Research on EPGIS Spatial Information Security for Smart Grid

Ji-ye WANG¹, Nan ZENG¹, Jin-chang LIU² and Cheng-yue YANG²,*

¹Department of Information and Communication, State Grid Corporation of China, Beijing, 10031, China
²State Grid Information & Telecommunication Group Co. Ltd., Beijing 100761, China
*Corresponding author

Keywords: EPGIS, Security, Smart grid.

Abstract. Through EPGIS, the power grid spatial data, accounting data and business process data are integratedly modeled and managed to form an integrated resource management map of electricity resources and spatial information that can support various activities of the grid and serve relevant businesses. However, due to the existing update and maintenance methods, there are some problems such as unsound update mechanism, cumbersome acquisition process, low efficiency, over-reliance on GPS, lack of security and other issues, seriously restricting the quality and safety of power grid resource information updates. In this paper, a general technical framework of power grid spatial information security management is proposed. Security design is carried out from three aspects: data layer, logical layer and presentation layer. EPGIS data processing security protection tool and application security protection tool are also designed. The mechanism achieved multi-dimensional, all-round security for EPGIS.

Introduction

Most power grid resources have natural connection with spatial location, and geographic information technology has significant advantages in the management and presentation of smart grid structure and topology. The power grid covers a vast area with a large power grid management and service area. It cannot meet the management requirements of current and future power grids only through the traditional text and digital informationization. The future direction of the power grid is cleaner, more sustainable and smarter. The first step in the smart grid is to digitize the power grid. Geo-information technology is an indispensable and important technology for building a digital power grid.

Geographic information system (GIS) is the traditional geography, mapping and measurement and other disciplines and modern remote sensing technology, global positioning system, computer science and other science and technology, the integrated application of spatial data processing technology [1]. Through the integrated modeling and management of power grid spatial data, accounting data and business process data through GIS technology, the power grid equipment and facilities information, operational status information, production management information and electricity consumption information can be integrated with mountains, rivers, terrain, streets, As well as the natural environment information such as meteorology, geology, resources, etc., are centralized in a unified system to form an integrated resource database of electricity, electricity, and space information that can support various activities of the entire enterprise and serve relevant businesses so as to standardize and scientifically work the power enterprises, Automation, refinement, to achieve management innovation, technological innovation, improve work efficiency and economic and social benefits. In smart grid, we call it as electric power GIS (EPGIS) [2].

For a long time, because of the lack of the key technical support for the spatiotemporal information security of complex large power grids, EPGIS often guarantees the safe and effective operation of the power grid by dividing power grid management rights and weakening the spatial and temporal information attributes [3], but cannot efficiently and efficiently implement the entire network of...
devices and states Uniform management results in inefficiencies in various application services in the power grid. This imbalance with the ever-increasing grid scale and increasingly in-depth core network applications cannot meet the urgent need of very large power grid enterprises for providing fine management, timely service and safe power supply.

System Model
The overall technical framework of power grid spatial information security management is divided into data layer, logic layer and presentation layer [4]. The data layer is a data object (management policy data and system log data) generated by the EPGIS data objects (basic geographic data and grid graphical data) and data protection tools that need to be protected. The logical layer is established on the basis of the data access layer Of the various functional components to achieve the various functions of data security; presentation layer is displayed to the user's application tools, the system's manifestations will be EPGIS platform C / S client combination, including acquisition, processing, application of protective tools And configuration tools. Specific technical architecture as follows:

![Figure 1. EPGIS platform spatial information security system technology architecture map.](image)

The overall framework consists of four parts: business architecture, application architecture, data architecture and technology architecture. Each component independently supports the specific protection functions of grid GIS security and cooperates with each other to form the spatial information security management architecture of EPGIS platform.

Business Architecture
The business architecture is based on the protection requirements of all kinds of spatial data of EPGIS in various stages of the data life cycle. The business functions are analyzed and summarized to form a detailed business function system. The business model is formed according to the business development needs and applied to the GIS spatial data security protection system Architecture, technology architecture and data architecture design basis. The scope of requirements includes grid GIS spatial data acquisition security protection, processing security protection and application security protection, combined with the original security protection work of grid GIS to form the following business architecture diagram:
Application Architecture

The application architecture describes the correspondence between each functional component of the GIS spatial data security protection system and the data in actual production and application process, and abstracts and designs according to the content and storage protection requirements of grid GIS spatial data in each phase. The grid GIS spatial data security Protective application architecture is divided into: grid GIS spatial data collection terminal security reinforcement, power grid GIS spatial data processing security tools and power grid GIS spatial data application security tools. Specific application diagram is as follows:
Space Data Acquisition Terminal Security Reinforcement

Grid Spatial Data Acquisition Terminal Security

Through the integration and utilization of the technical achievements already possessed by the power grid security access platform, the data acquisition terminal security protection function is realized, including the secure memory card and the technologies such as identity authentication and data anti-theft [5], so as to connect the secure memory card with the desk management system. Make sure the secure memory card is recognized and used properly by the desk tube system. To ensure that field collectors use PDA and other grid data collection tools to collect, store and transfer GIS spatial data security.

Security Storage Disk Security

All PC terminals in the power information network have a desktop management system installed [6]. The secure memory card needs to be connected to the desk-top system to ensure that the secure memory card is recognized and used normally by the desk-top system. Secure memory card access to the PC terminal, you need to ensure that the table can be identified by the system and the normal use. At the same time provide encryption and decryption interface and identity authentication interface, secure storage card with key function, data certificate through CA Center after verification can read and write.

Spatial Data Processing Security Tools

Sensitive Spatial Data Access Authentication

Before users can access the data, they need to log in, extract the identity information of the secure storage device and perform digital digest comparison to verify the validity of the identity information [7]. When the client performs data operations, online authentication needs to be performed through the network heartbeat technology to ensure that the client is a valid terminal. This function is mainly based on Socket technology, using TCP / IP protocol for authentication on the server side. When the client does not pass identity authentication or is offline, the policy will prohibit users from accessing and manipulating data.

Spatial Data Processing Process Detection and Audit

According to the set monitoring strategy (by tracking the PC terminal program process or identify the contents of the data file) automatically capture data processing personnel data operation process, record the operator, operation time, operation object, operation content and other log information. According to the data object, the use of personnel, time stamp, use of places, the use of such information, depicting the formation of different dimensions of the audit results. These results help managers grasp the ways, means and personnel of data flow, grasp the application trajectory of data and analyze the data application trajectory, so as to further strengthen the security management and prevent the occurrence of security information leakage.

GIS Data Copyright Protection

Through digital watermarking technology, copyright control and protection of watermark information embedded in GIS vector data [8]. GIS image data and grid space resource data are carried out. At the same time, watermark information is robust and not destroyed by data editing. The use of the system comes with watermark extraction function, if the accidental loss of data in the sharing, which can be embedded through digital watermarking technology for evidence, investigate and punish the illegal proliferation of data units and data users to protect the legitimacy of data sharing and order.
Spatial Data Application Security Tools

Spatial Data Export Security

In order to protect the spatial data of the EPGIS platform, the spatial data of the grid derived from the platform needs to be encrypted so that the exported data is ciphertext-protected to prevent the risk of data leakage after being exported and exported. Allows the authorized user to export data, encrypts the data and saves it to the PC terminal for exporting. Export the encrypted data, and automatically and transparently decrypt and view it on the PC where the GIS C/S client is installed. Provides data decryption and outgoing control functions, authorized users can apply for decryption, outgoing data can be made after the production.

GIS Client Database Security

In order to improve the response speed of the EPGIS platform, there is a local database SQLite in the C/S client of the EPGIS platform to store the cached data. The project aimed at the security problems of SQLite embedded database, based on the analysis of common database security mechanism, designed a set of feasible security mechanism for it. The combination of password authentication and data encryption, by increasing the key to create, data encryption and decryption, page coding and event logging code, SQLite database security. In addition, the local database and the client's hardware identification binding (such as the hard disk ID or network card MAC address), limiting the local database free to copy.

Summary

In this paper, we proposed a general technical framework of power grid spatial information security management. And the security design is carried out from three aspects: data layer, logical layer and presentation layer. Meanwhile, the business architecture, application architecture, data architecture and technology architecture are designed as components. Each component It not only supports the specific protection functions of EPGIS security independently but also cooperates with each other to form the spatial information security management architecture of EPGIS platform. Moreover, the design of the spatial data acquisition terminal security reinforcement tools, spatial data processing security protection tools and spatial data application security tools, to achieve multi-dimensional, all-round security of EPGIS.

References


