



# Analysis of security operation and maintenance system using privacy utility in media environment <sup>☆</sup>



Zhengwei Jiang <sup>a,\*</sup>, Guoen Chen <sup>b</sup>, Xueqi Jin <sup>a</sup>, Yueqiang Wang <sup>b</sup>

<sup>a</sup> State Grid Zhejiang Electric Power Co., LTD, China

<sup>b</sup> State Grid Jiaxing Electric Power Supply Company, China

## ARTICLE INFO

### Article history:

Received 24 June 2018

Revised 4 September 2018

Accepted 10 September 2018

Available online 12 September 2018

### Keywords:

KVM

Safety

Operation and maintenance control

Intelligent management

## ABSTRACT

At present, the power information room mostly adopts the analog KVM matrix, or adopts the digital KVM matrix, but there are various defects in the two methods. In order to solve the problem of traditional mode, this paper developed a new security operation and maintenance management system composed of 5 parts. It also has the advantages of traditional mode and overcomes the shortcomings of the traditional model. First, introduces the advantages and disadvantages of two kinds of traditional model, puts forward the necessity of improving; then, the security operation management system each part of the design, and set out to achieve its function; finally carries on the analysis of security. The results show that the security operation and maintenance management system improves the security of the system and helps the system to operate more intelligently and safely based on the guarantee of the required functions.

© 2018 Elsevier Inc. All rights reserved.

## 1. Introduction

KVM (Keyboard, Video, Mouse) is a kind of multi computer switching technology, KVM system can connect the devices controlled computer keyboard, mouse and graphics interface, using a set of equipment control computer system [1]. With its flexible access, easy management, data security and low cost [2], has been widely used in KVM systems. Centralized management of equipment by using KVM matrix has been adopted by most of the power enterprises, the vast majority of the original information room is simulated by the KVM matrix, and KVM matrix derived from the digital [3,2,4], but both in the use of the process has some disadvantages.

The analog KVM matrix transmits analog signals through the hub and extender, and the console is still in the computer room. Because of its access to fixed position, cannot disperse the visit, and must pass the physical cable way cascade expansion, has great limitations exist at the same time distance and quantity restrictions, expansion is very inconvenient; secondly, when the main KVM fault, there will be all KVM cannot access the situation, bring about serious consequences; in addition, simulation of KVM matrix still exists to transmit data between workstations and servers, no

operation audit, the problem of failure of traceability and logging is not reliable, the recording time is short, the query is not convenient to defect.

The digital KVM matrix converts analog signals into digital signals through the TCP/IP protocol to transmit digital newspaper, remote access, remote access support but its resolution is low, the highest early support of only 1600 \* 1200; the poor flexibility of the mouse remote access, can reach up to 20 frames per second, mobile mouse has obvious delay the network is not good, or even high resolution Caton phenomenon; on the other hand, access to the digital KVM PC client through the network, the diversity of the client, may cause compatibility issues at the time of the visit, at the same time, security is difficult to guarantee.

Security operation and maintenance system require a whole set of security solutions. For example, in video surveillance, the whole system contains camera equipment, face recognition system and pedestrian re-identification. Each part of the system will affect the result of the system. So an effective security operation and maintenance system is indispensable.

In order to overcome the above defects of traditional KVM matrix, the better the power system information room management, this paper presents a new type of safety operation and management control system, which is mainly composed of a centralized management server, audit server, server management, intelligent gateway station, intelligent user interface module and server PBX. This article will focus on each component of the

<sup>☆</sup> This article is part of the Special Issue on TIUSM.

\* Corresponding author.

E-mail address: [1668900100@qq.com](mailto:1668900100@qq.com) (Z. Jiang).

detailed design instructions, and its work process is described, and finally its security analysis.

## 2. System design

The security operation and maintenance management system is mainly divided into 5 parts, the topology of which is shown in Fig. 1.

The centralized management server is the core of security management system, including login entrance, distribution, log view etc.; and the audit server for audit records on the server operating video and keyboard characters; intelligent server management gateway is connected to a server entrance, is a bridge connecting server and the switch; the user station is the operation of the user terminal connect the monitor, mouse, keyboard, speakers and other equipment; intelligent server interface module is connected with the local server to server intelligent management gateway interface; PBX for network connection equipment. These five parts constitute the whole system safe and reliable work, the following specific for each part of the detailed design instructions.

### 2.1. User workstation

The user workstation can access either the centralized management server or the intelligent management gateway of the server directly. It uses special hardware and operating system, and it can guarantee access fast and stable because the server intelligent gateway adopts the latest algorithm technology.

In addition, the user workstation is independent of the application of high performance IP server access, using the standard Cat5 cable (Ethernet IP) cabling, can be single or dual to simultaneously access, check and control server; can be connected to the speakers, used for audio playback server, can also connect the USB storage peripherals, data transmission to the server. For security reasons, you can only identify the U disk with characteristic code to avoid the infection of the U disk virus. Access to the server in the user station, video recording and keyboard recording for post hoc traceability, and audit records playback review.

### 2.2. Intelligent server management gateway

The server intelligent gateway uses the latest compression algorithm technology, can achieve 1920 \* 1200@30FPS video transmission, single mouse movement effect is similar to the local, will not appear Caton. The gateway supports IE, Firefox and other browser access, also supports client mode access, while supporting access to the user's shared access, and can support the sharing of 8 users at most. In the visit, the full support of Chinese and English, the number of concurrent access, optional 4 or 8 Road, the latter 32 servers to provide support.

### 2.3. Server interface module

The interface type of interface module has PS2, USB and SRL, which can meet the access of different types of servers. The USB

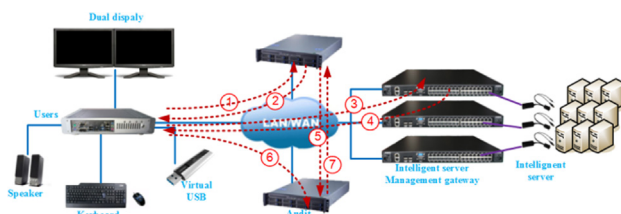


Fig. 1. Topology diagram of safety operation and maintenance management system.

interface module has double CAT5 interface output, and can be connected to the intelligent management gateway of the server all the way, and the other way is connected with the maintenance packet of the computer room, and the signals of the two signals are identical. The server interface module has built-in memory chip, which can store its serial number, identification name and other information. It also has the function of DDC2B and can automatically match the resolution.

### 2.4. Centralized management server

Centralized management server can manage multiple server intelligent management gateway, the unified login, unified authorization, unified log view, and the maintenance package authorized by the serial number of the license server interface, to which server can access interface module. In order to achieve safety and alarm system, centralized management server module with offline server module fault warning capability, predict or other man-made factors, and specific MAC address of the authorized user workstation access, ensuring access to safe. At the same time, the centralized management server also supports the main standby mode, supports load balancing, with complete log system, can make all kinds of alarm log view, and can integrate the audit server management, implementation of management integration.

### 2.5. Audit server

The audit server has a powerful audit function that allows simultaneous auditing of multiple user workstations, and the maximum number of concurrent calls to a single audit server is 40. The server also has intelligent audit function, system can detect the keyboard and mouse movements, in the process of the server session is open, if the keyboard and mouse for a period of time without action, the audit will be automatically closed; when the keyboard mouse recovery action, the audit can immediately open. Audit system can be retrieved according to time, user name, server name combination to achieve rapid positioning, and to support the main standby mode, to ensure that the audit will not be omitted.

## 3. Data flow control

The manager can access the server data stream through the user workstation, and the entire user workstation can be described from the launch access to the end of the session, as shown in Fig. 2.

The data flow process of the user workstation accessing the server can be described as follows:

1. The user workstation uses the key to log in to the centralized management server and requests to initiate access to a server;
2. The centralized management server, according to the user's permissions, returned to the user workstation following content:
  - (A) The IP address of the server intelligently managing the gateway;
  - (B) Request the port number of the access server;
  - (C) Temporary generated one-time authentication code used for identity authentication;
  - (D) Specific operational permissions, including keyboard, mouse, audio, and virtual media;
3. The user workstation accesses the server on the designated server of the intelligent management gateway by obtaining the information from the management server.

Download English Version:

<https://daneshyari.com/en/article/11031545>

Download Persian Version:

<https://daneshyari.com/article/11031545>

[Daneshyari.com](https://daneshyari.com)