We get technical

How to use FPGAs in resource-constrained applications

Smart beacons leverage Bluetooth system-on-a-chip for connected ML insights

Highly integrated MCUs simplify precise and efficient motor control design

DigiKey

contents

Editor's note

Welcome to the DigiKey eMagazine Volume 28 – Embedded and Microcontrollers.

This issue is packed with innovation, practical engineering insights, and looks at how leading manufacturers are shaping the next era of embedded design.

We begin with contributions from four industry trailblazers. Arduino introduces its versatile UNO Q Microcontroller Board, showing how accessibility and performance continue to coexist in the Maker ecosystem. Analog Devices explores advanced hardware security through its MAXQ1065, offering a deep dive into modern cryptography implementations that protect connected devices at scale. Hammond Manufacturing highlights the design considerations behind their 1551SNAP and 1551V enclosures that are compact, robust, and ready for today's miniaturized electronics. Rounding out these features, Texas Instruments presents the MSPM0G110x, an 80 MHz Arm® Cortex®-M0+ MCU, demonstrating how cost-effective microcontrollers can still deliver impressive performance headroom.

Beyond our manufacturer features, this issue also brings forward compelling technical articles that address the needs of engineers working at the edge of efficiency and capability. "How to Use FPGAs in Resource-Constrained Applications" examines clever design strategies that unlock flexibility without exceeding budgets or power envelopes. "Smart Beacons Leverage Bluetooth System-on-a-Chip for Connected ML Insights" shows how low-power wireless nodes are evolving into intelligent, context-aware devices. Finally, "Highly Integrated MCUs Simplify Precise and Efficient Motor Control Design" demonstrates how integration and smarter silicon reduce design complexity while achieving tighter control loops.

Whether you're designing secure IoT hardware, building real-time systems, experimenting with new development boards, or refining your motor control architecture, we hope this issue equips you with fresh knowledge and sparks your next engineering breakthrough.

Sponsored content provided by:

ARDUINO® ANALOG DEVICES HAMMOND® TEXAS INSTRUMENTS

Arduino UNO Q: Linux computing meets real-time control in the classic form factor

If you've ever needed to combine a Linux computer with an Arduino for AI and machine learning projects, the UNO Q offers both within a single board. This latest release from Arduino pairs a Qualcomm Dragonwing QRB2210 processor running Debian Linux with an STMicroelectronics STM32U585 microcontroller, all within the standard UNO form factor.

Launched in October 2025 following Qualcomm's acquisition of Arduino, the board solves a persistent problem in Edge AI development: you need Linux for running AI models and processing power, but you also need deterministic real-time control for sensors and actuators.

Rather than connecting separate boards, the UNO Q integrates both processors on one PCB, providing a complete platform for projects spanning machine learning, computer vision, and real-time hardware interfacing.

Qualcomm partnership and processor capabilities

Arduino's acquisition by Qualcomm brings industrial-grade silicon to the maker space while preserving Arduino's independence as a subsidiary. The Qualcomm Dragonwing QRB2210 sits at the heart of this design, providing a quad-core ARM Cortex-A53 processor operating at 2.0 GHz alongside an Adreno 702 GPU. You get 3D graphics acceleration via OpenGL ES and OpenCL, capabilities that extend well beyond typical Arduino applications.

Qualcomm originally designed this processor family for robotics and industrial IoT deployments, which means prototypes you develop on the UNO Q can scale directly to production hardware using identical silicon.

The imaging capabilities deserve particular attention for computer vision work. The QRB2210 contains dual Image Signal Processors that handle camera inputs up to 13 MP + 13 MP simultaneously, or a single 25 MP feed, all at 30 frames per second. You can process this visual data without offloading to external hardware. A dedicated low-power DSP takes care of audio tasks including keyword detection, while onboard AI acceleration handles inference workloads locally. Object recognition, anomaly detection, and similar applications run entirely on the board without requiring Internet connectivity or Cloud services.

Working alongside the Linux processor, the STM32U585 microcontroller runs at 160 MHz with 2 MB of flash memory and 786 KB of SRAM. This chip executes Arduino Core on top of Zephyr RTOS, giving you the familiar Arduino programming environment for real-time tasks. The architecture lets you run Python scripts and AI models on the Linux side while simultaneously handling time-sensitive operations like sensor sampling or motor control on the microcontroller.

Memory, connectivity, and physical specifications

You can choose between two memory configurations when selecting your UNO Q. The entry-level variant ships with 2 GB LPDDR4 RAM and 16 GB eMMC storage. Arduino also offers a higher-tier model with 4 GB RAM and 32 GB storage. If you're planning to run GUI applications or work with larger AI models, you should opt for the 4 GB version.

For wireless connectivity, the board uses a WCBN3536A module supporting Wi-Fi 5 across both 2.4 GHz and 5 GHz bands, plus Bluetooth 5.1. Antennas are built directly into the board. The single USB-C connector handles multiple functions: host and device modes, power delivery, and even video output. If you want to use the UNO Q as a standalone computer, you'll need to add a USB-C hub for connecting peripherals like keyboard, mouse, and additional displays. Power comes through either the USB-C port at 5 V / 3 A, or via the barrel jack accepting a 7 V to 24 V input.

At 68.85 x 53.34 mm, the physical dimensions match the classic UNO exactly, so your existing shields will fit without modification. Beyond the standard Arduino headers,

The Arduino UNO Q hybrid single-board computer and microcontroller development board (top view). Image source: Arduino

you'll find specialized high-speed connections for MIPI-CSI cameras, MIPI-DSI displays, and audio interfaces. The board includes built-in interaction elements: an 8 x 13 blue LED matrix, four RGB LEDs, and a user button. Communication protocols span the full range you'd expect: I2C/I3C, SPI, PWM, CAN, UART, and ADC. The Qwiic connector provides tool-free connections to compatible Modulino modules.

Choosing your development tools and programming approach

When you power on the UNO Q, you'll find the Arduino App Lab already installed and ready to use. This new integrated development environment brings together Arduino sketches, Python code, and containerized AI models in one workspace. Pre-built components called 'Apps and Bricks' speed up common prototyping tasks. The interface supports development for both the Linux processor (MPU) and the real-time microcontroller (MCU) without switching tools.

If you prefer established workflows, you can continue using Arduino IDE 2.0 or newer versions to program the STM32 microcontroller. For Linux development, standard SSH access gives you terminal control. The Debian operating system includes Docker and Docker Compose, so you can deploy AI models in containers just as you would on any Linux system. App Lab runs on your development computer under Windows 10 and later, macOS 11 and later, Ubuntu 22.04 and later, or Debian Trixie.

Programming language options match each processor's role. Write Arduino sketches in C/C++ for the STM32 microcontroller to handle hardware control tasks with deterministic timing. Use Python on the Linux processor for application logic and computationally intensive workloads.

For AI inference, the STM32 microcontroller runs TensorFlow Lite for Microcontrollers through Arduino's library system, handling lightweight models efficiently. The Linux processor manages heavier AI workloads and comes with six pre-configured models ready to deploy: object detection, human detection, anomaly detection, image classification, sound recognition, and keyword spotting. All inference runs locally without requiring internet connectivity.

Potential applications

Computer vision systems benefit from the dual Image Signal Processors and AI acceleration for tasks like object recognition or quality inspection, while the microcontroller precisely manages motors, servos, and other actuators. Robotics projects that combine visual navigation with motor control fit this profile perfectly. Industrial inspection systems can analyze images for defects while simultaneously controlling product handling mechanisms. Interactive installations and kiosks can process visual inputs locally without latency, and voice-controlled devices leverage the onboard keyword spotting without cloud dependencies.

The board's integration with Edge Impulse, which Qualcomm acquired in March 2025, provides your primary workflow for machine learning development. You can train custom models and deploy them to the UNO Q through Edge Impulse's platform. PyTorch isn't officially supported based on Arduino's documentation, but the underlying Debian system could theoretically run it with appropriate installation, though performance would depend on your model complexity.

The UNO Q vs. alternative platforms

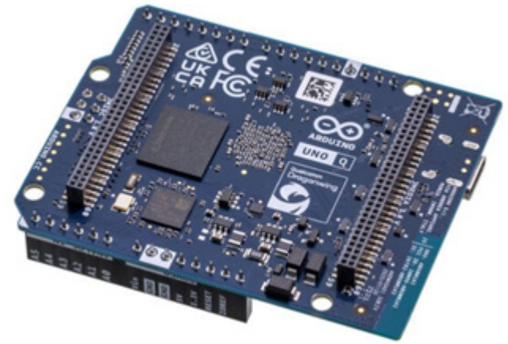
Understanding where the UNO Q fits in the overall development board market can help you make informed purchasing decisions. The Arduino UNO R4 serves as a pure microcontroller platform focused entirely on hardware control and simple embedded tasks. The UNO Q builds on this foundation by adding full Linux computing for AI, image processing, and network applications, while keeping the real-time I/O that makes Arduino useful. You gain substantially more capability but also more complexity.

Looking at Raspberry Pi 5 boards at similar price points, you'll notice different tradeoffs. The Pi 5 delivers faster processing for compute-intensive tasks but has no integrated microcontroller for deterministic timing. If your project needs both capabilities, you'd need to buy a Raspberry Pi and an Arduino separately, then handle the interconnection yourself. The UNO Q eliminates this two-board requirement.

Select the UNO Q when your project requires integrated Linux and real-time control, when power efficiency matters for battery operation, or when Arduino shield compatibility provides value through existing hardware investments. Choose alternatives for different scenarios: ESP32 or UNO R4 when you only need microcontroller functionality, Raspberry Pi 5 when maximum computing performance outweighs real-time requirements, and ESP32 when budget constraints favor simplicity over AI capability.

Software maturity and current limitations

Early adopters in Arduino's community forums report both successful projects and growing pains. Completed projects include smart speakers, weather stations, and face-tracking robots. Users specifically praise App Lab for simplifying tasks like creating web servers that control LEDs. However, you should expect some rough edges typical of new platforms. Reported issues include USB-C cables that don't establish reliable connections, compatibility problems with certain sensor libraries like DHT, and an initial bug in the Windows Serial Monitor that Arduino has since patched.



The Arduino UNO Q hybrid single-board computer and microcontroller development board (bottom view). Image source: Arduino

Plan for several practical requirements in your workflow. Since Wi-Fi connectivity is essentially mandatory during development and programming, the single USB-C port means you'll need a hub for standalone operation when using the board as a complete computer. You cannot run the STM32 microcontroller independently of the Linux system, so both processors operate together. Arduino continues releasing active updates and maintains responsive support in the forums. Complete hardware documentation including schematics and Gerber files is available for detailed technical reference.

Making the decision for your next project

The Arduino UNO Q successfully delivers enterprise-level processing from Qualcomm in a package accessible to makers and engineers. The dual-processor design directly solves the common requirement to combine single-board computers with microcontrollers for advanced projects involving AI.

If you're developing robotics systems with vision processing, industrial equipment with machine learning inspection, or IoT devices that need local intelligence paired with real-time sensor control, the UNO Q provides these capabilities on one board.

For more information please visit Arduino UNO Q.

Secure connectivity for at-home healthcare Part 1: challenges beyond the clinic

By Jackson Coole, Systems Applications Engineer and
Michael Haight, Director of Product Line Management

This article showcases how Analog Devices offers connectivity solutions that address the unique security and patient safety concerns across a broad range of medical devices used in at-home healthcare.

Building on the foundation of secure authentication for medical disposables described in "Secure Authentication for Medical Disposables," this article explores the growing trend of shifting healthcare from hospitals to patients' homes (Figure 1). It discusses the unique security challenges of providing healthcare outside a medical setting and the requirements for securing data during network transfer.

Growing move to guided patient self-care

The trend toward guided patient self-care is gaining momentum, driven by technological innovations that empower patients to manage their health conditions from the comfort of their homes. Advanced tools such as wearable devices, mobile health apps, and telehealth platforms provide real-time health data and professional guidance, enabling patients to monitor their conditions and make informed decisions about their care. This shift toward self-care is not only about convenience but also about promoting sustainable healthcare practices. By allowing patients to maintain their independence and quality of life, guided self-care supports long-term health management and expands access to healthcare while simultaneously reducing the burden on healthcare facilities.

Growing move to guided patient self-care
- Technological innovations enable patients to manage their health conditions from home with professional guidance
- Desire for sustainable care that allows patients to maintain their independence and quality of life

Increasing regulatory and quality concerns
- Regulatory bodies like the FDA are implementing more stringent guidelines to ensure the safety and efficacy of medical devices used at home
- All new devices and changes to previously authorized devices must include detailed cybersecurity plans

Figure 1. Trends in at-home healthcare.

Increasing regulatory and quality concerns

As at-home healthcare continues to expand, regulatory bodies like the FDA are implementing more stringent guidelines (FDA-2021-D-1158; Section 524B, HR 2617 Act of Congress; UL2900-2-1; and IEC62443) to ensure the safety and efficacy of medical devices used in home settings. These regulations are crucial for protecting patients and maintaining high standards of care. New devices, as well as modifications to existing ones, must now include detailed cybersecurity plans to address potential vulnerabilities and protect sensitive health data. This increased focus on regulatory compliance and quality assurance is essential for building trust in at-home healthcare solutions and ensuring that patients receive safe, reliable, and effective care.

Typical workflow for at-home healthcare

Initial evaluation and device programming: The process of at-home healthcare often begins with an initial visit to a hospital or clinic, where the patient meets with a clinician for a comprehensive evaluation (Figure 2). During this visit, the clinician assesses the patient's condition and determines the appropriate treatment plan. The clinician then programs the medical device with settings tailored to the patient's specific needs. Once configured, the patient receives detailed instructions for effectively using the device at home.

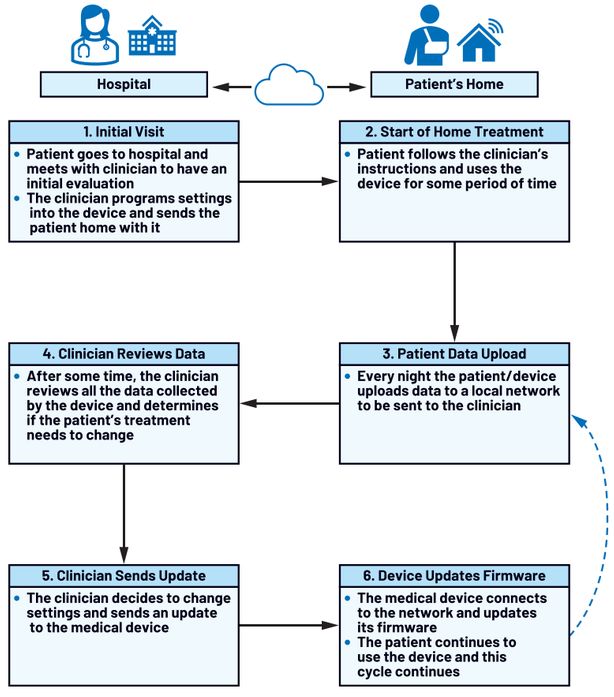


Figure 2. Typical at-home healthcare workflow.

Start of home treatment: Upon returning home, patients begin their treatment by following the clinician's instructions and using the medical device as prescribed. This period is critical for patients to become accustomed to the device and integrate it into their daily routine. Features like reminders, alerts, and user-friendly interfaces assist patients in adhering to their treatment plan, promoting independence and improving health outcomes.

Patient data upload: A key component of at-home healthcare is the continuous monitoring and transmission of patient data. This data can include vital signs, medication adherence, and other relevant health metrics. For example, daily activity tracking could be automatically uploaded to a local network when the device is attached to its charger while the patient sleeps. In other scenarios, the device could send data only when a specific event occurs such as a user error or an adverse event is detected, or perhaps the data transfer relies on the patient manually inserting values into a mobile application. The seamless transfer of information ensures that the clinician has access to up-to-date data, enabling timely interventions and adjustments to the treatment plan if necessary.

Clinician reviews data: After a designated period, the clinician reviews the data collected by the medical device. This comprehensive analysis allows the clinician to assess the patient's progress and determine whether any changes to the treatment plan are needed. The clinician's review is informed by the detailed data provided by the device, offering a more accurate picture of the patient's health status compared to traditional periodic check-ups. This proactive approach helps in identifying potential issues early and adjusting the treatment plan to better meet the patient's needs.

Clinician sends update: If the clinician decides that adjustments are necessary, the settings can be remotely updated on the medical device. These changes in treatment could be adjusting a key sensing parameter, such as the gain of a pressure sensor or changing the frequency of drug administration or therapy delivery. This usually manifests in the form of a new version of firmware that needs to be securely uploaded to the medical device in the patient's home. This update is sent securely to the device, ensuring that the patient receives the most current and effective treatment. The ability to make remote adjustments is a significant advantage of modern at-home healthcare systems, reducing the need for frequent in-person visits and allowing for more flexible and responsive care.

Device updates firmware: Once the clinician sends an update, the medical device typically connects to the network to receive and install the firmware update. This process is typically automated, minimizing the need for patient intervention and ensuring that the device operates with the latest settings and security protocols. Once the update is complete, the patient continues to use the device as part of ongoing treatment. This cycle of data collection, review, and adjustment continues, creating a dynamic and responsive healthcare environment that adapts to the patient's evolving needs.

Security challenges in home healthcare

Ensuring the security of patient data and medical devices presents significant challenges. The reliance on digital platforms and connected devices exposes sensitive health information to potential cyber threats, including data breaches and unauthorized access. Addressing these security challenges is crucial to maintaining patient trust, ensuring compliance with healthcare regulations, and protecting the integrity of at-home healthcare services. Security challenges unique to each step of the typical at-home healthcare workflow are described in the next section (Figure 3).

Initial evaluation and device programming: During the initial clinic visit and the start of home treatment, several security concerns must be addressed. One critical aspect is secure boot, which ensures that the device only runs trusted software at startup. This prevents malicious software from being loaded, which could compromise the device's functionality and patient safety. Additionally, secure data storage is essential to protect against unauthorized access and tampering. This involves encrypting data stored on the device and implementing robust access controls to ensure that only authorized personnel can modify the device settings. Finally, the integrity of the firmware parameters must be guaranteed. For example, ensuring that a dosage setting of 10 mL/hr is not erroneously changed to 100 mL/hr is crucial for patient safety. This can be achieved through cryptographic checksums and digital signatures that verify the authenticity and integrity of the firmware.

Patient data upload and transfer: When patient data is uploaded from the medical device to the clinician, several security measures are necessary to protect the data during transmission. Authenticity is a primary concern, ensuring that the data received by the clinician is indeed from the correct patient. This can be achieved through unique patient identifiers and secure authentication protocols. Integrity is also critical, as it ensures that the data has not been altered during transmission. Techniques such as hashing and digital signatures can be used to verify that the data remains unchanged. Clinicians rely on accurate and reliable data to assess a patient's condition and adjust treatment plans accordingly. If the data is corrupted, it can lead to incorrect assessments. For example, a corrupted data point might falsely indicate that a patient's blood pressure is stable when it is dangerously high. Finally, ensuring confidentiality is paramount to protect sensitive patient information from unauthorized access while it is in transit, ensuring that it remains private. This can be achieved through secure communication protocols like transport layer security (TLS) and virtual private networks (VPNs), which encrypt the data being transmitted. Additionally, implementing strict access controls and authentication mechanisms ensures that only authorized personnel can access patient information.

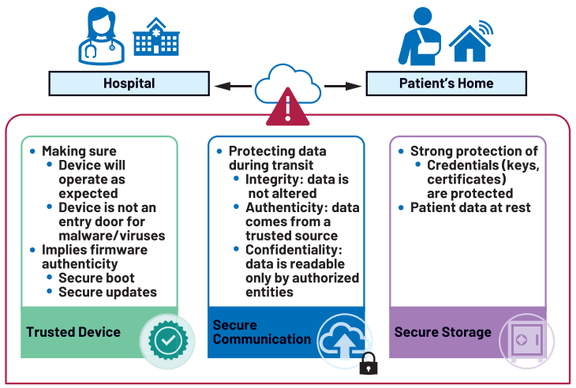


Figure 3. Security challenges in at-home healthcare.

Firmware updates: When the clinician sends an update to the medical device, it is essential to ensure that the update process is secure. Unauthorized access or updates can allow an intruder to alter the behavior of medical devices or, in the worst-case scenario, take complete control of them. One common attack method is malware injection, where malicious code is inserted into the firmware update. If an attacker successfully installs fraudulent firmware, it can lead to severe consequences. For instance, the compromised device might start transmitting confidential and sensitive data, such as private medical information from a portable health monitor, without authorization. In a broader context, malicious firmware could expose encryption keys to the public, undermining the security of the entire system. Additionally, the device could be forced to operate incorrectly, posing significant risks to patient safety and data integrity. Therefore, authenticity of the new firmware must be verified to confirm that it comes from a trusted source. This can be achieved through digital signatures and certificates that authenticate the source of the firmware. Just like when the medical device is first setup in the clinic, the integrity of the firmware update is crucial to ensure that all parameters are accurate and have not been tampered with. Cryptographic checksums and integrity checks can be used to verify the firmware. Finally, confidentiality must be maintained during the transmission of the firmware update to protect sensitive data. Encrypting the firmware update ensures that it cannot be intercepted and accessed by unauthorized parties.

How the MAXQ1065 addresses these security concerns

The MAXQ1065 is a security coprocessor that provides turnkey cryptographic functions for root-of-trust, mutual authentication, data confidentiality and integrity, secure boot, secure firmware updates, and secure communications (Figure 4). Key features are included in Table 1.

Secure boot and firmware updates

The fundamental principle of a secure firmware download based on asymmetric cryptography involves the use of a private key for signing by the firmware developer, and a corresponding public key for verification that is stored on the medical device. This method, particularly when using elliptic curve digital signature algorithm (ECDSA), ensures that an attacker cannot retrieve the private key used for signing the firmware and data, even with sophisticated invasive attacks. The only information an attacker can obtain from the medical device is the public key; and with ECDSA, it is mathematically infeasible to derive the private key from the public key.

When firmware needs to be executed by the medical device's

microcontroller, the host MCU boot manager first retrieves it and delivers it to the MAXQ1065 for SHA-256 hash computation (Figure 5). After the SHA-256 hash computation is completed, the processor provides the ECDSA signature of the firmware or data, which was computed during the development phase and appended to the file. The main processor then sends the firmware or data file and its expected digital signature. The security coprocessor verifies the signature and returns the result, indicating if it is successfully verified or if there was an error. If the signature verification is successful, the firmware can be executed.

A more in-depth explanation of this process can be found in the following article, "The Fundamentals of Secure Boot and Secure Download: How to Protect Firmware and Data Within Embedded Devices."

Secure storage and tamper detection: The MAXQ1065 includes tamper detection features to identify and respond to physical tampering attempts. This adds an extra layer of security, ensuring that the device remains trustworthy even in the face of potential intrusions. ADI's ChipDNA® embedded security physically unclonable function (PUF) technology provides an exponential increase in protection against the invasive and reverse engineering attacks that hackers use. Attempts to probe or observe ChipDNA operation modifies the underlying circuit characteristics, preventing the discovery of the unique value used by the chip cryptographic functions. Similarly, more exhaustive reverse-engineering attempts are defeated due to the factory conditioning required to make the ChipDNA PUF circuitry operational. The per-device unique key is generated by the ChipDNA PUF circuitry only when needed for cryptographic operations and is then instantaneously deleted.

Transport Layer Security (TLS) protection: The MAXQ1065 supports TLS/DTLS 1.2 protocols for secure data transmission, ensuring data confidentiality and integrity. This is crucial for at-home healthcare devices that need to communicate patient data to healthcare providers or cloud-based systems.

In this scenario, a medical device at the patient's home uses TLS for secure communication with a cloud server. TLS has two phases: the handshake and secure communication. Secure ICs like the MAXQ1065 enhance TLS by storing certificate authority (CA) root certificates in nonvolatile memory, ensuring only authenticated administrators can replace them. The handshake phase involves negotiating security settings and establishing shared keys, while the secure communication phase uses these keys for encryption and authentication. Implementing TLS on embedded devices can be complex, with risks like skipping certificate verification or using weak cipher suites. The MAXQ1065 provides hardware-based protections, preventing unauthorized access and ensuring the integrity of TLS processes.

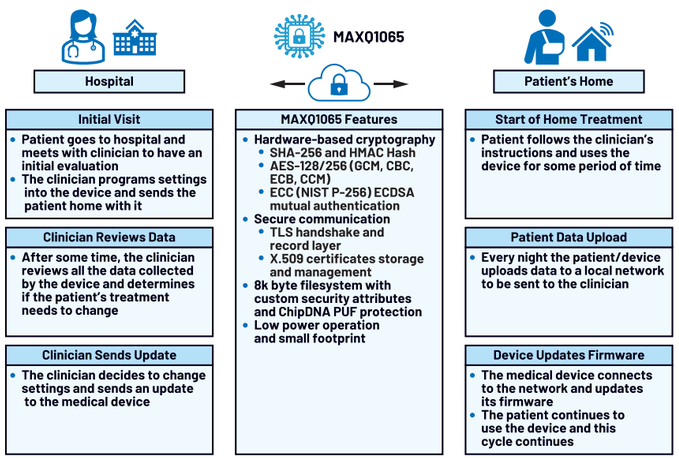


Figure 4. The MAXQ1065 addresses security concerns in at-home healthcare settings.

Feature	Description
Hardware-Based Cryptography	SHA-256 and HMAC hash; AES-128/256 (GCM, CBC, ECB, CCM); ECC (NIST P-256)
ChipDNA PUF Technology	Provides ultimate protection of cryptographic keys and sensitive data. Protects the secure key by ensuring it never resides statically in registers or memory, nor leaves the electrical boundary of the IC.
Secure Communication	Supports secure data transmission via TLS/DTLS 1.2 protocols. TLS handshake and record layer. X.509 certificates storage and management.
Secure Storage	8 kB of secure storage for user data, keys, certificates, and counters.
Tamper Detection	Identifies and responds to physical tampering attempts.
Communication Interface	SPI/I2C.
Low Power Consumption	At-home healthcare devices often rely on battery power, making energy efficiency a critical factor. The MAXQ1065's ultra low power consumption ensures that devices can operate for extended periods without frequent battery replacements. This is particularly beneficial for wearable health monitors and other portable medical devices.

Table 1. MAXQ1065 features

It defends against attacks like man-in-the-middle and session key exposure, maintaining the confidentiality and integrity of healthcare data without compromising device performance.

Additionally, this cryptographic controller allows device manufacturers to establish their own CA for connected devices, securely storing root public keys and preventing unauthorized modifications. ChipDNA technology further secures the private key by making it a byproduct of the IC's normal physical manufacturing distribution, making it resistant to hacking and reverse engineering.

For an in depth overview on using secure companion ICs to protect TLS implementations, please refer to the article "Using Secure Companion ICs to Protect a TLS Implementation."

Conclusion

As the demand for at-home healthcare solutions continues to grow, the need for secure and reliable medical devices becomes increasingly important. ADI's MAXQ1065 cryptographic controller addresses these needs with its advanced security features, low power consumption, and ease of integration. By incorporating this coprocessor into at-home healthcare devices, manufacturers can ensure that patient data remains secure and that devices perform reliably over the long term.

To learn more about the MAXQ1065 cryptographic controller and evaluate it for at-home healthcare designs, the full product details are available on DigiKey's website.

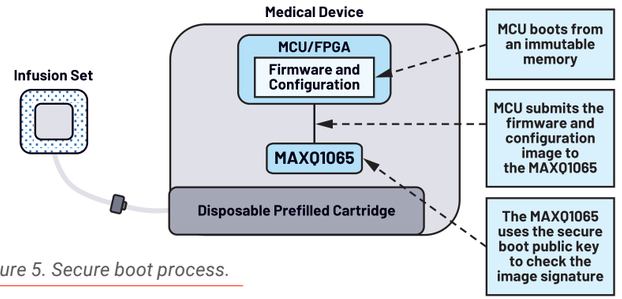


Figure 5. Secure boot process.

Hammond 1551SNAP and 1551V enclosures: tool-free housings for compact electronics

If you need to house small electronics without managing screws and fasteners, Hammond Manufacturing's 1551SNAP and 1551V series are a practical solution. These ABS miniature plastic enclosures snap together without tools, mount directly to walls through molded slots, and come in seven sizes covering both circular and rectangular profiles. At a 20 mm height for all sizes, these low-profile enclosures can fit into tight spaces and accommodate components like USB connectors and terminal blocks.

Snap-fit closure mechanism

Both enclosure series avoid the need for lid screws through a snap-fit design. The enclosure base includes a hinge feature at the rear edge, allowing the lid to pivot up for access. When you close it, the lid snaps firmly into place at the front without requiring any fasteners. This tool-free operation makes sense for prototyping work where you need frequent access to adjust components, swap batteries, or update the firmware through programming headers.

Hammond designed this closure to maximize internal PCB space. Typical screw-secured enclosures

A Hammond 1551SNAP Series plastic, general-purpose enclosure. Image source: Hammond

require clearance around mounting holes and space for your screwdriver to reach. The snap mechanism removes these constraints entirely. You can open and reseal the enclosure repeatedly during development without accumulating stripped threads or lost hardware.

Both series carry an IP30 protection rating, which prevents contact with objects larger than 2.5 mm. Your fingers and tools cannot reach internal components, but the enclosures provide no sealing against dust or water. If you need environmental protection, Hammond's standard 1551 series with screw-secured lids achieves an IP54 rating for dust and splash resistance, while their 1551W series provides IP68 waterproofing through integrated silicone gaskets.

Keep in mind that material specifications matter for regulatory compliance and fire safety. Both series use ABS plastic molded with a satin texture finish and rounded corners. The material carries a UL94-HB flammability rating, which means that it burns slowly under test conditions but self-extinguishes when the flame source is removed. Hammond designs these enclosures in Canada and confirms full RoHS and REACH compliance for sale in regulated markets.

Multiple size options

You can choose from seven distinct sizes, each maintaining a uniform 20 mm external height. This consistent profile provides adequate clearance for board-mounted RJ45 jacks, USB ports, and standard pin headers while keeping the overall footprint compact. The rectangular and square options suit PCBs with orthogonal layouts, while circular models work for symmetrical sensor arrangements or more aesthetic considerations.

Size 1 measures 40 × 40 × 20 mm externally, making it suitable for small modules like Bluetooth Low Energy radios or battery management circuits. Size 2 extends to 80 × 40 mm, which is ideal for longer boards like USB-to-serial converters or single-channel relay modules. Size 3 provides a 60 × 60 mm square profile for balanced layouts, while Size 4 at 80 × 80 mm is useful for larger microcontroller development boards or multi-sensor arrays.

The circular variants offer different diameters at the same 20 mm height. Size 11 at a 45 mm diameter fits compact disc-shaped PCBs. Size 12 at 60 mm provides moderate space, and size 13 at 80 mm matches the largest rectangular option's width. These circular profiles integrate naturally into environments where rounded aesthetics matter, such as consumer products or visible wall-mounted installations.

You can also specify black, grey, or white for any size and series. Hammond appends color codes to model numbers, e.g., BK for black, GY for grey, and WH for white. A complete part number for a black 60 × 60 mm solid enclosure would be 1551SNAP3BK, and a white 60 mm diameter vented version would be 1551V12WH. So, with seven sizes to choose from, as well as two series and three colors, you get 42 distinct part number offerings.

Installing PCBs and managing cables

Four PCB standoffs molded into the base rise 4 mm above the interior floor. These posts accept #2 self-tapping screws measuring 3/16 inch long, which thread directly into the plastic to secure your circuit board. Note that Hammond does not include these screws with the enclosure. You'll need to order them separately as accessory pack 1553WTS100 (100 nickel-plated screws), or source equivalent

The Hammond 1551V12GY Snap-fit enclosure. Image source: Hammond

hardware from your preferred fastener supplier.

Standoff positions vary by enclosure size, so you should download Hammond's dimensional drawings for your specific model to verify compatibility with your PCB mounting holes. Keep in mind that the internal usable area runs slightly smaller than external dimensions due to wall thickness and corner radii. For rectangular models, you can expect internal mounting areas ranging from approximately 34 × 34 mm for Size 1 up to 74 × 74 mm for Size 4.

Cable entry uses a 15 mm diameter knockout molded into the enclosure base. You can punch out this thin section with a screwdriver or similar tool for wire access. The knockout location varies by enclosure size, but typically sits near one edge to keep cables away from the PCB center. For applications requiring sealed cable entry, a separate cable gland or silicone sealant around the wire bundle would be necessary.

Wall mounting capability comes built into every enclosure through two oval slots molded into the base. These slots measure approximately 4 × 16 mm and accept user-supplied screws for securing the enclosure to vertical or horizontal surfaces. The oval shape also provides some tolerance for imperfect screw placement during installation. You can mount these enclosures with the lid opening upward, downward, or to either side depending on access requirements or your cable routing preference.

Vented models for ambient access applications

The 1551V series adds ventilation slots on all four vertical faces while keeping every other specification identical to 1551SNAP. Hammond explicitly designed these vented models for sensor applications where you need ambient air to reach the measurement devices. Temperature sensors, humidity detectors, pressure transducers, and air-quality monitors all require direct atmospheric contact for accurate readings. The ventilation pattern allows free airflow while maintaining the IP30 finger and tool protection.

Thermal management is a key application category for vented enclosures. Active components like voltage regulators, motor drivers, or high-power LED controllers generate waste heat that must be dissipated. The 1551V's four-sided ventilation promotes natural convection cooling. Hot air rises through upper vents while cooler air enters through lower openings, creating continuous circulation.

Choosing between solid versus vented models will come down to your primary concern. If dust, moisture, or electromagnetic interference poses the greater risk, select a 1551SNAP enclosure. Its solid walls provide better environmental protection and can be further sealed with gaskets if needed. If accurate sensing or thermal dissipation matters more, choose a 1551V model.

Conclusion

The 1551SNAP and 1551V series leverage a precision-molded ABS construction with snap-fit closure to eliminate screw clearance requirements, maximizing PCB real estate and simplifying iterative access during development. Uniform 20 mm profiles across seven form factors support standardized component heights, while integrated standoffs, knockout cable entry, and wall-mount slots enable streamlined mechanical integration. Vented variants further optimize thermal dissipation and sensor exposure without compromising IP30 ingress protection.

Visit DigiKey to explore the complete selection of Hammond enclosures for your next project.

Texas Instruments MSPM0G110x: integrated analog performance in an 80 MHz Cortex-M0+ package

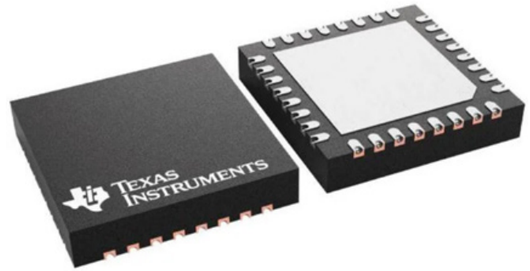
Texas Instruments

Adding discrete ADCs and operational amplifiers to microcontroller designs increases board space, component count, and bill-of-materials costs. Texas Instruments' MSPM0G110x family addresses these challenges by integrating the analog front-end directly into an 80 MHz Arm Cortex-M0+ microcontroller. The series delivers two simultaneous-sampling 12-bit ADCs running at 4 Msps, on-chip operational amplifiers, and configurable voltage references for demanding signal conditioning without external analog components.

A peek into the dual ADC architecture

The MSPM0G110x stands out with its dual 12-bit successive approximation register ADCs, each capable of 4 Msps conversion rates. You get up to 17 external analog input channels, allowing you to monitor multiple sensor inputs or measurement points simultaneously. The simultaneous sampling capability matters when you need to capture phase-aligned signals, such as in three-phase motor current sensing or synchronized multi-channel data acquisition.

If your application prioritizes precision over speed, you can enable hardware averaging to achieve 14-bit effective resolution at 250 ksps without writing averaging algorithms in software.



The Texas Instruments' MSPM0G1106TRHBR. Image source: TI

This on-chip oversampling reduces noise and improves measurement quality for applications like precision voltage monitoring or temperature sensing where you can trade conversion speed for better accuracy.

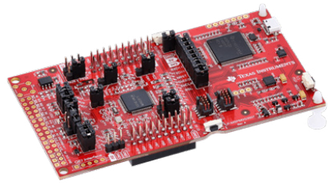
The integrated general-purpose amplifier uses chopper stabilization to minimize offset drift across temperature. You can configure this GPAMP as a unity-gain buffer, inverting or non-inverting amplifier, or programmable gain stage positioned directly before the ADC. Rail-to-rail input and output operation means you can condition signals spanning nearly the full supply range. For current sensing in motor drives or power monitoring applications, this avoids the need for discrete op-amps while keeping the analog signal path short and controlled.

Internal voltage references at 1.4 V or 2.5 V provide flexibility for different input signal ranges. When you need tighter reference accuracy than the internal sources provide, external reference inputs remain available. An integrated temperature sensor connects directly to the ADC channels for on-chip thermal monitoring. Keep in mind that when supply voltage drops below 2.7 V, only the 1.4 V reference continues operating.

Processing & memory options

An 80 MHz Arm Cortex-M0+ core delivers adequate headroom for signal processing algorithms alongside sensor management and communication tasks. You can choose from three memory configurations based on code complexity and data storage requirements. The MSPM0G1105 offers 32 KB flash with 16 KB SRAM for compact applications. The MSPM0G1106 doubles both to 64 KB flash and 32 KB SRAM, while the MSPM0G1107 provides 128 KB flash with 32 KB SRAM for more complex firmware or systems requiring extensive data logging.

Flash memory includes hardware error correction code to detect and correct single-bit errors, enhancing reliability for industrial



The LP-MSPM0G3507 LaunchPad development kit for 80 MHz Arm Cortex-M0+ MCUs. Image source: TI

environments. Selected flash sectors support up to 100,000 program and erase cycles for applications requiring frequent parameter updates or non-volatile data logging. SRAM includes optional hardware parity checking that detects single-bit errors in memory operations. These protection features address functional safety requirements without consuming processor cycles for software-based memory validation.

The memory protection unit allows you to partition application code from bootloaders or safety-critical routines, preventing unintended access between software modules. Two windowed watchdog timers provide system supervision, and hardware CRC-16 and CRC-32 acceleration verifies data integrity during communication or storage operations without overburdening the CPU.

Optimizing power consumption across operating modes

Power management operates across six primary modes, giving you control over current consumption based on system activity. At maximum performance, expect 101 microamperes per MHz when running CoreMark benchmarks from flash at 80 MHz. This active power consumption remains competitive for an M0+ core delivering this level of analog integration.

Low-power operation is critical in battery-powered or energy-harvesting systems. STANDBY mode consumes 1.5 microamperes while maintaining a 32 kHz crystal oscillator, real-time clock operation, and full SRAM retention with register states preserved. When you need minimal leakage, SHUTDOWN mode draws just 80 nanoamperes while keeping GPIO states intact and enabling wake-up from external signals. STOP mode at 190 microamperes with 4 MHz operation suits applications requiring periodic background processing without full-speed operation.

The wide operating voltage range from 1.62V to 3.6 V accommodates direct connection to lithium coin cells, two or three alkaline cells, or standard 3.3 V supplies. Wake-up from STANDBY to 32 MHz active operation completes in less than 4.5 microseconds, making event-driven architectures practical where you need fast response times without continuous processor operation.

Peripherals for motor control and industrial applications

The peripheral set targets industrial automation, motor drives, and smart appliances. Two 16-bit advanced control timers include deadband insertion and fault input handling crucial for driving half-bridge and full-bridge power stages. The complete timer subsystem provides up to 22 PWM channels across seven timers, with support for quadrature encoder input when you need position feedback in closed-loop motor control.

Communication interfaces cover standard embedded requirements through four UART ports, two SPI interfaces, and two I2C controllers. One UART supports LIN, IrDA, DALI, Smart Card, and Manchester encoding for specialized industrial protocols. One SPI interface operates at 32 Mbps for high-throughput sensor data or display updates. Both I2C controllers support Fast Mode Plus at 1 Mbps, plus SMBus and PMBus protocol variants common in power management applications.

A seven-channel DMA controller manages high-throughput data transfers between peripherals and memory without processor intervention. You can configure DMA to move ADC samples to memory buffers, feed DAC outputs from lookup tables, or handle serial communication without triggering interrupts on every byte. This automation reduces interrupt overhead and allows the processor to focus on signal processing or control algorithms.

Package options and GPIO configuration

Package choices range from 64-pin LQFP measuring 12 × 12 mm down to 24-pin VQFN at 4 × 4 mm, with a 28-pin DSBGA option measuring just 2.87 × 1.45 mm when board space is severely constrained. GPIO counts scale with package size: you get 60 general-purpose I/O pins on 64-pin packages and 20 GPIO on the smallest 24-pin variants. Two pins offer 5 V tolerant open-drain capability for interfacing with higher-voltage buses, while two high-drive outputs can source 20 mA for driving LEDs or small loads directly.

The MSPM0G1105 ships in 48-pin LQFP and VQFN packages. The MSPM0G1106 adds 64-pin LQFP options plus 32-pin VQFN and 28-pin DSBGA alternatives. The MSPM0G1107 with maximum memory offers the full range: 48-pin and 64-pin LQFP, 24-pin, 32-pin, and 48-pin VQFN, 28-pin VSSOP, and 28-pin DSBGA. The operating temperature is from -40°C to +105°C across all variants, supporting industrial and outdoor installations.

Getting started with development tools

For evaluation and development, the LP-MSPM0G3507 LaunchPad development board provides immediate access to the 80 MHz architecture. Code you develop for the MSPMG3507 transfers directly to G110x targets since both share the same core and peripheral architecture. The LaunchPad includes an onboard XDS110 debug probe with EnergyTrace technology for real-time power profiling during development.

The MSPM0 SDK version 2.08.00.03 includes DriverLib peripheral libraries, TI Drivers middleware, SysConfig graphical configuration tool, FreeRTOS support, and specialized middleware for motor control algorithms including field-oriented control implementations. Protocol stacks for SMBus, LIN, and DALI, plus EEPROM emulation libraries, accelerate common embedded tasks. Texas Instruments supports Code Composer Studio, IAR Embedded Workbench, and Keil (ARM) MDK development environments.

TI provides migration guides from STM32, STM8, PIC, and MSP430 families when you need to transition existing designs. The MSPM0-DIAGNOSTIC-LIB software library includes functional safety diagnostic routines targeting IEC 60730 Class-B requirements if your application requires certified safety measures.

Visit MSPM0G110x MCUs for more information.

Video spotlight

altera™

Agilex™ 3 FPGA C-Series Development Kit

The Agilex 3 FPGA C-Series development kit from Altera is a small form factor, power-efficient board targeting embedded design applications, such as industrial, surveillance, retail, consumer, video, and medical.

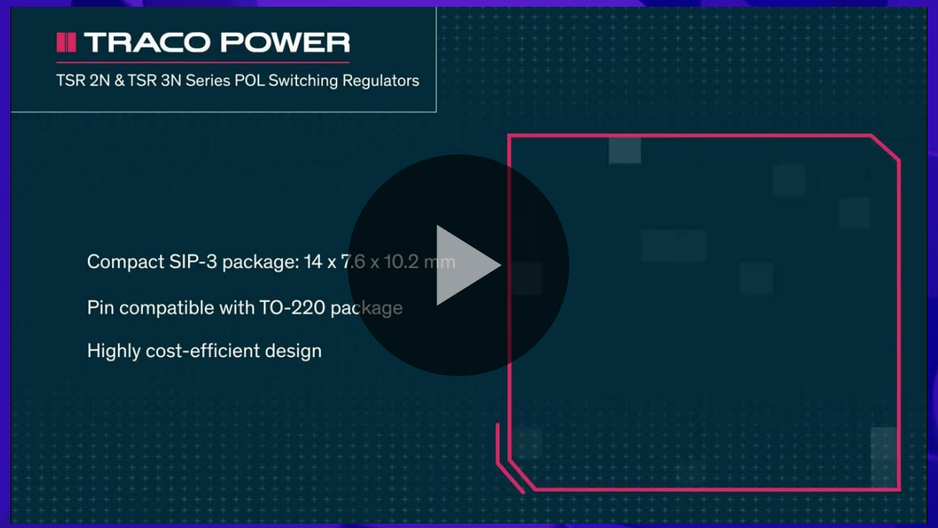
Learn more

STM32N6570-DK AI Demo with STM32N6

The STM32N6570-DK demo highlights advanced real-time AI neural network capabilities for computer vision applications. Equipped with the ST Neural-ART NPU and Arm® Cortex®-M55 processor, it ensures high-performance edge computing. Video animation uses NeoChrom GPU and an 800 MHz CPU to support AI model execution for intelligent vision-based and advanced graphics solutions.

Learn more

Video spotlight



TRACO POWER

Low Cost Power Solution from TRACO Power

The TSR 2N and TSR 3N step-down switching regulator series (2A and 3A) and a drop-in replacement for any TO-220 package linear regulators. These series come in a compact SIP-3 plastic package and complement our new generation of POL converters focusing strongly on a cost-efficient design while also improving on critical electrical specifications.

Learn more

ARDUINO

Raspberry Pi

Arduino vs. Raspberry Pi

Which should you use for your project, Arduino or Raspberry Pi? In this video, Becky Stern shows you the primary differences and explains why you would choose a microcontroller or single board computer (SBC) for your project.

Learn more

Written by David Ray, Cyber City Circuits

A sea of logic waiting for someone to shape it: from Signetics to Xilinx

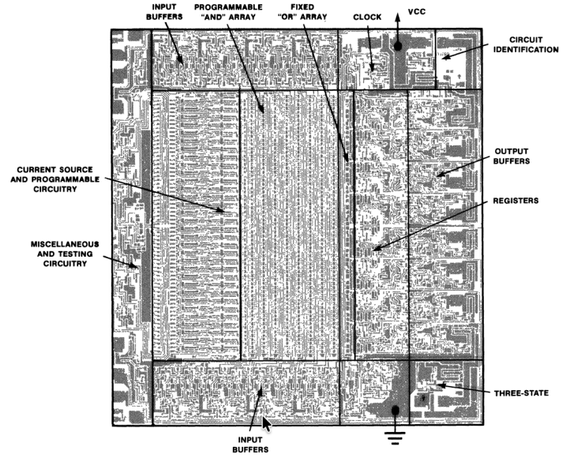
Field Programmable Gate Array

A Field-Programmable Gate Array (FPGA) is an integrated circuit that can be programmed to replace large groups of digital logic circuits. In the 1970s, as early 'computers' were being designed, they relied heavily on the 7400-Series TTL chips to implement every piece of combinational and sequential logic, resulting in boards populated with dozens or even hundreds of 'small' logic ICs. FPGAs would eventually collapse these sprawling networks of NANDs, NORs, inverters, counters, and decoders into a single programmable device. This is a brief milestone history leading to the first practical FPGA.

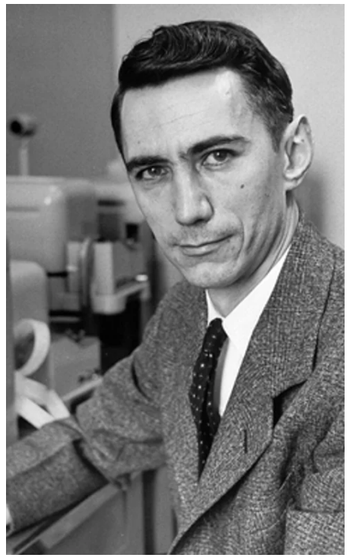
The lore behind digital logic

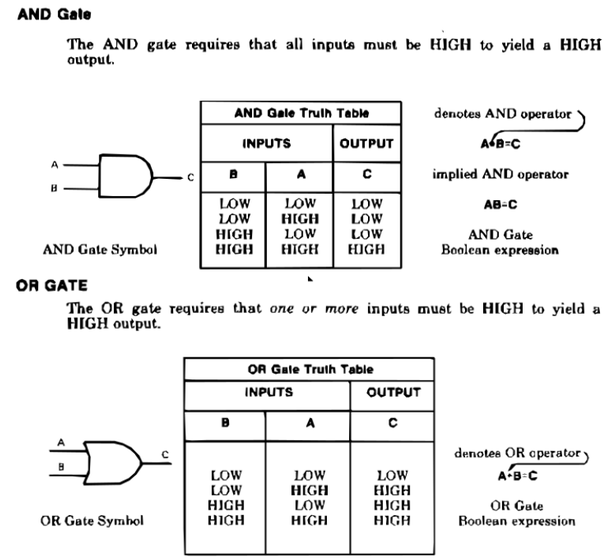
In 1937, mathematician and electrical engineer Claude Shannon wrote his master's thesis at MIT titled *'A Symbolic Analysis of Relay and Switching Circuits*,' officially establishing the field of switching theory and later information theory. It explains how someone can use standard Boolean Algebra/Logic (AND/NOT/OR) as a framework to encode, transmit, and decode information digitally using true and false statements. Shannon showed that every kind of message, letters, music, pictures, or data could be turned into bits of 1s and 0s, sent through a noisy channel, and still be recovered perfectly if encoded properly.

Using this methodology, it was found that any logic operation could be implemented using only AND and OR gates. Early on, this was done with vacuum tubes and later with discrete transistors. In the 1960s, TTL (Transistor-Transistor Logic) was formalized, and in 1964, Texas Instruments started producing the 7400-series of commercial TTL chips. Each step along the way, the pieces got smaller and smaller, going from tubes to transistors to integrated circuits, and by 1970, the size and cost of the standard through-hole DIP package were one of the major limiting factors of electronics design.

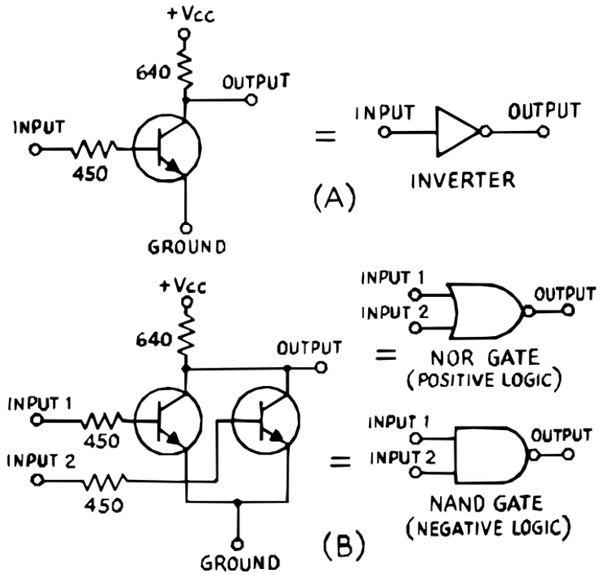


Annotated drawing of the MMI PAL16R6 die.



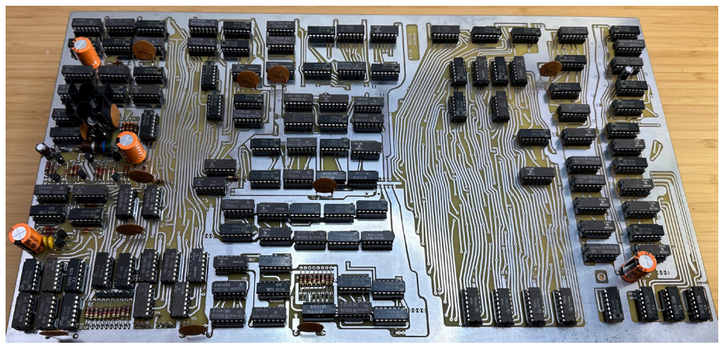


Claude Shannon showed that basic Boolean logic could be used to describe any type of information.



Before the proliferation of 7400-series logic ICs, discrete transistors were regularly used to build logic gates.

Early 'computer' boards consisted of a grid of 7400-series chips, with traces running in all directions, around, and through. At that time, the only alternative was for a designer to create an ASIC (Application Specific Integrated Circuit), but that was often too costly, making a field of ICs a more feasible option. To advance technology, it was necessary to integrate more of these logic chips together.



Before the invention of programmable logic devices, fields of logic ICs would have been needed to accomplish almost anything.

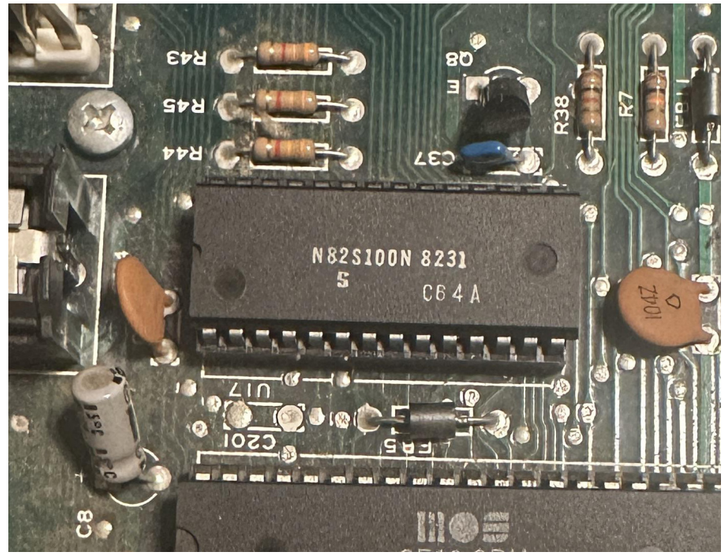
Retro Electro fun fact: in addition to his many accomplishments, Claude Shannon was also one of the organizers of the Dartmouth Summer Research Project in AI. Read more about that story in the Retro Electro article 'Programming a Calculator to Form Concepts.'

Programmable Logic Array (PLA) – Signetics 82S100

Signetics was founded in 1961 by a handful of former Fairchild Semiconductor employees. Fairchild had started developing the integrated circuit but did not want to shift its overall business focus from discrete transistors. The team left to start Signetics, the first company dedicated entirely to integrated circuits. The company designed many key op-amps, comparators, PROMs, DACs, and timers, as well as logic chips used in early computers.

In 1975, Signetics released the 82S100, Programmable Logic Array. The 82S100 consisted of an array of AND gates and an array of OR gates. It was 'programmable' by applying a higher voltage (typically 30V) to burn Ni-Cr fuses on the die, removing links in the array, allowing the developer to craft the logic series they want. Since it used burnable fuse links to connect the array, any mistakes made the IC unrecoverable. This particular series of chips never took the world by storm, but it was used in the Commodore 64, which, according to the Guinness Book of World Records, is the best-selling computer model of all time.

Later that year, Signetics was bought by Phillips, becoming Philips Semiconductor, and today, Signetics lives an assumed identity under the name NXP Semiconductors.



The Signetics 82S100 did not take the world by storm, but it was used in the Commodore 64.

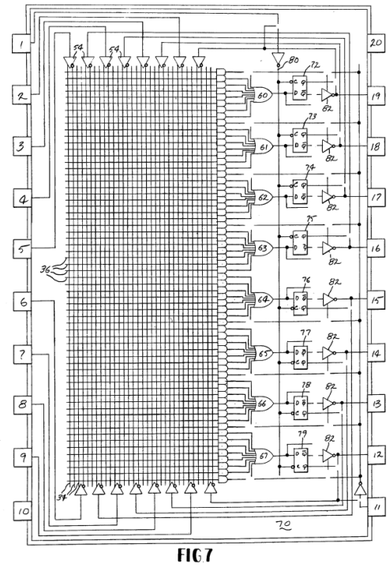
Programmable Array Logic (PAL) - Monolithic Memories Inc PAL16R6

Monolithic Memories Inc. was a company founded by another former Fairchild engineer in 1969, originally manufacturing PROM and 7400-series ICs. It turns out that the PROM manufacturing process was very conducive to making large gate arrays.

In 1974, they entered into a contract with General Electric to design a mask programmable logic device named 'Programmable Associative Logic Array,' so that GE engineers could design their sequential circuits into a silicon die mask quickly, making ASIC easier for them. Still, this PALA was never brought to the open market.

Retro Electro fun fact: Hans Camenzind, designer of the 555 timer, tried to solve this problem with the Monochip. An integrated circuit made up of a variety of logic gates was used to accomplish many routine tasks in the 1970s, serving as a middle ground between ASICs and discrete logic chips. Read more in the Retro Electro article 'Five-Five-Five: The Story of Interdesign Inc.'

In 1978, they released the Programmable Array Logic (PAL) chip, which had an architecture far simpler than Signetics' earlier attempt, and where Signetics didn't find much success, MMI did. They released custom software that could take an engineer's Boolean equations and output a fuse pattern to program the part.



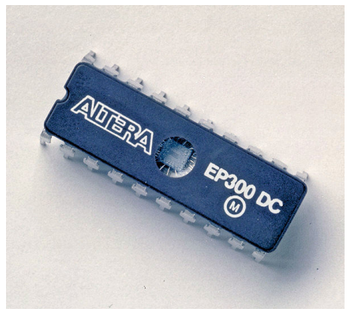
Basic schematic drawing of the PAL 16R6.

They later developed an alternative called Hard Array Logic (HAL), a mask-programmed version of the PAL architecture. Like GE's earlier PALA concept, HAL devices were not field-programmable; instead, MMI customized the metal mask for each customer, giving them a fast, low-cost path to ASIC-like devices without changing the underlying PAL structure.

In 1987, MMI was merged with Advanced Micro Devices (AMD), becoming the world's largest programmable logic manufacturer at the time. It was later spun off into its own company named 'Vantis' (1997), which was then acquired by Lattice Semiconductor (1999).

Erasable Programmable Logic Devices (EPLD) – Altera EP300

In 1980, engineers from Intel, Signetics, Hewlett-Packard, and Fairchild started a design consulting company named 'Source III.' They worked with other companies to be a 'middleman' for silicon suppliers. Doing this, they got to know the ASIC industry very well and got them thinking they could do it better. In 1983, they founded a new company, Altera, to enter the PAL market.



The EP300 was first in a successful series of programmable logic devices.

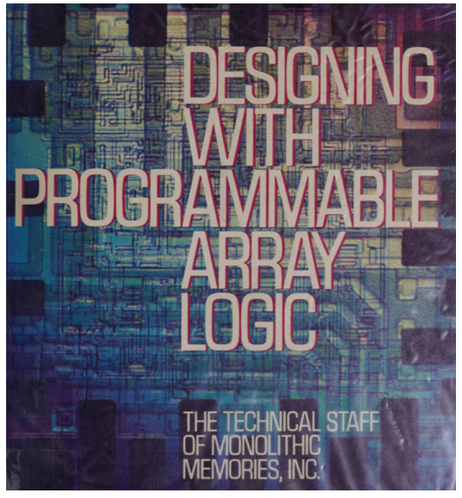
In July 1984, they released their first in a series of EPLDs named the EP300. The EP300 was built on the new CMOS logic technology and has a window on the top of the package that allows the internal EPROM to be erased and reused by shining an ultraviolet light through it. This is noteworthy as the first successful IC of its type that was reprogrammable.

Early on, Altera's business model included licensing the intellectual property and core logic designs behind its programmable devices to companies like Intel, enabling Intel to build and sell its own PLD product lines based on Altera technology. In 1994, Altera purchased Intel's entire PLD division for $50 million, and twenty years later, in 2015, Altera itself was acquired by Intel for over $16 billion in cash, forming Intel's new Programmable Solutions Group (PSG). In 2025, Intel spun off PSG as an independent company once again under the Altera name, restoring the company's legacy and brand.

Field Programmable Gate Array (FPGA) - Xilinx XC2064

In February 1984, just five months before Altera released the EP300, a group of ZILOG engineers left to start Xilinx. Led by former Director of Engineering Ross Freeman, Bernie Vonderschmitt, and Jim Barnett, Xilinx was started with the mission of providing a fast, flexible alternative to ASICs by making a logic device that customers could program after manufacturing. Not a PAL. Not a PLA. Not some kind of PROM-based logic. Something new.

Retro Electro fun fact: the name Altera is a portmanteau of the term 'alterable,' since their primary products would be reprogrammable devices.



The PAL was more popular than its competition because it was easier to use, and MMI published a lot of quality documentation about it.

Ross Freeman

In 1987, MMI was merged with Advanced Micro Devices (AMD), becoming the world's largest programmable logic manufacturer at the time.

Freeman's concept was fundamentally different from every programmable device that came before it. Where earlier devices were essentially large arrays of AND gates and OR gates. The designs were tied to Boolean logic. They were not easily scalable because, as they grew, their performance degraded. PLAs and PALS inherited fabrication methods similar to memory arrays, making it easy to manufacture, but Freeman's design, described in US Patent 4,870,302, removed the large field of AND gates altogether. Instead, it used a bunch of individual configurable logic blocks connected by programmable switches. Each logic block was built with its own lookup table, with the output of one serving as the input to the next.

The first Xilinx FPGA was designed by an engineer named Bill Carter, with the guidance of Ross Freeman. One of the limitations that Xilinx had was that they did not have any way to 'fab' their silicon dies in the US, so they built a relationship with Seiko, who use a 2.5 µm CMOS process for their digital wristwatch manufacturing. Nobody in the company had worked with those constraints before, as it was a newer technology and was not made available in American foundries.

This partnership with Seiko was beneficial to both parties: Seiko gained the license to sell the product in the Japanese market, and Xilinx did not have to worry about die fabrication. This is noteworthy in history as the first successful American

The XC2064 fundamentally changed how programmable logic devices could work, making them faster by many orders of magnitude.

semiconductor ‘start-up’ built entirely on the fabless model that dominates the industry today.

In 2020, Advanced Micro Devices (AMD) acquired Xilinx.

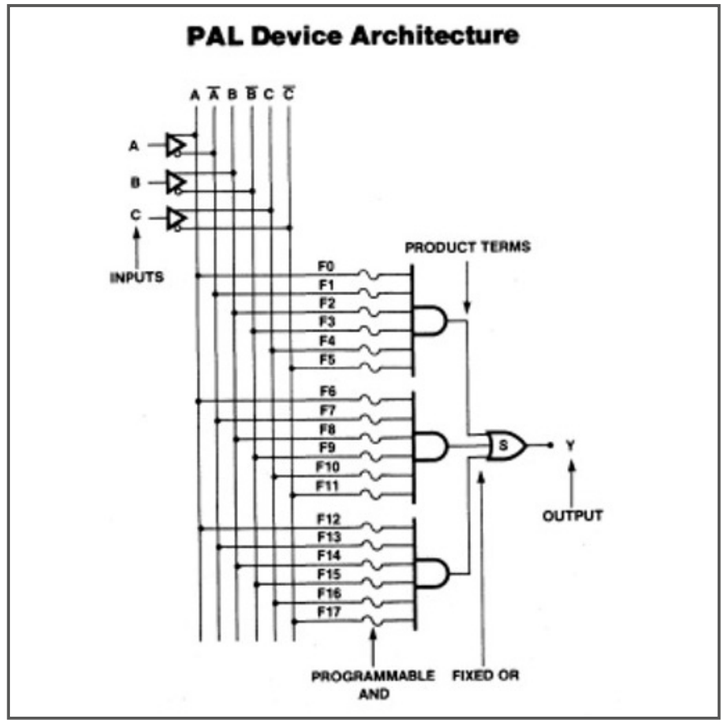
Today – the age of reconfigurable logic

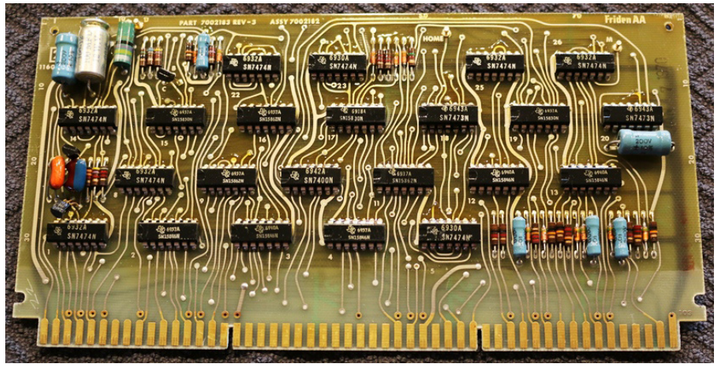
Today’s FPGAs bear little resemblance to the hand-drawn layouts and watch-chip-grade CMOS that birthed the XC2064 in 1985, yet the core idea remains unchanged: a sea of tiny logic blocks waiting for someone to give them purpose. What began as a workaround for slow ASIC turnarounds has become a foundational technology for everything from 5G radios to spacecraft to AI accelerators.

The lineage runs straight through Signetics’ fuses, MMI’s PALs, Altera’s erasable logic, and Xilinx’s first FPGA, to a world where logic is now limited less by silicon and more by imagination.

Digikey is a distribution partner for AMD and its Xilinx series of parts.

https://www.digikey.com/en/supplier-centers/xilinx





retroelectro

1937

Claude Shannon publishes his master’s thesis ‘A Symbolic Analysis of Relay and Switching Circuits.’

1964

Texas Instruments introduces the 7400-series TTL ICs.

1975

Signetics releases the 82S100 PLA, the first commercially available programmable logic device.

1978

MMI introduces the PAL, becoming a successful programmable logic controller.

1984

Altera releases the EP300, the first erasable and reprogrammable logic controller.

1985

Xilinx releases the first XC2064 FPGA.

Suggested reading

1. “How the FPGA Came To Be, Part 5” by Steven Leibson with EEJournal
2. “The History of the FPGA: The Ultimate Flex” by Asianometry
3. “Oral History of Bill Carter” Interviewed by Steve Trimberger for the Computer History Museum
4. “The Very First Programmable Logic Device: Signetics 82S100” by ElectronUpdate
5. “Altera EP300 Design & Development Oral History Panel” by Computer History Museum
6. “A Mathematical Theory of Communication” by Claude Shannon
7. “A Symbolic Analysis of Relay and Switching Circuits” by Claude Shannon
8. “Signetics FPLF Oral History Panel” by Computer History Museum
9. Signetics 82S100 Datasheet
10. “1978: PAL User-Programmable Logic Devices Introduced” by Computer History Museum
11. US Patent 4124899: Programmable Array Logic Circuits
12. “Programmable Array Logic Handbook Third Edition” by Monolithic Memories Inc.

How to use FPGAs in resource-constrained applications

By Kenton Williston

The need for configurable logic is growing across resource-constrained embedded systems. Applications such as Edge AI, machine vision, and industrial automation require flexible, application-specific logic to meet evolving performance demands while operating within strict power, size, and cost limits. Modern field programmable gate arrays (FPGAs) can address these competing demands.

This article reviews key design criteria to consider when selecting an FPGA for resource-constrained applications. It then describes how different product lines align with specific scenarios using examples from Altera's portfolio of power and cost-optimized FPGAs. It concludes by highlighting development kits and evaluation boards that can be used to prototype and validate design concepts.

Considerations for choosing an FPGA

Choosing an FPGA for a resource-constrained system involves consideration of multiple design requirements and matching those to the correct solution. There are several key FPGA characteristics to consider:

Logic element (LE) capacity: As the fundamental building block for an FPGA, the number of LEs determines how much custom logic can be implemented. Higher counts enable more complex designs: the tradeoff is increased power, cost, and package size.

I/O and memory: FPGAs are often used to connect disparate components within a system, making the number of I/O pins a key consideration. To boost I/O performance, many FPGAs incorporate hardened, fixed-logic blocks for interfaces such as PCI Express (PCIe), high-speed memory, and multi-gigabit transceivers.

In addition, some FPGAs integrate features such as analog-to-digital converters (ADCs) and Flash memory. These enhancements can reduce the need for companion chips, conserving board space and improving power efficiency.

Processor integration: Instead of using an external processor, a 'soft' microprocessor unit (MPU) can be implemented within the FPGA. This approach can reduce the footprint of a system, but it is best suited to applications with less demanding MPU workloads.

For applications that need faster, more efficient MPUs, designers can consider an FPGA with a hard processor system (HPS) that will implement an MPU as a fixed-logic block within the FPGA.

Hardware accelerators: FPGAs typically include dedicated digital signal processing (DSP) blocks that efficiently handle compute-intensive tasks like motion control. Higher-end devices may feature specialized tensor blocks for AI workloads. The capabilities of these accelerator blocks vary significantly between FPGA families and can dramatically influence overall system performance.

Package and power optimizations: Some FPGAs are specifically designed to minimize their physical and electrical footprint. For example, they may offer low-power sleep modes.

Tools: Crafting custom logic can be a daunting challenge, particularly for designers who are new to the process. Tools like Altera's Quartus Prime Design Software have emerged to streamline the process.

Built to make FPGA design more accessible, Quartus Prime offers a developer-friendly experience, an extensive catalog of pre-built logic blocks, and the ability to interconnect these logic blocks automatically. The tool integrates with popular AI and machine learning (ML) workflows, enabling developers to deploy popular operating systems (OSs) like Linux and Zephyr on an FPGA.

Capabilities like these can significantly accelerate FPGA design, making tool features a critical consideration when selecting a device.

High-performance compute for advanced embedded workloads

To illustrate how design requirements influence FPGA selection, it is helpful to begin with high-end applications that require exceptional compute density, bandwidth, and integration. Examples include advanced edge AI applications and high-performance industrial gateways.

Agilex 3 FPGAs (Figure 1) are designed to meet these application demands, offering up to 135K LEs. The chips are available in both FPGA-only and system-on-chip (SoC) variants. The SoC devices integrate a dual-core, 800 megahertz (MHz) Arm Cortex-A55, enabling the FPGA to take on complex software stacks like human-machine interfaces (HMIs) or network stacks.

The programmable fabric features AI Tensor blocks capable of delivering up to 2.8 INT8 tera operations per second (TOPS). These blocks support various compute formats, including FP16, FP19, FP32, and BFLOAT16, and are optimized for efficient execution of AI workloads. Variable-precision DSP blocks are also included, delivering up to 180 giga floating-point operations per second (GFLOPS) performance for general-purpose signal processing.

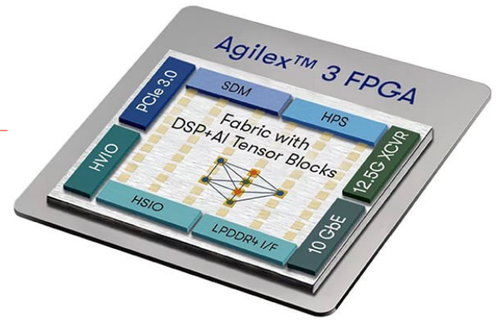
High-speed connectivity is another strength of the Agilex 3 architecture. Transceivers support data rates up to 12.5 gigabits per second (Gbits/s), with hardened I/O blocks available for PCIe 3.0, 10 gigabit Ethernet (GbE), and LPDDR4 memory interfaces. Support for IEEE 1588 precision time synchronization further enhances its suitability for real-time industrial networking.

The A3CZ135BB18AE7S device illustrates the capabilities of this family. It includes 135K LEs, 184 DSP blocks, and delivers 2.54 TOPS.

Advanced integration for complex systems

For applications like industrial automation and mid-range vision systems, raw compute power can be less important than the ability to support complex configurations

Figure 1: The Agilex 3 is notable for its high-performance DSP and AI Tensor blocks.
Image source: Altera



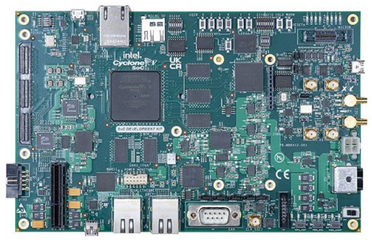


Figure 2: The DK-DEV-5CSXC6N-B Cyclone V development kit supports high-performance prototyping. Image source: Altera

with large amounts of custom logic and I/O. Cyclone V FPGAs are well-suited to these scenarios, offering up to 300K LEs and extensive high-speed interfaces. Like the Agilex 3, these chips are available in FPGA-only and SoC variants. In this case, the SoC devices integrate a dual-core Arm Cortex-A9.

The programmable fabric in these chips includes variable-precision DSP blocks that support triple 9 × 9 and dual 18 × 18 fixed-point multiplication, and 27 × 27 fixed or floating-point multiplication. These blocks can be used for advanced signal processing and AI.

A broad mix of I/O supports multiple voltage levels and interface types. Hardened logic blocks enable advanced high-speed connectivity, including PCIe 2.0, DDR3 controllers, and transceivers operating at up to 6.144 Gbits/s.

Developers can evaluate the Cyclone V SoC family using the DK-DEV-5CSXC6N-B Development Kit (Figure 2). This kit is designed for rapid prototyping of complex, high-throughput systems.

The kit includes several notable features:

- Dual Ethernet ports, a PCIe x4 connector, and a high-speed mezzanine card (HSMC) with 16 LVDS channels in each direction
- USB 2.0 OTG, CAN, UART, and a two-line text LCD interface
- 1 gigabyte (Gbyte) DDR3 SDRAM each for the FPGA and HPS sides, 128 megabytes (Mbytes) quad SPI Flash, and a 4 Gbyte microSD card

The board features the 5CSXFC5D6F31C8N device, which includes a dual-core Arm Cortex-A9 processor running at 600 MHz, with 85K LEs, 87 DSP blocks, and 288 I/O pins in a 31 mm × 31 mm, 896-FBGA package.

Power-efficient configurable logic in a compact package

Tight constraints around space and power consumption define many applications. Examples include sensor interfaces, power sequencing, and peripheral control. FPGAs such as the MAX 10 family offer an effective solution in these cases. MAX 10 devices are available in configurations from 2K to 50K LEs and packages as small as 3 mm × 3 mm.

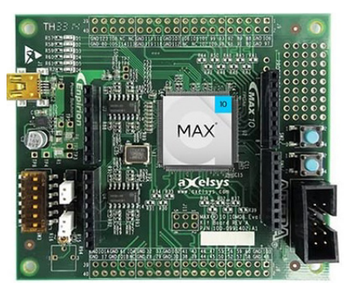
Key features include up to two integrated 12-bit ADCs, a DDR3 memory interface, and multiplier blocks that support 18 × 18 and dual 9 × 9 fixed-point modes. On-chip Flash with support for dual image storage allows the FPGA to configure itself without an external memory device.

Power-saving capabilities are one of the MAX 10 family's most distinctive attributes. A built-in sleep mode can reduce dynamic power consumption by up to 95%. Thanks to the on-chip Flash, devices can also be fully powered down and then resume operation in under 10 milliseconds (ms).

A single-supply option further simplifies power delivery. This makes MAX 10 devices especially well-suited to supervisory roles, where power domains may need to come online before the rest of the system.

Developers interested in the MAX 10 can evaluate the family using the EK-10M08E144 MAX 10 FPGA evaluation board (Figure 3). This board provides access to external signals via Arduino UNO R3 connectors and test points, with a layout designed to support the measurement of ADC performance and overall power behavior.

Figure 3: The EK-10M08E144 MAX 10 FPGA evaluation board provides easy access to key I/O. Image source: Altera



The board features the 10M08SAE144C8G device, which includes 8K LEs and a single ADC in a 144-pin LQFP package. In addition to its built-in hardware resources, this FPGA supports the RISC-V-based Nios V soft processor, enabling designers to implement lightweight control functions without needing an external microcontroller unit (MCU).

Balanced performance for mid-range applications

Some applications require more logic and I/O capacity than entry-level FPGAs can provide. Examples include sensor fusion, motion control, and chip-to-chip bridging. Cyclone 10 LP FPGAs address these requirements by offering up to 120K LEs and 525 I/O pins in devices optimized for balanced power and bandwidth in cost-sensitive applications.

Like the MAX 10, the family includes DSP blocks suitable for workloads such as filtering, control loops, and basic AI inferencing. Unlike the MAX 10, Cyclone 10 LP devices incorporate true LVDS transceivers and on-chip termination (OCT) to support high-speed digital interfacing.

Developers interested in the Cyclone 10 LP can evaluate the family using the EK-10CL025U256 Cyclone 10 evaluation kit (Figure 4). This board offers Arduino UNO R3 and Digilent Pmod connectors for easy expansion. Other features include GbE, USB 2.0, 128 megabits (Mbits) of SDRAM, and 64 Mbits of Flash memory.

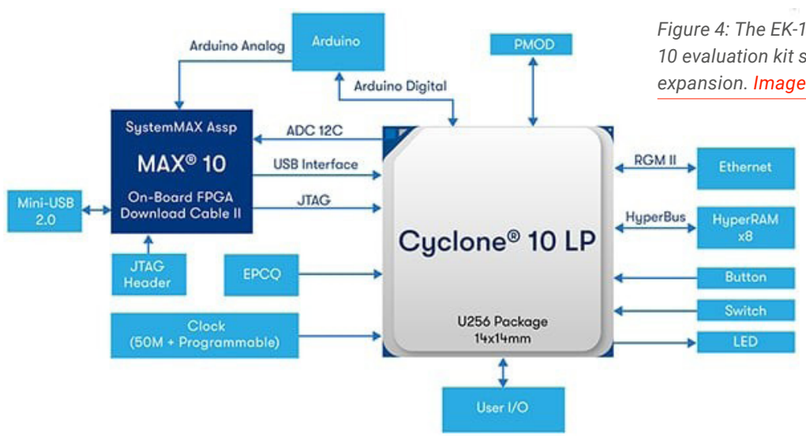


Figure 4: The EK-10CL025U256 Cyclone 10 evaluation kit supports easy peripheral expansion. Image source: Altera

The board features the 10CL025YU256C8G device, which includes 25K LEs, 66 DSP blocks, and 150 I/O pins in a 14 mm × 14 mm package. Like the MAX 10, the Cyclone 10 LP family supports the Nios V soft processor.

Conclusion

Designers now have more flexibility than ever when implementing custom logic in embedded systems. High-performance applications can benefit from FPGAs with integrated AI accelerators. Low-power designs can take advantage of devices with sleep modes. I/O-intensive systems can leverage chips with large pin counts and high-speed interfaces. Importantly, all these capabilities can be realized within the tight limitations of resource-constrained embedded systems with easy-to-use kits.

Smart beacons leverage Bluetooth system-on-a-chip for connected ML insights

By Jessica Shapiro

Today's product development and support cycles move fast. Embedded products that detect software and hardware faults and provide insight into user behavior, supply the data that engineers need to keep equipment working and improving.

But not all industrial equipment is wired for easy connectivity to support these embedded products. Even products designed for the Internet of Things (IoT) can encounter connectivity issues such as electromagnetic interference (EMI), limited bandwidth, and long cable runs.

The emergence of Bluetooth-enabled System-on-a-Chip (SoC) technology gives engineers access to seamless connectivity alongside microprocessor power that supports on-board machine learning (ML). This pairing of connectivity with smart analytics is a valuable tool in a proactive, instead of reactive, design and support cycle.

Smart data collection transforms product development and support

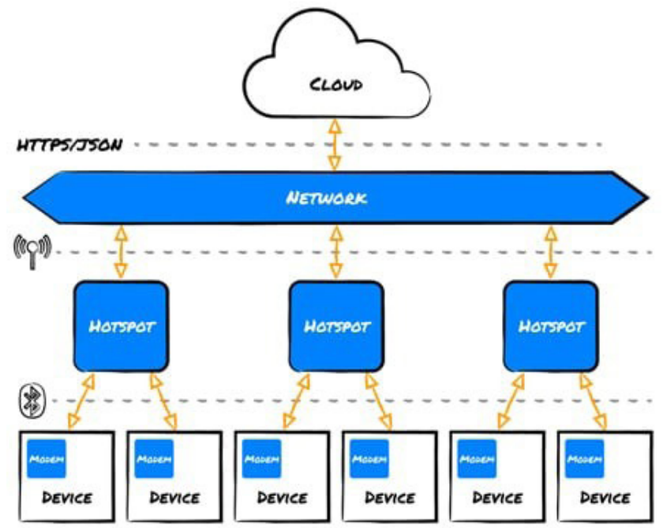
Successful product development and support require usage data. Designers who don't know how customers are using a product, including which features they rely on and which ones are cumbersome or buggy, will have trouble iterating the product to an upgrade users want. Likewise, support personnel can't adequately troubleshoot problems without knowing user behavior, system status, environmental conditions, and other key data right before or during the problem.

A product with modern onboard connectivity and analytics can make both design iteration and support more effective. Embedded products and smart beacons can detect environmental conditions like temperature, humidity, and barometric pressure, as well as sensing acceleration in multiple axes, ambient light, and magnetic fields. Timestamps from a real-time clock (RTC) allow the data to be correlated with other system events, either using onboard analytics or when broadcast to a Cloud server via Bluetooth.

For example, a smart beacon attached to a linear motion system in an industrial environment might detect that vibrations increase when humidity is elevated. On-board processors could then broadcast an alert to maintenance engineers that additional lubrication is needed. This kind of proactive troubleshooting reduces equipment downtime and maintenance costs.

Product designers might also use the logged vibration and environmental data to improve future versions of the linear motion system. For instance, they

Figure 1: Smart beacons and other devices can use Bluetooth to connect to the nearest hotspot without pairing. Hotspots can enable Bluetooth mesh networks or connect to cloud services via Wi-Fi. Image source: Blecon Ltd



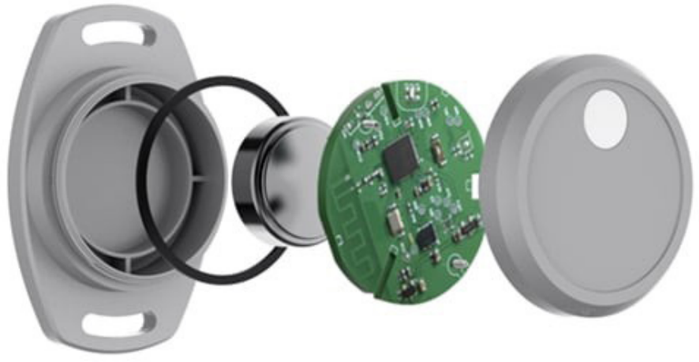


Figure 2: L02S-BCN smart beacons have BLE connectivity, multiple sensing options, high-visibility LEDs, and a field-replaceable battery in an IP67 enclosure.
Image source: Blecon Ltd

might recommend a different lubricant that lasts longer in humid conditions. They might also redesign the lubrication system to better protect it from the elements.

Implementation challenges and solutions

In order to realize the benefits of enhanced data collection in an IoT setting, engineers must optimize data collection and analysis. Any transfer of information to the cloud for analysis has inherent latency and reduces data security. Embedded systems and smart beacons combat this by packaging AI and ML capabilities into the units themselves. These Edge AI and TinyML systems contain scaled-down software models that allow the processors to make intelligent inferences based on the real-world data they receive.

Onboard ML capabilities can be as simple as matching vibration data, environmental data, and a global timestamp, or complex enough to predict maintenance needs based on data trends. Whether complex or straightforward, the ML module receives and processes real-time data without utilizing network resources, resulting in timely insights and minimal energy use.

Still, smart beacons and embedded systems eventually need to communicate status to other devices or to a server via a network. Many legacy systems are designed for wired serial connectivity with protocols like PROFIBUS, DeviceNet, CANOpen, and Modbus RTU. More modern equipment relies on low-latency Ethernet-based protocols like PROFINET, EtherCAT, EtherNet/IP, or Ethernet POWERLINK. However, both serial and Ethernet communication require cables for data and power across factory floors with the attendant challenges of EMI, signal degradation over long cable runs, and the facilities investment needed to mitigate trip hazards and provide pathways for driven or autonomous vehicles.

Short-range, radio frequency (RF) communication using Bluetooth protocols overcomes many of these challenges. Some versions of Bluetooth, like Bluetooth Low Energy (BLE), are designed to broadcast strong signals up to 150 m on the power available from a button battery, removing the need for both power and data cables.

A BLE signal runs in the 2.4 GHz band that also supports some cellular and Wi-Fi networks. While the shared band can lead to network interference and reduced signal integrity, it is also the most reliable band for overcoming line-of-sight obstacles, such as walls and equipment. To overcome line-of-sight and interference concerns, many BLE systems can be mesh networked to utilize Internet Protocol version 6 (IPv6) to connect BLE devices to each other and to the Cloud (Figure 1). Strategically placed Bluetooth hotspots can also boost signal strength and integrity within the mesh network.

Smart beacons bring analytics and networking together

Marrying data collection, AI and ML inference engines, and network connectivity, Bluetooth-enabled smart beacons provide product operation, user behavior, and predictive maintenance insights, even on equipment that's not designed for embedded systems. One example is the L02S-BCN by Blecon LTD (Figure 2).

L02S-BCN smart beacons are driven by nRF54L15 series multiprotocol SoCs (Figure 3) from Nordic Semiconductor. These chips combine a multiprotocol 2.4 GHz radio that supports Bluetooth version 5.4, IEEE 802.15.3-2020, and 2.4 GHz protocols at data transmission speeds up to 4 Mbps with a 128 MHz Arm Cortex-M33 processor running on 265 KB of RAM. The 1.5 MB of non-volatile memory can store sensor readings and analyses if network connectivity is unavailable.

The nRF54L15 chip has built-in security designed for IoT systems. TrustZone isolation, side-channel protection, and tamper-detection protocols certify it to platform security architecture (PSA) Level 3. These systems ensure data payloads transmitted from L02S-BCN beacons are encrypted for secure transport and that network node identities are verified from the Cloud via two-way communication.

The nRF54L15 chips also have built-in peripherals that allow L02S-BCN smart beacons to collect, analyze, and share data from IoT systems. A 14-bit analog-to-digital converter (ADC) translates signals from temperature, humidity, barometric pressure, acceleration, and photosensitive sensors into digital data, while a global RTC creates a time stamp for each reading. Five serial interfaces, including serial peripheral interfaces (SPIs), two-wire interfaces (TWIs), and universal asynchronous receiver/transmitters (UARTs), connect processing and sensing components.

In addition to these physical sensor options, L02S-BCN beacons also act as embedded devices, using pre-integrated Memfault software on open standard Reduced Instruction Set Computing version five (RISC-V) coprocessors to detect and report crashes, software faults, battery status, and user behavior to the cloud. Memfault also manages over-the-air (OTA) updates, so there's no need to recall deployed devices.

L02S-BCN beacons also demonstrate the use of Edge Impulse, an Edge AI platform, to deliver ML without using network resources. Edge AI removes latency and allows L02S-BCN beacons to operate on 1000 mAh CR2477 button batteries that can be replaced in the field. The 69.9 mm tall by 46.7 mm wide by 18 mm thick L02S-BCN beacons have IP67-rated enclosures that exclude dust and withstand immersion in 1 m of water for up to 30 minutes. The beacons can be mounted to equipment using double-sided adhesive, screws, or zip ties.

Figure 3: The nRF54L15 series multiprotocol SoCs have multifunction radios, PSA Level 3 security, a 128 MHz processor with 256 KB RAM, and hardware and software peripherals that support Edge AI and ML.
Image source: Nordic Semiconductor

Conclusion

Bluetooth smart beacons bring sensing, connectivity, and Edge AI and ML to industrial and IoT applications. Powered by SoCs like Nordic Semiconductor's nRF54L15 that support data collection, zero-latency analytics, and OTA updates, smart beacons such as Blecon's L02S-BCN overcome barriers to connectivity to turn industry-deployed equipment into embedded products with ML capabilities.

By Tawfeeq Ahmad

iWave telematics solutions aligned with international & EU cybersecurity standards

With the rapid expansion of connected automotive and telematics systems, cybersecurity has become a non-negotiable requirement. Driven by European regulations such as the Cyber Resilience Act (CRA) and the Radio Equipment Directive Delegated Act (RED DA), the expectation is clear: telematics devices must be secure by design.

iWave's telematics portfolio including TCUs (Figure 1), gateways, and data loggers – has been engineered with cybersecurity as a foundation. Each solution incorporates strong technical and process-oriented controls aligned with global and EU regulations, including ISO/SAE 21434, ISO 24089, UNECE WP.29 (UN R155, UN R156), CRA, RED DA, and the EN 18031 series. Conformance to these frameworks is critical not only for compliance but also for building trust and gaining access to regulated markets.

Figure 1: Typical iWave G26 telematics control unit. Image source: iWave

Key standards shaping telematics security

1. **ISO/SAE 21434 (road vehicles – cybersecurity engineering):** Establishes a structured, security-by-design development process. It mandates comprehensive Threat Analysis and Risk Assessment (TARA) to identify vulnerabilities in communication protocols, cloud integration, and firmware updates. Validation includes extensive penetration testing and simulation of both remote and physical attack vectors, covering the entire lifecycle of telematics devices.

2. **UN R155 (Cybersecurity Management System – CSMS):** Issued by UNECE WP.29, UN R155 requires vehicles to comply with a Cybersecurity Management System as part of type approval. It references ISO/SAE 21434, ensuring that processes like TARA and penetration testing are embedded in engineering workflows. Demonstrating adherence to ISO/SAE 21434 is the principal method of showing compliance with UN R155.

3. **UN R156 (Software Update Management System – SUMS):** Focuses on secure, traceable software updates. iWave's devices implement Secure Boot and Encrypted Boot, supported by hardware security elements, ensuring OTA updates meet the integrity and authenticity requirements of UN R156.

4. **ISO 24089 (software update engineering):** Complements UN R156 by detailing processes for safe, reliable software updates across the vehicle lifecycle – covering authenticity, delivery mechanisms, integrity, and traceability.

5. **EU Cyber Resilience Act (CRA):** Applicable to all digital products, including telematics, the CRA requires security across the complete product lifecycle. iWave's security features align with CRA's goals of lifecycle transparency and protection against vulnerabilities.

6. **EU RED Delegated Act (RED DA) and EN 18031 standards:** Effective from August 2025, RED DA mandates cybersecurity protections for internet-connected radio equipment. The EN 18031 series supports this with detailed requirements:

   - EN 18031-1 – network protection: prevents devices from harming communication networks. iWave achieves compliance through efficient communication protocols, TLS 1.3-based encryption, and robust error handling.
   - EN 18031-2 – user data & privacy protection: secures personal data with encryption in storage and transmission, protects against unauthorized tracking, and enforces strong authentication and access controls.

How iWave implements compliance

Secure boot: all iWave telematics products integrate secure boot technologies (Figure 2) – High Assurance Boot (HAB), Advanced HAB (AHAB), and cryptographically validated firmware loading – ensuring only trusted code runs at startup.

Figure 2: All of iWave's telematics products, including the pictured G41 telematics gateways, integrate secure boot technologies. Image source: iWave

- **Secure storage:** sensitive data, including encryption keys and critical application information, is safeguarded with hardware-backed encrypted storage, maintaining confidentiality and integrity.
- **Threat analysis & penetration testing:** consistent with ISO/SAE 21434, iWave continuously performs TARA and in-depth penetration testing to uncover vulnerabilities and validate resilience against attacks.
- **Authentication:** strong user and system authentication mechanisms prevent unauthorized access and reinforce telematics network integrity.
- **AppArmor access control:** by enforcing application-specific security profiles, iWave limits each program's capabilities, reducing the attack surface and adhering to the principle of least privilege.

Conclusion

By embedding cybersecurity into design and development, and by adhering to international and EU regulations such as ISO/SAE 21434, UN R155, UN R156, ISO 24089, CRA, and RED DA, iWave's telematics portfolio delivers resilient, regulation-ready solutions. With a combination of secure boot, encrypted storage, authentication, access control, and ongoing penetration testing, iWave ensures that its telematics systems provide the assurance required for connected vehicle applications in the European and global markets.

Highly integrated MCUs simplify precise and efficient motor control design

By Kenton Williston

When my high schooler joined the robotics club, I was one proud dad. However, it wasn't long before he began to share familiar design problems. A big challenge for him was finding motor control hardware that was precise, efficient, and user-friendly.

In our professional world, these same demands crop up when designing everything from home appliances to industrial automation. That's why I'm intrigued by Infineon's new PSOC Control C3 microcontroller units (MCUs).

An efficient architecture for advanced motor control

The PSOC Control C3 family is offered as a high-performance yet efficient solution for advanced motor control. These MCUs are built around an Arm Cortex-M33 core with digital signal processing (DSP) and a floating-point unit (FPU) (Figure 1). This core is complemented by high-performance peripherals optimized for systems using power devices based on wide-bandgap technologies such as silicon carbide (SiC) and gallium nitride (GaN).

Three Control C3 MCU peripherals are particularly noteworthy:

- The high-performance 12-bit successive approximation register (SAR) analog-to-digital converter (ADC) offers true synchronous idle sampling of up to 16 analog signals. This is crucial for accurately capturing fast-changing waveforms, such as motor phase currents in field-oriented control (FOC) systems or grid voltages in a solar inverter.

Figure 1: The PSOC Control C3 MCUs feature powerful peripherals built around an Arm Cortex-M33 core with DSP and an FPU. Image source: Infineon

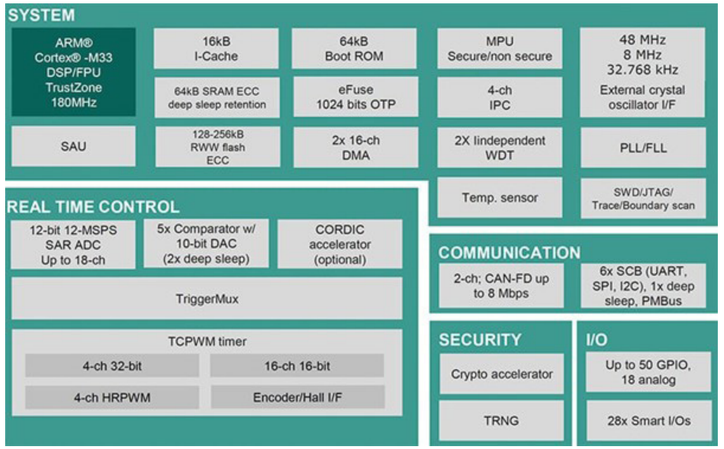


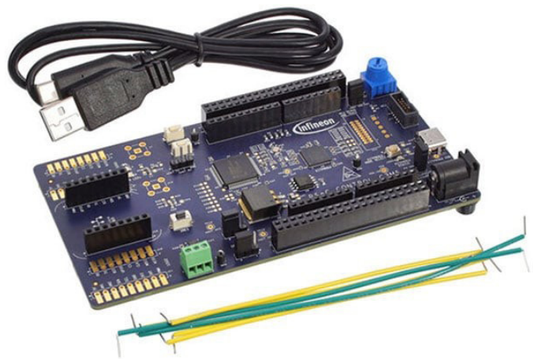
Figure 2: The PSC3M5FDS2AFQ1XQSA1 Main Line MCU combines the 180 MHz Arm Cortex-M33F core with 256 Kbytes of flash memory in a PG-LQFP-80 package. Image source: Infineon

- The optional coordinate rotation digital computer (CORDIC) math accelerator offloads trigonometric and other transcendental functions from the Arm core. This benefits algorithms like the Park transforms in FOC systems and phase-locked loops (PLLs) in grid-tied power conversion.
- The timer/counter pulse width modulation (TCPWM) blocks can generate precise switching signals and integrate a motion interface (MOTIF), providing direct hardware support for Hall and quadrature encoders used in sensor-based motor control designs.

Together, these features provide a tightly integrated solution for demanding applications, such as high-efficiency motor drives, digital power supplies, and renewable energy systems.

Other features I'd highlight include abundant I/O and low-power modes that can take power consumption below 1 microampere (µA). PSA Certified Level 2 security protects against tampering, while IEC 60730 Class B and IEC 61508 SIL 2 compliance ensure functional safety.

Figure 3: The KITPSC3M5EVK evaluation kit provides a variety of headers for proof-of-concept work using PSOC Control 3 MCUs. Image source: Infineon



Optimize cost vs. capabilities with two MCU lines

Not every design requires all available features, and budgets can be tight, so the PSOC Control C3 comes in two flavors: the cost-optimized Entry Line and a more capable Main Line. Key features of the Entry Line include a 100 megahertz (MHz) Arm core, a 6 megasamples per second (MSPS) ADC, and either a 48- or 64-pin package.

The Main Line steps up to a 180 MHz processor, a 12 MSPS SAR ADC, and adds an 80-pin package option. It also improves PWM timing to better than 100 picoseconds (ps), enabling control of switching frequencies above 200 kilohertz (kHz).

The PSC3M5FDS2AFQ1XQSA1 (Figure 2) exemplifies the Main Line's capabilities. This MCU combines the 180 MHz Arm Cortex-M33F core with 256 kilobytes (Kbytes) of flash memory in a PG-LQFP-80 package. It's particularly well-suited to challenging applications, such as robotics and e-bike motor controllers, where performance is paramount.

Accelerate motor control design with evaluation kits

For those interested in designing with the Control 3 family, the KITPSC3M5EVK evaluation kit (Figure 3) is a good starting point.

Overall, it's a viable choice for peripheral testing, proof-of-concept work, and initial code development.

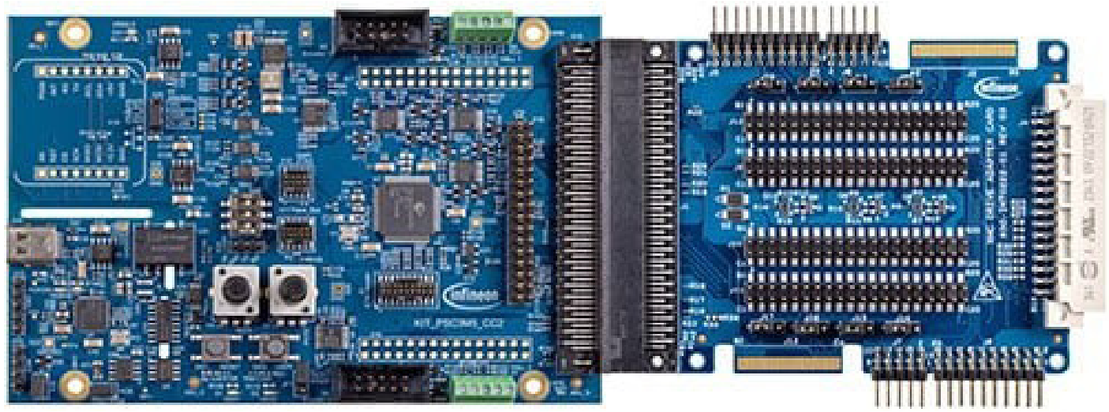
It features a PSC3M5FDS2AFQ1 MCU, giving designers access to the full suite of PSOC Control C3 capabilities.

The board features a straightforward design, making it suitable for breadboard experimentation. It also offers headers for MIKROE mikroBUS shields, Arduino Uno R3, and the Infineon Shield2Go interface for easy expansion. Overall, it's a viable choice for peripheral testing, proof-of-concept work, and initial code development.

For those looking to jump directly into motor control design, more advanced kits, such as the KIT_PSC3M5_CC2 (Figure 4), are also available. Built around the same PSC3M5FDS2AFQ1 MCU, this comprehensive platform includes integrated gate drivers for power stage control, current sensing circuits for phase current measurement, and an on-board power supply for standalone operation. It's an excellent choice for motor controller development, FOC algorithm testing, and system-level validation.

Both boards and the PSOC Control C3 family are supported by ModusToolbox, the Infineon development ecosystem. The ModusToolbox Motor Suite provides ready-to-use code examples and tools specifically designed for motor control applications, enabling you to move quickly from evaluation to implementation. It also supports direct integration with numerous third-party IDEs and build systems, giving you flexibility to adapt the workflow to their preferred toolchain.

Figure 4: The KIT_PSC3M5_CC2 is a flexible platform for prototyping motor control. Image source: Infineon



Conclusion

Whether you're new to motion control, like my son, or an experienced designer looking for the latest technology, the PSOC Control C3 MCUs have a lot to offer. Advanced features, such as the CORDIC accelerator and synchronized ADC, give it impressive motor control capabilities. Best of all, these features are packed into a highly efficient MCU, opening up intriguing new possibilities for cost-sensitive designs.

This month in history

1800

March 20

Alessandro Volta first describes the Voltaic Pile

In an effort to disprove Luigi Galvani's theories on 'Animal Electricity,' Volta developed a source of electricity based on chemical reactions. This invention allowed for the first source of continuous current, enabling electrical research in ways like never before.

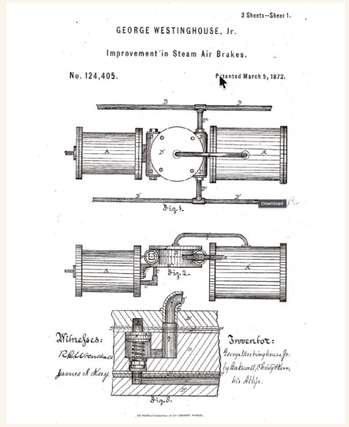
Volta giving an early demonstration of his Voltaic Pile.

1872

March 5

George Westinghouse patents the improved air brake

Before Westinghouse's air brake, deadly railroad crashes occurred daily. Quickly, his air brake was mandated for passenger trains by regulations, making Westinghouse very wealthy and securing his place in technology history. Westinghouse went on to fund developments in electrical transmission and help bring alternating current to the front of the 'War of the Currents'.



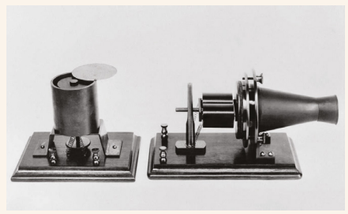
The Westinghouse Air Brake saved countless lives and allowed the railroad industry to flourish safely.

1876

March 10

First telephone call made

Less than a week after securing the patent for the telephone, Alexander Graham Bell made a voice transmission to his engineer Thomas Watson, "*Mr. Watson, come here. I want to see you.*" He would give many public demonstrations at the 1876 World's Fair the following June.



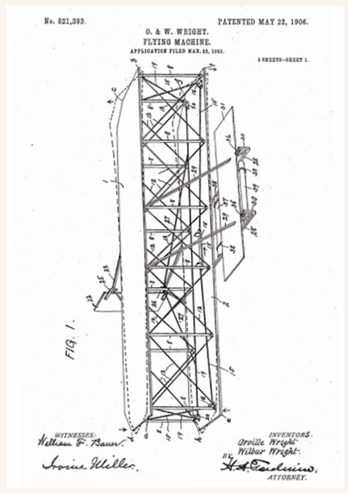
The 'first telephone' is on display at the Bell Museum in Canada.

1903

March 23

Wright Brothers file 'Flying Machine' patent

Orville and Wilbur Wright submit a patent application for their 'Flying Machine,' nine months before their first successful powered flight. Their design introduced a revolutionary innovation in the three-axis control system that managed roll, pitch, and yaw, enabling stable flight and becoming the foundation of all modern aviation.



The Wright Brothers' patent.

1976

March 4

First supercomputer delivered

The iconic CRAY-1, known as the world's first commercial supercomputer, is delivered to the Los Alamos National Laboratory. It cost approximately $8.8M and could perform 160,000,000 operations a second. Designed by Seymour Cray, it became the benchmark for high-performance computing and set the aesthetic direction for supercomputers for decades.

Cray supercomputers have a unique aesthetic, unlike anything else.

1979

March 8

Philips demos the compact disc

Before the 62nd AES Conference in Brussels, Philips first demonstrated the compact disc with a playtime of 150 minutes to a bunch of journalists. It would be another three years before the technology was released to the commercial market in 1982.

The 1982 Billy Joel album, 52nd Street, was the first album released commercially on compact disc.

What does passion, curiosity, and creativity have in common?

Answer: **You**

Whatever you call yourself (Student, Maker, Tinkerer, Hobbyist, Tech-Wizard...) you embody the spirit of invention–and that spirit is what creates a better world for us all.

If you can dream it up, we'll help you build it at digikey.com

DigiKey

we get technical