Dawid Gądkowski
email: dgadkowski@wsb-nlu.edu.pl
ORCID: 0009-0005-2841-8323
Wyższa Szkoła Biznesu – National Louis University

Analiza kierunku rozwoju oraz zastosowania systemów wbudowanych

Analysis of the Direction of Development and Applications of Embedded Systems

DOI: 10.66935/978-83-65926-17-3.19

© 2025 Dawid Gądkowski
Praca opublikowana na licencji Creative Commons Uznanie autorstwa – Na tych samych warunkach 4.0 Międzynarodowe (CC BY-SA 4.0).
Treść licencji dostępna jest pod adresem: https://creativecommons.org/licenses/by-sa/4.0/deed.pl

Cytuj jako: Gądkowski, D. (2025). Analiza kierunku rozwoju oraz zastosowania systemów wbudowanych. W: J. Lizak, M. W. Sidor (red.), *Nowe wyzwania w naukach społecznych i technicznych: podejście interdyscyplinarne* (T. 2). (s. 299-309). Wydawnictwo WSB-NLU.

Streszczenie: Systemy wbudowane stanowią fundament współczesnej automatyki oraz elektroniki, będąc nieodłącznym elementem prawie każdego urządzenia elektronicznego – od sprzętu użytku domowego, przez urządzenia medyczne, po autonomiczne pojazdy i infrastrukturę krytyczną. Artykuł przedstawia analizę: systemów wbudowanych, architektury, metody projektowania, obszarów zastosowań oraz aktualnych trendów rozwojowych. Omówiono również wyzwania związane z bezpieczeństwem, energooszczędnością i integracją z systemem IoT. Celem artykułu jest ujęcie aktualnego stanu wiedzy oraz wskazanie przyszłych kierunków rozwoju tej szybko rozwijającej się dziedzinie elektroniki.

Abstract: Embedded systems currently form the foundation of modern automation and electronics, being an integral part of nearly every electronic device-from household appliances and medical equipment to autonomous vehicles and critical infrastructure. This article presents an analysis of embedded systems, their architectures, design methodologies, application areas, and current development trends. It also discusses challenges related to security, energy efficiency, and integration with IoT systems. The aim of the article is to summarize the current state of knowledge and to indicate future directions for the development of this rapidly evolving field of electronics.

Słowa kluczowe: systemy wbudowane, mikrokontrolery, IoT, elektronika, cyberbezpieczeństwo

Keywords: embedded systems, microcontrollers, IoT, electronics, cybersecurity

Wprowadzenie

Systemy wbudowane stały się jednym z podstawowych elementów współczesnej elektroniki i automatyki. W przeciwieństwie do komputerów ogólnego przeznaczenia są one skierowane do wykonywania wąsko zdefiniowanych zadań w większych urządzeniach technicznych lub instalacjach. Ich dedykowany charakter umożliwia optymalizację funkcjonalności, niezawodności, zużycia energii i kosztów wdrożenia dla konkretnej aplikacji (Wolf, 2007; Henschen i Lee, 2023).

Obecnie systemy wbudowane są stosowane w szerokiej gamie rozwiązań, w tym w urządzeniach gospodarstwa domowego, przemysłowych systemach sterowania, urządzeniach medycznych, elektronice samochodowej i inteligentnych urządzeniach sieciowych. Ich rola nadal rośnie wraz z rozwojem Internetu Rzeczy, przetwarzania brzegowego, sztucznej inteligencji i technologii autonomicznych. Z tego powodu systemy wbudowane są obecnie uznawane nie tylko za jednostki sterujące, ale także za ważne elementy nowoczesnej infrastruktury cyfrowej (Elhanashi i in., 2024; Fabre i in., 2024; Heydari i Mahmoud, 2025). Celem artykułu jest omówienie charakterystyki systemów wbudowanych, ich architektury, zastosowań, metod projektowania i wyzwań technologicznych we współczesnym świecie.

Chociaż systemy wbudowane zostały szeroko opisane w literaturze, wiele dostępnych badań koncentruje się wyłącznie na wybranych aspektach, takich jak architektura sprzętu, kontrola w czasie rzeczywistym, komunikacja IoT lub cyberbezpieczeństwo. Nadal istnieje potrzeba przeprowadzenia syntetycznego i aktualnego badania, które zintegruje te perspektywy i przedstawi systemy wbudowane nie tylko jako elementy techniczne, ale także jako kluczowe elementy nowoczesnej infrastruktury cyfrowej. W związku z tym, celem niniejszego artykułu jest przedstawienie ustrukturyzowanego przeglądu architektury, metod projektowania, obszarów zastosowań i aktualnych trendów rozwojowych systemów wbudowanych, ze szczególnym uwzględnieniem cyberbezpieczeństwa, efektywności energetycznej i integracji IoT.

Systemy wbudowane – definicje, klasyfikacja i architektura

Definicja systemów wbudowanych

Systemy wbudowane stanowią odrębną kategorię systemów komputerowych przeznaczonych do wykonywania określonych funkcji w ramach większego urządzenia, maszyny lub procesu technicznego. W przeciwieństwie do uniwersalnych platform obliczeniowych są one opracowywane do jasno określonych zadań operacyjnych, takich jak kontrola, pomiar, nadzór lub komunikacja. W wielu przypadkach ich działanie pozostaje niewidoczne dla użytkownika końcowego, ponieważ funkcjonują one jako wewnętrzna część szerszego rozwiązania technicznego. Jednocześnie oczekuje się, że takie systemy zapewnią niezawodne i powtarzalne działanie przy szczególnych ograniczeniach środowiskowych i funkcjonalnych (Wolf, 2007).

Z technicznego punktu widzenia system wbudowany można rozumieć jako zintegrowaną strukturę sprzętu i oprogramowania, która obejmuje jednostkę przetwarzania, zasoby pamięci i interfejsy wejścia-wyjścia wykorzystywane do interakcji z otaczającym środowiskiem. Takie systemy są zwykle opracowywane pod ścisłymi ograniczeniami związanymi z wydajnością, pojemnością pamięci, zużyciem energii, wielkością fizyczną i niezawodnością. Charakterystyczną cechą wielu wbudowanych implementacji jest zastosowanie mikrokontrolerów, które łączą przetwarzanie, pamięć i funkcje peryferyjne w jednym chipie. W rezultacie systemy wbudowane są zazwyczaj związane z dedykowaną funkcjonalnością, ograniczonymi zasobami, długoterminową autonomiczną pracą i częstymi wymaganiami w czasie rzeczywistym (Henschen i Lee, 2023).

Klasyfikacja według zastosowania

Systemy wbudowane mogą być klasyfikowane zgodnie z obszarem ich zastosowań, co pozwala na lepsze zrozumienie ich przeznaczenia i specyfiki projektu. Jedną z najważniejszych grup są systemy sterowania. Odpowiadają za zarządzanie procesami fizycznymi i technologicznymi w czasie rzeczywistym. Są one często stosowane w automatyce przemysłowej, liniach produkcyjnych i systemach zrobotyzowanych, gdzie wykonują określone zadania związane z regulacją parametrów pracy maszyny, synchronizacją ruchów i kontrolą bezpieczeństwa.

Drugą ważną kategorię tworzą systemy pomiarowe, których głównym zadaniem jest pozyskiwanie, przetwarzanie i rejestrowanie danych pochodzących z różnego rodzaju czujników zewnętrznych lub wewnętrznych. Systemy te są wykorzystywane w monitorowaniu, diagnostyce technicznej, energetyce i sprzęcie badawczym.

Kolejna grupa składa się z systemów multimedialnych, odpowiedzialnych za przetwarzanie sygnałów audio i wideo, które są obecne w telefonach, aparatach cyfrowych, telewizorach, konsolach do gier i innych urządzeniach mobilnych.

Wyróżnia się również systemy bezpieczeństwa, których zadaniem jest ochrona mienia i życia ludzkiego poprzez wdrożenie funkcji ostrzegawczych, kontroli dostępu i nadzoru wideo, a także systemy komunikacyjne umożliwiające transmisję danych między urządzeniami w sieciach lokalnych i rozległych, które stanowią podstawę działania routerów, modemów, urządzeń sieciowych oraz infrastruktury IoT.

Klasyfikacja według wymagań czasowych

Wymogi związane z czasem są jednym z kluczowych kryteriów stosowanych przy klasyfikacji systemów wbudowanych. W wielu aplikacjach poprawność działania systemu zależy nie tylko od logicznej dokładności wyniku, ale także od czasu, w którym generowana jest odpowiedź. Z tego powodu systemy wbudowane są powszechnie podzielone na twarde systemy czasu rzeczywistego, miękkie systemy czasu rzeczywistego i systemy bez krytycznych ograniczeń czasowych (Dritsas i Trigka, 2025).

W trudnych systemach czasu rzeczywistego każde zadanie musi zostać wykonane w ściśle określonym terminie. Utrata terminu jest traktowana jako awaria, ponieważ może prowadzić do niebezpiecznej eksploatacji, utraty kontroli lub poważnych konsekwencji technicznych. Takie wymagania są typowe dla zastosowań o krytycznym znaczeniu dla bezpieczeństwa, w tym wybranych systemów przemysłowych, motoryzacyjnych i medycznych (Heydari i Mahmoud, 2025).

Miękkie systemy czasu rzeczywistego działają również zgodnie z wymaganiami związanymi z czasem, ale sporadyczne opóźnienia nie powodują natychmiast awarii systemu. Zamiast tego zwykle skutkują obniżoną jakością działania lub niższą wydajnością usługi. Grupa ta obejmuje na przykład systemy multimedialne i systemy transmisji danych, w których tymczasowe odchylenia czasu mogą być zauważalne, ale nie są katastrofalne (Fabre i in., 2024).

Trzecia kategoria obejmuje systemy, w których czas nie jest dominującym ograniczeniem projektowym. W takich rozwiązaniach główne priorytety mogą obejmować poprawność, prostotę, efektywność energetyczną lub niskie koszty wdrożenia, a nie deterministyczny czas reakcji. Można to zaobserwować w wielu nieskomplikowanych urządzeniach konsumenckich i monitorujących (Mustafa i in., 2024).

W praktyce jednak rozróżnienie między twardymi i miękkimi systemami czasu rzeczywistego nie zawsze jest w pełni jednoznaczne, ponieważ wiele współczesnych aplikacji wbudowanych łączy funkcje krytyczne dla bezpieczeństwa z niekrytycznymi zadaniami komunikacji i obsługi użytkownika. Dlatego projektanci systemów często muszą równoważyć determinizm czasowy ze złożonością funkcjonalną i ograniczeniami kosztów.

Architektura sprzętu i oprogramowania

Architektura systemu wbudowanego zakłada ściśle zintegrowaną część sprzętową i programową, które razem wykonują przypisane funkcje urządzenia (Wolf, 2007). Część sprzętowa składa się zwykle z mikrokontrolera lub mikroprocesora zawierającego jednostkę centralną, pamięć operacyjną i pamięć programu, a także jednostki wejścia-wyjścia umożliwiające komunikację z czujnikami, siłownikami i innymi modułami. W zależności od przeznaczenia system może być dodatkowo wyposażony w dodatkowy obwód komunikacyjny, moduł zarządzania zasilaniem lub inne zabezpieczenia sprzętowe.

Część oprogramowania jest odpowiedzialna za kontrolowanie działania całego urządzenia i implementuje określone algorytmy, często w ścisłym związku z ograniczeniami sprzętowymi i wymaganiami czasowymi (Elhanashi i in., 2024). Składa się z programu startowego, możliwego systemu operacyjnego w czasie rzeczywistym i ostatecznej aplikacji. To oprogramowanie zarządza zasobami sprzętowymi, obsługuje przerwy, wykonuje komunikację i zapewnia ścisłą pracę systemu zgodnie z przyjętymi wymaganiami funkcjonalnymi i czasowymi. Jednak wybór architektury systemu zawsze wiąże się z kompromisami inżynierskimi. Zwiększenie wydajności obliczeniowej i możliwości komunikacyjnych zwykle poprawia funkcjonalność systemu, ale może również zwiększyć zużycie energii,

koszty wdrożenia i złożoność projektu. Z tego powodu architekturę systemu wbudowanego należy rozpatrywać nie tylko pod względem wykonalności technicznej, ale także w odniesieniu do niezawodności, możliwości utrzymania i wymogów bezpieczeństwa.

Cykl projektowania systemu i języki programowania

Projektowanie systemu wbudowanego to złożony proces. Łączy zagadnienia elektroniki, informatyki i automatyki. Jego podstawą jest dogłębna analiza wymagań funkcjonalnych i środowiskowych, na podstawie których dobierana jest architektura sprzętowa i programowa. Istotnym elementem jest również określenie ograniczeń związanych z kosztami lub zużyciem energii i niezawodnością, które w dużym stopniu wpływają na wybór komponentów i technologii.

W praktyce projektowanie odbywa się etapami, często z wykorzystaniem ustrukturyzowanych podejść do rozwoju, takich jak model V, obejmujących analizę, projektowanie, wdrażanie, a także testowanie i uruchamianie systemu (Henschen i Lee, 2023). W części oprogramowania wykorzystywane są głównie języki C i C++, a coraz częściej także Rust, które umożliwiają bezpośredni dostęp do urządzeń peryferyjnych i wydajne zarządzanie pamięcią w środowiskach o ograniczonych zasobach (Heydari i Mahmoud, 2025). Ważnym aspektem jest również testowanie systemu w warunkach zbliżonych do docelowych, co pozwala na wczesne wykrywanie błędów i zapewnia stabilną pracę gotowego urządzenia.

Zastosowania systemów wbudowanych

Systemy wbudowane mają szerokie zastosowanie zarówno w życiu codziennym, jak i w przemyśle, stanowiąc nieodłączną część większości urządzeń elektronicznych. W automatyce przemysłowej są szeroko stosowane do sterowania maszynami, liniami produkcyjnymi, a także robotami przemysłowymi i autonomicznymi. Odpowiadają tam za realizację zadań kontrolnych, monitorowanie parametrów operacyjnych, gromadzenie danych oraz zapewnienie ciągłości procesów technologicznych.

Systemy wbudowane występują również w przemyśle motoryzacyjnym, gdzie odgrywają ważną rolę w zarządzaniu pracą silnika, układu hamulcowego, systemów wspomagania kierowcy, a także są stosowane w nowoczesnych pojazdach autonomicznych. W medycynie znajdują zastosowanie w sprzęcie diagnostycznym i urządzeniach podtrzymujących życie, m.in. takich jak pompy infuzyjne czy monitory życia pacjenta, gdzie wymagana jest wysoka precyzja i skuteczność działania, a także niezawodność. Są one również powszechnie spotykane w elektronice użytkowej, w tym smartfonach, telewizorach, systemach inteligentnego domu i sprzęcie multimedialnym, w których są odpowiedzialne za obsługę funkcji użytkownika i komunikację z innymi urządzeniami.

Różnorodność tych aplikacji pokazuje, że systemów wbudowanych nie można projektować według jednego uniwersalnego modelu. Wymagania związane z czasem, nieza-

wodnością, bezpieczeństwem, zużyciem energii i komunikacją różnią się znacznie między aplikacjami konsumenckimi, przemysłowymi, motoryzacyjnymi i medycznymi, co sprawia, że kontekst aplikacji jest jednym z kluczowych czynników w procesie projektowania.

Wyzwania bezpieczeństwa w systemach wbudowanych

Bezpieczeństwo stało się jednym z głównych wyzwań projektowych w systemach wbudowanych, zwłaszcza że więcej urządzeń jest podłączonych do sieci lokalnych, platform w chmurze i usług internetowych. W przeszłości wiele rozwiązań wbudowanych działało w stosunkowo odizolowanych środowiskach. Obecnie jednak łączność sieciowa znacznie zwiększyła ich narażenie na nieautoryzowany dostęp, manipulację oprogramowaniem, przechwytywanie danych i ataki zdalne (Fagan i in., 2020; Zhou i in., 2023; Dritsas i Trigka, 2025).

Zagrożenie bezpieczeństwa jest szczególnie istotne w urządzeniach o ograniczonych zasobach obliczeniowych i pamięciowych, w których wdrożenie zaawansowanych mechanizmów ochronnych może być technicznie ograniczone. Dodatkowe problemy wynikają ze słabych metod uwierzytelniania, niewystarczających mechanizmów aktualizacji i długiego okresu eksploatacji urządzeń wdrożonych w terenie. Jest to szczególnie widoczne w systemach IoT, które często pozostają stale połączone i działają przy minimalnym nadzorze użytkownika (Zhou i in., 2023; ETSI, 2024; Dritsas i Trigka, 2025).

Aby zmniejszyć te zagrożenia, współczesne systemy wbudowane w coraz większym stopniu wykorzystują bezpieczne procedury rozruchowe, metody szyfrowania, mechanizmy kontroli dostępu, podpisy cyfrowe i możliwości zdalnej aktualizacji oprogramowania. W rezultacie cyberbezpieczeństwo nie jest już traktowane jako opcjonalne rozszerzenie, ale jako podstawowy wymóg projektowy, który należy uwzględnić w całym cyklu życia systemu (Fagan i in., 2020; ETSI, 2024; Zhou i in., 2023).

Jednocześnie zapewnienie wysokiego poziomu cyberbezpieczeństwa w systemach wbudowanych pozostaje szczególnie trudne, ponieważ same mechanizmy ochronne zużywają zasoby sprzętowe i mogą wpływać na wydajność, koszty i efektywność energetyczną. Oznacza to, że bezpieczeństwo w systemach wbudowanych powinno być traktowane jako ograniczenie projektowe, które należy zoptymalizować wraz z funkcjonalnością i wymaganiami w czasie rzeczywistym, a nie jako odizolowana funkcja techniczna.

Efektywność energetyczna w systemach wbudowanych

Efektywność energetyczna jest jedną z głównych kwestii w projektowaniu systemów wbudowanych, zwłaszcza w urządzeniach zasilanych bateriami lub rozmieszczonych w miejscach, w których konserwacja jest trudna, a wymiana źródła zasilania jest ograniczona. W takich przypadkach zmniejszenie zużycia energii bezpośrednio wpływa na żywotność, niezawodność i praktyczną użyteczność urządzenia (Mustafa i in., 2024; Elhanashi i in., 2024).

Na poziomie sprzętowym efektywność energetyczna poprawia się dzięki zastosowaniu mikrokontrolerów małej mocy, selektywnej aktywacji modułów peryferyjnych oraz starannemu doborowi czujników i interfejsów komunikacyjnych. Bezprzewodowa transmisja danych jest często jedną z najbardziej wymagających operacji, dlatego wiele systemów zaprojektowano tak, aby zminimalizować czas komunikacji i przesyłać dane tylko w razie potrzeby (Mustafa i in., 2024; Elhanashi i in., 2024).

Na poziomie oprogramowania oszczędność energii osiąga się poprzez skrócenie aktywnego czasu procesora, stosowanie pracy z przerwami zamiast ciągłego głosowania i przełączanie systemu na tryb uśpienia lub tryb niskiego poboru mocy, gdy pełna aktywność nie jest wymagana. W bardziej zaawansowanych rozwiązaniach stosuje się również dynamiczną adaptację częstotliwości zegara i napięcia zasilania. W praktyce projektowanie energooszczędnych systemów wbudowanych wymaga zrównoważenia niskiego zużycia energii z oczekiwaną wydajnością, zdolnością komunikacyjną i czasem reakcji (Mustafa i in., 2024).

Z praktycznego punktu widzenia poprawa efektywności energetycznej rzadko jest odosobnionym celem, ponieważ niższe zużycie energii może odbywać się kosztem wydajności obliczeniowej, częstotliwości komunikacji lub czasu reakcji. W rezultacie projektowanie systemów wbudowanych o niskim poborze mocy wymaga kompromisu między autonomią operacyjną a oczekiwaniami funkcjonalnymi aplikacji docelowej.

Integracja z Internetem Rzeczy

Integracja systemów wbudowanych z Internetem Rzeczy rozszerza ich rolę poza lokalną kontrolę i umożliwia im wymianę danych z bramami, serwerami, platformami w chmurze i aplikacjami użytkownika. W ten sposób urządzenia wbudowane stają się elementami większych rozproszonych środowisk, w których dane mogą być gromadzone, przetwarzane i wykorzystywane do monitorowania, automatyzacji i wspierania decyzji (Fagan i in., 2020; Mustafa i in., 2024; Dritsas i Trigka, 2025).

Taka integracja wymaga doboru technologii komunikacyjnych odpowiednich dla danej aplikacji. W zależności od założeń projektowych systemy wbudowane mogą wykorzystywać rozwiązania przewodowe, takie jak Ethernet lub technologie bezprzewodowe, takie jak Wi-Fi, Bluetooth Low Energy, Zigbee, Thread lub komunikacja komórkowa. W praktyce wybór ten zależy od wymaganego zakresu, przepustowości, zużycia energii i złożoności systemu (Mustafa i in., 2024).

Warstwa oprogramowania systemów wbudowanych obsługujących IoT jest powszechnie oparta na lekkich protokołach komunikacyjnych dostosowanych do urządzeń z ograniczeniami. MQTT jest często używany w telemetrii i komunikacji opartej na zdarzeniach, podczas gdy CoAP jest przeznaczony do interakcji niskonapowietrznych w środowiskach o ograniczonych zasobach. W innych przypadkach można również użyć HTTP lub HTTPS, zwłaszcza gdy potrzebna jest bezpośrednia komunikacja internetowa. Integracja IoT wprowadza jednak również większą złożoność projektu, ponieważ

komunikacja, interoperacyjność, cyberbezpieczeństwo, zdalna diagnostyka i możliwość aktualizacji muszą być rozpatrywane łącznie (Fagan i in., 2020; ETSI, 2024; Mustafa i in., 2024; Dritsas i Trigka, 2025).

Dlatego integracja IoT nie powinna być rozumiana wyłącznie jako rozszerzenie funkcjonalności komunikacji, ale także jako źródło nowej złożoności projektu. Konieczność zapewnienia interoperacyjności, długoterminowej konserwacji oprogramowania i odporności na cyberzagrożenia sprawia, że systemy wbudowane oparte na IoT są znacznie bardziej wymagające niż izolowane rozwiązania wbudowane.

Przyszłe kierunki rozwoju

Na przyszły rozwój systemów wbudowanych duży wpływ ma postęp w elektronice, automatyce, telekomunikacji i inżynierii komputerowej. Jednym z najbardziej widocznych trendów jest rosnąca integracja platform wbudowanych ze sztuczną inteligencją i metodami uczenia maszynowego. Ponieważ możliwości przetwarzania stale się poprawiają, więcej urządzeń wbudowanych jest w stanie wykonywać wybrane zadania analityczne lokalnie, w tym rozpoznawanie wzorców, wykrywanie anomalii i interpretację danych z czujników. Zmniejsza to zależność od infrastruktury chmury i wspiera szybszą reakcję systemu w aplikacjach wrażliwych na czas (Elhanashi i in., 2024; Fabre i in., 2024; Heydari i Mahmoud, 2025).

Inną ważną tendencją jest rosnąca rola przetwarzania brzegowego, w którym urządzenia wbudowane nie służą już tylko jako pasywne jednostki akwizycji danych, ale także uczestniczą we wstępnej analizie i lokalnym podejmowaniu decyzji. Jest to szczególnie ważne w zastosowaniach, w których wymagana jest szybka reakcja, zmniejszone opóźnienia transmisji i ograniczona zależność od przetwarzania w chmurze, w tym automatyzacja przemysłowa, inteligentne monitorowanie i systemy autonomiczne (Fabre i in., 2024; Heydari i Mahmoud, 2025).

Kolejnym kierunkiem rozwoju jest rosnące znaczenie autonomicznych systemów wbudowanych. Autonomiczne systemy wbudowane są w stanie samodzielnie dostosować się do zmieniających się warunków pracy. Dotyczy to przede wszystkim pojazdów autonomicznych, dronów, robotów mobilnych i przemysłowych, a także inteligentnych systemów logistycznych. W takich aplikacjach systemy wbudowane przetwarzają dane z wielu czujników, jednocześnie wdrażając zaawansowane algorytmy obliczeniowe i decyzyjne, a także komunikując się z innymi urządzeniami systemu w czasie rzeczywistym. Prowadzi to do coraz większych wymagań dotyczących mocy obliczeniowej, niezawodności i bezpieczeństwa pracy urządzeń.

Nieodłącznym elementem przyszłego rozwoju jest również cyberbezpieczeństwo systemów wbudowanych. Staje się integralną częścią projektowania systemów wbudowanych już na etapie początkowej koncepcji. Wraz ze wzrostem liczby urządzeń podłączonych do projektowanej sieci rośnie znaczenie mechanizmów sprzętowych i programowych wspierających bezpieczeństwo. Moduły takie jak TPM, bezpieczne enklawy pamięci

lub sprzętowe generatory liczb losowych są tutaj ważne. Jednocześnie opracowywane są standardy i normy systemowe, które wspierają ujednolicenie wymogów bezpieczeństwa w obszarach takich, jak motoryzacja, medycyna i przemysł.

Ważnym elementem rozwojowym jest również dalsza miniaturyzacja i integracja złożonych funkcji w pojedyncze układy scalone systemu wbudowanego. Najnowsze rozwiązania system-on-chip łączą procesor, pamięć, moduł komunikacyjny i akceleratory obliczeniowe w jednym urządzeniu, co wspiera rosnącą rolę kompaktowych i inteligentnych platform wbudowanych (Henschen i Lee, 2023; Fabre i in., 2024). Pozwala to na zmniejszenie wielkości urządzenia, obniżenie kosztów produkcji oraz poprawę efektywności energetycznej. Pomimo tych zalet rosnąca integracja funkcji w rozwiązaniach jednoukładowych może również zmniejszyć przejrzystość projektu i utrudnić walidację, aktualizację i diagnostykę usterek. W związku z tym przyszły rozwój systemów wbudowanych będzie wymagał nie tylko bardziej zaawansowanego sprzętu, ale także lepszych metod projektowania w celu zarządzania rosnącą złożonością funkcjonalną. Jednocześnie opracowywane są technologie umożliwiające pozyskiwanie energii ze środowiska, takie jak ogniwa fotowoltaiczne, generatory piezoelektryczne czy generatory termiczne, co w przyszłości doprowadzi do powstania systemów wbudowanych zdolnych do pracy przez wiele lat bez wymiany źródła zasilania.

Przyszłość systemów wbudowanych będzie kształtowana przez połączenie coraz większej mocy obliczeniowej, sztucznej inteligencji, autonomii i wysokiego poziomu bezpieczeństwa. W rezultacie systemy te staną się nie tylko elementami wykonawczymi, ale także inteligentnymi węzłami infrastruktury cyfrowej, odgrywającymi kluczową rolę w rozwoju nowoczesnych technologii.

Wnioski

Celem artykułu była analiza istoty systemów wbudowanych w elektronikę, ich architektury, metod projektowania, obszarów zastosowań oraz najważniejszych wyzwań stojących przed inżynierami projektującymi systemy wbudowane. Omówiono przede wszystkim kierunki rozwoju, ze szczególnym uwzględnieniem zagadnień cyberbezpieczeństwa, efektywności energetycznej oraz integracji z Internetem Rzeczy. Przeprowadzona analiza pozwoliła na syntetyczną prezentację aktualnego stanu wiedzy i uwypukliła rosnące znaczenie systemów wbudowanych w nowoczesnych rozwiązaniach technicznych.

Systemy wbudowane są jednym z najważniejszych elementów nowoczesnej elektroniki. Umożliwiają wdrożenie funkcji sterowania, pomiaru i komunikacji w bardzo szerokim spektrum urządzeń, od prostych systemów konsumenckich po krytyczne systemy w przemyśle, medycynie i zastosowaniach motoryzacyjnych. Ich przewaga wynika z zaprojektowania pod konkretne zadania, co pozwala osiągnąć wysoką efektywność operacyjną, niskie zużycie energii oraz optymalizację kosztów produkcji. Jednocześnie wymaga to jednak świadomego projektowania uwzględniającego ograniczone zasoby sprzętowe i wymagające warunki pracy.

Wraz z rozwojem Internetu Rzeczy rośnie również znaczenie komunikacji sieciowej i możliwości zdalnego zarządzania urządzeniami (Fagan i in., 2020; Dritsas i Trigka, 2025). Zwiększa to funkcjonalność systemów wbudowanych, ale także wprowadza znaczne ryzyko w cyberprzestrzeni dla całego systemu. Z tego powodu mechanizmy ochrony, takie jak bezpieczne uruchamianie, szyfrowanie transmisji danych i częste aktualizacje oprogramowania, są standardem i należy je traktować jako integralną część procesu projektowania całego systemu (Fagan i in., 2020; ETSI, 2024). Jednocześnie efektywność energetyczna projektowanych systemów zyskuje na znaczeniu, szczególnie w urządzeniach rozproszonych i zasilanych bateryjnie, gdzie czas pracy i stabilność działania mają kluczowe znaczenie dla prawidłowego funkcjonowania systemu wbudowanego.

Obserwowane kierunki rozwoju wskazują, że systemy wbudowane będą w coraz większym stopniu łączyć cechy klasycznych systemów sterowania z lokalnym przetwarzaniem danych oraz elementami sztucznej inteligencji wdrażanymi na obrzeżach sieci. W związku z tym przyszłe systemy wbudowane odegrają rolę inteligentnych, autonomicznych węzłów infrastruktury cyfrowej, od których w coraz większym stopniu zależeć będzie niezawodność i bezpieczeństwo nowoczesnych technologii.

Przeprowadzona analiza pokazuje, że przyszły rozwój systemów wbudowanych będzie zależał od potrzeby połączenia wysokiej wydajności obliczeniowej, niskiego zużycia energii, zdolności komunikacyjnych i cyberbezpieczeństwa w coraz bardziej kompaktowych i autonomicznych platformach. Szczególnie ważnym obszarem dalszych badań jest integracja nowatorskiej sztucznej inteligencji z bezpiecznymi i energooszczędnymi architekturami wbudowanymi, zwłaszcza w zastosowaniach związanych z przemysłem, medycyną i infrastrukturą krytyczną.

Bibliografia

Dritsas, E., Trigka, M. (2025). A Survey on Cybersecurity in IoT. *Future Internet, 17*(1), 30. https://doi.org/10.3390/fi17010030

ETSI. (2024). *Cyber Security for Consumer Internet of Things: Baseline Requirements (ETSI* EN 303 645 V3.1.3). European Telecommunications Standard Institute.

Elhanashi, A., Dini, P., Saponara, S., & Zheng, Q. (2024). Advancements in TinyML: Applications, Limitations, and Impact on IoT Devices. *Electronics, 13*(17), 3562. https://doi.org/10.3390/electronics13173562

Fabre, W., Haroun, K., Lorrain, V., Lepecq, M., & Sicard, G. (2024). From Near-Sensor to In-Sensor: A State-of-the-Art Review of Embedded AI Vision Systems. *Sensors, 24*(16), 5446. https://doi.org/10.3390/s24165446

Fagan, M., Megas, K., Scarfone, K. Smith, M. (2020), IoT Device Cybersecurity Capability Core Baseline, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8259A

Henschen, L. J., Lee, J. C. (2023). *Embedded System Design: Methodologies and Issues.* Morgan Kaufmann.

Heydari, S., Mahmoud, Q. H. (2025). Tiny Machine Learning and On-Device Inference: A Survey of Applications, Challenges, and Future Directions. *Sensors, 25*(10), 3191. https://doi.org/10.3390/s25103191

Mustafa, R., Sarkar, N. I., Mohaghegh, M., Pervez, S. (2024). A Cross-Layer Secure and Energy-Efficient Framework for the Internet of Things: A Comprehensive Survey. *Sensors, 24*(22), 7209. https://doi.org/10.3390/s24227209

Wolf, W. (2007). *High-Performance Embedded Computing: Architectures, Applications and Methodologies.* Morgan Kaufmann.

Zhou, X., Wang, P., Zhou, L., Xun, P., Lu, K. (2023). A survey of the security analysis of embedded devices. *Sensors, 23*(22), 9221.

Nota o autorze

Dawid Gądkowski, mgr inż., Wyższa Szkoła Biznesu – NLU. Zainteresowania badawcze obejmują automatyzację, robotykę, systemy wbudowane, Internet Rzeczy, obwody elektroniczne i cyberbezpieczeństwo.