

CYBERBEZPIECZEŃSTWO DŹWIGÓW, SCHODÓW I CHODNIKÓW RUCHOMYCH

Nowy filar bezpieczeństwa technicznego



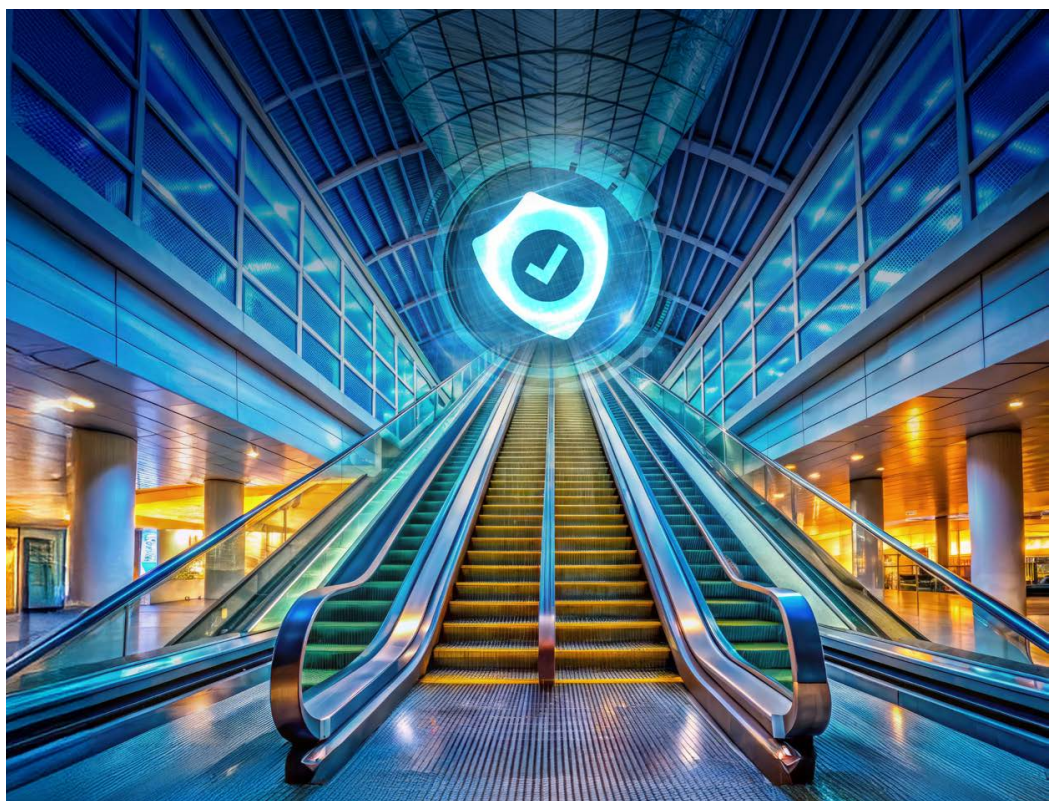
**MGR INŻ.
GRZEGORZ BACA**

Starszy Specjalista
Urzędzeń Transportu Bliskiego
Biuro w Tarnowie
Oddział w Krakowie
Urząd Dozoru Technicznego



**MGR INŻ.
PAWEŁ RAJEWSKI**

Kierownik Wydziału
Urzędzeń Technicznych
Departament Techniki
Urząd Dozoru Technicznego



Czy dźwig może zostać zhakowany? Jakie zagrożenia niesie za sobą podłączenie dźwigu lub schodów ruchomych do sieci? Czy system sterowania schodami ruchomymi jest odporny na atak z zewnątrz? Jeszcze kilka lat temu te pytania brzmiały jak scenariusz science fiction. Dziś to realne wyzwania, z którymi mierzy się cały sektor urządzeń transportu bliskiego.

Cyfryzacja branży dźwigowej stała się faktem. Nowoczesne dźwigi, schody i chodniki ruchome coraz częściej wyposażane są w zaawansowane systemy sterowania, zdalne zarządzanie, komunikację z BMS (ang. Building Management System) lub chmurą. Te rozwiązania zwiększają funkcjonalność i komfort, ale jednocześnie otwierają drzwi dla nowych zagrożeń – ataków cybernetycznych. Cyberbezpieczeństwo przestało być domeną wyłącznie bankowości, IT czy przemysłu energetycznego. Dziś dotyczy także dźwigu w biurze, schodów w centrum handlowym czy platformy w metrze i stanowi istotny element dyskusji o bezpieczeństwie eksploatacyjnym tych urządzeń.

Poziomy i zasady bezpieczeństwa

Systemy sterowania dźwigami, szczególnie te wyposażone w komponenty cyfrowe i podłączone do sieci, mogą stać się celem ataków hakerskich. Naruszenie ich integralności może prowadzić nie tylko do zakłóceń działania, ale w skrajnych przypadkach – do zagrożenia dla życia i zdrowia ludzi. W odpowiedzi na te ryzyka Komisja Europejska przyjęła Cyber Resilience Act – rozporządzenie, które od grudnia 2024 roku wprowadza obowiązki w zakresie

Kluczowym dokumentem uzupełniającym nowe przepisy jest norma ISO 8102-20:2022 [1], stanowiąca pierwsze kompleksowe opracowanie wymagań cyberbezpieczeństwa dla dźwigów, schodów i chodników ruchomych.



Określa ona m.in. zasady bezpiecznego projektowania (Secure by Design), zarządzania incydentami, segmentacji sieci, testowania systemów oraz ich bezpiecznego wycofania z eksploatacji. Wprowadza także pojęcie Secure Development Lifecycle (SDL), czyli cyklu życia produktu zintegrowanego z wymaganiami bezpieczeństwa.

Norma ISO 8102-20 bazuje na dojrzałych rozwiązaniach znanych z automatyki przemysłowej, jak np. seria IEC 62443 [2]. Uwzględnia poziomy bezpieczeństwa dla poszczególnych funkcji systemu sterowania – od funkcji bezpieczeństwa (SL3), przez podstawowe (SL2), po funkcje alarmowe (SL1). Tym samym definiuje precyzyjne wymagania dla każdej warstwy funkcjonalnej systemu.



Od grudnia
2027 roku

Wdrożenie tych zasad stanie się koniecznością, zwłaszcza że od grudnia 2027 roku ich stosowanie stanie się obowiązkowe przy wprowadzaniu urządzeń na rynek.

Wymagania normy

Nowa norma ISO 8102-20:2022 [1] opracowana przez Międzynarodową Organizację Normalizacyjną ISO dotyczy właśnie cyberbezpieczeństwa. Wraz ze wzrostem liczby zastosowań zdalnych i internetu rzeczy (Internet of things IoT) w dźwigach, schodach ruchomych i chodnikach ruchomych jest to jak najbardziej odpowiedni czas na wydanie standardu w zakresie cyberbezpieczeństwa.

Specyfikacja [1] określa wymagania cyberbezpieczeństwa dla nowych dźwigów, schodów ruchomych i chodników ruchomych, określanych jako „sprzęt pod kontrolą” (EUC. Ang. Equipment under control), zaprojektowany zgodnie z serią norm dźwigowych ISO 8100. Norma ma również zastosowanie do innych norm dotyczących dźwigów, schodów ruchomych i chodników ruchomych, które określają podobne wymagania, a także do innego sprzętu związanego z dźwigami podłączonego do EUC.

W normie ISO 8102-20:2022 określono wymagania dotyczące produktów i systemów związanych z zagrożeniami cyberbezpieczeństwa podczas projektowania produktu (wymagania dotyczące procesu i produktu), produkcji, instalacji, eksploatacji i konserwacji oraz likwidacji.

W normie ISO 8102-20:2022 omówiono też rolę dostawcy produktu i integratora systemów dla EUC. Norma definiuje wymagania dla dostawcy produktu i integratora systemów EUC w celu stworzenia dokumentacji umożliwiającej właścicielowi osiągnąć i utrzymać bezpieczeństwo EUC. Określono w normie minimalne wymagania cyberbezpieczeństwa dla podstawowych funkcji bezpieczeństwa oraz funkcji alarmowych.

Norma ISO 8102-20:2022 ma zastosowanie do EUC, które mogą łączyć się z systemami zewnętrznymi, takimi jak sieci budynkowe, usługi w chmurze lub narzędzia serwisowe. Możliwość podłączenia może wynikać ze sprzętu stale dostępnego na miejscu lub sprzętu tymczasowo dostarczonego na miejsce na etapie instalacji, obsługi i konserwacji lub wycofania z eksploatacji.

Norma określa minimalne wymagania cyberbezpieczeństwa dla funkcji:

- zasadniczych (użytkowanie dźwigów, schodów ruchomych lub chodników ruchomych),
- bezpieczeństwa (dla ochrony przed niebezpieczeństwem),
- alarmowych (uruchomienie alarmu i nawiązanie łączności ze służbami ratowniczymi w przypadku awarii).

Norma ISO 8102-20:2022 ma trzy poziomy bezpieczeństwa. W przypadku funkcji bezpieczeństwa należy zastosować ścisły poziom bezpieczeństwa 3, w przypadku funkcji alarmowych wystarczający jest poziom bezpieczeństwa 1.

W projekcie normy EN ISO 8100-1:2019 [3] jest odniesienie do ISO 8102-20:2022, co wskazuje, że zasadnicze wymagania zawarte w 1.1.9 i 1.2.1 rozporządzenia maszynowego [4] są częściowo już uwzględnione. Poniżej fragment załącznika ZA.3.

Essential health and safety requirements of Annex 1 to Directive 2006/42/EC	Clause(s)/sub-clause(s) of this EN	Remarks/Notes
1.1.2 (a)	4, 5, 6	
...	...	
1.1.9	Clause referencing ISO 8102-20, clause 5 Clause of ISO 8100-1 having requirements for "easily accessible sw identification"	
1.2.1	4.9.2.2.3 a), 4.9.2.5, 4.9.3.4, 4.10.3, 4.11, 4.12, Annex A	I

Cyberbezpieczeństwo dźwigów to nie tylko problem producenta. To temat, który dotyczy konserwatorów, administratorów budynków, projektantów, a także jednostek notyfikowanych w ramach procedur oceny zgodności.

Literatura:

1. ISO 8102-20:2022 Electrical requirements for lifts, escalators and moving walks Part 20: Cybersecurity
2. Seria IEC 62443 Industrial Communication Networks – Networks and System Security
3. EN ISO 8100-1:2019 Lifts for the transport of persons and goods Part 1: Safety rules for the construction and installation of passenger and goods passenger lifts
4. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1230 z dnia 14 czerwca 2023 r. w sprawie maszyn oraz w sprawie uchylecia dyrektywy 2006/42/WE Parlamentu Europejskiego i Rady i dyrektywy Rady 73/361/EWG
<https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CE-LEX:32023R1230>
[dostęp: 6.2025]
[https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CE-LEX:32023R1230R\(01\)](https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CE-LEX:32023R1230R(01))
[dostęp: 6.2025]