Keywords: near-field communications, NFC, radio frequency identification, RFID, SHA-256 ,

APPLICATION NOTE 5995

NEED NFC/RFID? TOMORROW IS TODAY IN THIS CONSTANT STATE OF INNOVATION

By: Hamed Sanogo, Executive Business Manager, Maxim Integrated

Abstract: New applications for near-field communications (NFC) and radio frequency identification (RFID) continue to emerge every day in many consumer and industrial markets. This application note provides a short overview of the NFC/RFID technology. It proposes a common circuit block based on the DeepCover® MAX66242, a secure dual-interface passive tag. The proposed circuit will make it easy to add NFC/RFID short-range wireless technology to any embedded electronic platform. Now OEMs can enable new, contactless NFC/RFID capabilities in portable electronic products.

Most of the NFC/RFID-capable devices have not been invented yet. So, hurry up!

Is near-field communications (NFC) caught between hyped promises and compromise? Not any longer. Previously considered as merely the next generation of bar codes, this technology has proven to be much more than practical and robust. New applications for NFC and radio frequency identification (RFID) continue to emerge every day in many consumer and industrial markets. The applications have moved quickly from their traditional simple, intuitive, safe, contactless transactions such as the exchange of information (e.g., telephone numbers, pictures, poster data, others) between two NFC/RFID-enabled devices. All you have to do is simply touch them together or bring them into close proximity. Today the primary concepts and traditional usages of NFC/RFID are evolving with new, unconventional thinking. We are, in fact, seeing a constant state of innovation.

Today you hear someone ask, "How different is NFC from traditional RFID?" At the physical or RF layer, not very different! NFC is essentially an evolved form of RFID. In fact, NFC was built over the 13.56MHz frequency band (HF) of RFID. The NFC Forum, an industry consortium,[1] started with the RFID physical layer protocol and improved it by adding a few new layers to the protocol stack. The NFC Data Exchange Format (NDEF) was added to identify, encapsulate, and exchange application data between NFC-enabled devices. This standardized format has made NFC/RFID an emerging wireless technology with highly promising applications for future pervasive computing.

To remain based and inclusive to a wide application base, the terms RFID and NFC will be used interchangeably during this discussion. In this article, we provide a short overview of the NFC/RFID technology and propose a common circuit block which OEMs can use to enable new contactless NFC/RFID capabilities in portable electronic products. The example circuit will be based on the DeepCover® MAX66242, a secure dual-interface passive tag. The proposed circuit will make it easy to add NFC/RFID short-range wireless technology to any embedded electronic platform. We will conclude the discussion with a few real-world use cases.

Readers and Tags: the Basics of NFC/RFID

NFC/RFID is a short-range radio and standards-based wireless connectivity technology that enables communication between devices held or positioned a relatively short distance from one another. NFC/RFID works over a distance of a few inches up to a meter. The technology uses inductive coupling, a process that transfers energy through a shared magnetic field between two devices. This practice is effectively the same working concept as in an air-core transformer where the reader's antenna coil represents the primary side and the tag's antenna coil represents the secondary side. The reader uses magnetic induction to create a radio-wave field that the tag detects. Therefore, when a tag is placed in close proximity to the reader, the field from the reader's antenna coil will couple to the tag's antenna coil. A voltage is induced in the tag, which is then rectified and used to power the tag's internal circuitry.

Figure 1 shows how the reader modulates the field to communicate its data with the tag. To pass data back from the tag to the reader, the tag's circuitry changes the load on its coil (while the unmodulated carrier from the reader remains on), and this is detected by the reader, again as a result of the mutual coupling. This load-changing scheme is called load modulation. NFC/RFID operates at a carrier frequency of 13.56 MHz, which is part of the globally available and unlicensed radio frequency ISM band. The technology has a few existing released standard specifications, including ISO/IEC 14443 Types A&B and ISO/IEC 15693.[2]

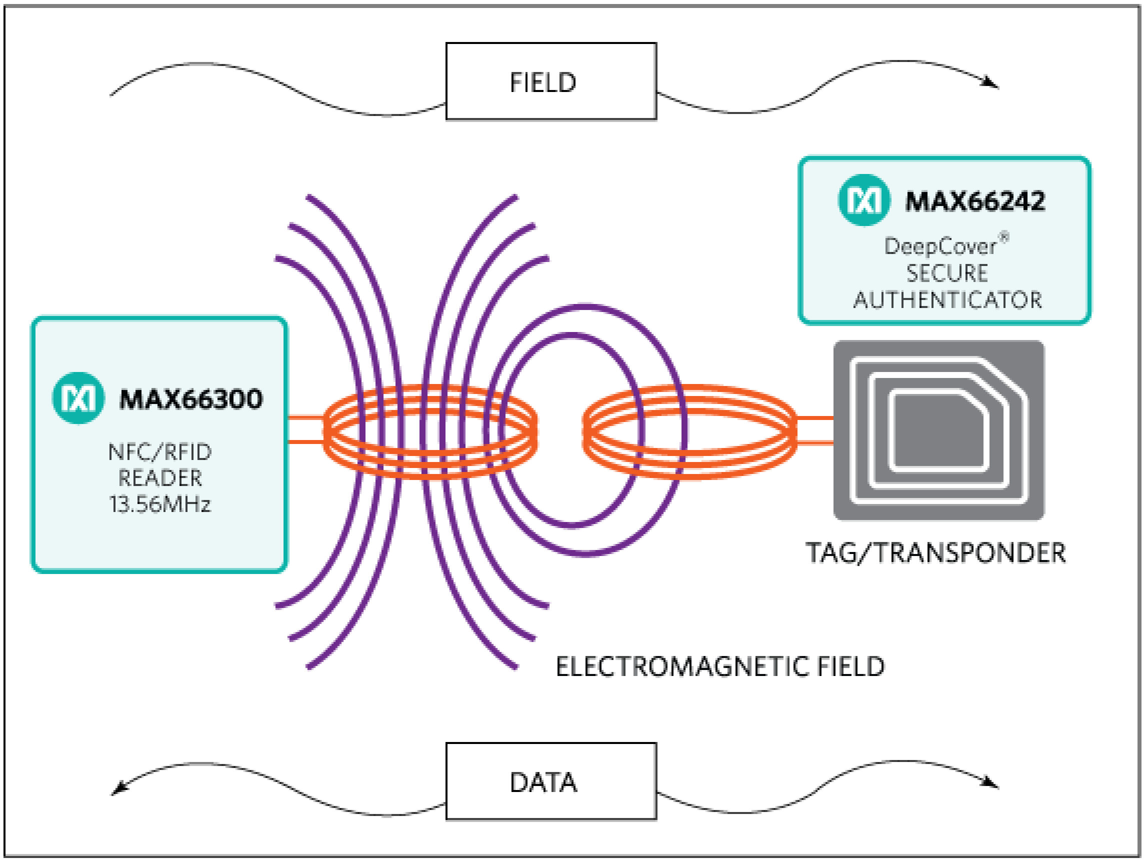

Figure 1. NFC/RFID tag, the MAX66242, coupled to a reader's, the MAX66300, magnetic field.

In this example, the MAX66242 is essentially a passive IC, a passive tag that does not need an external energy source to function. Instead, a passive tag obtains its energy from the reader's electromagnetic field. Typical applications that use this NFC/RFID technology include access control, smart posters, loyalty cards and coupons, mobile payments (contactless credit cards), ticketing and transportation toll collection.

Why It Works–the Passive Tag Authenticator

Designers can now collect and exchange secure system configuration/calibration data with their portable electronic products, even when the portable device has lost its main power source or is not operational. The solution in **Figure 1** allows any embedded electronic product to interface wirelessly with any surrounding devices and networks over the I^2C interface.

Several capabilities are essential for wireless NFC/RFID applications: advanced security integrated into the passive tag authenticator (**Figure 2**) that combines a wireless NFC/RFID interface with an I^2C interface; data protection modes; fast data transfer; and energy harvesting in the tag. The MAX66242 integrates SHA-256 crypto engine which provides a symmetric challenge-and-response authentication capability based on a shared secret key. This is the best means to control who and how NFC/RFID readers communicate with the MAX66242. A 32-byte SRAM buffer facilitates fast data transactions over the I^2C interface. The energy-harvesting V_{OUT} pin on the tag lets it use its antenna to gather power from the reader's HF field.

So it is SHA-256 security, fast data transfer, and energy harvesting–the key differentiating features–that make this passive tag an attractive component for any OEM who wants their NFC/RFID embedded portable system on an open and scalable platform.

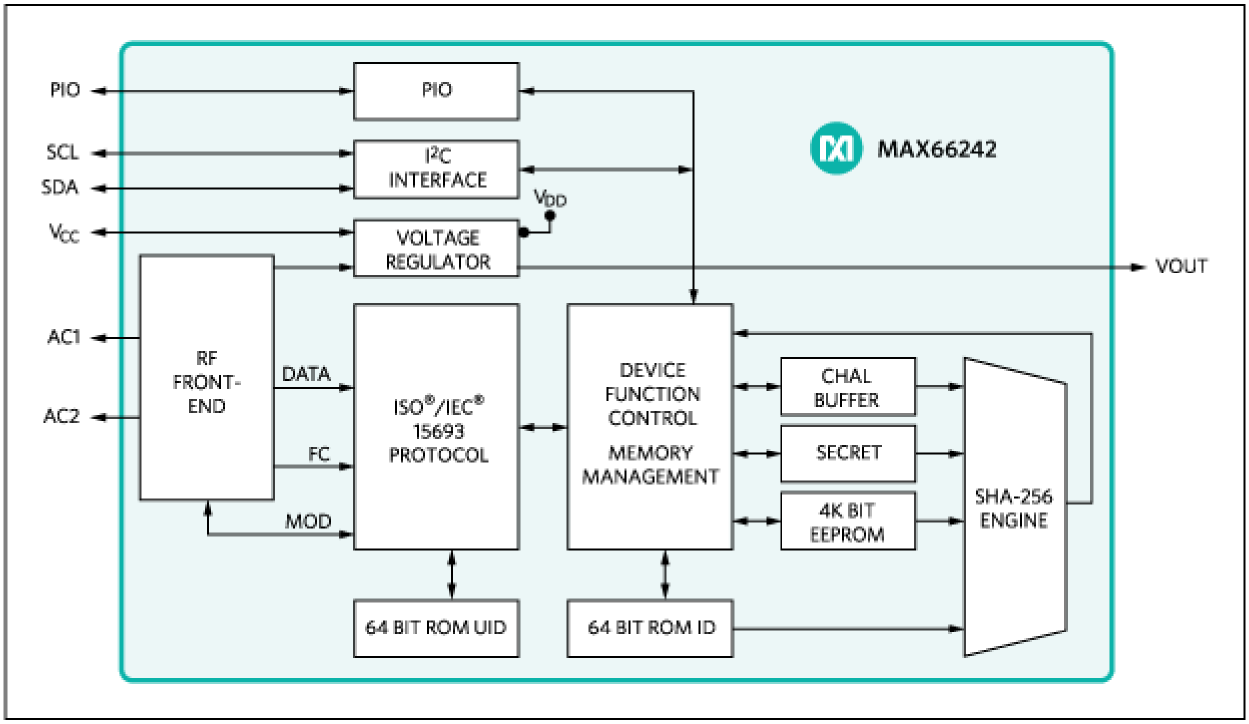

Figure 2. The functional block diagram for the MAX66342 passive tag.

Securing the Data–Only Vetted or Genuine Slaves Are Trusted

The MAX66242 uses a SHA-256 crypto engine to implement secure, symmetrical, bidirectional secret key authentication between the reader and slave device. The SHA-256 hash algorithm is based on a secure hashing standard, publication FIPS PUB 180-4, defined by the National Institute of Standards and Technology (NIST). A SHA-256 challenge-and-response security exchange between a master and slave device is the best means to control who and how NFC/RFID readers communicate with the MAX66242 passive tag.

SHA-256 is a symmetric key-based, bidirectional, authentication scheme where the reader (i.e., the initiator) only accepts a genuine tag; only a genuine reader can change the tag's memory. This scheme assumes that both the portable device (with the MAX66242) and the reader system have the same SHA-256 secret. When SHA-256 is enabled, the portable device must first provide a valid answer or response to the NFC/RFID reader in order to be authenticated. The portable device's response, moreover, depends on both the challenge that it receives and its stored secret. If the portable device answers the question incorrectly, then the reader system (e.g., a smartphone) will reject the portable device.

The major components of this authentication scheme include the 256-bit random challenge, the MAX66242's ROM ID, and the secret itself. The ROM ID is a unique 64-bit serial number, which is embedded into the tag during manufacturing. The same secret must be programmed and protected in the reader. **Figure 3** shows a secure-door example where the NFC/RFID initiates the challenge-and-response authentication before releasing the command to unlock the door of the house, fire safe, or gun safe.

To ensure the highest affordable protection against an (inevitable) malicious attack on these types of security ICs, this passive tag employs proprietary die-level physical techniques, circuits, and crypto methods. These defenses prevent hackers from extracting the secret key (to compromise the system's security implementation) for the sole purpose of cloning it or for changing the proprietary calibration data.

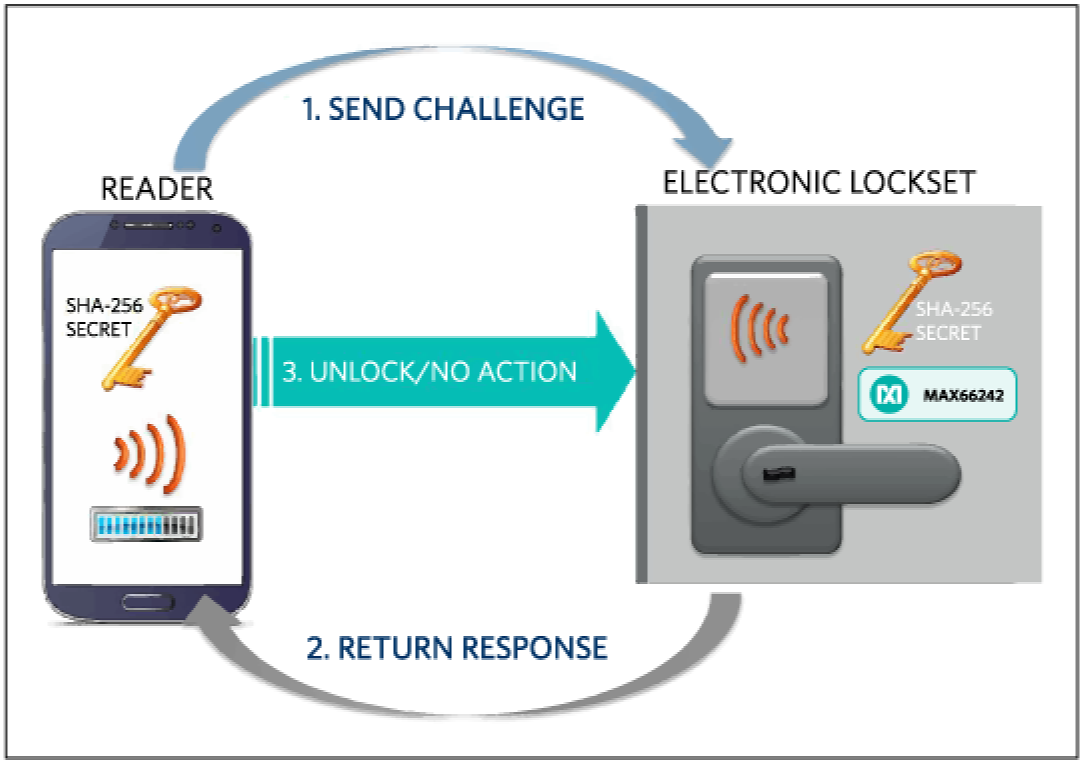

Figure 3. NFC/RFID-based electronic lockset authentication is centered on the MAX66242 passive tag.

Ensuring Data Protection—Configuration and Limit Usage Settings

Protecting the data is critical. This is why the MAX66242 comes with 4kbits of user EEPROM that can be partitioned into areas with open access (e.g., unprotected) or into areas where the reader must authenticate itself for EEPROM write access. Several protection modes are available, including the EPROM Emulation (EM) mode which allows for the support of nonresettable counter and limit usage applications. When the EM mode is activated, individual memory bits in the tag can only be changed from 1 to 0, but not from 0 to 1. Once the EM mode is selected, this cannot be reversed. This process, the best way to implement a countdown or the limit usage feature in the portable device, can be extremely challenging to defeat.

The EM mode also lets OEMs have better control over which NFC/RFID reader system can interface with their product. It is a sure way to protect their calibration, configuration, and diagnostic proprietary data stored on the device.

Faster Data Transfer Without an External Microcontroller

The MAX66242 passive tag is essentially an I^2C-to-NFC/RFID protocol translator gateway. The tag's I^2C port can operate as a master port or a slave port for data exchanges. With the applications shown in **Figure 3** above, the NFC/RFID reader can access an I^2C-based electronic component which is directly connected to the MAX66242. Because of this, an additional microcontroller is not necessary (on the sensor card, for example) to access data.

As already mentioned, the IC's integrated 32-byte SRAM buffer helps to speed up I^2C-to-HF data transactions. While similar solutions have to pass data through their EEPROM cells, the example MAX66242 uses its SRAM buffer to manage such hand-offs. The access time for SRAM is faster than with EEPROM, an advantage that translates into a relatively faster overall, coast-to-coast transaction time compared to other solutions.

The IC also provides a programmable input-output (PIO) pin which can be used for many purposes including interrupting the microcontroller of the portable device in certain applications. This PIO pin can also be configured as an RF Busy or RF-Access-In-Progress alert signal. A great use of an alert signal is to wake up a sleeping embedded system at the presence of the 13.56MHz HF field. In short, this multifunction PIO pin provides the means for a better data flow control through the system.

Energy Harvesting, Added Flexibility and Scalability

Energy harvesting is very useful because it makes the MAX66242 a highly flexible and scalable solution for a wide range of NFC/RFID applications.

As a generic passive tag, the IC does not require an external power source. It only requires a very small amount of power to operate, around 50µA or slightly more depending on the features supported. The tag extracts all its energy from the reader's 13.56MHz HF electromagnetic field. When the antennae have been constructed correctly and tuned for an efficient and optimized link, this passive tag gets much more energy than is necessary to power itself. The left-over energy is often shunted to ground. Instead, the rectifier's unused harvested energy in the MAX66242 is collected and sent out of the IC through its V_{OUT} pin. This harvested power can now be used to power surrounding ICs in an application such as the temperature-sensor patch from which temperature conversion data is also collected. The IC's V_{OUT} pin can be configured to provide either 1.8V or 3.3V (typical). This configurable supply output can deliver up to 5mA, given adequate field strength.

Optimize Antenna Design for Maximum Power and Efficiency

The energy-scavenging scheme in a passive tag only works effectively when an optimal design of the RF circuitry has been implemented to maximize the RF energy transfer. The efficiency of the energy transfer between the reader's and tag's antenna coils greatly depends on the precision of the resonant circuits and/or how the antennas are tuned. An efficient draw or transfer of energy between the antenna coils is archived at electrical resonance. In this case, getting the antenna coil of the MAX66242 tag and its tuning capacitor to resonate at the 13.56 MHz operating frequency are key.

The antenna design principle is relatively simple and straightforward. The tag's antenna inductance ($L_{INDUCTOR}$) must be constructed on a PCB (or an inlay substrate) to match the on-chip tuning (C_{TUNING}) capacitor value to achieve LC resonance at 13.56MHz. Thus, the sum of all capacitive and inductive reactances must be zero. This is achieved when $LCw^2 = LC\,(2\pi f)^2 = 1$ (with $f = f_{RES}$). This theoretically represents the scenario where the flow of energy (I_{RF}flow) into the MAX66242 tag is maximized, or the impedance is minimized. This leads to the resonance frequency f_{RES} and $L_{INDUCTOR}$ in Equation 1 below.

$$f_{RES} = \frac{1}{2\pi \times \sqrt{L_{INDUCTOR} \times C_{TUNING}}};\ L_{INDUCTOR} = \frac{1}{4\pi^2 \times (f_{RES} \times C_{TUNING})^2}$$

$$f_{RES} = 13.56\text{MHz}, C_{TUNING} = 21\text{pF};\ L_{INDUCTOR} = \frac{1}{(2\pi \times 13.56\text{MHz})^2 \times 21\text{pF}} = 6.56\mu\text{H}$$

Equation 1. The external antenna inductance ($L_{INDUCTOR}$) integrated on the PCB must match the tag's internal tuning capacitor (C_{TUNING}) in order to create a circuit resonating at 13.56MHz.

When this equation is met, this means that the tuned circuit is resonating. Equation 1 also shows an example of an actual computed $L_{INDUCTOR}$ with a known C_{TUNING} value. With the L value computed, the designer will construct the external antenna so that the L is achieved. When this has happened, the antenna design is said to have maximized the amount of current received in the LC loop.

It is worth noting that, in reality, design engineers must always design the NFC/RFID antenna coils for maximum power in their actual system. There often exists a tag "loading effect" which results from placing a tag in the HF field. To account for this loading effect, antenna coils designers may often have to overtune or undertune their designs to resonance frequencies slightly below or above 13.56MHz for their circuits to be efficient. However, constructing the antenna coil itself is beyond the subject of this article.

Enabling NFC/RFID in a Portable Device

It is fair to say that NFC/RFID is currently making a grand entrance in the consumer wearables technology mass market. Operating under the banner of the Internet of Things (IoT), more sensor-enabled embedded systems will be designed and set up to collect user-biometric and other data from multiple device systems on a network. There will be so many NFC/RFID-enabled medical and industrial applications that we have yet to see the limits.

Before we present some specific applications, let's first examine the basic circuit architecture that will enable NFC/RFID in an embedded design (**Figure 4**). Note that the system needs a communication path to the outside world.

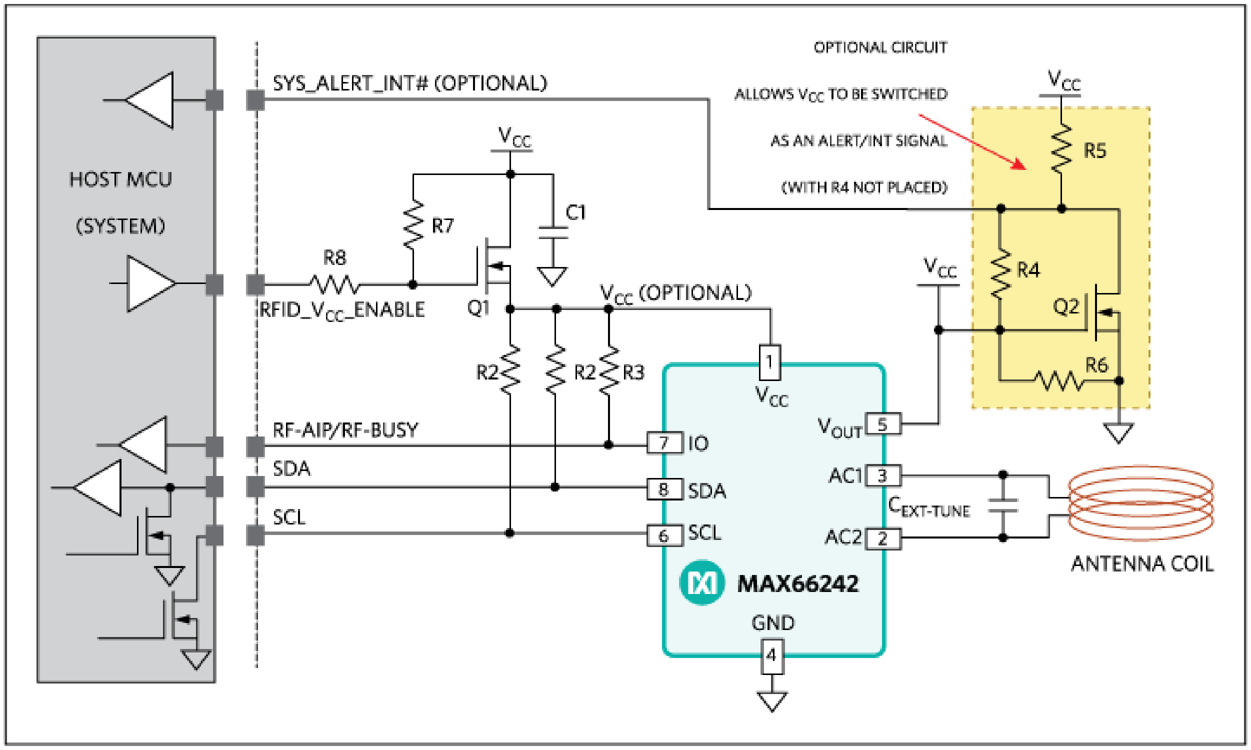

Figure 4. Typical circuit block to enable NFC/RFID capability in any embedded design. This circuit block, when combined with the key features of the MAX66242 secure authenticator tag, lets any embedded system enable new contactless applications for today's portable and secure embedded systems.

In **Figure 4**, while the I^2C interface (SDL and SDA) and the PIO signals (a multiplexed line of the RF-AIP and RF-BUSY functions) are necessary to connect to the host microcontroller, the RFID_V_{CC}_ANABLE and SYS_ALERT_INT# signals are optional. The MOSFET Q1 is used for isolation. Since the tag's internal EEPROM is accessible through both the RF and I^2C interfaces, Q1 powers the tag when the host microcontroller must interface with it in the absence of an HF field. The optional Q2 is, however, used to switch the open-drain SYS_ALERT_INT# with a regulated V_{CC} on the board. (R4 is not placed in this case.)

With a variant of this proposed circuit block (**Figure 4**) implemented in the device schematics, the OEM's product is ready to communicate with any NFC/RFID reader or initiator system. Once the board enters an HF field, V_{OUT} comes up and turns on Q2. The open-drain signal SYS_ALERT_INT# goes to low, which interrupts or wakes up the host microcontroller, thereby indicating that the system is in an HF field. The host microcontroller then drives the RFID_V_{CC}_ANABLE into a logic-high state, switching the MOSFET Q1 on. The host microcontroller is now ready to exchange data bytes with the NFC/RFID reader device that supplied the HF field. Again, the V_{CC} pin of the MAX66242 does not need to be connected to power, as the IC's internal circuit is powered from the energy harvested from the HF field. However, the V_{CC} pin is left connected in **Figure 4** so the host microcontroller can access the IC in the absence of an HF field. As a wired-to-wireless conversion box, the I^2C signals carry data to the outside world. The data flow is controlled by the RF-AIP (RF-Access-In-Progress) pin, also multiplexed as the RF-BUSY pin.

This NFC/RFID tag IC comes with an integrated tuning capacitor. The external tuning capacitor, $C_{EXT-TUNE}$ shown in the circuit, is optional. However, the $C_{EXT-TUNE}$ capacitor gives designers a way to retune their system relatively quickly, depending upon the loading effect encountered in the environment in which the tag is placed.

NFC/RFID Tag Empowers New Applications

As noted above, NFC/RFID promises to empower new potential usages in the industrial and medical sectors. A partial list of these new applications includes automated device configuration (also known as behavior setting), usage limit setting, system alert setting (e.g., system wake-up), slave-device secure authentication, and sensor-tag implementation, just to name a few.

Sensor-Enabled NFC/RFID Tag–a Sensor Tag

An emerging growth area for NFC/RFID is the sensor tag. A sensor tag is an assembly (e.g., a patch) which contains a sensor IC to monitor defined physical parameters from the user's behavior and the surrounding environment (**Figure 5**). These parameters include temperature, pressure, light, shock, vibration, humidity, acceleration, and chemistry, just to name a few. This sensing operation happens in addition to the tag's normal identification function. An attractive feature of a secure sensor tag is its ability to collect and report physical parameter measurements without a wired connection. The great benefit here is that the example MAX66242 is the key components for a sensor-tag discrete implementation.

Two medical consumable application examples of a sensor tag are the temperature patch and the sun protection factor (SPF) patch. Once the patient is fitted with the disposable temperature-sensor tag patch, the nurse can take core body temperature measurements without physically touching the patient. Given our global concerns about hidden and dangerous viruses, this is a healthy way to mitigate or completely eliminate cross-contamination situations in a hospital or medical clinic. In the same manner, an SPF sensor-tag patch can help a beach goer to apply the correct sun-screen lotion to avoid a sunburn. The user would only need to read the SPF patch occasionally with a smartphone.

A sensor tag can also help to monitor the integrity of a shipment. For example, a shock or vibration sensor tag will provide evidence of shock during the transportation of a valuable and/or fragile item.

In this example the MAX66242 is a key enabler for these applications, with its innovative support of a

master I^2C port the critical differentiating feature. If there was no master I^2C port, the design would need a small microcontroller to collect the temperature conversion data, and then write this data into the tag's memory for collection later by the reader (**Figure 5**).

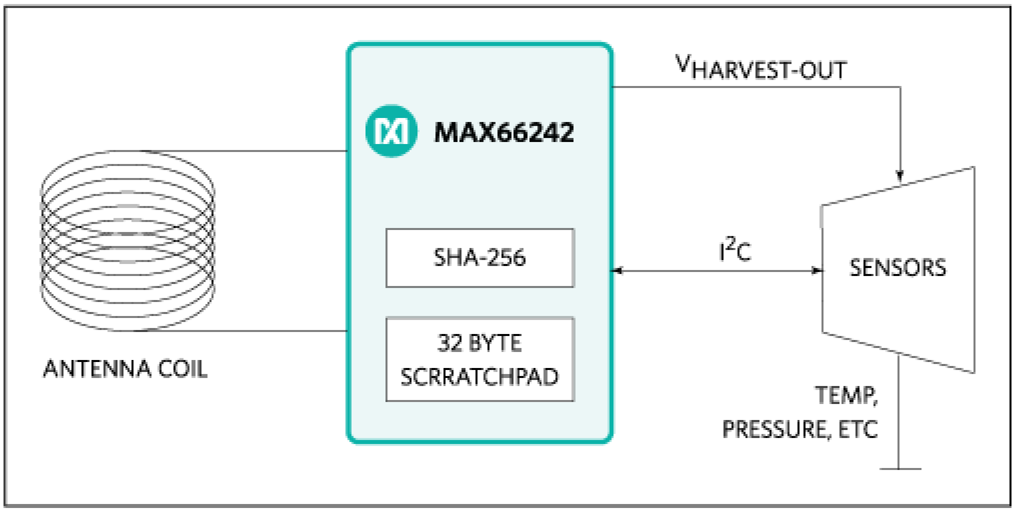

Figure 5. A high-level circuit diagram of a generic discrete sensor-tag. The MAX66242 master I^2C port allows a smartphone to access a sensor and collect temperature data without using a microcontroller.

As mentioned above, the sensor tag transforms (or transduces) physical analog quantities into digital outputs. Here the MAX66242 is essentially the bridge or conduit connecting these outside analog parameters to useful information that the user can read on the screen of a smartphones or tablet. Again, no external energy source is needed with a sensor tag using this IC, because it uses its energy-harvesting V_{OUT} pin as a power source for the sensor IC. **Figure 6** shows detailed typical discrete sensor-tag schematics.

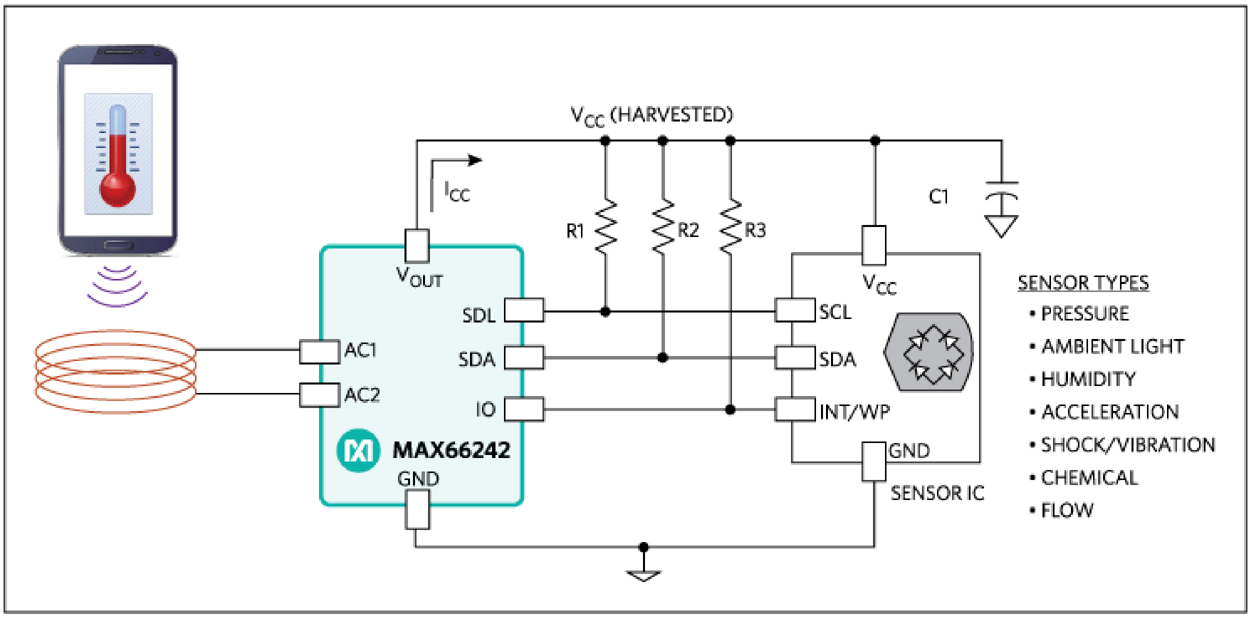

Figure 6. Evolved discrete embedded sensor tag architecture.

Diagnostics and Error Data Collection Address Long-Term Reliability Concerns

To summarize briefly, the MAX66242 tag literally enables any embedded system to communicate with NFC-enabled portable communication devices. The NFC/RFID port can also represent a warning display to the service technician similar to the service-engine-soon light seen on a car's dashboard.

After implementing the circuit architecture of **Figure 4** in any embedded design, the system can now exchange wireless information with the outside world, including diagnostics and error codes, data gathered from failing circuits, runtime warnings, and other system configuration/commissioning and calibration data. All this flexibility gives an OEM the opportunity to add even more value-added features to their end products.

Designers can use the MAX66242 to store system runtime vital diagnostics and error data. This data will be uploaded later after the system is "dead" or is not powered. The collection of this system health and faults data is done over the NFC/RFID tag's interface. **Figure 7** below shows a typical power-management system where each of the point-of-load regulators (POLs) is configured and monitored by a common power-management bus (PMBus). The PMBus is just a variation of the I^2C bus. During normal system operation, certain vital operating parameters of each POL are continuously monitored. While in this constant monitoring mode, the system manager can also perform corrective measures in response to faults or operational warnings.

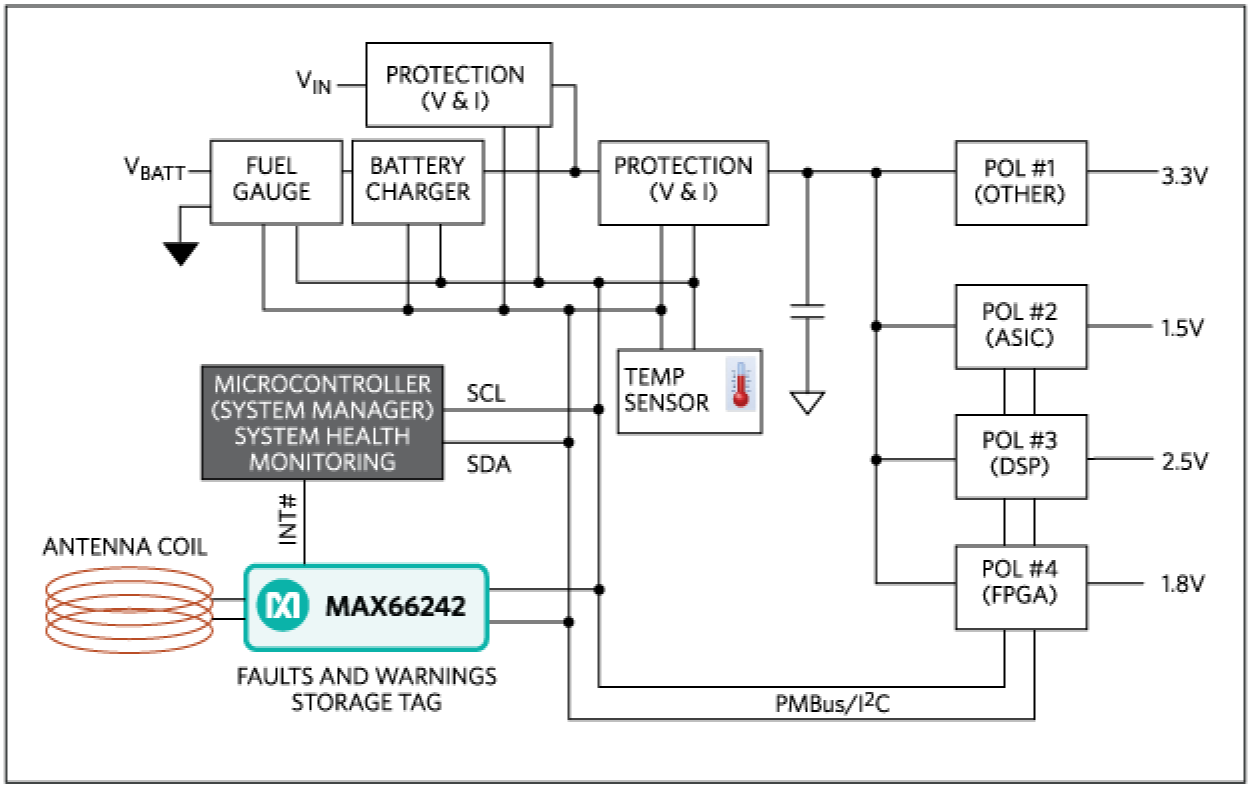

Figure 7. Block diagram of a power conversion system augmented with the MAX66242 NFC/RFID tag for faults logging.

With the example MAX66242 in this architecture, OEMs can create a "message-in-the-bottle" or "black-box flight recorder" scenario where the vital out-of-range parameters can be stored (e.g., the parameters of trip points from all the monitored fault protections circuits). Using the RFID/NFC reader, the technician now has access to the deregulation measurements recorded an instant prior to the actual failure. This data can also be used later for predicting certain specific faults and to help recognize abnormal operating conditions much earlier than before. This added intelligence about faults will help predict, mitigate, or even eliminate certain root causes of known catastrophic failures with next-generation products.

An NFC/RFID application can be found with field sensor and I/O cards in industrial control and automation. The MAX66242 tag allows for the commissioning of the sensor card while the device is sitting unpowered on the shelves. Analog calibration data, key parameters, or other system-level information is downloaded into the tag on the sensor or I/O card using a smartphone just before it is installed. Thus, a consumer can use their smartphone to buy credits for certain devices and use the smartphone application (app) to load the credits or enable the feature via the portable device's NFC/RFID connection.

Conclusion

The adoption of NFC/RFID technology has jumped dramatically in recent years. But why add NFC/RFID to your portable devices? Because it will open the embedded platform to many more applications. It is enabling new, secure portable communication applications. It will provide OEMs with a remarkable business opportunity. Not surprisingly, the technology is developing relatively quickly with a potentially long list of applications, and there is little doubt that NFC/RFID is considered one of the imminent cornerstones of the IoT.

We proposed an NFC/RFIC application circuit centered on the DeepCover MAX66242 secure authentication. Using this new approach, embedded portable systems will easily interface with the outside world. OEMs can enhance their product differentiation. With smartphone and tablet makers continuing to enable NFC/RFID technology in their products, this is greatly helping to complete the ecosystem.

So, everyone will soon have an NFC/RFID reader. Then everyone needs something to read. This is where the OEMs can, again, win. The example MAX66242 tag provides designers a flexible configuration, secure authentication, and the ability to do diagnostic data reporting. It is the core for a very easy and straightforward way of implementing NFC/RFID capability in embedded systems. In fact, the MAX66242 will leave system architects saying, "What if?" So, hurry up! Most of the NFC/RFID-capable devices have not yet been invented.

References

1. For more information go to http://nfc-forum.org/.
2. These specifications are in an ISO Standard document. They are known but not freely available on the Internet. One must pay to receive a copy. For more information, go to http://www.ansi.org/.

A similar version of this article appeared February 23, 2015 in Electronic Design.

Related Parts

Related Parts

MAX66240	DeepCover Secure Authenticator with ISO 15693, SHA-256, and 4Kb User EEPROM	Free Samples
MAX66242	DeepCover Secure Authenticator with ISO 15693, I²C, SHA-256, and 4Kb User EEPROM	Free Samples
MAX66300	DeepCover Secure Authenticator with SHA-256 and RFID Reader	Free Samples

More Information
For Technical Support: https://www.maximintegrated.com/en/support
For Samples: https://www.maximintegrated.com/en/samples
Other Questions and Comments: https://www.maximintegrated.com/en/contact

Application Note 5995: https://www.maximintegrated.com/en/an5995
APPLICATION NOTE 5995, AN5995, AN 5995, APP5995, Appnote5995, Appnote 5995