A Novel Power-down Protection Mechanism for Secure Chip Based on CRC Check

Qing-qin FU\textsuperscript{1,2}, Xin KONG\textsuperscript{3}, Yan-fang YUAN\textsuperscript{1,2}, Ping-jiang XU\textsuperscript{1,2}, Peng HE\textsuperscript{1,2}, Rui NIE\textsuperscript{1,2}, Jia LIU\textsuperscript{1,2} and Hong ZHANG\textsuperscript{1,2}

\textsuperscript{1}State Grid Key Laboratory of Power Industrial Chip Design and Analysis Technology, Beijing, Smart-Chip Microelectronics Technology Co., Ltd. Beijing 100192, China

\textsuperscript{2}Beijing Engineering Research Center of High-reliability IC with Power Industrial Grade, Beijing Smart-Chip Microelectronics Technology Co., Ltd. Beijing 100192, China

\textsuperscript{3}Beijing Redlink Information Technology Co., Ltd. Room1-3, South of Deshi Building, 9th East Street of Shangdi, Haidian District, Beijing

Keywords: Security chip, CRC check, power-down protection mechanism.

Abstract. This paper analyzes the shortcomings of traditional security chip power-down protection mechanism, and puts forward a new CRC-based power-down protection mechanism of security chip. The security chip can use its own CRC algorithm to calculate the CRC check value, thus completing the power-down protection mechanism algorithm validation. The proposed power-down protection mechanism in the write-protected data, can reduce the operating data area 2 times. In the restoration of protection data, erase data area can be reduced 1 times. This mechanism can reduce the number of erase and write data area, can effectively extend the life of security chip.

Introduction

Now, security chips have been widely used in electric power, finance and other industries, and each industry on the security chip trading time, transaction speed, data recovery have different requirements. Such as: financial PBOC applications require trading time of less than 500ms, which will provide secure chip applications, secure, fast transactions. Security chip is mainly used for automation terminal real-time status data and control data information security protection, requiring fast processing, and in the case of failure to restart after the resumption of application data before power-down, to ensure timely business data updates. At the same time, security chip life expectancy of more than 10 years, which also puts forward the requirements of the data write mechanism. While the data is written, you need to consider the power-down chip, how to protect data, that is the power-down protection mechanism. So how to meet the fast write, fast recovery, long chip life requirements, is the more critical issues, which have to study the security chip power-down protection mechanism.

At present, the general chip application developers have adopted the power-down flag TAG mechanism. In the protection of data write: first write the data to be protected to the backup area, and then set the power-down flag TAG, the backup area after the protection of data according to the circumstances were written to the corresponding data area, and finally power-down flag TAG cleared 0. In the protection of data recovery: first determine whether the chip power-down flag TAG is set, if set, then the need for protection of data recovery. Thus, the chip backup the protection data according to the circumstances were written to the corresponding data area, then clear the power-down flag TAG.
Traditional Chip Power-Down Protection Mechanism

The traditional power-down protection mechanism to complete a write protection data operation, erase E2 at least 4 times; complete a protection data recovery, erase E2 at least 2 times. Write erase E2 times more, to extend the application processing time, but also reduces the chip life.

In this paper, a power-down protection scheme based on CRC is proposed to improve the write protection data, protect the data recovery speed and prolong the service life of the chip. There are two shortcomings in traditional power-down protection mechanism[1-11].

Chip Power-down Protection Mechanism Based on CRC Check

This paper presents a new CRC-based power-down protection mechanism, including write protection data method and recovery protection data method. Write data operations, erase E2 only need at least 2 times, as shown in Figure 1; for data recovery, erase E2 only need at least 1 time, as shown in Figure 2. This greatly reduces the E2 erase the number of times to enhance the application processing time, effectively extending the life of the chip.

In addition, different security chips, the hardware supports different CRC algorithms, such as: CRC16, CRC32 and other algorithms, the invention can be used to calculate the power CRC chip CRC check algorithm, the CRC check mode according to Security chip support algorithm flexible configuration, power-down mode with scalability.

Write Protection Data Method Design

Write protection data method specific steps are:
Step 1 Clear the CRC value, the number of write protection data operations N, and the protection data length.
Step 2 Modify the number of write protection operations N, N> = 1 according to the application execution.
Step 3 Calculate the CRC value according to the protection data length and the protection data;
Step 4 Write the CRC check value, the write protection data operation number N, the protection data length, and the protection data into the backup area at one time.

Specific implementation process shown in Figure 1.

Methods for Recovering Protected Data

Recovery of data protection methods specific steps are:
Step 1: Read the CRC value of the backup area, the number of write protection data operations N, the length of the protection data, and the protection data. Calculate the CRC check value according to the chip CRC algorithm;
Step 2 compares the calculated CRC value with the CRC value in the backup area. If the two match, the protected data in the backup area is written N times to the corresponding data area.
Specific implementation process shown in Figure 2.

Write Protection Data Mechanism

The two sets of protection data 112233, 4455667788 are described below.
Step 1 Clear the CRC check value, the write protection data operation count, and the protection data length before executing write protection data.
Step 2 The organization protects the data length and protects the contents, and sets the write protection data operation number to 2.
Step 3: Write the data protection operation number 2, protect the data length and protect the data, and calculate the CRC check value by CRC algorithm specified by the chip.
Step 4 Write the CRC check value, the write protection data operation number 2, the protection data length, and the protection data into the backup area at one time.

Step 5 Write the protection data 112233,4455667788 twice to the corresponding data area.

Figure 1. Design Scheme of Write Protect Data Based on CRC Check.
Implementation of Recovery Protection Data Mechanism

When the write protection data in the process of the implementation of power-down, you need to protect the data recovery, the following two groups to restore the protection of data 112233, 4455667788 to explain.

Step 1 Read out the CRC value of the backup area, the number of write protection data operations 2, the protection data length, and the protection data.

Step 2: Calculate the corresponding CRC check value according to the CRC algorithm specified by the chip by reading the number of write protection data operation times 2, the protection data length and the protection data.

Comparing the calculated CRC check value with the CRC check value in the backup area.

Step 4 If the two are the same, the backup data in the backup area 112233,4455667788 write twice the corresponding data area.

Step 5 Otherwise, the operation of recovering the protected data is not performed.

Comparison of Power-Down Protection Mechanism

This paper presents the advantages of power-down mechanism, compared with the traditional authentication method, as shown in Table 3. As can be seen from Table 3, the proposed mechanism of power-down has a higher timeliness, which can effectively extend the chip life.
Table 3. Power-down mechanism comparison.

<table>
<thead>
<tr>
<th>Power-down strategy</th>
<th>The mechanism of power-down in this paper</th>
<th>Traditional power-down mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Write Protect Data</td>
<td>2 times</td>
<td>4 times</td>
</tr>
<tr>
<td>Restores the number of protection data operation data areas</td>
<td>1 times</td>
<td>2 times</td>
</tr>
<tr>
<td>Power-down protection</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Chip life</td>
<td>High</td>
<td>Low</td>
</tr>
</tbody>
</table>

Summary

In this paper, a novel power-down protection scheme based on CRC is proposed, which makes the security chip calculate the CRC value according to the CRC algorithm, and compare it with the CRC value in the backup area. Complete power-down protection mechanism of the algorithm validation. As a result of using CRC algorithm to verify, the proposed power-down protection mechanism in the write protection data and restore protection data, can reduce the number of erase data area, thus extending the life of the security chip.

References

[9] Yan Ying. WEDM numerical control system power-down protection function research and implementation [D], Nanchang University, 2012.