarczego. Firma zawsze występuje jako podmiot profesjonalny.

Jakie będą skutki bycia „Producentem" we własnej firmie? W omawianym przypadku (zmiana prędkości o 10% + wymiana napędów), jeśli zlecenia nie otrzyma integrator, który dostarczy komplet dokumentów, to firma zlecająca staje się producentem. Oznacza to: konieczność wystawienia Deklaracji Zgodności UE, przechowywanie dokumentacji technicznej przez 10 lat, pełną odpowiedzialność za ewentualny wypadek wynikający z błędu w projekcie modyfikacji.

6. Rozporządzenia (UE) 2023/1230 a projektowanie nowej maszyny

Projektowanie nowej maszyny zgodne z Rozporządzeniem (UE) 2023/1230 wymagać będzie zmiany podejścia, szczególnie w obszarze cyfryzacji i oprogramowania. Choć fundamenty oceny ryzyka pozostają podobne, pojawiają się nowe, rygorystyczne wymogi. Projektant będzie musiał postrzegać maszynę jako system cyber-fizyczny, a nie tylko mechaniczny.

- Bezpieczeństwo zintegrowane (Safety Integrated): To już nie tylko osłony i wyłączniki, należy uwzględnić odporność na błędy w oprogramowaniu i uszkodzenia układów sterowania.
- Analiza ryzyka IT: Należy ocenić, czy podłączenie maszyny do sieci (OT/IT) może stworzyć zagrożenie fizyczne (np. czy haker może zdalnie wyłączyć funkcję bezpieczeństwa).
- Sztuczna Inteligencja: Jeśli maszyna używa uczenia maszynowego (np. do rozpoznawania obrazu w sortowni), należy zapewnić, że algorytm nie podejmie niebezpiecznej decyzji po „nauczeniu się" nowych danych.
- Dokumentacja cyfrowa: Już na etapie projektu można zaplanować udostępnienie instrukcji przez kod QR, co ułatwia aktualizację danych dla użytkownika.

6.1. W zakresie nowych obszarów

a) Ocena Ryzyka – projektant powinien przewidzieć zagrożenia, które w starej dyrektywie były pomijane lub traktowane ogólnikowo:

- Cyberbezpieczeństwo: jeśli maszyna jest podłączona do sieci, należy zaprojektować ochronę przed atakami, które mogłyby doprowadzić do niebezpiecznych sytuacji (np. przejęcie kontroli nad napędami).
- Sztuczna Inteligencja (AI): jeśli maszyna wykorzystuje algorytmy uczenia maszynowego (np. w wizji maszynowej do sortowania), należy zapewnić przewidywalność ich zachowań.
- Interakcja człowiek-maszyna: większy nacisk na aspekty psychologiczne i ergonomiczne przy pracy z robotami współpracującymi (cobotami).

b) Dokumentacja i Cyfryzacja – Rozporządzenie idzie z duchem czasu, co ma ułatwić pracę producentom:

- Instrukcje cyfrowe: można dostarczyć instrukcję w formie pliku PDF, kodu QR na maszynie lub online. Na prośbę klienta należy jednak bezpłatnie dostarczyć wersję papierową w ciągu miesiąca.
- Deklaracja Zgodności: Również może być udostępniona cyfrowo.
- Dane źródłowe: Należy archiwizować dowody na to, że oprogramowanie sterujące (Safety PLC) jest chronione przed przypadkową lub celową zmianą przez osoby nieuprawnione.

c) Maszyny „Wysokiego Ryzyka" (Załącznik I) – to największa zmiana proceduralna. Jeśli nowa maszyna znajduje się na liście w Załączniku I (dawny Załącznik IV), np.: niektóre typy pras, maszyny z funkcjami AI zapewniającymi bezpieczeństwo, przenośne maszyny montażowe ładunków wybuchowych, … to można nie mieć prawa do samodzielnej oceny zgodności (wewnętrzna kontrola produkcji). W niektórych przypadkach udział Jednostki Notyfikowanej będzie obowiązkowy – wykaz [8].

6.2. Sugestie dla projektanta

- Bezpieczeństwo z założenia (Safety by design): norma EN ISO 12100 od pierwszego szkicu, uwzględnienie odporności na zakłócenia elektromagnetyczne i stabilność oprogramowania.
- Wybór norm zharmonizowanych: weryfikacja, czy normy typu C dla projektowanej maszyny zostały już zaktualizowane pod nowe rozporządzenie (trwa proces aktualizacji bazy norm).
- Kontrola dostępu: zaprojektować fizyczne i logiczne bariery (hasła, klucze RFID), aby nikt nie mógł zdalnie „zmienić" prędkości maszyny powyżej bezpiecznych limitów bez pozostawienia śladu w logach.

Należy pamiętać, że maszyny wprowadzone do obrotu po 20 stycznia 2027 r. muszą bezwzględnie spełniać wymogi nowego Rozporządzenia. Maszyny zaprojektowane w tym czasie, ale oddane do użytku w lutym 2027, będą również musiały mieć deklarację zgodną z 2023/1230. Jeśli nowa maszyna będzie posiadać funkcje zdalnego dostępu (serwis przez Internet) lub algorytmy autonomiczne to finalnie zdecyduje o poziomie skomplikowania certyfikacji, gdyż projekt musi uwzględniać najnowocześniejsze i najbardziej rygorystyczne wymagania Rozporządzenia 2023/1230.

6.3. Zdalny dostęp i autonomiczne algorytmy

Zdalny dostęp i autonomia to obecnie tzw. „gorące punkty" dla audytorów. Sugerujemy uwzględnienie:

1. Cyberbezpieczeństwo (Art. 20 i Załącznik III) – w nowym rozporządzeniu ochrona przed atakami hakerskimi nie jest już opcją – to wymóg bezpieczeństwa maszyny. Ochrona przed ingerencją: należy udowodnić, że połączenie zdalne nie pozwala na ominięcie funkcji bezpieczeństwa (np. zdalne zmostkowanie kurtyny). Logowanie zdarzeń: maszyna musi zapisywać, kto, kiedy i co zmieniał w oprogramowaniu (tzw. evidence of intervention). Odporność (Resilience): awaria połączenia internetowego nie może spowodować niekontrolowanego ruchu maszyny. Cyberbezpieczeństwo i komunikacja zdalna to nowy fundament w Rozporządzeniu Maszynowym. Proponujemy weryfikację następujących norm:

- IEC 62443 (seria): Kluczowa norma dla cyberbezpieczeństwa systemów automatyki przemysłowej.
  - 62443-3-3: Wymagania dotyczące bezpieczeństwa systemów i poziomy zabezpieczeń.
  - 62443-4-1: Bezpieczny cykl życia produktu (dla producentów).
- EN ISO 13849-1: W nowej wersji (2023) kładzie większy nacisk na odporność oprogramowania na ingerencję osób trzecich.
- TR 60601-4-5: (Pomocniczo) Wytyczne dotyczące bezpieczeństwa technicznego w sieciach IT.

2. Algorytmy autonomiczne (AI) – jeśli maszyna sama podejmuje decyzje (np. dobiera trasę przejazdu lub parametry cięcia), podlega pod szczególny nadzór:

- Przewidywalność: Należy wykazać, że „nauka" algorytmu nie doprowadzi do przekroczenia limitów bezpieczeństwa (np. maszyna nie uzna, że szybciej będzie przejechać przez strefę z ludźmi).
- Nadzór człowieka: System musi pozwalać operatorowi na natychmiastowe przejęcie kontroli (tzw. *human-in-the-loop*).

- Załącznik I (Wysokie ryzyko): Jeśli algorytm AI pełni funkcję bezpieczeństwa (np. system wizyjny zastępuje kurtynę), maszyna może wymagać certyfikacji przez Jednostkę Notyfikowaną (nie wystarczy Twoja deklaracja).

W przypadku autonomii należy dbać o przewidywalność zachowań. Proponujemy weryfikację następujących norm:

- ISO/IEC 22989: Terminologia i pojęcia dotyczące Sztucznej Inteligencji (podstawa do dokumentacji).
- ISO/IEC 23894: Zarządzanie ryzykiem w systemach wykorzystujących AI.
- EN ISO 3691-4: Jeśli Twoja maszyna jest pojazdem autonomicznym (AGV/AMR) – najważniejsza norma określająca wymagania dla funkcji bezpiecznej jazdy.
- ISO/TR 4808: (W opracowaniu/dostępna) Specyfikacja techniczna dotycząca bezpieczeństwa systemów autonomicznych.

3. Bezpieczeństwo funkcjonalne (Sterowanie) – te normy określają, jak „pewne" są układy bezpieczeństwa:

- EN ISO 13849-1: Ocena poziomu zapewnienia bezpieczeństwa (PL – *Performance Level*). Niezbędna do walidacji logiki sterowania.
- EN 62061: Alternatywa dla powyższej, skupiająca się na bezpieczeństwie funkcjonalnym elektrycznych systemów sterowania (SIL).
- EN ISO 13849-2: Walidacja – czyli proces udowadniania, że zaprojektowane funkcje bezpieczeństwa faktycznie działają.

4. Normy ogólne i mechaniczne – to podstawa dla każdej nowej maszyny:

- EN ISO 12100: Podstawowa norma dotycząca oceny ryzyka i redukcji ryzyka.
- EN 60204-1: Bezpieczeństwo elektryczne maszyn (wymogi dla szaf sterowniczych, okablowania i napędów).
- EN ISO 13850: Funkcja zatrzymania awaryjnego (E-Stop).
- EN ISO 13855: Umiejscowienie wyposażenia ochronnego (kluczowe przy skanerach i kurtynach).

5. Kluczowe kroki w projektowaniu – weryfikacja oprogramowania:

- Należy stosować normę EN ISO 13849-1 w odniesieniu do bezpieczeństwa oprogramowania.
- Wymagana jest separacja: kod odpowiedzialny za autonomię nie może wpływać na kod odpowiedzialny za E-Stop.

6. Zdalny serwis (*Remote Access*):

- Zaprojektować fizyczny przełącznik na maszynie: „Tryb Lokalny/Tryb Zdalny".
- Zdalny dostęp powinien być ograniczony czasowo i potwierdzony przez operatora na miejscu.

7. Wytyczne dla dokumentacji:

- W instrukcji należy opisać limity autonomii (co maszyna może zrobić sama, a czego jej nie wolno).
- Należy określić wymagania dla sieci IT klienta (np. minimalne szyfrowanie).

8. Proponowana lista kontrolna dla tworzonego projektu:

- Czy wdrożono system zarządzania bezpieczeństwem informacji (np. wg IEC 62443)?
- Czy algorytm autonomiczny ma zdefiniowane „bezpieczne granice", których nie zmieni proces uczenia?
- Czy każda próba zdalnego połączenia jest rejestrowana w pamięci maszyny w sposób nieusuwalny?

Dla funkcji autonomicznych opartych na AI, Rozporządzenie 2023/1230 jest ściśle powiązane z nadchodzącym AI Act. Jeśli nowa maszyna pełni funkcje bezpieczeństwa za pomocą AI, należy sprawdzić, czy nie należy skorzystać z Załącznika I, co wymusza certyfikację przez jednostkę zewnętrzną.

7. Przykład opisu Zabezpieczenia Dostępu Zdalnego i Funkcji Autonomicznych

Zgodnie z Rozporządzeniem (UE) 2023/1230 (Załącznik III, sekcja 1.1.9):

1. Identyfikacja i Kontrola Dostępu (*Cybersecurity*):

- Fizyczna bariera dostępu: Maszyna została wyposażona w kluczowy przełącznik trybu pracy (Lokalny/Zdalny). Aktywacja dostępu zdalnego wymaga fizycznej obecności operatora przy maszynie i manualnego przełączenia trybu.
- Logiczna kontrola dostępu: Dostęp realizowany jest poprzez szyfrowany tunel VPN (min. AES-256). Każdy użytkownik posiada unikalny identyfikator. System wymusza cykliczną zmianę haseł zgodnie z normą IEC 62443-4-2.
- Rejestracja zdarzeń (*Logging*): Maszyna posiada nieulotną pamięć zdarzeń (*Log-file*), rejestrującą każdą próbę połączenia, czas trwania sesji oraz zakres wprowadzonych zmian w parametrach. Dane te są zabezpieczone przed usunięciem przez osoby nieuprawnione.

2. Bezpieczeństwo Funkcji Autonomicznych (*AI & Control*):

- Granice decyzyjne: Algorytmy autonomiczne działają wyłącznie w zdefiniowanej „przestrzeni operacyjnej". Parametry krytyczne dla bezpieczeństwa (np. prędkość maksymalna, droga hamowania) są zablokowane na poziomie sprzętowym (*Hardware-based limits*) i nie podlegają modyfikacji przez proces uczenia się algorytmu.
- Priorytet funkcji bezpieczeństwa: Zgodnie z EN ISO 13849-1, wszystkie funkcje bezpieczeństwa (E-Stop, skanery laserowe) mają priorytet nadrzędny nad komendami generowanymi przez algorytmy autonomiczne. Awaria systemu AI skutkuje natychmiastowym przejściem maszyny w stan bezpieczny (Stop kategorii 0 lub 1).
- Nadzór (*Human-in-the-loop*): System autonomiczny informuje operatora o planowanych działaniach poprzez interfejs HMI. Operator ma możliwość natychmiastowego przerwania cyklu autonomicznego za pomocą fizycznego przycisku sterowniczego.

3. Odporność na Zakłócenia i Utratę Łączności

- Zasada Fail-Safe: W przypadku utraty stabilności połączenia zdalnego (*timeout* > 500ms), maszyna automatycznie przerywa procedurę zdalną i powraca do bezpiecznego trybu lokalnego lub zatrzymuje się, zależnie od wyniku oceny ryzyka.

8. Lista pytań kontrolnych (Checklista) dla programów PLC/AI

Poniżej proponowana lista kontrolna (Checklista) dla programisty PLC/AI. Odpowiedzi na te pytania pozwolą zweryfikować, czy kod maszyny jest zgodny z wymogami

Rozporządzenia 2023/1230 i czy nie narażamy się na odrzucenie dokumentacji przez audytora. Lista pytań dla programisty (Weryfikacja techniczna).

I. Separacja i Priorytety (Safety vs. AI):

1. Czy logika bezpieczeństwa (Safety PLC) jest fizycznie lub logicznie odizolowana od kodu autonomicznego?
   Cel: Algorytm AI nie może mieć możliwości nadpisania zmiennych w sterowniku bezpieczeństwa.
2. W jaki sposób kod wymusza nadrzędność sygnałów z czujników (skanery/kurtyny) nad decyzjami AI?
   Cel: Jeśli AI daje rozkaz jechać, a skaner widzi przeszkodę, sygnał skanera musi być przetwarzany sprzętowo/priorytetowo (*hard-wired* lub Safety BUS).
3. Czy istnieją „sztywne limity" (*Hard Limits*) w kodzie, których algorytm AI nie może zmienić?
   Cel: Np. czy prędkość maksymalna jest wpisana jako stała (*constant*), czy jako zmienna, którą AI mogłoby teoretycznie podbić o 50%?

II. Cyberbezpieczeństwo i Dostęp Zdalny:

4. Czy system odróżnia „podgląd danych" od „sterowania zdalnego"?
   Cel: Zdalny dostęp do diagnostyki jest bezpieczny, ale zdalny ruch maszyną musi wymagać dodatkowego potwierdzenia przez operatora na miejscu.
5. Gdzie są zapisywane logi interwencji i czy są odporne na modyfikację (*Read-only* dla użytkownika)?
   Cel: Rozporządzenie wymaga dowodów na to, kto i kiedy zmieniał oprogramowanie.
6. Co dzieje się z maszyną w przypadku ataku typu „DoS" (zalanie sieci ruchem) lub nagłego zerwania sesji VPN?
   Cel: Maszyna musi przejść w tryb Safe-Stop w przewidywalnym czasie (*Watchdog timer*).

III. Autonomia i Przewidywalność:

7. Czy proces „uczenia się" algorytmu odbywa się w czasie rzeczywistym na maszynie (*Online Learning*), czy w środowisku deweloperskim (*Offline*)?
   Cel: Jeśli Online – jak gwarantujemy, że po 1000 cykli maszyna nie wypracuje niebezpiecznego ruchu?
8. Czy program przewiduje funkcję „Human Override" dostępną w każdym momencie?
   Cel: Zgodność z zasadą nadzoru człowieka nad AI.
9. Podsumowanie

Poniżej przykładowe odpowiedzi służb utrzymania ruchu lub programisty systemu:

- „Dostęp zdalny mamy przez prosty pulpit zdalny/aplikację VPN bez dodatkowych zabezpieczeń na PLC". – Niezgodne z Rozporządzeniem.
- „System bezpieczeństwa i AI działają w tym samym bloku funkcyjnym, bo tak było szybciej". – Błąd krytyczny (brak separacji).
- „Logi są kasowane po każdym restarcie maszyny". – Niezgodne (brak ścieżki audytowej).

9. Przykładowy raport walidacji oprogramowania

Można przygotować krótki Raport Walidacji Oprogramowania, który powinien zawierać:

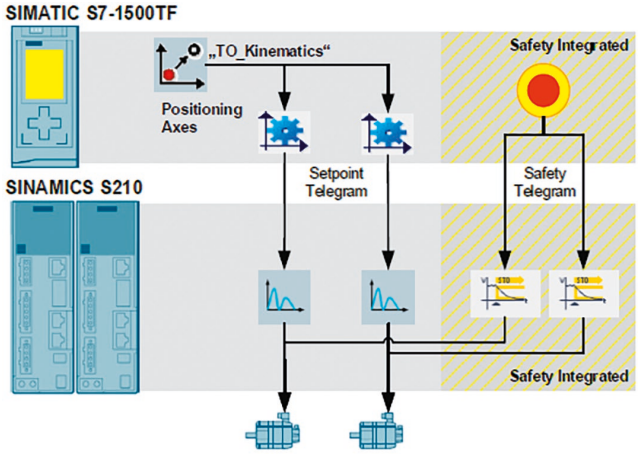
- Opis struktury blokowej (pokazujący separację *Safety/Standard*).
- Wynik testu komunikacji (co się dzieje po wyjęciu kabla sieciowego).
- Potwierdzenie sum kontrolnych (*Checksum*) dla programu bezpieczeństwa.

Uproszczony wzór Raportu Walidacji Oprogramowania, stanowi kluczowy dowód dla jednostek certyfikujących, że testowany system sterowania jest bezpieczny i odporny na ingerencję. RAPORT WALIDACJI OPROGRAMOWANIA STERUJĄCEGO, zgodnie z normą EN ISO 13849-1 oraz Rozporządzeniem (UE) 2023/1230 będzie posiadał pozycje:

1. Identyfikacja Oprogramowania: nazwa projektu, wersja software (*Standard/AI*), wersja software (*Safety*), suma kontrolna (*Safety Checksum*).
2. Architektura i Separacja (Zgodność z Art. 20): opis separacji:
   - Potwierdzam, że kod odpowiedzialny za funkcje bezpieczeństwa (Safety PLC) jest odizolowany od kodu sterowania standardowego i algorytmów autonomicznych.
   - Zabezpieczenie przed nadpisaniem: Zmienne krytyczne (prędkość, czasy hamowania) są zdefiniowane jako stałe systemowe. Zmiana parametrów z poziomu AI nie ma fizycznej możliwości nadpisania rejestrów Safety.
3. Walidacja Funkcji Zdalnych i Cyberbezpieczeństwa: Funkcja Testowana, Scenariusz Testowy, Wynik (P/F), Uwagi
4. Walidacja Algorytmów Autonomicznych:
   - Mechanizm „Watchdog": System AI przesyła sygnał „Lifebeat" do sterownika Safety. Brak sygnału >100 ms skutkuje przejściem w stan bezpieczny.
   - Ograniczenie uczenia (*Envelope*): Granice ruchu maszyny są zdefiniowane sprzętowo za pomocą wyłączników krańcowych i stref skanerów, niezależnie od ścieżki wyliczonej przez AI.
5. Oświadczenie Weryfikatora:
   Niniejszym potwierdzam, że oprogramowanie zostało przetestowane pod kątem błędów logicznych oraz odporności na ingerencję osób trzecich zgodnie z wymaganiami Rozporządzenia 2023/1230.

10. Komunikacja PROFINET i standard PROFISAFE [9]

Przygotowując artykuł na temat bezpieczeństwa maszyn i Rozporządzenia 2023/1230, pod względem rozwiązań cyfrowych należy wymienić rozwiązania firm takich jak Siemens, Pilz, Sick i wielu innych. Z uwagi na doświadczenia praktyczne skoncentrujemy się na rozwiązaniach TIA PORTAL, komunikacji PROFINET, falowników SINAMICS i standardzie PROFIsafe firmy Siemens [9]. Analizowanym przykładem będzie konfiguracja komunikacji PROFIsafe w środowisku TIA Portal pozwala na przesyłanie sygnałów bezpieczeństwa (np. E-Stop, Light Curtain) do napędów (np. SINAMICS) lub wysp rozproszonych (ET 200) za pomocą standardowego kabla Ethernet (PROFINET). PROFIsafe to standard (Black Channel), co oznacza to, że dane



Rys. 5. Wykorzystanie zintegrowanego systemu bezpieczeństwa SINAMICS z funkcjami kinematycznymi i synchronizacyjnymi – SIMATIC S7-1500TF [9]

bezpieczeństwa są przesyłane tym samym kablem co zwykłe dane, ale są chronione przed błędami transmisji poprzez:

- Numerację sekwencyjną: Każdy pakiet ma numer, co zapobiega zamianie kolejności.
- Watchdog (*Timeout*): Jeśli dane nie dotrą w określonym czasie (np. 100 ms), system przechodzi w stan bezpieczny (STOP).
- Unikalne ID (F-Address): Zapobiega pomyleniu urządzeń w sieci.
- Sumę kontrolną CRC: Wykrywa przekłamania bitów w ramce.

Telegram nr 30 to standardowy profil PROFIsafe, służący do sterowania funkcjami bezpieczeństwa w napędach SINAMICS (np. G120, S120). Jest to ramka danych o stałej strukturze, która przesyła tzw. słowa sterujące i statusowe bezpieczeństwa. Struktura Telegramu 30 – Telegram ten składa się z 6 bajtów danych wysyłanych i odbieranych:

- 2 bajty (PZD1): Dane użytkownika (*Safety User Data*) – zawierają bity sterujące konkretnymi funkcjami.
- 4 bajty: Nakładka PROFIsafe (*Trailer*) – dane kontrolne (np. suma CRC, licznik pakietów), które zapewniają integralność transmisji „czarnym kanałem”.

1. Słowo sterujące (S_STW1) – od PLC do Napędu. Wysyłane przez sterownik F-CPU w celu aktywacji funkcji. Wartość „0” zazwyczaj oznacza stan bezpieczny (aktywacja funkcji, np. zatrzymanie), a „1” to zezwolenie na pracę.

2. Słowo statusowe (S_ZSW1) – od Napędu do PLC - Informuje sterownik o aktualnym stanie napędu.

Aby Telegram 30 działał poprawnie, w napędzie muszą zostać ustawione dwa krytyczne parametry:

- F_Dest_Add (p9810): Unikalny adres PROFIsafe urządzenia, który musi zgadzać się z konfiguracją w TIA Portal.
- F_WD_Time (p9811): Czas monitorowania (Watchdog). Jeśli sterownik nie wyśle ramki w tym czasie, napęd natychmiast przejdzie w stan bezpieczny.

W przypadku potrzeby monitorowania stanów wejść cyfrowych bezpiecznych (F-DI) bezpośrednio w napędzie, zaleca się użycie rozszerzonego Telegramu 900. Główna różnica polega na tym, że tam gdzie zapada decyzja, tam następuje wykonanie bezpiecznego ruchu. W systemach Siemens te dwa elementy współpracują ze sobą przez PROFIsafe, ale pełnią skrajnie inne role.

Zestawienie kluczowych różnic:

1. Sterownik PLC Failsafe (Logika Bezpieczeństwa) – Sterownik (np. S7-1500F) pełni rolę „mózgu”. Zbiera informacje z zewnątrz i decyduje, co ma się stać z całą maszyną.

- Analiza sygnałów: Przetwarza dane z przycisków E-Stop, kurtyn świetlnych, rygli drzwi czy mat bezpieczeństwa.
- Logika złożona: Pozwala na programowanie zależności (np. „jeśli drzwi A są otwarte, to zatrzymaj tylko silnik nr 3, ale silnik nr 4 niech pracuje wolniej”).
- Koordynacja: Wysyła komendy do wielu falowników jednocześnie przez sieć PROFIsafe.
- Funkcje programowe: W TIA Portal używasz bloków takich jak, czy .ESTOP1SFDOORMUTING

2. Falownik SINAMICS (Wykonanie i Monitorowanie Ruchu) – Falownik pełni rolę „mięśni”. Nie wie, czy ktoś nacisnął E-Stop – on tylko wykonuje rozkaz zatrzymania lub zwolnienia otrzymany od PLC.

- Reakcja fizyczna: Odpowiada za bezpieczne odcięcie momentu obrotowego silnika () lub bezpieczne hamowanie ().STOSS1/SS2
- Monitorowanie parametrów: Falownik posiada wbudowane funkcje monitorujące ruch (np. czy prędkość nie przekracza bezpiecznego limitu SLS).
- Szybkość reakcji: Funkcje wbudowane w falownik reagują szybciej na błędy samego napędu (np. zwarcie) niż program w PLC.

Jak taki nowoczesny system współpracuje:

- Operator naciska E-StopPLC.
- PLC przelicza logikę i wysyła przez (Telegram 30) rozkaz do : „Aktywuj funkcję SS1”.PROFIsafeFalownika.
- Falownik przejmuje kontrolę: wyhamowuje silnik po rampie, a na końcu odcina moment obrotowy ().STO.
- Falownik odsyła do PLC status: „Silnik zatrzymany, moment odcięty”.

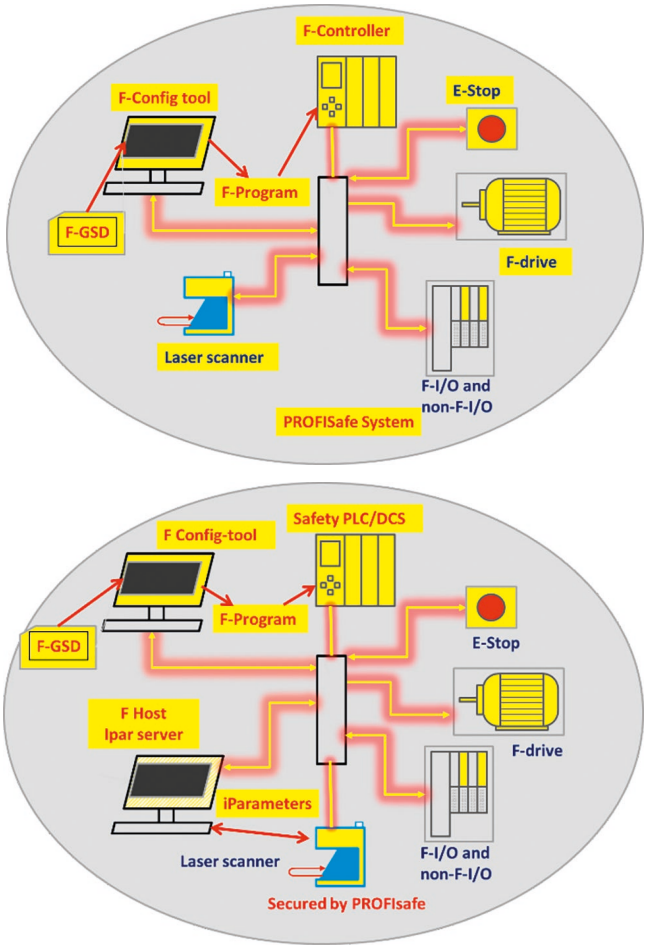
W systemach Siemens komunikacja realizowana jest poprzez wspomniany wcześniej profil PROFINET z funkcjami bezpieczeństwa PROFIsafe. Kluczem do zrozumienia tej komunikacji jest podział na warstwę sprzętową (kabel, switche) oraz warstwę logiczną (bezpieczny protokół).

Dzięki tej komunikacji, sterownik PLC może w czasie rzeczywistym aktywować zaawansowane funkcje wbudowane w falownik:

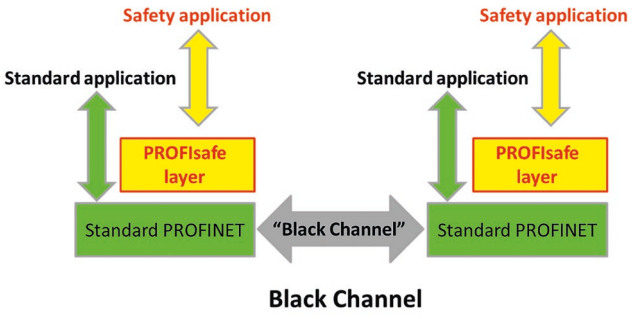
- STO (Bezpieczny moment obrotowy wyłączony): Bezzwłoczne odcięcie energii generującej moment obrotowy.
- SS1 (Bezpieczny Stop 1): PLC nakazuje falownikowi hamowanie po rampie, a po zatrzymaniu falownik sam aktywuje STO.
- SLS (Bezpiecznie Ograniczona Prędkość): PLC informuje falownik: „Teraz operator otworzył bramkę, monitoruj czy silnik nie przekracza 100 obr./min”. Jeśli silnik przekroczy limit, falownik samoczynnie go zatrzyma.

Tabela 4. Porównanie funkcji bezpieczeństwa dla PLC i falownika [12]

Cecha	Sterownik PLC (F-CPU)	Falownik (SINAMICS)
Typowe funkcje	E-Stop, kontrola drzwi, muting kurtyn, sterowanie kaskadowe.	STO (odcięcie momentu), (limity prędkości), (kierunek). SLSSDI
Obszar działania	Cały system / linia produkcyjna.	Konkretny silnik / oś.
Sygnały wejściowe	Wejścia bezpieczne (F-DI) z czujników.	Dane z enkodera (bezpieczne monitorowanie obrotów).
Główny cel	Realizacja logiki bezpieczeństwa maszyny.	Bezpieczne zatrzymanie lub ograniczenie ruchu osi.



Rys. 6. Rozwiązania komunikacji bezpieczeństwa PROFIsafe [10]



Rys. 8. Rozwiązania komunikacji bezpieczeństwa PROFIsafe [10]

3. Diagnostyka i Reintegracja

Komunikacja PROFINET Safety wymaga obsługi tzw. reintegracji. Jeśli np. odłączysz kabel sieciowy, sterownik PLC przejdzie w stan błędu (pasywny moduł).

- Po ponownym podłączeniu kabla komunikacja nie ruszy automatycznie.
- W programie F-PLC należy wywołać blok lub ustawić bit w bloku systemowym danego urządzenia, aby „potwierdzić", że kanał komunikacyjny jest znów bezpieczny.

Podsumowanie korzyści:

- Mniej kabli: Jeden przewód Ethernet zastępuje kilkanaście przewodów sterowniczych.
- Precyzyjna diagnostyka: W TIA Portal widzisz dokładnie, który bit bezpieczeństwa powoduje zatrzymanie maszyny.
- Elastyczność: Można zmieniać limity prędkości (SLS) dynamicznie z poziomu programu PLC.

11. Dokumentacja do maszyn w świetle Rozporządzenia 2023/1230 [12]

Brak dokumentacji to jeden z najczęstszych problemów przy audytach, ale z punktu widzenia prawa , nawet jeśli technicznie jest sprawna. Maszyna bez pełnej dokumentacji jest uznawana za niespełniającą wymagań bezpieczeństwa. Brak dokumentacji w następujący sposób wpływa na spełnienie wymagań w zależności od wieku maszyny:

1. Maszyny „stare" (sprzed 2004 r. – Minimalne Wymagania)

Jeśli maszyna nie ma znaku CE i została wyprodukowana przed wejściem Polski do UE, musi spełniać Minimalne Wymagania (Dyrektywa Narzędziowa). Wymagane minimum: nawet jeśli nie mamy instrukcji producenta, jako pracodawca, należy stworzyć instrukcję stanowiskową BHP. Ocena ryzyka: należy posiadać dokument potwierdzający przeprowadzenie kontroli (audytu) dostosowawczego. Brak tego dokumentu podczas kontroli PIP (Państwowej Inspekcji Pracy) skutkuje mandatem i nakazem natychmiastowego uzupełnienia.

2. Maszyny „nowe" (ze znakiem CE – Zasadnicze Wymagania). Dla tych maszyn brak dokumentacji jest krytyczny. Zgodnie przepisami, maszyna jest bezpieczna tylko wtedy, gdy towarzyszy jej:

- Deklaracja Zgodności WE: Dowód prawnego dopuszczenia do obrotu. Jeśli jej nie masz, nie masz pewności, czy producent w ogóle przeprowadził procedurę oceny zgodności.

- Instrukcja Oryginalna (i tłumaczenie): Musi zawierać informacje o konserwacji, przeglądach i ryzyku resztkowym. Bez niej serwisowanie maszyny jest działaniem „na oślep", co jest naruszeniem zasad bezpieczeństwa.
- Dokumentacja Techniczna (u producenta): jeśli producent zgubił dokumentację techniczną (analizę ryzyka, schematy), traci domniemanie zgodności i w razie wypadku nie ma dowodu, że maszyna została zaprojektowana bezpiecznie.

3. Skutki braków (Ryzyko prawne i techniczne):

- Domniemanie winy: W razie wypadku na maszynie bez dokumentacji, stosowne organy uznają, że pracodawca nie dopełnił obowiązku zapewnienia bezpiecznego stanowiska pracy (brak informacji o zagrożeniach).
- Problem z modernizacją: Jakakolwiek zmiana w maszynie bez schematów elektrycznych i analizy ryzyka jest skrajnie niebezpieczna i utrudnia wykonanie rzetelnej „istotnej modyfikacji" wg nowych przepisów.
- Brak możliwości odsprzedaży: Maszyna bez deklaracji zgodności i instrukcji nie może być legalnie sprzedana jako urządzenie kompletne.

Procedura naprawcza w kwestii dokumentacji:

- Odtworzenie instrukcji: można zlecić wyspecjalizowanej firmie przygotowanie nowej instrukcji obsługi i konserwacji na podstawie inwentaryzacji maszyny.
- Nowa ocena ryzyka: konieczne przeprowadzenie pełnego audytu bezpieczeństwa, który zastąpi brakującą dokumentację projektową w zakresie analizy zagrożeń.
- Weryfikacja dobiegu: konieczne wykonanie pomiarów dobiegometrem, aby potwierdzić, że systemy bezpieczeństwa działają poprawnie, co jest kluczowym elementem „dokumentacji zastępczej".

Poniżej główne punkty do opracowania przykładowej listy kontrolnej (checklista), która pomoże uporządkować stan bezpieczeństwa maszyny w przypadku braków w dokumentacji pierwotnej. Realizacja tych punktów pozwoli na stworzenie tzw., wymaganej podczas kontroli PIP lub audytów ubezpieczeniowych dokumentacji zastępczej:

1. Inwentaryzacja i Identyfikacja (Podstawa prawna).
2. Ocena Techniczna i Bezpieczeństwo (Zgodnie z PN-EN ISO 12100).
3. Wyposażenie Elektryczne i Mechaniczne.
4. Osłony i Środki Ochronne.
5. Dokumentacja Eksploatacyjna (Wymagana przez PIP).

Jeśli maszyna już pracuje w zakładzie, a dokumentacji programowej brak można również wykonać czynności takie jak:

- Backup „z natury": próba wykonania upload programu ze sterownika (o ile nie jest zablokowany hasłem). Należy pamiętać, że upload często nie zawiera komentarzy i nazw zmiennych, co utrudnia analizę.
- Walidacja „czarnoszynowa": Przeprowadzanie testów funkcjonalnych (tzw. *Black Box Testing*). Symulacja usterek i sprawdzanie reakcji maszyny, dokumentując to w protokole. To nie zastąpi kodu, ale jest dowodem, że sprawdzano działanie systemu.
- Pomiary dobiegu: Wykonanie pomiarów dobiegometrem. To kluczowy dowód na to, że niezależnie od tego, co jest w kodzie, maszyna fizycznie zatrzymuje się w bezpiecznym czasie.
- Umowy z dostawcami: Przy zakupie nowych maszyn należy wymagać przekazania i kopii projektów (TIA Portal, Starter itp.) jako warunków odbioru technicznego - niezablokowanych kodów źródłowych.

Należy również pamiętać, że brak interfejsu operatora (HMI) w języku polskim, to nie tylko kwestia wygody producenta, ale przede wszystkim naruszenie, które bezpośrednio rzutuje na bezpieczeństwo użytkowania maszyny i stanowi poważne naruszenie wymagań prawnych.

Opisane powyżej zagadnienia z pewnością są przedmiotem współpracy praktycznej wielu podmiotów posiadających maszyny z dostawcami rozwiązań bezpieczeństwa. Firmy Siemens, Pilz, Sick i inni producenci rozwiązań bezpieczeństwa posiadają bogate doświadczenie doradcze oraz oferują wykorzystanie gotowych, certyfikowanych zestawów do dostosowywania, retrofitów i modernizacji (np. kompletne zestawy do zabezpieczenia pras czy robotów), co skraca proces certyfikacji CE.

12. Rola instytucji: CIOP-PIB oraz PIP w procesie zapewnienia bezpieczeństwa

W Polsce kluczowymi filarami wiedzy i nadzoru są Centralny Instytut Ochrony Pracy (CIOP-PIB) oraz Państwowa Inspekcja Pracy (PIP).

- CIOP-PIB: Pełni rolę naukowo-badawczą. W dobie nowego rozporządzenia instytut ten dostarcza wytycznych dotyczących ergonomii oraz bezpieczeństwa systemów sterowania wykorzystujących AI. Publikacje CIOP są nieocenione przy interpretacji norm typu C dla specyficznych procesów (np. hałas, drgania).
- PIP: To organ nadzorczy, który weryfikuje stan faktyczny maszyn w zakładach. Inspektorzy PIP podczas kontroli opierają się na liście sprawdzającej wynikającej z tzw. Minimalnych Wymagań (dla maszyn sprzed 2003 r.) oraz Zasadniczych Wymagań (dla maszyn nowszych).

Nowe podejście UE idzie w parze z zaostrzeniem nadzoru rynku. Brak zgodności maszyny z wymaganiami to nie tylko ryzyko wypadku, ale i sankcje:

- Kary administracyjne: Organ nadzoru rynku może nałożyć karę pieniężną (często liczoną w tysiącach euro) oraz nakazać wycofanie maszyny z eksploatacji lub obrotu.
- Odpowiedzialność karna: Zgodnie z Art. 220 Kodeksu Karnego, osoba odpowiedzialna za bezpieczeństwo i higienę pracy, która nie dopełnia obowiązków i przez to naraża pracownika na bezpośrednie niebezpieczeństwo utraty życia albo ciężkiego uszczerbku na zdrowiu, podlega karze pozbawienia wolności do lat 3.
- Odpowiedzialność cywilna: Roszczenia odszkodowawcze pracowników w przypadku udowodnienia zaniedbań w procesie modernizacji (np. braku walidacji w SISTEMA) mogą być liczone w milionach złotych.

Podsumowanie

Warto zwrócić uwagę, że nadchodzące Rozporządzenie (UE) 2023/1230 rzuca nowe światło na definicję ‚istotnej modyfikacji'. Kluczowym wyzwaniem dla przemysłu staje się teraz precyzyjne wyznaczenie granicy odpowiedzialności przy modernizacjach – szczególnie gdy w grę wchodzą algorytmy autonomiczne i zdalny dostęp. Artykuł trafnie punktuje te zmiany, które są niezbędne dla zapewnienia bezpieczeństwa w dobie Industry 4.0. Z praktycznego punktu widzenia, najtrudniejszym elementem modernizacji maszyn pozostaje weryfikacja drogi hamowania po zmianie parametrów pracy. Nowe przepisy unijne wreszcie precyzują, kiedy modernizujący staje się producentem, co ma fundamentalne znaczenie dla działów utrzymania ruchu i zewnętrznych integratorów. Edukacja w zakresie cyberbezpieczeństwa maszyn to dziś nie opcja, a konieczność. Wprowadzenie wymogów dotyczących odporności systemów sterowania na ingerencję osób trzecich (zgodnie z nowym rozporządzeniem maszynowym) to ogromny krok w stronę realnej ochrony nie tylko procesów, ale przede wszystkim operatorów. Materiał ma charakter edukacyjny i należy traktować go w formie propozycji podjęcia działań przygotowawczych.

Literatura

[1] DYREKTYWA 2006/42/WE PARLAMENTU EUROPEJSKIEGO I RADY z dnia 17 maja 2006 r. wsprawie maszyn, zmieniająca dyrektywę 95/16/WE (przekształcenie) – l_15720060609pl00240086.pdf

[2] Akademia Elokon: Baza wiedzy bezpieczeństwo maszyn | Akademia ELOKON

[3] ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2023/1230 z dnia 14 czerwca 2023 r. w sprawie maszyn oraz w sprawie uchylenia dyrektywy 2006/42/WE Parlamentu Europejskiego i Rady i dyrektywy Rady 73/361/EWG – CL2023R1230PL0000010.0001_cp 1..1

[4] Rozporządzenie maszynowe 2023/1230 – co zmienia u producentów maszyn? – ELMARK - Rozporządzenie maszynowe 2023/1230 – co zmienia dla producentów? – Elmark Automatyka

[5] Nowe przepisy dotyczące maszyn – Ministerstwo Rozwoju i Technologii, Nowe przepisy dotyczące maszyn – Ministerstwo Rozwoju i Technologii – Portal Gov.pl

[6] FAQ – Rozporządzenie w sprawie maszyn 2023/1230 – JM SAFETY, FAQ – Rozporządzenie w sprawie maszyn 2023/1230

[7] Instrukcja obsługi i zakres zastosowania dobiegometru Safety Man firmy HHB Electronic – Safetyman DT3-page | SIMLOGIC.

[8] Wykaz jednostek notyfikowanych w Polsce – EUROPA – European Commission – Growth – Regulatory policy - SMCS

[9] Materiały dotyczące komunikacji PROFINET, standardy PROFISAFE i bezpieczeństwa maszyn firmy Siemens

[10] Standard PROFIsafe – Industrial Safety: PROFIsafe Profile Overview – PROFINET University

[11] Ustawa o Państwowej Inspekcji Pracy oraz publikacje CIOP-PIB „Bezpieczeństwo systemów sterowania maszynami".

[12] Materiały opracowane na bazie wspomagania przez AI Google GEMINI

Politechnika Łódzka
Katedra Aparatów Elektrycznych

dr inż. Mariusz Jabłoński
e-mail: mariusz.jablonski@p.lodz.pl
Katedra Aparatów Elektrycznych
Wydział Elektrotechniki, Elektroniki, Informatyki i Automatyki
Politechnika Łódzka