Large Memory RFID System Solutions

By David Dressen
Secure RF Product Development Manager

ATMEL'S CRYPTORF™ FAMILY PROVIDES 1 BITS TO 8K BYTES OF EEPROM MEMORY WITH A 13.56 MHZ RF INTERFACE. THE CRYPTORF FAMILY HAS MANY OPTIONAL SECURITY FEATURES, ALL OF WHICH CAN BE ENABLED OR DISABLED BY THE CUSTOMER AS REQUIRED FOR THE APPLICATION. CRYPTORF IS IDEAL FOR RFID WHEN SECURITY IS DISABLED.

Many industrial RFID applications require storage of large amounts of data with minimal or no security. Atmel's CryptoRF product family is ideally suited for these applications, as well as for others that require security, providing exactly the needed amount of memory and security at reasonable cost. CryptoRF is also ISO14443 Type B compliant.

When selecting RFID transponder integrated circuits, the primary selection criteria are memory size, transaction speed, communication range and cost. A suitable write lock feature is also a consideration.

CryptoRF is available in seven EEPROM user memory sizes: 1K, 2K, 4K, 8K, 16K, 32K, and 64K bits. The entire family shares the same command set and architecture, allowing an application to mix memory sizes or to migrate from one memory size to another.

To keep the transaction time reasonable in large memory RFID systems, a high RF communications speed is required. ISO14443 compliant integrated circuits, like CryptoRF, provide the highest available RF communication speed. The ISO14443 communication protocol has a raw data communication rate of 106K bits per second (kbps). Reading a 512-byte block of memory from an ISO14443 transponder takes only 62 milliseconds. Writing a 512-byte block of memory takes only 125 milliseconds for a transponder with a 2-millisecond write cycle time. While the ISO14443 standard was written for contactless smart cards in a credit card size package, ISO14443 integrated circuits are well suited for industrial RFID applications.

The communication range of an RFID system is highly dependent on the transponder antenna and the RF reader design. Depending on the specific antenna configuration and RF power of the reader, the maximum communication distance may vary from 1 cm to more than 10 cm in ISO14443 RFID systems. Tag tuning, antenna size and environmental factors strongly influence range.

In systems where only a single tag is likely to be in the RF field, the best communication range is obtained by tuning the tag antenna for a resonant frequency equal to the carrier frequency of 13.56 Mhz. A tag tuned to the carrier frequency can more easily extract sufficient power to operate, which maximizes the communication range.

If multiple tags are simultaneously in the RF field, the resonant frequency should be higher than the carrier frequency to compensate for the detuning effect. Detuning causes the resonant frequency of each tag in the system to drop due to the mutual inductance between the multiple tags. The detuning effect can shift the resonant frequency more than 1 Mhz.

The relative sizes of the tag and reader antennas have a greater impact on the communication range than tag tuning. Large diameter tag antennas provide longer communication range than small loop antennas because they capture more current from the magnetic field. In general, larger antennas on the reader also result in a longer communication range, but it is also possible to make the reader antenna too large. If an antenna is too large, the tag may operate at long distance, but not at short range near the center of the reader antenna. For readers embedded in industrial or manufacturing equipment, the antenna space is restricted by construction of the equipment. A small spiral antenna on the reader often provides the best range in these applications.

Water does not interfere with 13.56 MHz RFID systems, but metal does. It is not possible to communicate with an RFID tag if there is metal between the tag and the reader. Even the thinnest metallic foil will short out the magnetic field from the reader, preventing the tag antenna from capturing the current it needs to operate. The space between the two antennas must be clear of metallic material. Insulating materials do not interfere with the magnetic field, so tags can be embedded in plastic or epoxy with minimal impact on range.

Mounting a 13.56 MHz RFID tag directly on a metallic object can also prevent it from communicating with the reader. Metal behind the tag antenna will short out the field just as it does when in front of the antenna. Placing the tag on an insulating spacer or on a ferrite spacer can restore communications. If a reader antenna must be mounted on a metal surface, a ferrite spacer must be used under the antenna. If the metal is one inch or more from the antenna, no ferrite is necessary. Metal near the edge of the antenna is less detrimental than metal in parallel with the antenna. The reader antenna may need to be retuned if installed in the vicinity of metal.

CryptoRF integrated circuits are delivered with all security features disabled. If a customer decides to utilize a data protection feature, the feature can be activated when the RFID tag is initialized. For industrial RFID applications, the zone write lock and password features are often used. Simply writing the appropriate configuration register enables these features.

Videotape RFID Application Example

A typical large memory RFID application is tagging of videotape cartridges for television studios. The RFID tag stores information about the contents of the tape as well as the usage history. All of the information in the tag can be quickly and easily read with a hand-held reader or by a reader installed in the tape players without viewing the tape. Errors are prevented and advertising revenue maximized by using an RFID device, like CryptoRF.

There are several different videotape applications within the television studio and each type of tape will contain slightly different data in the RFID tag. All these types of tapes, including archive, field report, production and advertising tapes, contain a general information area. This header file describes the type of tape, tape ID, production date, location, subject, length of video for each subject, production team members (reporter, cameraman, editor, etc.) and equipment IDs. This area will also typically contain a copyright notice.

The type of tape determines what additional information is stored in the RFID tag. An archive tape containing the recording of a specific broadcast or group of broadcasts may contain only a small amount of additional information such as source information for video segments played during this broadcast.

A field report tape will typically contain a large number of video segments that are collected in the field. For each video segment, the RFID tag will contain timestamps and comment fields for use by the reporter and video editor.

The GPS coordinates for each video segment can also be stored, if the video camera contains a GPS locator module.

A production tape is produced by gathering video segments from various field report and studio tapes, then editing them to make them suitable for broadcast. The production tape will contain a log with the subject of each broadcast segment and the sources of video used within that video clip. The RFID tag in a production tape may also contain a broadcast log.

Advertising tape RFID tags have an expiration date and contain a broadcast log listing the date, timestamps, and equipment ID for each time it is broadcast. This information is important, because the television station can only collect advertising revenue if the correct tape is played within the broadcast time constraints of the advertising contract. If an expired ad is played or the broadcast is prematurely interrupted, then the advertising revenue is lost. The broadcast log can be quickly and easily downloaded from the tape and sent to the advertising customer or stored in the billing system.

The security settings of the videotape RFID tags are configured so that all of the data can be read by anyone without restriction. Write permission is restricted by requiring passwords to write data to the files. The RFID readers built into the studio equipment contain the write passwords for the type of tapes they are allowed to use. An application program stored in the RFID reader manages the data formatting and security.

As you can see, using CryptoRF RFID tags in broadcast systems allow collected video to be systematically managed from collection to broadcast. Videotape contents can be easily identified and more precisely described than on an adhesive label. Broadcast and file footage archives are more easily maintained by downloading RFID tag data into the studio database system. Efficiency is improved and advertising revenue maximized by reducing errors, so the system pays for itself. ■

CryptoRF Security Options and Operating Features

- All security can be disabled
- 64-Bit Key Encryption
- Symmetric Private Key Encryption Algorithm
- Family of Seven Devices, from 1 Kbit (128 Bytes) to 64 Kbits (8K Bytes); different densities can be used in the same application
- Dynamic Mutual Authentication between Device and Host
- Four Completely Independent Secret Key Sets for Multi-application Systems
- Contactless 13.56 MHz Interface, Compliant with ISO/IEC 14443 Type B
- Anticollision Protocol
- Tolerant of Type A Signaling for Multi-protocol Applications
- Integrated Tuning Capacitor
- High Reliability Memory, 100K Write Cycles with 10-year Data Retention
- Stream Encryption with Changing Session Keys Ensures Data Privacy
- Encrypted Passwords with Attempts Counters for Additional Security
- Read and Write Encrypted Checksum, Guarantees Data Integrity and Authenticity of Source
- Anti-Tearing, Avoids Data Corruption or Recovers Data in Case of Power Loss

Contactless Smart Card and Token Applications

- Security-focused ID and Access Cards (Biometric ID cards, visas, etc.)
- Health Care Cards
- Loyalty Cards, such as Restaurant and POS E-purse
- RFID Tags and Labels
- Energy Meters and E-government
- Multi-applications

CryptoRF devices are available in wafer and bumped wafer form, RF smart card modules and pre-laminate sheets.