

Bezpieczne mikrokontrolery i moduły dla IoT

Rozwiązania Internetu Rzeczy wchodzą w kolejną fazę rozwoju. W dzisiejszych czasach nie chodzi głównie o wybranie najbardziej energooszczędnego standardu, ponieważ układy pod wieloma względami osiągnęły już granice technologiczne energooszczędności. Producenci zaczęli większą wagę przywiązywać do aspektów bezpieczeństwa danych oferowanych przez ich produkty.

Momentem zwrotnym zarówno w dziedzinie bezpieczeństwa, jak i poprawy energooszczędności było wprowadzenie rozwiązań opartych na architekturze ARMv8-M, takich jak Cortex-M33. W dziedzinie bezpieczeństwa nowe układy oferują dostęp do szyfrowanej pamięci umożliwiającej przechowywanie danych krytycznych (rysunek 1).

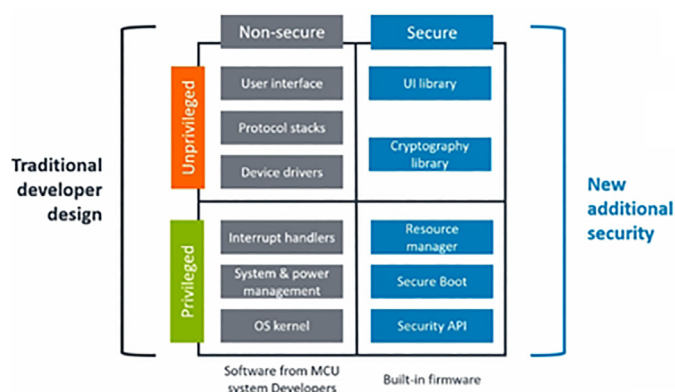
ARM Cortex-M33 – krok w stronę bezpieczeństwa

Bezpieczeństwo danych w systemach IoT opiera się na czterech głównych aspektach. Są to:

- poufność – zagwarantowanie, że dane są odczytywane tylko przez docelowego odbiorcę,
- autentyczność – zapewnienie, że dane wysłane są przez oryginalne źródło,

Więcej informacji:

Computer Controls Sp. z oo
43-300 Bielsko-Biała, ul. Budowlanych 1
tel. +48 33485 94 90, info@ccontrols.pl
www.ccontrols.pl



Rysunek 1. Architektura układów ARMv8-M oferująca funkcjonalność TrustZone

PREZENTACJE

- integralność – zapewnienie, że informacja zawiera oryginalną i nienaruszoną wiadomość,
- niezaprzeczalność – zapewnienie, że cyfrowy podpis danych nie może zostać odrzucony.

Powyższe aspekty kryptografii danych w całości zapewnia nowa, architektura Cortex-M33 (rysunek 2), dostarczająca użytkownikowi możliwość bezpiecznego:

- debugowania kodu z użyciem funkcjonalności Lock/Unlock,
- uruchamiania oraz aktualizacji kodu,
- przechowywania kluczy szyfrujących,
- weryfikacji „użytkowników” sieci,
- detekcji włamania/sabotażu,
- generowania liczb losowych TRNG.

Dla zwiększenia bezpieczeństwa w rozwiązaniach istniejących, gdzie zmiana układu MCU jest zbyt kosztowna, projektanci mogą dalej zwiększyć bezpieczeństwo, stosując zewnętrzne układy autentykacji. W zależności od końcowej aplikacji oraz jej wymagań, do dyspozycji jest weryfikacja symetryczna oraz asymetryczna (rysunek 3).

Zaawansowane rozwiązania autentykacji oraz bezpieczeństwa danych

Maxim Integrated jest jednym z wiodących dostawców układów scalonych do weryfikacji oraz bezpieczeństwa danych. Portfolio producenta zawiera układy do autentykacji symetrycznej SHA-256 oraz niesymetrycznej ECDSA, które kilka lat temu zostały wzbogacone o mikrokontrolery z rodziny DeepCover. W zależności od aplikacji możemy zastosować odpowiednie rozwiązanie oraz sposób szyfrowania (rysunek 4).

Dobór układu autentykacji może na początku przysparzać wielu problemów. Bazując na zestawieniu z rysunku 4, możemy uporządkować wszystkie ważne kwestie. Projektując system lub urządzenie, należy dokonać analizy rodzaju ochrony, jaki musimy zapewnić dla danych urządzeń – punktów sieci, i na tej podstawie wybrać odpowiednie rozwiązanie. Właściwa analiza oraz wybór pozwolą na zbudowanie systemu odpornego na dostęp niepożądanych użytkowników. W zestawieniach pokazanych na rysunku 5 i rysunku 6 umieszczono najnowsze układy autentykacji symetrycznej (rysunek 5) oraz asymetrycznej (rysunek 6).

Pomimo bardzo dużych możliwości układów z rodziny produktów do autentykacji systemy złożone mogą wymagać dodatkowych funkcjonalności, takich jak szyfrowanie kodu aplikacji czy wsparcie dla komunikacji TLS. Przy wymagających aplikacjach projektanci mają do dyspozycji układy z rodziny DeepCover (rysunek 7). Jako jedne z nielicznych oferują one wsparcie dla pełnej komunikacji TLS, dostarczane przez producenta.

Rozwiązania bezprzewodowe dla popularnych standardów IoT

Silicon Laboratories jest jednym z czołowych dostawców rozwiązań bezprzewodowych dla Internetu Rzeczy. Swoje portfolio wzbogacił

o układy oparte na architekturze Cortex-M33 oferujące zaawansowane bezpieczeństwo. Nowa rodzina układów EFR32xG21 oraz EFR32xG22, wspiera takie standardy jak Bluetooth, Thread, ZigBee i 2,4 GHz Proprietary, i bazuje na rdzeniu Cortex-M33 (rysunek 8). Nowe układy serii EFR32xG oferują nie tylko zaawansowaną funkcjonalność w kwestii bezpieczeństwa, ale również większą energooszczędność w porównaniu do poprzednich serii.



- ARM Cortex M33 Core with TrustZone
 - Provides cost effective hardware isolation
- Hardware Accelerated Crypto
 - Faster, more energy efficient and secure than software
- True Random Number Generator (TRNG)
 - Compliant with NIST SP800-90 and AIS-31
- Secure Debug with Lock/Unlock
 - Allows authenticated access for enhanced Failure Analysis (FA)
- Secure Boot with Root of Trust and Secure Loader (RTSL)
 - Prevents malware injection and rollback
 - Ensures authentic firmware execution and OTA updates

Rysunek 2. Funkcjonalności rdzeni Cortex-M33 zapewniające bezpieczeństwo danych

Security Services and Feature Implementation	Algorithm Method	
	Symmetric Key	Asymmetric Key
Confidentiality	Yes	Yes
Identification and Authentication	Yes	Yes
Integrity	Yes	Yes
Non-repudiation	Yes-Combined with public/private key algorithm	Yes
Encryption	Yes-Fast	Yes-Slow
Decryption	Yes-Fast	Yes-Slow
Overall Security	High	High
Key Management	Key Exchange and Securing the Key on both the Sender and Recipient side is needed.	One party holds the private key: the sender (for asymmetric message authentication and decryption) or the receiver (for asymmetric encryption)
Algorithm Complexity	Easy to understand	Can be difficult to understand
Key Size	128 bits, 192 or 256 bits or longer but do not need to be as long as asymmetric key (Depends on secrecy of keys)	256 bits, 1024 bits, 2048, 3072 bits or longer. Depends on the intractability (The amount of time and resources needed to solve)
System Vulnerabilities	Improper key management, generation and usage	Improper implementation
Attack Approaches	Brute Force, Linear/Differential Cryptanalysis	Brute Force, Linear/Differential Cryptanalysis and Oracle

Rysunek 3. Porównanie właściwości autentykacji symetrycznej i niesymetrycznej

Requirements	DeepCover Secure Authentication ICs		DeepCover Secure Microcontrollers
	SHA-Based	ECDSA-Based	
Trust	Device authentication	✓	✓
	Usage control/features enablement	✓	✓
	Secure boot/download	✓	✓
IP Protection	Hardware and firmware anticloning	✓	✓
	Firmware encryption		✓
Secure Communications	Certificate distribution and verification		✓
	Packet encryption	✓	✓
	Full TLS support		✓
	Small message encryption	✓	✓

Rysunek 4. Zestawienie właściwości układów szyfrujących na potrzeby bezpieczeństwa IoT

Zestawienie funkcjonalności z zakresu bezpieczeństwa zostało pokazane na **rysunku 9**. Pozwala ono na porównanie poszczególnych serii. Podobnie jak w przypadku układów autentykacji oraz DeepCover firmy Maxim Integrated, podczas analizy oraz projektowania systemu musimy dobrać rozwiązanie gwarantujące kompleksową ochronę zarówno danych, jak i komunikacji.

Układy SoC, SiP oraz moduły dla komunikacji Bluetooth, ZigBee, Thread oraz 2,4 GHz Proprietary

Produkty firmy Silicon Labs to zarówno układy System on Chip, jak i moduły w wersji System in Package oraz moduły jako standardowe PCB.

Bluetooth 5, 5.1, 5.2 AoA oraz AoD

Popularny standard komunikacji Bluetooth, dzięki wprowadzeniu na rynek stosu komunikacyjnego w wersji 5.2, który umożliwia lokalizację użytkowników w przestrzeni, zyskał nowe obszary zastosowań. Układy serii EFR32BG22 umożliwiają rozwijanie aplikacji wykorzystujących funkcjonalność AoA/AoD. Projektanci stosujący standard Bluetooth mają do dyspozycji zarówno układy SoC (**rysunek 10**), jak i w pełni certyfikowane moduły (**rysunek 11**).

W zależności od standardu oraz kluczowych cech aplikacji projektanci mają do wyboru układy należące do serii 1. oraz serii 2., które różnią się pomiędzy sobą wieloma aspektami. Na uwagę zasługuje pobór prądu przypadający na MHz, rdzeń układu, wsparcie dla kryptografii oraz maksymalna moc wyjściowa. Wybór rozwiązania zarówno spośród układów SoC, jak i modułów, jest możliwy tylko po przeanalizowaniu wszystkich kwestii.

ZigBee 3.0, OpenThread oraz Bluetooth 5.0, 5.1 – układy wieloprotokolowe

Rodzina produktów serii EFR32MG od zawsze umożliwia komunikację z użyciem wielu standardów bezprzewodowych. Pierwsza seria układów umożliwiała komunikację w standardach ZigBee, Thread, Bluetooth, 2,4 GHz Proprietary oraz SubGHz (oddzielny tor radiowy w serii EFR32MG13). W najnowszych rozwiązaniach drugiej serii – EFR32MG21 lub EFR32MG22, obsługiwana jest większość z tych standardów, jednak należy zapoznać się ze specyfikacją (**rysunek 12**). W celu zróżnicowania swoich rozwiązań, zarówno pod względem budowy systemu, jak i ceny, producent przygotował dwie nowe rodziny układów charakteryzujące się inną funkcjonalnością.

Podobnie jak w przypadku rozwiązań obsługujących standard Bluetooth, tutaj również dostępne są układy w wersji SoC, SiP oraz moduły PCB mające certyfikacje na dany rynek (**rysunek 13**). Dla takich branż, jak oświetlenie, firma Silicon Labs opracowała

Part Number	Type	Interface	Operating Voltage	User EEPROM	Package Options		
DS28C22	Authenticator	I ² C	3.3V	3kb	TDFN		
DS2465	Coprocessor	I ² C/1-Wire	3.3V	0.5kb	TSOC		
DS28E15	Authenticator	1-Wire	3.3V	0.5kb	SFN, TSOC, TDFN		
DS28E22				2kb	TSOC, TDFN		
DS28E25	Authenticator	1-Wire	1.8V	4kb	SFN, TO92, TSOC, TDFN		
DS24L65				Coprocessor	I ² C/1-Wire	0.5kb	TSOC
DS28EL15				0.5kb	SFN, TDFN		
DS28EL22	Authenticator	1-Wire	1.8V	2kb	TDFN		
DS28EL25				4kb	TDFN		
MAX66240	Authenticator	NFC	Passive	4kb	SOIC, TDFN, 8-Bump WLP		
MAX66242	Transponder	NFC/I ² C	Passive (optional 3.3V)				
MAX66300	Coprocessor Transceiver	NFC/UART/SPI	3.3V, 5V	1kb	TQFN		

Rysunek 5. Układy autentykacji symetrycznej SHA-256

Part Number	Type	Interface*	User EEPROM	Package Option
DS28E38	Authenticator with ChipDNA	1-Wire	2kb	TDFN
DS28C36	Authenticator	I ² C	4kb	TDFN
DS2476	Coprocessor	I ² C	4kb	TDFN
DS28E35	Authenticator	1-Wire	1kb	TSOC, TDFN
DS2475	Coprocessor	I ² C/1-Wire	—	SOT

Rysunek 6. Układy autentykacji asymetrycznej ECDSA

Part Number	Core	Frequency	Key Storage	USB	I ² C	SPI	Symmetric Crypto	Asymmetric Crypto	Hash Algorithms
MAXQ1061	Built-in Firmware		Tamper-proof EEPROM		•	•	AES 128, 256	ECDSA P-256, P-384, P-521 ECDH	SHA-256, SHA-384, SHA-512
MAX32555	Cortex® M3	60MHz	Active tamper reaction	•	•	•	AES 128, 192, 256 3DES	RSA 1024, 2048 ECDSA P-256, P-384, P-521 ECDH	SHA-224, SHA-256, SHA-384, SHA-512
MAXQ1050	MAXQ30	20MHz	Active tamper reaction	•		•	AES 128, 192, 256	RSA 1024, 2048 ECDSA P-192, P-256	SHA-224, SHA-256

Rysunek 7. Mikrokontrolery rodziny DeepCover

- Optimized for IoT Protocols
 - Zigbee, Thread, Bluetooth, Z-Wave and Wi-Fi
 - Multiband and **multi-protocol portfolio**
- High performance and integration
 - Arm Cortex-M33 processor core
 - Up to 125 dBm link budget with fully integrated PA/LNA
- Ultra-low power
 - Very low active current (27 µA/MHz)
 - Low sleep current (1.4 µA)
- Dedicated security core
 - Hardware crypto
 - Secure Boot
 - Secure Debug Access
 - True random number generator (TRNG)

Rysunek 8. Kluczowe cechy układów rodziny EFR32xG21 oraz EFR32xG22

Feature	Basic	+Root of Trust	+Secure Element	Secure Vault
TRNG with continuous health check	✓	✓	✓	✓
Crypto Engine	✓	✓	✓	✓
Secure Boot	✓	✓	✓	✓
Secure Boot with RTSL	-	✓	✓	✓
ARM® TrustZone®	-	✓	✓	✓
Debug Access Lock/Unlock	-	✓	✓	✓
DPA Countermeasures	-	-	✓	✓
Anti-Tamper	-	-	-	✓
Secure Attestation	-	-	-	✓
Secure Key Management	-	-	-	✓
Secure Key Storage	-	-	-	✓
Advanced Crypto	-	-	-	✓

Rysunek 9. Porównanie funkcjonalności z zakresu bezpieczeństwa dla poszczególnych serii układów EFR32

PREZENTACJE

	Series 1 - xG13	Series 2 - xG21	Series 2 - xG22
Target applications	General purpose Bluetooth LE and mesh	Mains powered Bluetooth LE and mesh	Lowest power Bluetooth LE, Direction Finding and Bluetooth mesh LPNs
Bluetooth features	5.1 and mesh 1.0 (1M, 2M, LE Coded PHYs and AE)	5.1 and mesh 1.0 (1M, 2M, LE Coded PHYs and AE)	5.2 and Bluetooth mesh LPN (1M, 2M, LE Coded PHYs, AE and AoA/D)
Proprietary 2.4G	2/4(G)FSK, OQPSK/(G)MSK, DSSS, BPSK/DBPSK TX, OOK/ASK	N/A	2/4(G)FSK, (G)MSK, OQPSK, DSSS
TX / RX (1M, GFSK)	+19 dBm / -95.8 dBm	+20 dBm / -97.5 dBm	+6 dBm / -99 dBm
TX Current (0 dBm)	10.5 mA	10.5 mA	4.1 mA 7.4 mA (6 dBm)
RX Current (1M, GFSK)	9.5 mA	8.8 mA	3.6 mA
CPU / Clock Speed	Cortex M4 (38.4 MHz)	Cortex M33 (80MHz)	Cortex M33 (up to 76.8MHz) Cortex M0+ for radio
Flash (kB)	512	Up to 1024	Up to 512
RAM (kB)	64	Up to 96	32
Sleep Current (EM2)	1.3µA (16kB RAM)	4.5 µA (96 RAM)	1.24 µA (8kB RAM) - 1.44 µA (32kB RAM)
Active Current (EM0)	70µA/MHz	51µA/MHz	25µA/MHz
Security	2x AES-128/256, ECC, SHA-1/224/256, TRNG	AES-128/256, SHA-1/2, ECC, ECDSA and TRNG DPA countermeasures Secure boot with RTSL Secure debug with debug lock/unlock	AES-128/256, SHA-1/2, ECC, ECDSA and TRNG Secure boot with RTSL Secure debug with debug lock/unlock
Operating Voltage	1.8V - 3.6V	1.8V - 3.8V	1.71V - 3.8V
Packages (mm)	7x7 QFN48, 5x5 QFN32	4x4 QFN32 (20x GPIO)	5x5 QFN40 (26x GPIO) 4x4 QFN32, TQFN32 (18x GPIO)

Rysunek 10. Porównanie układów serii EFR32BG firmy Silicon Labs

	BGM13P	BGM13S	BGM210P	BGM210L	BGM220P (Q3'20)	BGM220S (Q3'20)
Protocols	5.1 and mesh (1M, 2M, Coded PHY and AE)	5.1 and mesh (1M, 2M, Coded PHY and AE)	5.1 and mesh 1.0 (1M, 2M, Coded PHY and AE)	5.1 and mesh 1.0 (1M, 2M, Coded PHY and AE)	5.2 and mesh 1.0 LPN (1M, 2M, Coded PHY, AE and AoA/D)	5.2 and mesh 1.0 LPN (1M, 2M, Coded PHY, AE and AoA/D)
EFR32 SoC	BG13	BG13	BG21	BG21	BG22	BG22
Antenna	Built-in or U.FL	Built-in or RF pin	Built-in or RF pin	Built-in	Built-in	Built-in or RF pin
Max TX power	+8 / +19 dBm	+8 / +18 dBm	+10 / +20 dBm	+12.5 dBm	+8 dBm	+6 dBm
Sensitivity (1M)	-94.8 dBm	-94.1 dBm	-97 dBm	-97 dBm	-98 dBm	-98 dBm
Flash (kB)	512	512	1024	1024	512	512
RAM (kB)	64	64	96	96	32	32
GPIO	25	30	20	12	24, 25	25
Operating Voltage	1.8V - 3.6V	1.8V - 3.6V	1.8 - 3.8V	1.8 - 3.8V	1.71V - 3.8V	1.71V - 3.8V
Operating Temp.	-40 to +85C	-40 to +85C	-40 to +125C	-40 to +125C	-40 to +105C	-40 to +105C
Dimensions W x L x H (mm)	13.0 x 15.0 x 2.2	6.5 x 6.5 x 1.4	13.0 x 15.0 x 2.2	13.0 x 15.0 x 2.2	13.0 x 15.0 x 2.2	6 x 6 x 1.3
Certifications	BT, CE, FCC, ISED, Japan, S-Korea and Taiwan	BT, CE, FCC, ISED, Japan & S-Korea	BT, CE, FCC, ISED, Japan & S-Korea	BT, CE, FCC, ISED, Japan & S-Korea	BT, CE, FCC, ISED, Japan & S-Korea	BT, CE, FCC, ISED, Japan & S-Korea

Rysunek 11. Porównanie modułów Bluetooth firmy Silicon Labs

	Series 1 - MG12	Series 2 - MG21	Series 2 - MG22
Target applications	Mesh Routers and End Devices	Mesh Routers and End Devices	Zigbee End Devices only
Availability	Now	Now	Now
Zigbee features	Zigbee 3.0, Green Power, Concurrent Zigbee/Thread Multiprotocol (Zigbee/BLE)	Zigbee 3.0, Green Power, Concurrent Zigbee/Thread, Multiprotocol (Zigbee/BLE)	Zigbee 3.0 (SoC only), Green Power Green Power Device
Proprietary 2.4G	2/4(G)FSK, OQPSK/(G)MSK, DSSS, BPSK/DBPSK TX, OOK/ASK	N/A	2/4(G)FSK, (G)MSK, OQPSK, DSSS
TX / RX (802.15.4)	+19 dBm / -102.7 dBm	+20 dBm / -104.5 dBm	+6 dBm / -102.3 dBm
TX Current (802.15.4)	9.5 mA (@ 0 dBm)	9.3 mA (@ 0 dBm)	4.1 mA (@ 0 dBm), 8.2 mA (@ +6 dBm)
RX Current (802.15.4)	11.9 mA	9.4 mA	3.9 mA
CPU / Clock Speed	Cortex M4 (38.4 MHz)	Cortex M33 (80MHz)	Cortex M33 (76.8MHz), Cortex M0+ for radio
Flash (kB)	1024	Up to 1024	Up to 512
RAM (kB)	256	Up to 96	32
Sleep Current (EM2)	1.5µA (16kB RAM)	4.5 µA (96 RAM)	1.4 µA (32kB RAM)
Active Current (EM0)	70 µA/MHz	51 µA/MHz	26 µA/MHz
Security	2x AES-128/256, ECC, SHA-1/224/256, TRNG	AES-128/256, SHA-1/2, ECC, ECDSA and TRNG DPA countermeasures Secure boot with RTSL Secure OTA and secure debug unlock + Secure Enclave (BG21B)	AES-128/256, SHA-1/2, ECC, ECDSA and TRNG Secure boot with RTSL Secure OTA and secure debug unlock
Operating Voltage	1.8V - 3.6V	1.71V - 3.8V	1.71V - 3.8V
Packages (mm)	7x7 QFN48	4x4 QFN32 (20x GPIO)	5x5 QFN40 (26x GPIO) 4x4 QFN32 / TQFN32 (18x GPIO)

Rysunek 12. Porównanie układów serii EFR32MG firmy Silicon Labs

	MGM12P	MGM13P	MGM13S	MGM210P	MGM210L
Protocols	Bluetooth 5.0 & mesh Zigbee or Thread	Bluetooth 5.1 & mesh Zigbee or Thread	Bluetooth 5.1 & mesh Zigbee or Thread	Bluetooth 5.1 & mesh Zigbee or Thread	Bluetooth 5.1 & mesh Zigbee or Thread
Status	Production	Production	Production	Production	Production
EFR32 SoC	xG12	xG13	xG13	xG21	xG21
Antenna	Chip or U.FL	Chip or U.FL	Chip or RF pin	Chip or RF pin	PCB trace antenna
Max TX power (250 kbps O-QPSK)	+8 / +19 dBm	+8 / +19 dBm	+8 / +18 dBm	+10 / +20 dBm	+12.5 dBm
TX (125 kbps GFSK) (1Mbps GFSK)	-95 dBm	-95 dBm	-94 dBm	-104.5 dBm	-104.5 dBm
Flash / RAM	N/A	-103.2 dBm	-102.1 dBm	-105 dBm	-105 dBm
GPIO	512 / 64 kB	512 / 64 kB	512 / 64 kB	1024 / 96 kB	1024 / 96 kB
Operating Voltage	1.8 to 3.6 V	1.8 to 3.6 V	1.8 to 3.6 V	1.71 to 3.8 V	1.8 to 3.8 V
Operating Temperature	-40°C to +85°C	-40°C to +85°C	-40°C to +85°C	-40°C to +125°C	-40°C to +125°C
Dimensions W x L x H (mm)	12.9 x 15 x 2.2	12.9 x 15 x 2.2	6.5 x 6.5 x 1.4	12.9 x 15 x 2.2	15.5 x 22.5 x 2.3
Certifications	BT, CE, FCC, ISED, Japan, S-Korea and Taiwan	BT, CE, FCC, ISED, Japan, S-Korea and Taiwan	BT, CE, FCC, ISED, Japan & S-Korea	BT, CE, FCC, ISED, Japan & S-Korea	BT, CE, FCC, ISED, Japan & S-Korea
Other	Options with LNA available	Pin compatible with xGM111	World Smallest IoT Solution	No LF XTAL	No LF XTAL

Rysunek 13. Porównanie modułów ZigBee firmy Silicon Labs

moduł MGM210L, który może być łatwo wbudowany w docelowe urządzenie.



Z-Wave odświeżony standard oraz nowa rodzina produktów

Firma Silicon Labs, po przejęciu firmy Sigma Design, wprowadziła na rynek dwa nowe układy bazujące na serii SoC EFR32ZG, pracującej w zakresie częstotliwości SubGHz. Standard Z-Wave został w 2017 roku odświeżony i wprowadzony jako wersja Z-Wave S2 oferująca większe bezpieczeństwo w zakresie komunikacji wewnątrz sieci oraz identyfikacji nowych urządzeń. Obecnie wszystkie nowe produkty rozwijane są na układach serii ZGM130S lub EFR32ZG14 (rysunek 14).

Wi-Fi Low Power – najpopularniejszy standard komunikacji w wersji niskomocowej

Moduły WF200 oraz WFM200 umożliwiły projektantom urządzeń nowe podejście do projektowania układów zasilanych bateryjnie, wyposażonych w komunikację Wi-Fi. Parametry układów (rysunek 15 i rysunek 16) pozwalają na projektowanie urządzeń oraz systemów, które mogą cyklicznie transmitować pakiety w standardzie Wi-Fi. Mocną stroną obu rozwiązań są bardzo niskie prądy uśpienia oraz wyłączenia, pozwalające maksymalizować czas pracy na baterii.

W kwestii bezpieczeństwa obydwa rozwiązania pozwalają na tworzenie aplikacji

ZGM130S - SIP MODULE	EFR32ZG14 - MODEM SoC
	
End-devices & gateways LGA64 9x9 mm SIP	Gateways only QFN32 5x5 mm SoC

Rysunek 14. Rozwiązania dla standardu Z-Wave

Power Consumption

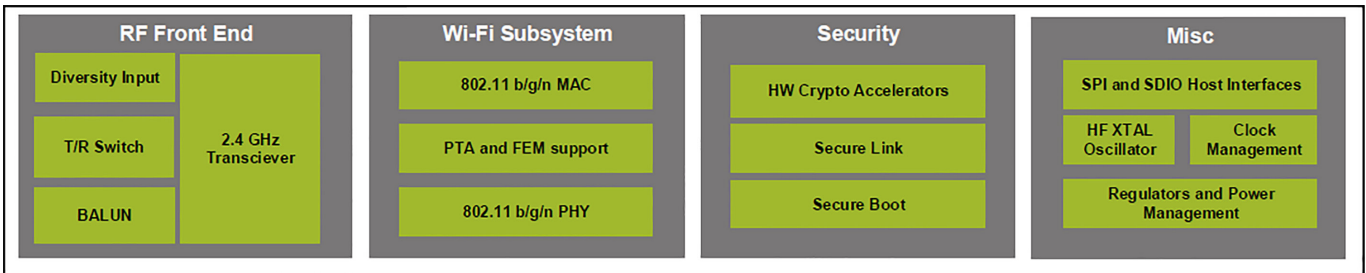
- Rx (@1DSSS): 41.6 mA
- Tx (17 dBm @1DSSS): 152.6 mA
- Associated: DTIM3: 298 µA
- Sleep: 22 µA
- Power off: < 0.5 µA

Rysunek 15. Pobór prądu w układzie WF200

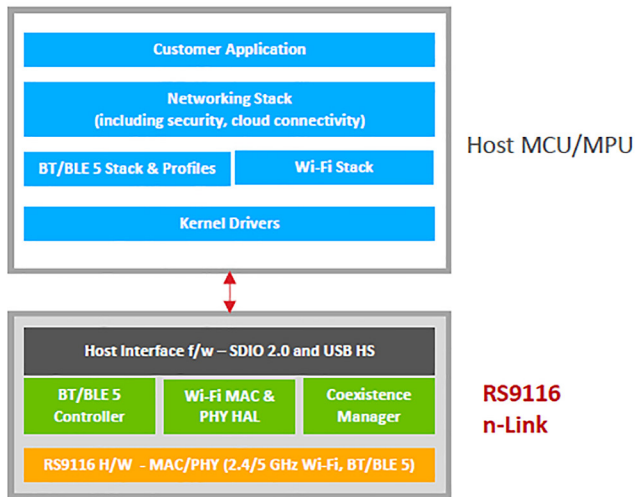
Power Consumption

- Rx (@DSSS-1Mbps): 42.3 mA
- Tx (15.1 dBm @DSSS-1Mbps): 145 mA
- Associated DTIM3 average current: 298 µA
- Associated Sleep Current: 22 µA
- Shutdown mode: 0.5 µA

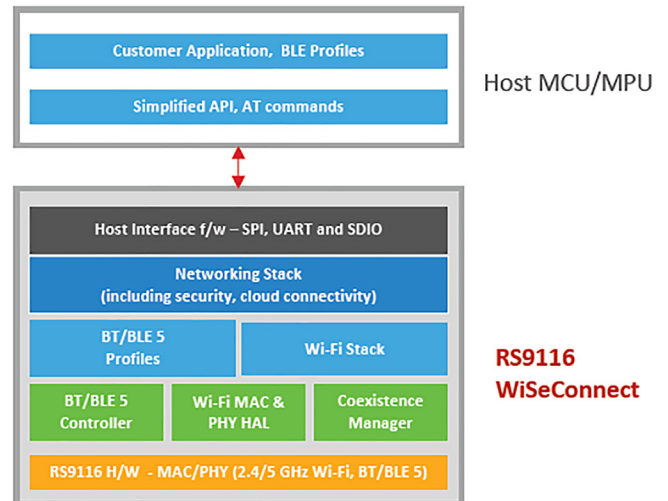
Rysunek 16. Pobór prądu w układzie WFM200



Rysunek 17. Diagram blokowy budowy układów WFM200S oraz WF200S



Rysunek 18. Diagram blokowy budowy układu RS9116 n-Link



Rysunek 19. Diagram blokowy budowy układu RS9116 WiSeConnect

odpornych na zewnętrzne ataki dzięki wbudowanym funkcjom bloku zabezpieczeń (rysunek 17).

Wi-Fi + Bluetooth, układy łączące dwa popularne standardy

Przejęcie firmy Redpine Signals przez Silicon Labs wzbogaciło rozwiązania producenta o układy Wi-Fi dwuzakresowe, integrujące również komunikację Bluetooth. Rozwiązania Redpine Signals obejmują układy RS9116 wersji n-Link (rysunek 18) oraz WiSeConnect (rysunek 19). Obydwie wersje się miejscem implementacji stosu sieciowego, protokołów oraz specyfikacją dla host MCU/MPU.

Podsumowanie

Projektanci aplikacji oraz systemów bezprzewodowych, oprócz dobrania właściwego protokołu, muszą również przeanalizować dostępne rozwiązania pod kątem kluczowych wymagań aplikacji. Zadanie nie jest łatwe, biorąc pod uwagę liczbę dostępnych układów oraz przyzwyczajenia projektantów, którzy nierzadko bazują na rozwiązaniu znanym z poprzednich projektów.

Implementacja nowej konfiguracji jest dla wielu bardzo trudna już na etapie wyboru, gdzie zwykle należy nauczyć się technologii producenta, zdobyć potrzebną wiedzę oraz wsparcie. Dlatego projektanci coraz częściej korzystają ze wsparcia inżynierów aplikacyjnych, posiadających wiedzę w zakresie technologii danych dostawców. Ponadto wiele informacji dostępnych jest po podpisaniu umów poufności lub wymaga dostarczenia szczegółowych danych do producenta. Korzystanie ze wsparcia inżynierów aplikacyjnych oraz sprzedaży dystrybutora znacznie skraca i upraszcza proces rozpoczęcia pracy przy nowych projektach.

Kamil Prus
Business Development Manager
Field Application Engineer Poland
Computer Controls Sp. z o.o.
<https://www.ccontrols.net/pl/>

REKLAMA

ELEKTRONIKA
PRAKTYCZNAMATERIAŁY
DODATKOWE

MEDIA

Aby skorzystać z materiałów dodatkowych dołączonych do numeru, należy:

1. Wejść na stronę www.media.avt.pl,
2. Zarejestrować się lub zalogować,
3. Wybrać wydanie „Elektroniki Praktycznej”, które ma trafić do biblioteki osobistej,
4. Odpowiedzieć na proste pytanie dotyczące bieżącego numeru,
5. Pobrać pliki.