Secure Your Next Design with Microchip Technology

Security in microcontroller designs has never been more important, what with the increased desire for secure products combined with regulations preventing unsecure designs from getting into the market. Integrating security features into inherently unsecure products is a monumental task, which is why Microchip has created a wide range of microcontrollers and development boards that integrate security from the ground up.

What challenges are faced with modern IoT products?

The rate at which the internet of things is growing is phenomenal, and with more than 20 billion IoT devices around the globe, the importance of securing the IoT cannot be understated.

The first IoT devices were benign in nature due to their limited capabilities (such as being a temperature or humidity sensor), and this is something that many believed would be of no interest to cybercriminals. While the data gathered by such devices is indeed irrelevant to attackers, the very ability for a device to connect to a local network, and from there on to the internet, makes IoT devices of particular interest to attackers.

A single unsecure device can easily be accessed by an attacker, whereupon they can obtain network credentials and then either use the device to access the network or use the obtained credentials to connect to the local network. This has been done countless times, with one famous example of a casino whose sensitive high-roller client database was obtained by accessing the casino's internal network via an unsecure IoT aquarium thermometer.

For over a decade, billions of IoT devices have been manufactured with security that has not been fully considered. This is becoming more of a cause for concern now that modern IoT devices can readily have access to microphones and cameras, which could turn them into a platform for spying on and, from there, blackmailing unsuspecting individuals. The large number of unsecure devices also enables them to be used as zombies in large-scale denial-of-service attacks.

How has the world reacted to this growing challenge?

The lack of action from designers to incorporate security features has resulted in governments around the world introducing legislation to prevent the sale and distribution of unsecure devices. For example, the U.K. has recently introduced legislation that bans the use of default passwords, non-unique passwords, and the need for manufacturers to clearly state for how long a device will receive updates.

Another example of government legislation is in California, which introduced its own law on what IoT devices must do regarding protection. This bill, SB 327, states that devices must use appropriate security measures for protecting user data as well as the use of unique pre-programmed passwords that are used on only one device.

Why choose Microchip for your next IoT project?

Software security routines can be used on any platform for providing a basic level of security, but if the hardware used is fundamentally flawed, then no amount of software security measures will protect the device from physical and/or software attacks. Microchip has designed microcontrollers with security in mind from the ground up, and multiple levels of hardware security enable devices to be protected from attack as well as protect intellectual property.

For instance, features like CodeGuard prevent program memory from being accessed while also ensuring that only trusted code direct from the manufacturer can be executed. The use of OTP flash also prevents malicious code from being injected into memory, which adds a level of trust that cannot be obtained from systems that run programs in RAM. Furthermore, the use of cryptographic accelerators helps move intensive cryptographic operations away from the CPU and instead into hardware that is not only infallible but helps free up CPU resources. Microchip also has MCUs based on ARM Cortex-M23 with TrustZone, as well as SiP option (MCU + Secure Element) for hardened security.

This book will explore at a deeper level some of the products Microchip has designed with security in mind.

Contents

Real-time IoT for space-constrained designs PIC16F15244

Smart appliance control with low energy PCI32CM

Offload intensive I/O operations and get real-time response ..... AVR DA

Automotive embedded security ..... dsPIC33C and the PIC24 range

IoT sensing, home appliances, and smart devices PIC18-Q41

Biowearable devices with BLE ..... SAMD21, SAML21, and SAME51

Low-power analog and IoT sensing ..... AVR DB

Real-time motion surveillance and sensors ..... SAME54 and SAME70

PIC16F15244 FOR REAL-TIME CONTROL IN IOT & AUTOMOTIVE APPLICATIONS

What is the PIC16F15244 family?

The PIC16F15244 is a family of microcontrollers aimed at cost-sensitive and space-constrained applications. Being a PIC16 microcontroller, prototyping can be easily done with individual chips and a PICKIT3, but for those looking for a development board, they can use the Curiosity Nano. This development board integrates everything needed to program the PIC16F15244 as well as experiment with GPIO and peripherals.

This family of microcontrollers also integrates advanced memory features such as Memory Access Partition, which provides data and bootloader protection. The use of Peripheral Pin Select allows for the microcontroller pin functions to be mapped as needed, making it easy to integrate into existing PCB designs. Plenty of code examples can be found online via GitHub and its full compatibility with the MPLAB X environment, which allows use of a wide range of hardware tools, including code configuration and peripheral setup.

PIC16F15244 FOR REAL-TIME CONTROL IN IOT & AUTOMOTIVE APPLICATIONS

What can the PIC16F15244 family be used for?

The PIC16F15244 family is perfect for use as a companion microcontroller for applications needing real-time control of digital signals. While SoCs and microprocessors often have significantly more processing power, they are not designed to interface with GPIO and other peripherals in real time, instead focusing on operating systems and memory management. Thus, the PIC16F15244 can be used as a hardware interface for devices including I2C, SPI, UART, GPIO, and ADC.

The low-power capabilities and cost-sensitive nature of the PIC16F15244 also make it ideal for use in large-scale IoT applications. When combined with a communication controller (e.g., Wi-Fi or Bluetooth), the PIC16F15244 can be used to interface with sensors and other IoT-related hardware. What's more, thanks to the automotive qualifications held by the PIC16F15244, it can also be used in automotive applications.

PIC16F15244 FOR REAL-TIME CONTROL IN IOT & AUTOMOTIVE APPLICATIONS

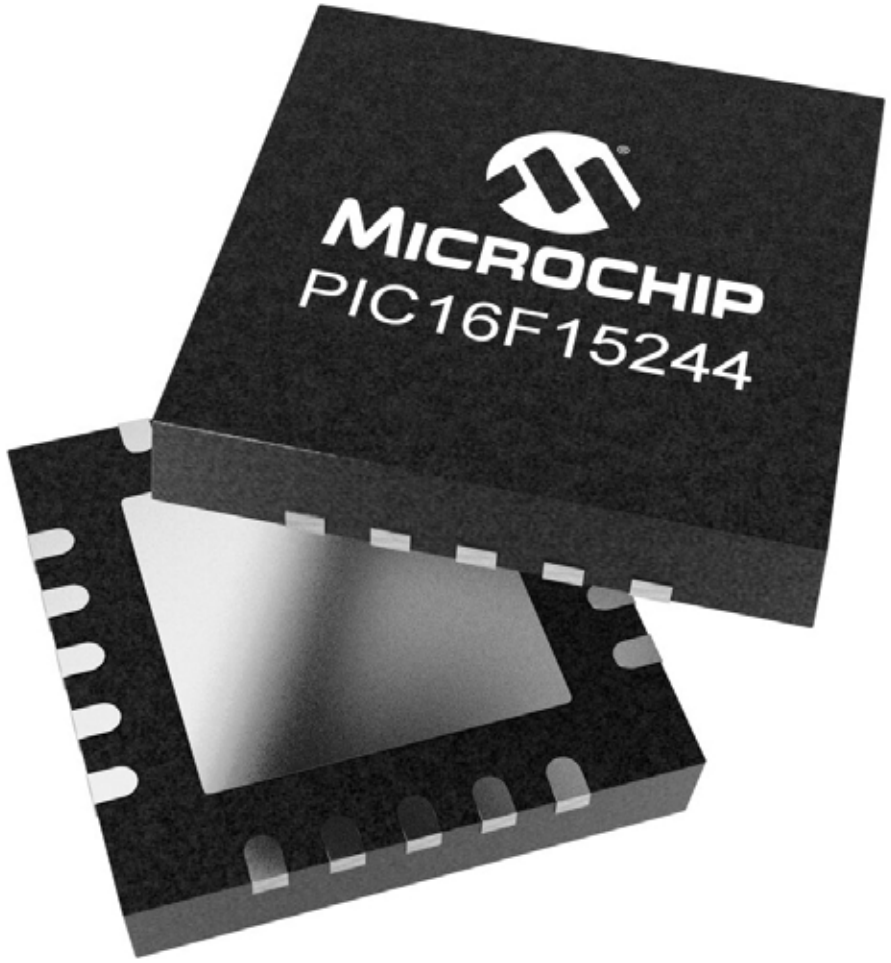
What are the key features of the PIC16F16F15244?

At the heart of the PIC16F15244 is a proprietary Microchip CPU, which has a maximum operating frequency of 32 MHz, giving a minimum instruction cycle of 125 ns. The family offers data memory of up to 2 KB, program memory of up to 28 KB, and a wide operating voltage of 1.8 V to 5.5 V.

On-board peripherals include a 10-bit 28-channel differential ADC, one 8-bit timer, two 16-bit timers, two 10-bit PWMs, and two capture/compare ports. Communication peripherals include ESUART and MSSP supporting I2C and SPI, and all peripherals can be routed to any I/O via the Peripheral Pin Select.

Where can I order the PIC16F15244?

The PIC16F15244 microcontroller family is available from Microchip Direct as well as many other authorized Microchip distributors, including Arrow Electronics.



IoT Smart Appliance Control Using the PIC32CM

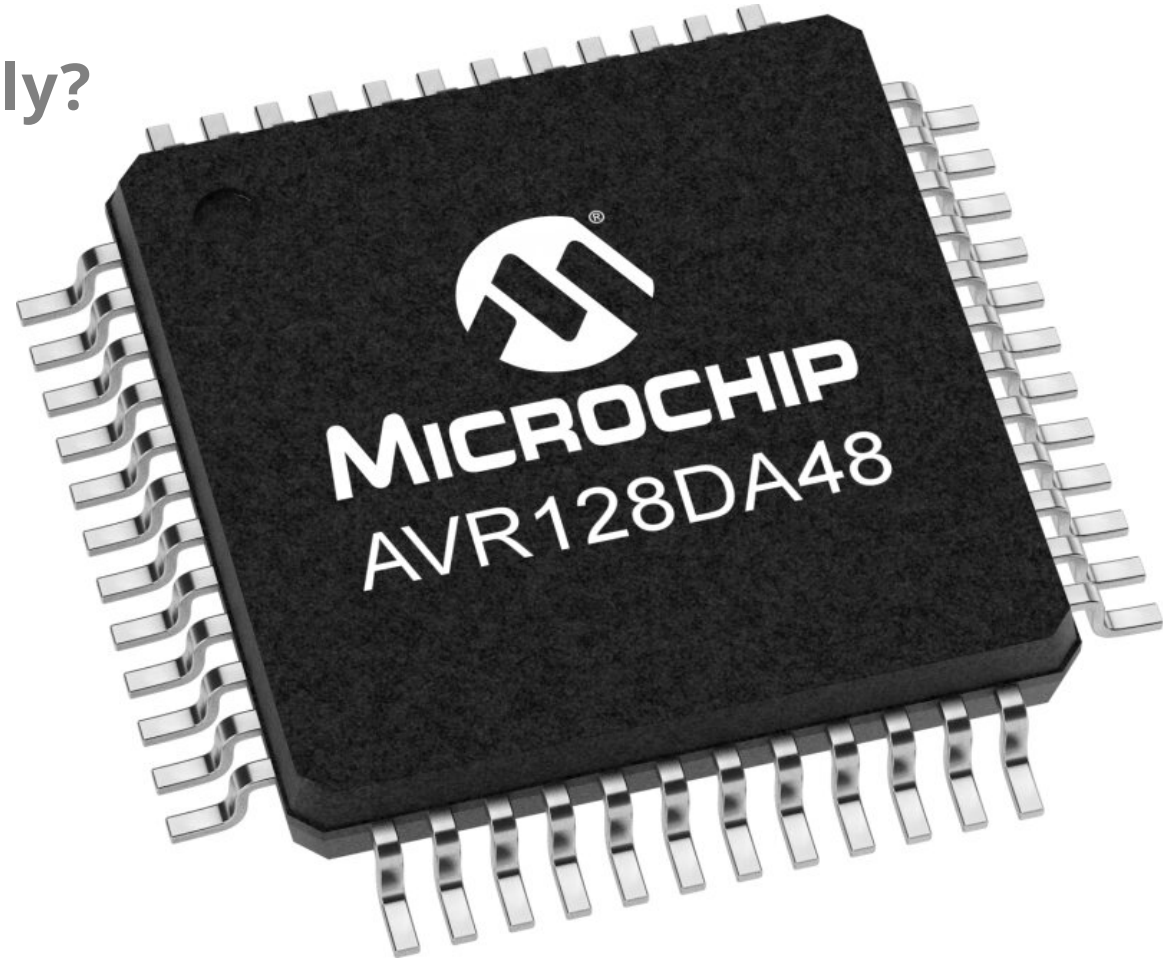
The IoT sector is one of the fastest-growing industries today, and the widespread adoption of these technologies across all markets demonstrates that the processing and energy demands on IoT devices will only continue to grow. The PIC32CM range of devices is ideal for such applications, thanks to its wide range of on-board peripherals and low-energy capabilities.

With the latest developments in smart appliance technology, including the IoT, the way we interact with our homes and appliances is changing. The resulting user-friendly smart appliances make our everyday lives more efficient, and with the emergence of smartphones and Wi-Fi, this technology is more convenient and affordable than ever. Although it might sound like science fiction, you can now control all the appliances in your home right from your smartphone.

Microchip provides all the tools, application software, and hardware needed to create complex IoT solutions on easy-to-use prototyping boards and modules, including the EMC2301 PWM fan driver, the BM70/71 Bluetooth Low Energy module, the MIC3305 buck regulator, and the MCP73871 battery charger. All these peripherals being available on MikroElektronika click boards makes it trivial to create a complete system with functioning hardware. Additionally, the use of the Curiosity Nano Adapter's embedded debugger allows for testing various microcontrollers manufactured by Microchip.

AVR DA PRODUCT FAMILY

What is the AVR DA product family?



The AVR DA product family is a range of AVR microcontrollers designed to be used either on their own or as a co-processor for complex designs. The integration of Core Independent Peripherals allows for the operation of key peripherals entirely independent from the main system processor while also allowing for low-latency operation to external signals. The high memory density on the AVR DA product range also allows for use with wired and wireless communication stacks, and the IEC 60730 UL classification ensures safe operation in safety-critical applications.

Prototyping the AVR DA family can be done with the use of the AVR128DA48 development board that combines a programmer, the main microcontroller, and several I/Os into a single device. The use of I/O headers allows for easy prototyping, while the integrated programmer allows for engineers to work with the ACR DA family immediately with the MPLAB X environment.

AVR DA PRODUCT FAMILY

What can the AVR DA product family be used for?

The AVR DA family is ideal for use either as a standalone microcontroller or as a co-processor used to offload intensive I/O operations in which real-time response is critical. The high memory density of the AVR DA allows it to be used in heavy communication protocols such as TCP/IP and Wi-Fi. This allows the AVR DA to be used as a real-time sensor in IoT applications requiring low latency.

The on-board analog peripherals have been designed to work well with capacitive-touch applications, and the combination of this with the ability to operate in safety-critical applications opens the AVR DA up to industrial sites and interfaces such as HMIs.

AVR DA PRODUCT FAMILY

What are the key features of the AVR DA?

The AVR DA family includes an internal 24-MHz oscillator, and the use of pipelining gives 1 MIPS/MHz, for a total of 24 MIPS. The family of microcontrollers has up to 16-KB SRAM for data memory and 128 KB for program memory. Analog peripherals include a 22-channel 130-ksps 12-bit differential ADC, a 10-bit 350-ksps DAC, and an analog comparator with scalable reference input.

An on-board 16-bit real-time clock and periodic interrupt timer allow for regular system interrupts, and a Configurable Custom Logic peripheral allows for the creation of core-independent logic functions that react to peripheral events. Communication peripherals include USART, SPI, and TWI.

Where can I order the AVR DA?

The AVR DA family is available from Microchip Direct as well as many other authorized Microchip distributors, including Arrow Electronics, among others.

DSPIC33C PRODUCT FAMILY

Automotive Embedded Security Using the dsPIC33C DSCs

It cannot go understated the importance of electronics in modern automotive vehicles with the use of smart fuel injection systems, battery management systems, on-board chargers, and engine condition sensors. With vehicles getting connected, the need for security in car networks and hardware is essential.

Microchip's dsPIC33C Digital Signal Controllers (DSCs) work together with Trust Anchor TA100 to offer a range of security features to help strengthen your next automotive project. Such features enable you to realize immutable secure boot, secure provisioning, encryption, secure firmware upgrades, node authentication, and secure key storage. These features can be used to create unique passwords for every chip programmed, keys that cannot be accessed externally, authentic firmware execution, and trust in every device used. Visit www.microchip.com/16b-security for more information on the dsPIC33C DSC security solution.

DSPIC33C PRODUCT FAMILY

Optimize System Cost in Your Intelligent Smart Embedded LED Designs Using the dsPIC33C Family DSCs

Applications requiring the use of long LED chains with smart capabilities can make use of Microchip's solution for Intelligent Smart Embedded LED (ISELED) technology, which has been developed in collaboration with the ISELED Alliance.

These LEDs are connected as a two-wire chain that allows for messages to be sent to individual LEDs in the chain and receive messages back from each LED. The maximum number of LEDs in a chain using the ISELED technology is 4,079, and the use of 2-Mbps bus speed allows for an update rate of up to 25 frames per second. Each LED allows for diagnostics on its operation, and this can enable for the host controller to determine the condition of each LED. Such LEDs can be used in interior lighting with dynamic effects in automotive environments. Another advantage of having intelligence in the LED is that it can be individually calibrated by the LED vendor, so you do not need any complicated calibration or binning during the production of the light fixture to get color accuracy.

The dsPIC33C Digital Signal Controllers offer Core Independent Peripherals with special modes, such as SPI, CRC, and DMA. These peripherals enable implementing ISELED protocol with low CPU overhead, reserving CPU bandwidth for user's requirements. The 3-V dsPIC33C DSCs can be directly interfaced with a 5-V ISELED string by taking advantage of the 5-V tolerant I/Os with open drain configuration, which eliminates the need for external glue logic or level shifters. The high-performance CPU facilitates implementing additional functions such as CAN or LIN communication, housekeeping, and monitoring. Offering these features and enabling high-level integration of various system functions, the 3-V dsPIC33C DSCs enable optimizing the overall system cost.

In next-generation vehicles, ISELED lighting will be part of the advanced driver-assistance system (ADAS), wherein the interior lighting is used for alerting the driver. Such ADAS-linked ISELED design is safety-critical in nature. The ISO 26262 Functional Safety Ready dsPIC33C DSCs with certified safety resources accelerate the design process. Experimenting with the ISELED range of devices can be done with the use of the dsPIC33C Curiosity Ecosystem along with the ISELED interface and development boards. Learn more about our dsPIC33C ISELED development platform at ***www.microchip.com/ISELED.***

PIC18-Q41 FOR IOT SENSING APPLICATIONS, HOME APPLIANCES, AND SMART DEVICES

What is the PIC18-Q41 product family?

The PIC18-Q41, as the name suggests, is a range of PIC18 microcontrollers specifically aimed at real-time sensing applications. The use of Core Independent Peripherals allows for peripheral control without the need for CPU intervention, which helps free critical system resources. Furthermore, the integration of an operational amplifier with programmable gain settings allows for the creation of amplifier circuitry without the need for external components.

Experimenting with the PIC18-Q41 range of microcontrollers can be done with the PIC18F16Q41 Curiosity Nano development board, which integrates a programmer, debugger, the main microcontroller, and various I/Os. The use of 2.54-mm pin connections on either side allows for connecting the Curiosity Nano with breadboards as well as various shield connectors. The PIC18-Q41 is fully compatible with the MPLAB X IDE development environment as well as the MPLAB Code Configurator, which allows for the easy configuration of peripherals via a graphical user interface.

PIC18-Q41 FOR IOT SENSING APPLICATIONS, HOME APPLIANCES, AND SMART DEVICES

What can the PIC18-Q41 product range be used for?

The cost-sensitive design of the PIC18-Q41 combined with its advanced peripheral capabilities makes the PIC18-Q41 ideal for real-time sensing applications in IoT and for use as a co-processor in complex designs that require real-time operation of hardware (such as motor controllers). The many ADC channels combined with the on-board op-amp also make the PIC18-Q41 perfect for wearable medical applications such as the internet of medical things, telehealth devices, and drug delivery.

The on-board Custom Logic peripheral allows for the creation of custom logic functions, which can be particularly useful in applications requiring instantaneous response to logic signal, while the on-board waveform generator is ideal for driving a wide range of sensors and controllers that may not use standardized communication protocols.

PIC18-Q41 FOR IOT SENSING APPLICATIONS, HOME APPLIANCES, AND SMART DEVICES

What are the key features of the PIC18-Q41?

The PIC18-Q41 has a C-optimized CPU core with a maximum operating frequency of 64 MHz, resulting in a maximum instruction speed of 16 MIPS. The PIC18-Q41 has up to 4-KB SRAM for data memory, up to 64 KB for program memory, and up to 512 bytes of E2PROM (can be used for serial numbers, configuration, and last good settings).

A wide range of on-chip analog peripherals include a 12-bit ADC with up to 17 channels, two 8-bit buffered DACs, two analog comparators, and a fully programmable op-amp with programmable gain functions. Digital peripherals include four Custom Logic Peripherals, three 16-bit PWMs, three 16-bit timers, one numerically controlled oscillator, one capture/compare/PWM module, and a programmable CRC with memory scan that can check the integrity of the memory contents while in operation. Various communication peripherals include three UART modules, two SPIs, and one I2C/SMBus.

Where can I order the PIC18-Q41?

The PIC18-Q41 family is available from Microchip Direct as well as many other authorized Microchip distributors, including Arrow Electronics.

Fitness Tracker Using the SAMD21, SAML21, and SAME51

Consumers have shown a growing interest in fitness trackers and other biowearable devices, and Microchip offers a wide range of different semiconductor solutions that can work well in such applications. The 32-bit MCU SAM D21/L21/E51 device range is ideal for use as a low-energy controller, while the BM70/71 can provide low-energy Bluetooth connectivity. Furthermore, the combination of the MCP73830/L can combine battery management and charging via USB, an industry standard for communication and power. Such a setup can be constructed using the Curiosity Nano Adapter board utilizing the SAM D21 host board, MikroElektronika Heart Rate 9 click board, eINK screen, and BM71 Bluetooth module.

The SAMD21 range of MCUs integrate an ARM Cortex M0+ running at 48 MHz with a maximum flash memory of 256 KB and a maximum data memory of 32 KB. On-chip peripherals include up to five 16-bit counters, four 24-bit counters, a 32-bit counter, and a dedicated watchdog counter, as well as a USB full-speed port, six communication channels, I2S, 12-bit ADC, 10-bit DAC, peripheral touch controller, and up to four analog comparators. The SAMD21 also include up to 52 programmable I/Os and is available in a wide range of packages, including TQFP, QFN, and WLCPSP.

AVR DB FAMILY FOR IOT SENSING APPLICATIONS, HOME APPLIANCES, AND SMART DEVICES

What is the AVR DB family?

The AVR DB family is a range of AVR microcontrollers that specializes in low-power analog applications, either as the main microcontroller of a system or as a co-processor to provide additional I/O capabilities to a more complex system. With Core Independent Peripherals and an Intelligent Analog portfolio, the AVR DB devices can create complex analog processors that do not require intervention from the main CPU, which helps to free up critical system resources for other tasks.

Its 5-V operation allows for improved noise immunity, while the Configurable Custom Logic and Event System allows for the development of low-latency responses to changes in a circuit in real time. Developing the AVR DB range of devices can be done with the Microchip Curiosity Nano Evaluation Kit that integrates the AVR128DB48 IC, a debugger, a programmer, and various I/Os. Furthermore, the kit has 2.54-mm–spaced I/O pin headers, which allow for easy use with breadboards.

AVR DB FAMILY FOR IOT SENSING APPLICATIONS, HOME APPLIANCES, AND SMART DEVICES

What can the AVR DB range of devices be used for?

Thanks to the AVR DB range of devices having automotive and industrial qualifications, they can be used in safety-critical applications, and the use of the MPLAB XC8 Functional Safety Compiler License can further help ensure that running applications operate exactly as intended. The ability to perform real-time signal processing via the various analog and digital peripherals makes the AVR DB range ideal for use in IoT sensing applications, home appliances, and smart devices.

Another potential application for the AVR DB range is as a co-processor on a complex design. While many SoCs are significantly more powerful than microcontrollers such as the AVR DB, they generally specialize in running operating systems and often lack decent I/O capabilities. Thus, the AVR DB could be easily paired with a SoC to perform real-time signal processing and monitoring, while the SoC handles operating system calls and networking.

Moreover, the AVR128DB48 supports eight level-shifting, or multi-voltage, I/O channels capable of bidirectional communication with external devices running at a higher or lower voltage than the MCU itself.

AVR DB FAMILY FOR IOT SENSING APPLICATIONS, HOME APPLIANCES, AND SMART DEVICES

What are the key features of the AVR DB?

The AVR DB range of microcontrollers utilizes an AVR CPU with a maximum operating frequency of 24 MHz and a maximum instruction execution speed of 24 MIPS. The range of microcontrollers supports internal data memory of up to 16 KB, 128 KB of program flash memory, 32 B of user row, and 512 B E2PROM data that can be used for configuration data, serial numbers, and security keys.

Timer peripherals that the AVR DB range integrate include two 16-bit Type A timers, five 16-bit Type B timers, 12-bit PWM, and a 16-bit RTC. Communication peripherals include up to six USARTs, two SPIs, and two TWIs with I2C compatibility.

A wide range of analog peripherals — including one 12-bit 130-ksps differential ADC, one 10-bit DAC, up to three zero-cross detectors, and an analog signal-conditioning unit with up to three op-amps with programmable gains — allows for the creation of advanced analog circuity. Furthermore, a configurable custom logic unit with up to six programmable lookup tables allows for the creation of hardware-driven processing that requires no interaction with the CPU.

Where can I order the AVR DB?

The AVR DB family is available from Microchip Direct as well as many other authorized Microchip distributors, including Arrow Electronics.

Motion Surveillance Using the SAME54 and SAME70

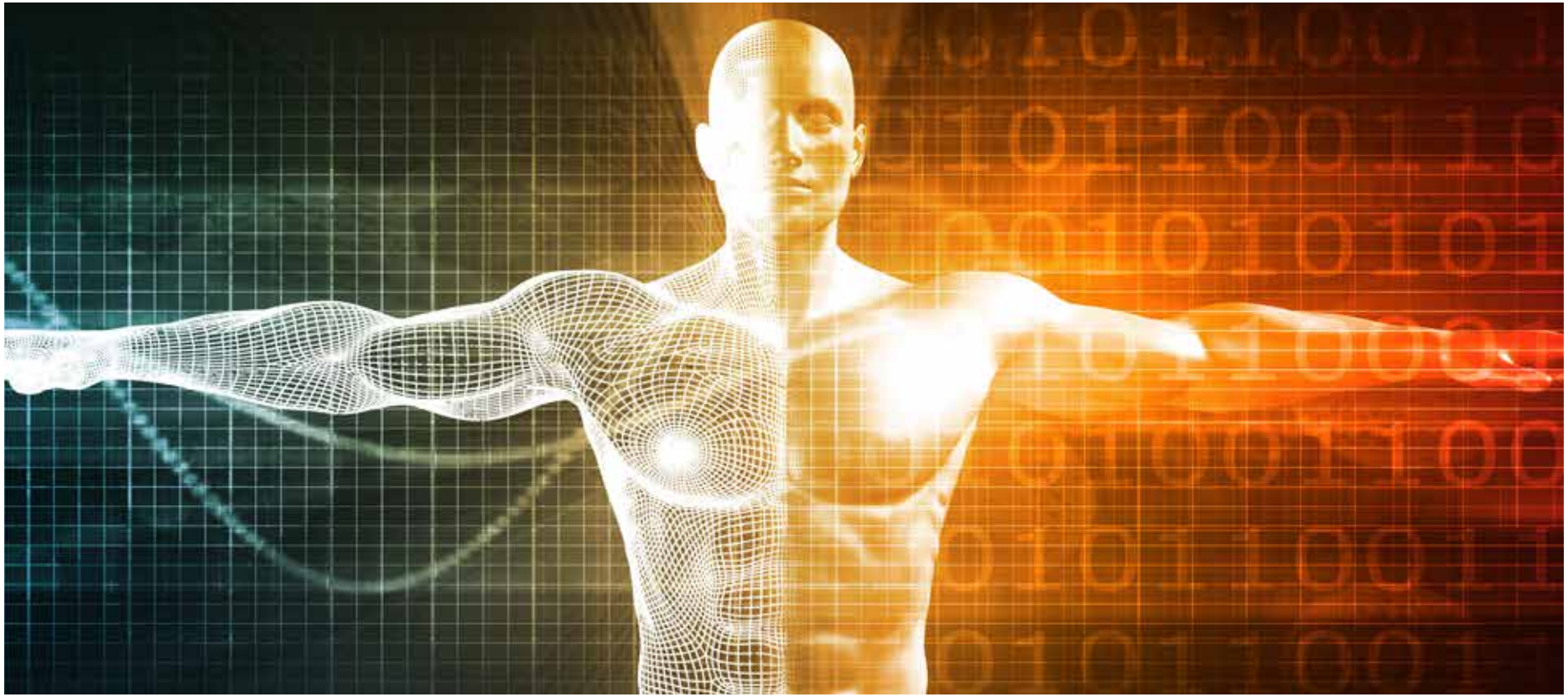
The ever-growing threat from unsuspecting individuals frequently sees us needing to protect goods and property. Traditional security cameras would be wired into closed-circuit television networks, but such camera systems are outdated and difficult to maintain. Furthermore, trying to record the camera feed from each camera can be challenging, especially for aging camera systems that use VCR tapes.

The Microchip SAME54 or SAME70 microcontrollers, when combined with additional Microchip products, make the ideal solution for motion surveillance. The processing capability of the 32-bit SAM range of microcontrollers can process video from cameras in real time, and the use of infrared sensors can be used to wake up the microcontroller upon detection of motion.

Such a system can be constructed using the Microchip Curiosity Nano Adapter together with the ATWINC1510 Wi-Fi module for connectivity, an Arducam, and the MikroElektronika PIR click board for motion detection.

The SAME54 range of microcontrollers integrates a 32-bit ARM Cortex-M4 clocked at 120 MHz with a 4-KB instruction cache, up to 1-MB self-programmable flash, up to 256-KB SRAM, up to 4-KB tightly coupled memory, and up to 8 KB of additional SRAM. With up to 16 external interrupts, the SAME54 range supports a wide range of various peripherals, including two SD/MMC host controllers, one quad SPI port, one Ethernet MAC port, two CAN controllers, and one full-speed USB. Hardware cryptography is also supported with the use of on-chip AES, a true random-number generator, and a Public Key Cryptographic Controller, which includes elliptic-curve cryptography, RSA, and DSA.

Conclusion



When designing products for use in safety-critical applications, whether it is IoT, automotive, or security, having a platform that you can trust is essential.