Architecture Design of Application Specific Power Chip Security for Power Terminal in Smart Grid

Zhining Lv\textsuperscript{1}, Tao Tang\textsuperscript{2}, Yu Du\textsuperscript{1}, Huiqin Wang\textsuperscript{1}, Xiangjun Zeng\textsuperscript{1} and Dongqi Liu\textsuperscript{2}

\textsuperscript{1}Shenzhen Power Supply Bureau CO., LTD, Shenzhen 518001, China.
\textsuperscript{2}Hunan Provincial Key Laboratory of Smart Grids Operation and Control, Changsha University of Science and Technology, Changsha 410114, China.
Email: ttqzh0102@163.com

Abstract. Power terminal based on chip is the development demand of smart grid. Aiming at the problems faced by the current power terminal based on chip, an architecture design scheme, which includes power security subsystem (PSS) and application special power system (ASPS) is proposed in this paper for power terminal in smart grid. Then, concrete subsystem architectures of the PSS and ASPS are designed and described. The PSS provides data encryption and decryption, identity authentication and other security services while ASPS can improve the efficiency of data parallel execution and processing efficiency of power terminal. Therefore, the proposed architecture design can solve the problem of security and efficiency better for power terminal in smart grid.

1. Introduction

Under the continuous construction and development of smart grid, more and more measurement, protection, control, monitoring, transformation and other devices are connected to the power system, the operation of the various power equipment produces large amounts of data\cite{1}. This data is transmitted remotely to the control centre. On the one hand, the burden of the control centre is heavy; on the other hand, the transmission channel is vulnerable to network attacks and there are security risks. The existing power terminals have low intelligence and poor security\cite{2-3}. However, the power terminal based on the power chip can fully solve this problem. It has the characteristics of high precision, low power consumption, miniaturization, intelligent computing and high security\cite{4-7}. For example, the principle and setting value of relay protection terminal has been on the road to standardization, so that its performance has approached the limit to protection function. In order to further improve the reliability, security and complexity of the protection terminal, the protection terminal based on chip can be studied\cite{8}. Paper \cite{8} proved that power chip protection terminal has the advantages of low complexity, high security, easy maintenance and high reliability.

With the preliminary construction of ubiquitous electric power Internet of things in China, the demand for power main control chips reaches hundreds of millions of pieces every year, covering power terminals of various business scenarios. However, the current terminals based on chip mainly focus on power focus\cite{9,10} and data communication\cite{11}. Power terminal based on chips are faced with the following two problems.

1) So far, the power terminal security protection coverage rate is low, the security level is low. In the middle and high-end power application scenarios, such as relay protection terminals and distribution network terminals, chip level power data transmission and control signal communication are directly exposed to the environment without encryption and anti-attack measures\cite{12}. A few smart meter terminals use an external encryption chip security scheme separated from the MCU to provide...
data encryption, decryption and identity authentication services for the terminals. Although this scheme can realize data encryption and decryption, the data transmission through SPI interface has a low rate of the interface itself, which makes the overall encryption efficiency low. The off-chip transmission of encrypted data also reduces its security, which is easy to be attacked by the probe at the board level. At the same time, the adoption of external security chip scheme increases the complexity of power terminal board level design, which increases the manufacturing cost and design difficulty.

2) At present, power terminal chips often adopt ARM architecture series and other general chips. Application special power algorithms, such as FFT, phase sequence calculation, differential calculation, rely on the operation of CPU software, limited by the CPU instruction cycle, speed and its sequential execution characteristics. Thus, execution efficiency is low. In the communication process of power terminal network, network storms often occur. The processing of network storms by using CPU will result in heavier CPU load, slower response, and even packet loss and reception failure. Therefore, the existing power terminal chips have a pool specificity.

As a result, the researches of application specific power chip (ASPC) with safety protection mechanism have considerable practical significance and value for the power terminal in smart grid. In this paper, the design of ASPC is finished, including chip system overall architecture, power safety subsystem, and power application specific subsystem.

2. Overall Architecture Design for ASPC
Through the investigation and analysis of the power characteristics and functional requirements of power terminal chips, this paper sorted out the power specificity requirements of general chips in terms of performance, function and safety, etc., which were difficult to meet the power needs of smart grid. The architecture of ASPC was mainly divided into two subsystems: power security subsystem and application special power subsystem. The overall architecture of ASPC of the power distribution network protection terminal is shown in figure 1, which includes high speed peripheral interfaces, low speed peripheral interfaces, such as SPI, UART, and other interface modules.

![Figure 1. The overall architecture of ASPC of the power distribution network protection terminal](image-url)
- Power security subsystem (PSS): Aiming at the security hidden danger from the traditional SoC chip, the PSS realizes small hardware resources, controllable performance and power consumption security CPU core through customization, integrates memory protection unit and security protection module, and provides data encryption and decryption, identity authentication and other security services based on hardware logic of anti-attack state secret security algorithm.

- Application special power subsystem (ASPS): Aiming at the problem of limited efficiency of the power application program based on the general processor, it integrates the functional realization and operation requirements of the special power pre-data processing class, power protection calculation class, network communication class and data management class, develops the application special power hardware IP module, and proposes the self-controlled application special power DSP customized solutions.

Take the power distribution network protection power terminal as the application scenario, and consider the chip performance, power consumption, business functions and security requirements of power terminal.

3. Subsystem Architecture Design

3.1. The PSS Architecture Design

The power security subsystem is composed of application special power security CPU core, anti-attack state encryption algorithm hardware acceleration engine, true random number generator, physical circuit level security protection unit, memory protection unit, security communication module and other modules, as shown in figure 2.

![Figure 2. Architecture design for PSS](image)

The concrete functions of each module in the PSS are as follows:

- Application specific power security CPU core: the application special power security CPU core is the core of the PSS, which controls the operation of the whole system. The secure CPU core implements a number of security mechanisms. These security mechanisms that are shown as table 1, are coupled in the processor core, bus interface unit and on-chip memory, which can improve the protection capability of the application specific power security CPU core against time attack, power...
analysis attack, error injection and buffer overflow. At the same time, the hardware resources of the security mechanism are small, the performance and power consumption are controllable.

- Cryptographic service module: it includes asymmetric state encryption algorithm SM2 hardware acceleration engine, symmetric state encryption algorithm SM1 and SM4 hardware acceleration engine, state encryption algorithm SM3 hardware acceleration engine, and hardware true random number generator. The hardware acceleration engine of SM1 is mainly used to provide public key encryption and decryption, digital signature and verification, key exchange, identity recognition and other functions. The hardware acceleration engine of SM2 mainly provides high-speed encryption and decryption of symmetric algorithm for the system. SM3 hardware engine provides integrity measure for internal data and code of chip, and provides high speed hash operation function for external. Hardware true random number generator mainly provides high speed safe and high quality true random number for the system.

- Physical circuit level safety protection unit: due to the importance of sensitive information such as program and data in the chip, the adversary may obtain sensitive information of system operation by means of physical anatomy of the chip or by changing the system clock frequency, external environment temperature of the chip and internal voltage of the chip to make the chip unsafe. The security logic module is to set the corresponding detection circuit to collect the changes of the external environment such as voltage, temperature and frequency. According to the intensity of the attack, the corresponding security strategy is implemented. The chip can stop working or clear the sensitive information inside the chip to protect the chip assets from being stolen by the enemy.

- Memory protection unit: program and data storage are important assets to be protected by the security subsystem. In order to meet the requirements of system hierarchical startup, trust transfer, hierarchical protection of assets, and support system code configuration and update, the memory protection unit is used for management and configuration, so as to realize code download configuration, code and data hierarchical protection, and ensure that the code is started and transmitted step by step. Through the configuration of the memory protection unit, access control based on security attributes is realized.

- Full communication module: it mainly includes Mailbox and Shared storage which serves as the communication and information exchange medium between the security subsystem and the other subsystem.

| Number | Security mechanism                          | Number | Security mechanism                          |
|--------|--------------------------------------------|--------|--------------------------------------------|
| 1      | Random execution cycle                      | 11     | Branch execution cycle unification         |
| 2      | Random clock noise source                   | 12     | Data path polarity reversal                |
| 3      | Hardware random instruction                 | 13     | Explicit memory access properties          |
| 4      | General register check                      | 14     | Standalone stack pointer                   |
| 5      | Control register check                      | 15     | External universal register reset          |
| 6      | Pipeline calibration                        | 16     | Key register backup                        |
| 7      | Configurable calibration algorithm           | 17     | Bus data interference                      |
| 8      | Program counter check                       | 18     | Bus data verification                      |
| 9      | Protection area executable check            | 19     | Safety violation detection                 |
| 10     | Multiplication execution cycle unification  |        |                                             |

For the PSS, it will make traditional security encryption chip embedded within the safety function inside the main control chip, avoid the encrypted data transmission outside. The encryption properties depend on the security subsystem work frequency and single chip solutions also reduces the board level design complexity, which bring power terminal chip level safety protection, promote the
efficiency of security and encryption, and reduce power terminal in smart grid board level design complexity and cost.

3.2. The ASPS Architecture Design

The ASPS mainly includes application special DSP CPU core, application special power algorithm module (power data management engine, network communication engine, power pre-data processing engine and electrical protection calculation engine), and power custom Ethernet-MAC interface which is shown in figure 3. The application special power module is integrated based on standard bus protocol in the form of IP core according to chip’s special requirements for protection terminal in smart grid.

Application special power DSP instruction set, not only can improve the efficiency of data parallel execution, accelerate the arithmetic operation, but also maintain the characteristics of the flexible programmable by using very long instruction word (VLIW) flow and single instruction multiple data (SIMD) technology. The ASPS integrates application special power algorithm engine, can be applied to a variety of power application scenarios (such as protection terminal, FTU, DTU), having a good expansibility.

![Figure 3. Architecture design for ASPS](image)

The application special power DSP core has three bus interfaces, which are set to access instruction storage, data storage and control register respectively. Application special power DSP uses VLIW technology to improve the parallelism of instruction level, integrates 4-channel VLIW decoder, 2 channels for data reading and writing, and 2 channels for logical operation. The instruction decoder transmits control signals to the data read-write module and the operation module, in which the data read-write module has the function of data alignment and packaging, and transfers the data to the register heap of the operation module. The operation module consists of scalar operation and vector operation, which are respectively composed of register heap and processing unit. The single instruction and multiple data flow (SIMD) technology is adopted in the vector operation, which can effectively improve the efficiency of data parallel processing.

The application special power DSP core realizes common power algorithms at the instruction level, which gives consideration to flexibility and computing performance. The special power algorithm module can realize the power algorithm by hardware-curing for smart grid, providing the strongest performance for power application.
4. Conclusion
In this paper, the architecture of application specific power chip (ASPC) which mainly includes power security subsystem (PSS) and application special power subsystem (ASPS) for power terminal in smart grid is designed. The PSS is configured with secret algorithm module, application special power CPU core, and security communication module, etc., that embedded in the chip. It can provide data encryption and decryption, identity authentication and other security services based on the hardware logic of anti-attack state secret security algorithm, so as to improve the security and encryption efficiency of chip-level security protection. The ASPS contains application special power DSP core and application special power algorithm engine, adopts VLIW, SIMD technology and application special power DSP instruction set. Therefore, the efficiency of data parallel execution can be increased and the processing efficiency of power terminal in smart grid can be improved.

5. Acknowledgments
This paper is supported by the National Key R&D program of China (2018YFB0904900, 2018YFB0904903).

6. References
[1] Z. Guan, J. Li, L. Wu, Y. Zhang, et al., "Achieving Efficient and Secure Data Acquisition for Cloud-Supported Internet of Things in Smart Grid," in IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1934-1944, Dec. 2017.

[2] X. Wang, Jiang. X, Zhe. W, et al., "An Analytical Study of Power Delivery Systems for Many-Core Processors Using On-Chip and Off-Chip Voltage Regulators," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 34, no. 9, pp. 1401-1414, Sept. 2015.

[3] W. Xi, S. Suo, T. Cai, et al., "A Design and Implementation Method of IPSec Security Chip for Power Distribution Network System Based on National Cryptographic Algorithms," 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, China, 2019, pp. 2307-2310.

[4] Qi Huang, Xiaoping Chen, Bingfeng Wang, et al., "The Concept of Computing on Chip (CoC) for Electric Power System Application," International Symposium on Parallel Computing in Electrical Engineering (PARELEC’06), Bialystok, 2006, pp. 433-437.

[5] E. ul Haq, M. K. Hafeez, M. S. Khan, et al., "FPGA implementation of a low power, processor-independent and reusable System-on-Chip platform," 2009 International Conference on Emerging Technologies, Islamabad, 2009, pp. 337-341.

[6] C. J. Lukas, F. B. Yahya and B. H. Calhoun, "An Ultra-low Power System On Chip Enabling DVS with SR Level Shifting Latches," 2018 IEEE International Symposium on Circuits and Systems (ISCAS), Florence, 2018, pp. 1-4.

[7] X. Ma and H. Sun, "The Research of Power Quality Real Time Monitor for Coal Power System Based on Wavelet Analysis and ARM Chip," 2010 Asia-Pacific Power and Energy Engineering Conference, Chengdu, 2010, pp. 1-4.

[8] W. Xi, H. Yao, T. Cai, et al., "Research on chip-based protection and measuring and control devices," Power System and Clean Energy, vol. 32 no. 11, pp. 92-97, Nov. 2016.

[9] R. Bondade and D. Ma, "Hardware-software co-design of an embedded power management module with adaptive on-chip power processing schemes," Proceedings of 2010 IEEE International Symposium on Circuits and Systems, Paris, 2010, pp. 617-620.

[10] Y. Chi, W. Cui, L. Qiao, et al., "Hardware Architecture Design of the Deep-learning-based Machine Vision Chip," 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, China, 2019, pp. 1110-1113.

[11] Y. Chi, W. Zhang, Z. Zheng, et al., "A Cortex-M3-Based System-On-Chip Architecture for Wireless Communications in Power Grid," 2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC), Chongqing, China, 2018, pp. 16-19.