SECURITY ICs

Contactless tech toughens passport integrity

By Calvin Lee
Marketing Manager
Identification
E-mail: calvin.lee@infineon.com

Peter Lockmann
Principal
Product Security
E-mail: peter.lockmann@infineon.com

Marcus Janke
Senior Staff Specialist
Product Security
E-mail: marcus.janke@infineon.com

Infineon Technologies AG

Under the Visa Waiver Program (VWP), any passport issued on or after October 26, 2006, must be an ePassport for VWP travelers entering the United States without a visa. This ePassport—an electronic travel document with an integrated contactless security controller that holds the same information printed on the passport data page—must comply with the International Civil Aviation Organization standards body, which also dictates the security levels and biometric data to be stored on the security controller.

With the VWP as the main driver of ePassport implementation as of November last year, around 33 countries have issued or started issuing ePassports. There have also been much public discussions about the security of contactless controllers for the ePassport.

There exists in the market three main classes of "contactless" chips: "pure" RFID chips, standard MCUs and contactless security controllers. Only contactless security controllers properly designed, are able to meet the high requirements for data security and privacy protection needed in the ePassport sector. The pure RFID chips are used mainly for object identification and do not contain an MCU. Therefore, their functionality and security is limited to an extent that is reasonable for the applications they are used for. Standard MCUs, equipped with an appropriate RFID interface, can be used for non-security contactless applications but are also not suitable for personal identification documents.

For a semiconductor chip to be utilized in an ePassport, it must be designed to protect the stored data against illegal tampering. The general specifications for such chips include:

- Low power non-standard CPU core
- More than 64Kbytes of secure EEPROM for application program and data
- EEPROM data retention for 20 years at 85°C
- Minimum of 500,000 write/erase cycles at 25°C per page of EEPROM
- Support of contactless interface according to ISO/IEC 14443 for both Type B and Type A
- Certified true random number generator supporting AIS-31 requirements
- Dual-key triple data encryption standard (DES) accelerators to support symmetric DES algorithms
- Advanced crypto engine with support of asymmetric RSA and elliptic curve algorithms
- Common criteria certification according to CC EAL 5+, with protection profile B5-PP-0002

In addition, the target for a chip manufacturer is to set up effective, tested and certified countermeasures against malicious threats that can be assigned to three main groups: fault induction, physical and side-channel attacks.

Countermeasures
Today, disturbing the functionality of a smart card has evolved into an art form, carried out by thousands of attackers around the world ranging from amateurs to consummate professionals. Therefore, fault induction attacks (also called semi-invasive attacks) have become a major focus for both the security evaluation and certification of security controllers.

ICs that are used as smart card controllers are usually made of silicon wafers. The electrical properties of silicon may react to different voltages, temperatures, light, ionizing radiation and also to the influence of electrical and magnetic fields. By changing these environmental parameters, an attacker may then try to induce faulty behavior, including errors in the program flow of the smart-card controller. Usually, an attacker would try to force a chip to make a wrong decision (for instance, to accept a wrong entry authentication code), allowing access to the secret data stored in its memory.

Another interesting variant is the "memory dump." Instead of giving out its non-secret identification data, the security controller would, after a fault induction attack, output much more data, including parts of the software, secret data or even stored keys. In some cases, only a single faulty computation is sufficient for an attacker to extract the complete secret key by using a sophisticated mathematical algorithm.

Various methods for inducing faults are known, including the alteration of power consumption, electromagnetic induction, irradiation of the chip surface with visible light or by using radioactive materials, and temperature manipulation. Some of these methods can be performed using low-cost equipment, which makes them a suitable choice for amateur attackers.

Thorough evaluation
Although countermeasures against such attacks are available in datasheets for today's security controllers, only tests can show if such flaws are actually effective in practice. As the performance of these different controllers may vary by orders of magnitude, it is extremely important that the security controller be thoroughly tested.
Cut domestic energy with speed control

An integrated power module (IPM) eases design and delivers additional benefits such as reduced component count and increased reliability. The IPM absorbs much of the engineering effort associated with power electronic design for motor control applications. For example, gate impedances are penalized for lower EMI noise and power loss, and bootstrap diodes and resonators are also integrated to drive high-side IGBTs. Driver layout challenges are addressed to minimize losses due to parasitic effect and to maximize thermal performance, and protection against overcurrent and overtemperature are also built-in. The engineer simply has to choose the right IPM for the application.

However, even this can be a daunting task. The performance of the IPM in a system depends on many application-related parameters, such as the switching frequency, modulation index and module case temperature. Data sheets provide some guidance but usually relate to standard operating conditions. Designers need extra help to predict performance in a specific application, including choosing the right module, matching selectable parameters including the switching frequency and sizing the heat sink to maintain the junction temperature within manufacturer-specified limits under worst-case operating conditions.

To choose the right IPM, the designer needs to collect information about the application. Consider a washing machine controller intended for operation at up to 3A rms phase current and 16kHz switching frequency with a DC bus voltage of 32V. If enhanced reliability is an intended selling point for the end product, the specified maximum junction temperature may be set well within the module vendor's recommended limit, say 125°C. The IR IRAM family of IPMs is available in a number of current ratings, including 6A and 10A modules, either of which is suitable for this application. However, because the power losses will be different for each module under the given operating conditions, the heat sink necessary to maintain junction temperature under 125°C will also be different. Calculating the required heat-sink thermal resistance requires complex knowledge of IPM thermal and electrical behavior to identify conduction and switching losses and predict the junction temperature based on these data. Although modeling steady-state conditions is relatively straightforward, the power losses in practice are not constant. In operation, the junction temperature will fluctuate beyond the steady-state average because power losses vary at a fundamental frequency equivalent to the modulation frequency of the inverter. Another important aspect is mutual heating, since the multiple heat sources within the IPM share the same parts from case to ambient. This effect must be taken into account if the model of the IPM is to be accurate.

Detailed models of IPMs and power modules can be a great benefit when identifying and selecting appropriate modules. IPSine software tool, for example, incorporates electrical and thermal models for currently available IRAM-series modules. This tool is published online to help engineers optimize module selection and determine the required heat-sink rating. The IPSine tool uses the appropriate models for the selected module to generate a series of performance curves describing IPM behavior under the application conditions entered by the user. Users can also change parameters such as switching frequency, power factor and modulation index to obtain performance curves customized for the application. Figure 1 shows the IPSine user interface, with menu-style entry of application parameters and part number selection. When the user selects the part, IPSine uses the associated model for loss and thermal calculation, and provides three analysis tools to help the user choose the optimal IPM:

- Switching frequency analysis to calculate the maximum motor current under different switching frequencies;
- Power-loss analysis to produce power loss vs. switching frequency curves for up to three IRAM-series parts;
- Component comparison, which produces power loss and case temperature curves for heat sink selection.

Considering the design example earlier, ISIS can be used to calculate the 10A IRAM10UP060. Figure 2 presents the Component Comparison analysis results from ISIS, showing both the power loss of the inverter and the maximum heat-sink temperature for the application.

At 3A rms, the power losses are 31W for the 6A module and 31W for the 10A module. The maximum allowable case temperature is 88°C and 99°C for the 6A and 10A modules, respectively. The Rjs can be calculated as Rjs = (Tjmax - Tj) / Ploss.

The calculations indicate that the smaller IPM will require a larger heat sink. Therefore, the final choice should be made based on minimizing total system cost and size, including both the IPM and heat sink. The same method can be used to select an IPM for an air-conditioner application. These typically combine a 400Vdc bus and PFC front-end. The switching frequency will be lower than a washers application to limit EMI noise. If the application requires 16A rms current at 6kHz switching frequency, ISIS can show the trade-offs between 16A and 20A IPMs. This tool can also be used to analyze the effect of modulation index, switching frequency, heat sink temperature and power factor on the current rating of the power module. This information can help engineers define suitable system parameters for an optimal solution. One important design parameter is the switching frequency. In this case, ISIS can be used to investigate the maximum motor current and power losses of IPM at different switching frequencies. Selecting up to three parts in each case of analysis shows that power loss increases and maximum current decreases with increasing switching frequency.

Figure 3: ISIS can be used to investigate the maximum motor current and power losses of IPM at switching frequencies.

Figure 2: Results show both the power loss of the inverter and the maximum heat-sink temperature for the app.