SysKeeper-2000 安全隔离装置

（正向型）

技术白皮书

V2.0

南京南瑞信息通信科技有限公司

南京市南瑞路 8 号 210003

技术服务热线 025-81082222

www.sgepri.sgcc.com.cn

2021 年 01 月

一、产品定位

电力专用网络安全隔离装置（正向型）应用于电力企业生产控制大区安全区 I/II 到管理信息大区安全区 III 的单向数据传递。它可以识别非法请求并阻止超越权限的数据访问和操作，从而有效地抵御病毒、黑客等通过各种形式发起的对电力网络系统的恶意破坏和攻击活动，保护实时闭环监控系统和调度数据网络的安全；同时它采用非网络传输方式实现这两个网络的信息和资源共享，保障电力系统的安全稳定运行。

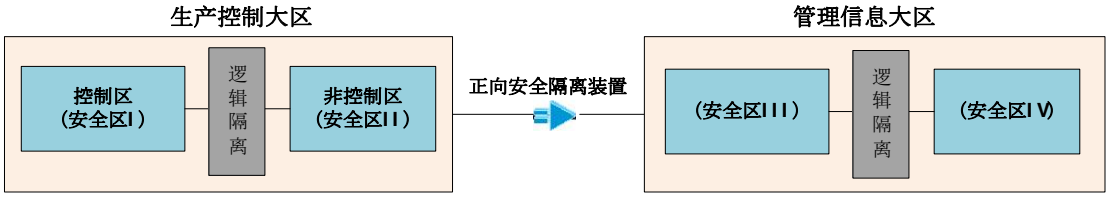

图 1 部署位置图

二、体系结构

SysKeeper-2000 网络安全隔离产品(正向型)的硬件结构如图 1 所示。本产品硬件采用 RISC 体系结构高性能嵌入式计算机芯片，双机之间通过四片高速物理传输芯片进行物理连接，底板上各有两个 10M/100M 以太网接口(IA1/IA2 和 IB1/IB2)用来连接要隔离的两个网络。内网**双机接口**（IA3）采用网络方式实现隔离装置的双机热备份，内外网的**告警接口**(IA4、IB3)采用标准串口进行告警信息输出，同时支持网络方式上报到后台监控主机。内网串口可以用来连接配置终端，方便管理人员对网络安全隔离设备的控制，硬件看门狗时刻监视系统状态，保证隔离装置的稳定、可靠运行。

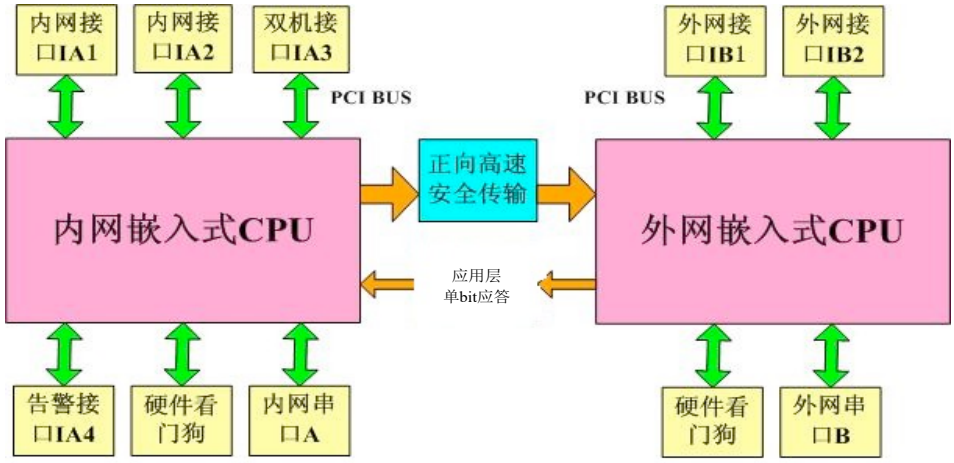

图 2 正向型网络安全隔离装置硬件结构图

三、产品特点

为满足电力系统二次安全防护的需要，南瑞集团公司依托在网络安全产品中的广泛技术积累和应用实践经验，以性能好、功能全、使用简便、运行稳定为网络安全隔离产品的设计原则，自主研制并推出 SysKeeper-2000 网络安全隔离系列产品。通过长时间的测试，网络安全隔离设备具有很高的可靠性、稳定性和可以满足用户需要的执行效率。

3.1 产品外观

■ 百兆型

图 3 SysKeeper-2000 网络安全隔离装置(正向型百兆)

■ 千兆型

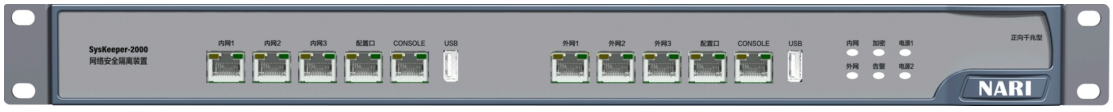

图 4 SysKeeper-2000 网络安全隔离装置(正向型千兆)

3.2 硬件特色

✧ **高安全隔离能力的硬件结构**

SysKeeper-2000 网络安全隔离系列产品由两个高性能嵌入式微机及辅助装置形成安全隔离系统，嵌入式微处理器采用 RISC 体系结构，减少受攻击的概率；实现两个安全区之间的非网络方式的数据交换,并且采用安全算法保证安全隔离装置内外两个处理系统不同时连通,在保证安全隔离的前提下，实现数据的高速交换。

✧ **高可靠性硬件设计**

SysKeeper-2000 网络安全隔离系列产品硬件供电采用的是国外进口开关电源，符合 EN55022 class B,IEC801-2,3,4,5, EN60555-2,3 EMC 标准，平均无故障时间达 64223 小时。在 PCB 板的设计中，加有线性稳压及滤波装置，并严格按照 EDA 对高频电路设计的要求,设计了单独的电源层与地层,进一步保证了整个板上电源的稳定性。

✧ **硬件优化设计**

充分考虑电厂和变电站的特殊运行环境，SysKeeper－2000 网络安全隔离系列产品装置设计遵循分布均匀、布局合理的原则，风扇处增加了防尘罩，而且紧靠散热源，起过滤作用，避免灰尘和湿气；机箱散热风扇也采用滚轴风扇，保证了风扇的长期可靠运行；通过增加专用转接板，起到了更好的加固和抗震作用；即使在长途的运输过程中，也能充分地保障设备内部的完整性和可用性能

✧ **严格的生产流程控制**

南瑞网络安全隔离系列产品严格遵循 ISO9000 2000 版质量认证体系，对每一台隔离产品的关键芯片和元器件进行产品老化试验,所有的隔离产品在出厂前必须经过 240 小时以上的连续通电测试，确保每一台网络安全隔离产品运行的稳定性和硬件的高可靠性。

✧ **支持双电源**

实践经验及理论都证明，一个产品最易出故障的部位在电源部分。在南瑞安全隔离系列产品中，设计有双电源。在工作的时候,有一个电源作为主电源供电,一个作为辅电源作备份，实现了主备电源的**在线无缝切换**，有效地提高整个电源工作的可靠

性及延长整个系统的平均无故障工作时间。**南瑞安全隔离系列产品为国内第一家采用双电源设计的物理隔离产品。**

✧ **支持双机热备**

在实际应用中，可以设置有双机备份，一台工作在主机位置，一台工作于备用位置，两台机器时刻进行通信并进行信息备份，一旦当主用设备出现故障（包括掉电、连接的网络线路至少有一根出现故障）时，或者处于看门狗复位阶段，备机可以以承担起主机的工作，以避免重要数据的丢失。

✧ **支持系统告警**

南瑞网络安全隔离系列产品支持完备的安全事件告警机制，当发生非法入侵、装置异常、通信中断或丢失应用数据时，可通过隔离装置专用的告警串口输出报警信息。

3.3 产品特点

✧ **安全裁剪内核，系统的安全性和抗攻击能力强**

为了保证系统安全的最大化，南瑞网络安全隔离产品（正向型）已经将嵌入式内核进行了裁剪和优化。目前，内核中只包括用户管理、进程管理，裁剪掉 TCP/IP 协议栈和其它不需要的系统功能，进一步提高了系统安全性和抗攻击能力，免于黑客对操作系统的攻击，并有效抵御 Dos/DDos 攻击。

✧ **数据单向传输控制**

物理上控制反向传输芯片的深度，在硬件上保证从低安全区到高安全区的 TCP 应答禁止携带应用数据，大大增强了高安全区业务系统的安全性。在物理上实现了数据流的纯单向传输，数据只能从内网流向外网。

✧ **割断穿透性的 TCP 连接**

南瑞网络安全隔离产品（正向型）采用截断 TCP 连接的方法，剥离数据包中的 TCP/IP 头，将内网的纯数据通过正向数据通道发送到外网，同时只允许应用层不带任何数据的 TCP 包的控制信息传输到内网，保护内网监控系统的安全性。

✧ **基于状态检测的综合报文过滤**

SysKeeper-2000 正向网络安全隔离产品采用基于状态检测技术的报文过滤技术，可以对出入报文的 MAC 地址、IP 地址、协议和传输端口、通信方向、应用层标记等进行高速过滤。状态检测技术采用的是一种基于连接的状态检测机制，将属于同一连接的所有包作为一个整体的数据流看待，构成连接状态表，通过规则表与状态表的共同配合，对表中的各个连接状态因素加以识别，连接状态表里的记录可以随意排列，提高系统的传输效率。因此，与传统包过滤技术相比，具有很好的系统性能和安全性，可以极大的提高数据包检测的效率。

✧ **NAT 与虚拟主机 IP 技术**

SysKeeper-2000 系列网络安全隔离系列产品完全支持透明工作模式，隔离装置本身没有 IP 地址，MAC 地址隐藏（无法通过标准的网络扫描方式获得），极大地提高了隔离产品的安全性。同时，SysKeeper-2000 系列网络安全隔离产品支持多种网络地址转换技术（NAT），包括静态地址转换、地址池和动态地址转换技术，充分隐藏内网监控系统的网络地址，保证内网监控系统的安全性。

✧ **基本安全功能丰富，可实现在网络中的快速部署**

采用综合过滤技术，在链路层截获数据包，然后根据用户的安全策略决定如何处理该数据包；实现了 MAC 与 IP 地址绑定，防止 IP 地址欺骗；支持静态地址映射(NAT)以及虚拟 IP 技术；具有可定制的应用层解析功能，支持应用层特殊标记识别，为用户提供一个全透明、安全、高效的隔离装置。

✧ **独特的自适应技术**

南瑞网络安全隔离系列产品采用独特的自适应技术，隔离设备没有 IP 地址，隐藏 MAC 地址，非法用户无法对隔离设备进行网络攻击，有效的提高了系统的安全性能。

✧ **网络数据处理流畅，不会成为网络通讯瓶颈**

隔离设备采用 motorola 高性能 RISC 体系结构 CPU，内核使用高效的过滤算法，充分发挥良好的硬件性能，采用高速传输芯片实现数据的高速安全传输，百兆状态下的有效网络吞吐率最高可达 80Mbps，每秒处理数据包个数为》8000（1024 字节）不会造成网络通讯的瓶颈。

✧ **丰富的通信工具软件和 API 函数接口**

为了使隔离设备达到预期的安全效果,经过隔离设备进行数据传输的软件必须按照《全国电力二次系统安全防护总体方案》的规定进行开发。针对 I/II 区到 III 区通信内容规定,南瑞 SysKeeper-2000 网络安全隔离设备提供了丰富的通信工具软件）和 API 函数接口，方便用户进行二次系统安全隔离改造。

✧ **丰富的电力二次系统安全改造经验**

南瑞 SysKeeper－2000 网络安全隔离设备（正向型）与南瑞所有的监控系统（包括网、省调、地调、县调和变电站 SCADA 系统以及水电、火电监控系统）进行了安全改造工作和现场的实际运行；同时与国内外主流的监控系统厂商进行了广泛、深入的合作（国内：包括东方电子、鲁能积成、上海申贝等；国外：阿尔斯通监控系统、原 CAE 公司监控系统、PI 实时数据库、Valmet SCADA 系统等），保证电力二次系统安全防护工程的顺利实施。

✧ **操作简单的图形化用户界面**

南瑞 SysKeeper-2000 网络安全隔离设备提供了友好的图形化用户界面，可以进行全新的可视化管理与配置。整个界面使用全中文化的设计,通过友好的图形化界面，网络管理员可以很容易地定制安全策略和对系统进行维护管理。用户只需进行简单的培训就可以完成对隔离设备的管理与配置。

✧ **完善的日志审计功能**

日志在南瑞 SysKeeper-2000 正向隔离设备每天的运行中起着很重要的作用,由于许多攻击、系统漏洞不具备机器可分析的特征，或者新的攻击的特征还不为人所知，因此，日志是发现攻击、发现系统漏洞和记录攻击证据的重要手段。隔离设备内、外网各板载安全存储区用于系统日志的记载，循环更新保持最新的系统日志。同时支持专用网络方式将日志发送到后台日志处理程序,供用户分析使用,日志规范符合《电力二次系统安全告警日志格式规范》,可以接入电力二次系统内网安全监视功能模块集中监视。

四、安全隔离装置硬件指标及性能参数

南瑞 SysKeeper-2000 系列安全隔离产品关键元器件的主要技术指标和参数如下所示。

百兆型：

指示项	内网侧	外网侧
网口	100/1000M Base-T,3 个	100/1000M Base-T,3 个
串口	RS232，一个，Console	RS232，一个，Console
USB	USE 3.0 Host，Type A，一个	USE 3.0 Host，Type A，一个
电源	双路冗余电源，支持 AC/DC/110V/220V	
功耗	30W	
尺寸	440*350*44（mm）	
工作温度	-20~+70℃	
数据包吞吐量	≥340Mbps	
数据转发延时	≤1ms	

千兆型：

指示项	内网侧	外网侧
网口	100/1000M Base-T,3 个	100/1000M Base-T,3 个
串口	RS232，一个，Console	RS232，一个，Console
USB	USE 3.0 Host，Type A，一个	USE 3.0 Host，Type A，一个
电源	双路冗余电源，支持 AC/DC/110V/220V	
功耗	45W	
尺寸	440*400*44（mm）	
工作温度	-20~+70℃	
数据包吞吐量	≥800Mbps	
数据转发延时	≤1ms	

五、技术服务

南京南瑞信息通信科技有限公司

地址：江苏省南京市鼓楼区南瑞路 8 号

邮编：210000

技术服务热线：025-81082222（周一至周五：9:00-11:30 13:30-17:30）