ETSNW0001 - A Design and Implementation Method of IPSec Security Chip for Power Distribution Network System Based on National Cryptographic Algorithms

Abstract

The target of security protection of the power distribution automation system (the distribution system for short) is to ensure the security of communication between the distribution terminal (terminal for short) and the distribution master station (master system for short). The encryption and authentication gateway (VPN gateway for short) for distribution system enhances the network layer communication security between the terminal and the VPN gateway. The distribution application layer encryption authentication device (master cipher machine for short) ensures the confidentiality and integrity of data transmission in application layer, and realizes the identity authentication between the master station and the terminal. All these measures are used to prevent malicious damage and attack to the master system by forging terminal identity, replay attack and other illegal operations, in order to prevent the resulting distribution network system accidents. Based on the security protection scheme of the power distribution automation system, this paper carries out the development of multi-chip encapsulation, develops IPSec Protocols software within the security chip, and realizes dual encryption and authentication function in IP layer and application layer supporting the national cryptographic algorithm.

Index Terms the power distribution automation system; network security; national cryptographic algorithm; sercurity chip; IPSec protocol