文章编号：1005-8451（2015）02-0017-06

物理安全监控平台的研究与实现

温桂玉
（北京经纬信息技术公司，北京 100081）

摘 要：在整个信息安全体系中，物理安全处于基础地位，必须给予足够的重视。采用信息技术手段监控保障物理安全，成为必然的选择。本文通过介绍研发背景，从平台功能、系统架构、网络方案等角度出发，基于远程监控单元（RMU）、平台通信协议及多线程监控数据采集处理技术等关键技术手段，提出了一套物理安全监控平台主要技术方案，同时对平台特点和应用效果进行了分析与总结。

关键词：物理安全；现场总线；监控系统；多线程；Socket
中图分类号：U29-39 **文献标识码：**A

Research and implementation of physical security monitoring platform

WEN Guiyu
(Beijing Jingwei Information Technology Co., Beijing 100081, China)

Abstract: In the Information Security System, physical security was in the basic position, should be paid enough attention. Using information technology to monitor and support physical security became an inevitable choice. Through the introduction of research background, from the view of platform function, system architecture and network, based on remote monitoring unit (RMU), platform communication protocol and multi thread monitoring data collection and processing technology etc., the paper presented the main technical scheme of a set of physical security monitor platform, analyzed and summarized the platform characteristics and application effect.

Key words: physical security; field bus; monitoring system; multi thread; Socket

物理安全又叫实体安全（Physical Security），是保护计算机设备、设施（网络及通信线路）免遭地震、水灾、有害气体和其他环境事故（如电磁污染等）以及人为操作失误或各种计算机犯罪行为导致的破坏的措施和过程。在信息安全体系中，物理安全是基础，如果物理安全得不到保障，如计算机设备遭到破坏或被人非法接触，那么其它的一切安全措施就成了无本之木，无源之水，无从谈起[1]。本文从保障物理安全角度出发，借鉴工业控制领域的现场总线技术与理念，依据机房安全技术标准，对物理安全监控平台（以下简称平台）进行研究与实现，提出了一套完整的解决方案。

1 平台技术方案

1.1 平台功能

平台主要从机房环境安全、电源安全、设备安全、通信线路安全及媒体安全等5方面进行物理安全保障。平台功能由环境安全监控、电源安全监控、设备安全监控、通信线路安全监控、媒体安全监控、物理安全评测及系统管理7部分构成[2]，如图1所示。

1.1.1 环境安全监控

环境安全监控主要针对系统所在环境的安全进行保护，主要包括区域保护及灾难保护两部分内容。

平台通过安防监控，门禁系统进行区域安全保护防止非法入侵行为的发生。安防监控提供区域实时画面预览、入侵侦测告警、录像、抓拍及追踪等功能。门禁系统对出入机房的相关工作人员进行统一管理与约束，配合安全管理制度，保障机房区域安全。

灾难保护主要包括防火监控、防水监控、防雷监控、防鼠监控等内容，当有灾难发生时，平台及时提供灾难预警、应急处理及告警恢复等功能，尽可能降低灾难产生的不利影响，避免更大灾害及次生灾害的发生，最大限度保障机房安全。

温度、湿度及洁净度并称为机房“三度”，为使机房内的“三度”达到相关标准规定的要求，专用精密空调、洁净度检测仪及除尘器等相关设备成了

收稿日期：2014-10-08
作者简介：温桂玉，工程师。

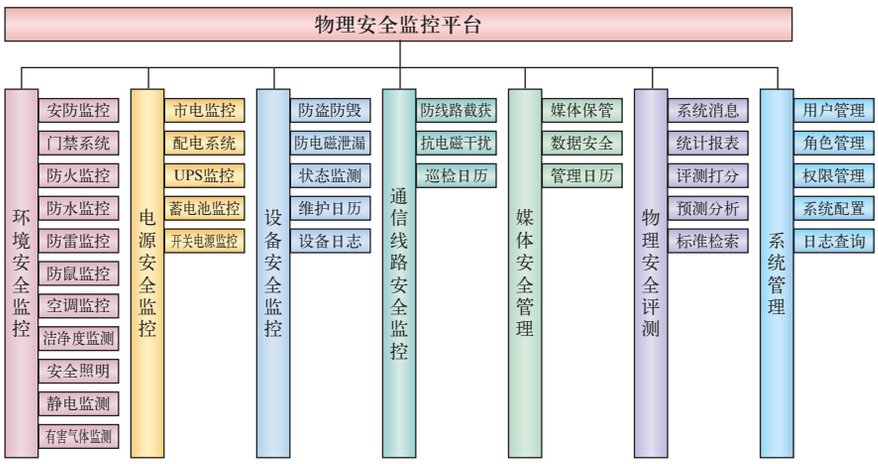

图1 平台功能结构图

机房必备的基础设施部分。平台通过对空调的工作状态监测与远程控制等技术手段，达到机房恒温恒湿的目的。通过洁净度检测仪，自动进行洁净度监测，当洁净度超过限定阀值时，根据系统设置，平台可通过短信，电子邮件等手段通知维护人员或自动启动除尘器进行除尘工作，以满足机房洁净度要求[3]。

平台支持照明控制，应急联动功能。平台能够根据参数配置适时自动开启、（部分）关闭照明系统，从而达到节约能源，低碳环保，降低运营成本的目的。

通过在容易引起静电的关键位置，如门口、机架过道等处，安装静电检测仪、静电接地报警仪等传感设备，平台支持静电全方位监测，提供静电监测预警，应急处理，恢复等功能。

通过在关键位置部署有毒有害气体检测仪，平台支持有毒有害气体预警，应急联动处理，应急恢复等功能。

1.1.2 电源安全监控

电源是机房各种计算设施的动力源泉，电源的稳定性、高效性及可靠性对机房物理安全与否，发挥着举足轻重的作用。电源安全监控功能主要包括市电监控、配电监控、UPS 监控、蓄电池监控及开关电源监控 5 部分内容。当平台侦测到电源部分有异常告警产生时，通过平台界面、短信及电子邮件等多种渠道及时通知工作人员，排除故障，平台亦可以根据系统配置自动执行某些逻辑动作，提高处理问题的反应时间和自动化水平。通过统一的异常告警处理流程，对电源进行全方位安全监控。

市电监控主要监控输入市电的线电压、相电压、相电流及频率等内容，防止市电电网的波动与干扰波及到电源安全。

配电监控主要监控机房配电情况，包括各路配电的电学指标，主要包括线电压、相电压、相电流、频率、有功功率、无功功率、功率因数、正有功电能、负有功电能等。

UPS 监控主要监控输入电压、输入电流、输入频率、输出电压、输出电流、输出频率、有功功率、无功功率、有功电能、无功电能、UPS 工作状态、逆变器状态、整流器状态、蓄电池状态、空开状态及其它部件工作状态等。

蓄电池监控主要监控蓄电池组电压，组电流和单体电压、温度及内阻等。平台根据单体电压、温度及内阻等信息，提供蓄电池单体工作状态评价功能，当平台侦测到蓄电池单体因老化，损毁等原因不能正常工作，需要更换时，会及时通知管理人员，进行蓄电池单体更换。

开关电源监控主要监控开关电源的输出电压、输出电流、输出是否过压、输出是否欠压、输入是否过压、输入是否欠压、是否过流、是否过热、是否限流、运行 / 停止等信息。

1.1.3 设备安全监控

防盗防毁功能包括防止设备遭受非法盗窃和防止设备被恶意损毁两部分。当有设备盗窃损毁的行为发生时，平台会及时触发告警，通过平台界面及短信等第一时间通知管理员，根据逻辑配置亦可执行联动动作，调用相应区域安防系统摄像头进行录像、抓拍、跟踪及播放警告语音等，确保设备安全。

计算机及其外部设备在工作时能够通过地线、信号线、电源线、寄生电磁信号或谐波将秘密信息辐射出去，造成电磁泄漏，危害信息安全，必须对计算机电磁泄漏引起足够的重视与关注。平台通过屏蔽与干扰两种方式，防止设备电磁泄漏的发生。

为保障设备安全、稳定、高效的提供服务，平台支持设备状态监测功能，主要监测设备对象包括主机服务器、数据库、网络设备、安全设备、中间件及存储设备等。通过对监测设备进行实时监控和

全面管理，及时掌握信息系统的运行状态和存在的安全隐患并及时进行闭环处理。

通过维护日历功能，平台提供对设备维护工作的统一规范管理，确保设备维护工作及时开展，保证维护设备对象不缺不漏，维护内容不缺不漏。平台根据维护计划安排，自动将维护日期、维护对象及维护内容等维护任务信息通过系统短息及电子邮件等通知到相应的工作人员。维护人员完成维护工作后，将维护结果录入维护日历，确保维护工作流程完整、规范、闭环。

平台在设备防盗防毁、防电磁兼容、状态监测、维护日历等安全监测过程中，会自动生成若干日志信息，供工作人员浏览查询，方便故障定位、问题追踪及事故追责等。对于管理人员确认有必要录入平台的设备日志信息，系统提供录入界面，方便录入，为设备物理安全提供更全的数据支持。

1.1.4 通信线路安全监控

防线路截获主要用来防止通信线路中传输的信息被非授权截获，保障敏感信息在传输过程中的安全性。采用相关信息安全技术手段，当探测到线路截获时，首先发现线路被截获并告警然后定位线路截获，发现线路截获设备工作的位置。

抗电磁干扰主要采用接地、屏蔽及滤波 3 大技术手段，提高通信线路抗电磁干扰能力。平台通过在接地处、屏蔽箱体等关键位置设置电磁分析仪，实时对电磁强度进行监控，当电磁强度超过设定阀值时，主动报警，提示工作人员进行巡查处理。

由于防线路截获、抗电磁干扰安全侦测技术手段的局限与不足，通信线路安全主要采用人工巡检的方式来进行保障。平台提供巡检日历功能，根据巡检计划的安排，平台自动将巡检日期、巡检对象及巡检内容等巡检任务信息通过系统短信及电子邮件等通知到巡检人员。巡检人员进行巡检，巡检完成后，将巡检结果录入巡检日历并及时处理巡检过程中发现的问题，确保巡检工作流程完整、规范、闭环。

1.1.5 媒体安全监控

为保障媒体的存放安全和使用安全，媒体的存放和管理应有相应的制度和措施。 为了保证媒体安全，平台从媒体保管、数据安全及管理日历 3 方面，对媒体安全进行辅助保障。

媒体保管主要包括媒体防盗、防毁及防霉 3 部分内容，平台提供媒体保管信息录入功能，用于记录媒体编号、种类、数量、持有人、存放位置等内容。通过加装声磁条码，平台支持声磁防盗功能。

数据安全主要包括数据防拷贝、数据防消磁及数据防丢失等内容。通过专用媒介、软件监控及定期备份等措施与手段，防止数据被拷贝、消磁及丢失。

管理日历主要用于记录媒介使用情况追踪、备份提醒等功能，包括使用时间、使用人、使用地点、使用内容等信息。根据媒介的备份计划与备份周期，平台会发出备份提醒，及时通知媒体管理人员。

1.1.6 物理安全评测

在环境安全监控、电源安全监控、设备安全监控、通信线路安全监控及数据安全管理过程中，监控平台会适时产生告警、恢复及通知等系统消息，为方便用户操作，平台提供系统消息功能，提供统一的查询浏览处理入口。

根据统计周期的不同需要，平台可以生成日报、周报、月报、年报等各种统计周期的统计报表。统计报表可以根据用户的不同要求进行私有化定制。平台统计报表支持导出功能，支持多种导出格式。

平台针对当前物理安全的监控情况，提供评测打分功能，通过对当前物理情况进行打分与评测，直观量化物理安全状态，并指出安全风险与改进措施。

平台依据物理安全的历史监控数据，结合相关算法，提供物理安全预测分析功能。该功能主要包括风险分析、关联分析及态势分析等分析内容。根据分析结果，平台提供专家级的改进建议及改进措施，供相关人员参考引用。

为了方便相关人员检索物理安全相关标准，快速学习相关标准，平台提供标准检索功能，检索内容包含了当前物理安全相关标准的全部内容。标准内容可以在线升级与更新，方便管理。

1.1.7 系统管理

系统管理完成监控平台自身管理功能，包括用户管理、角色管理、权限管理、系统配置日志查询等。

用户管理包括创建用户、编辑用户、删除用户、创建用户组、编辑用户组、删除用户组等功能，完

成平台操作人员的定义。

角色管理包括创建角色、编辑角色、删除角色等，完成操作角色的定义。根据平台部署规模和管理实际情况，定义若干角色。

权限管理包括对角色授予权限、修改权限及回收权限等操作。平台权限完全定义在角色之上，通过对不同的角色分配不同的相应级别的权限，实现控制用户行为的目的。

系统配置主要用于完成监控对象管理、监控策略管理、存储策略管理及系统参数配置等工作。监控对象管理包括编辑监控对象信息，修改监控对象监控参数，添加、修改、删除监控对象监控指标阀值等。监控策略管理包括编辑报警策略和定义告警事件级别等。存储策略管理包括编辑监控指标存储频率，编辑告警记录存储周期，编辑历史数据库连接地址等功能。系统参数配置提供对平台正常运行必须设置的参数的编辑修改功能。

为保障平台自身安全，平台对用户所做的所有操作行为，均会记录操作日志。操作日志支持多种查询条件下的组合查询功能，方便平台管理员跟踪用户操作行为，为责任追查，事故定性提供必要信息。

1.2 系统架构

结合物理安全特点及日常管理实践，平台采用分散式控制，集中式管理的设计原则进行架构。平台从下到上可以依次划分为远端设备层、远程终端处理层、业务应用层及 GUI 表现层 4 层。平台系统架构如图 2 所示。

远端设备层主要包括各种监控设备、采集卡、传感器、变送器及现场总线等。通过现场总线将各种监控对象，构建成具有全分散、全数字化、智能、双向、互联、多变量特点的现场网络。远端设备层位于整个系统结构的最底层，构成了整个平台的基础设施部分 [4]。

远程终端处理层通过现场网络，完成与远端设备层各种监控对象的双向数据通信。(1) 远程终端处理层周期性从下层采集数据，格式化后临时存储于本地，等待上层请求获取。(2) 远程终端处理层转发上层控制命令给相应的监控对象，并将执行结果反馈给上层。远程终端处理层发起接口调用，远

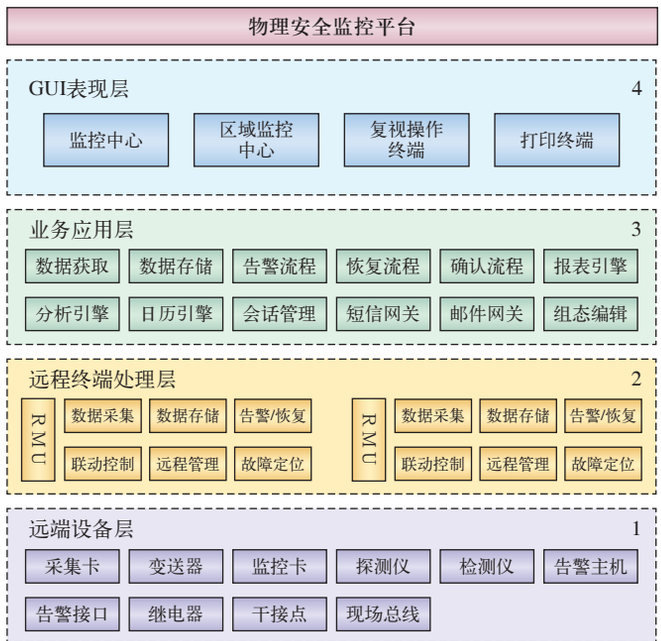

图2 平台系统架构图

端设备层为其提供服务。

远程终端处理层所需要的逻辑功能，由一体化的嵌入式专用设备—远程监控单元（RMU）来提供物理实现。RMU 拥有各种电气规格的物理接口及扩展插槽，以满足现场总线搭建的需要。 RMU 是现场总线对上层提供服务的网关接口，它屏蔽掉了现场总线内部纷繁复杂的物理接线，异构网络等技术差异。RMU 是整个平台中最为关键、最为核心的专用设备，在整个平台中发挥着不可替代的作用。

业务应用层完成各种监控业务的处理，平台的全部业务流程都在此层实现，是平台的核心处理层。主要包括监控数据处理、业务流程执行、用户操作响应及历史数据的统计分析预测和知识挖掘等。监控数据处理包括监控数据的获取、格式转换、持久化存储等。业务流程主要包括告警流程、恢复流程及确认流程等。业务应用层采用模块化设计，降低各种应用间的耦合度，提高应用内的内聚性，确保关键性应用的事物完整性。

GUI 表现层对平台不同级别、不同角色的用户提供权限范围内的平台操作途径与手段，完成整个监控平台的人机交互。GUI 表现层必须坚持从用户角度出发，使用用户术语开展的设计原则。

需要强调的是物理安全是相对的，平台根据安全等级分类的不同，综合考虑需要保护的硬件、软件

及其信息价值，采用不同规模与强度的保护措施。

1.3 网络方案

平台整个网络由监控中心、区域监控中心以及现场网络3级构成，形成一个以监控中心为根节点，监控对象为端节点的大型星形网络拓扑结构，该拓扑结构具有结构简单、维护方便、扩展性强以及任何网络节点发生故障均不会波及到整个网络的特点，对平台稳定运行提供有力通信保障。

平台网络方案属于典型的混合型网络，通过综合运用Internet、E1、RS232、RS485及CAN等网络，实现监控中心、区域监控中心及各监控站点间数据传输。监控中心与区域监控中心，区域监控中心与现场远程监控单元（RMU）之间采用Internet、E1等网络并结合VPN技术进行数据传输，RMU与监控对象之间，灵活选用数字量、模拟量和串口通讯的通信方式进行组网，完成现场网络的设计。综合监控平台网络结构如图3所示。

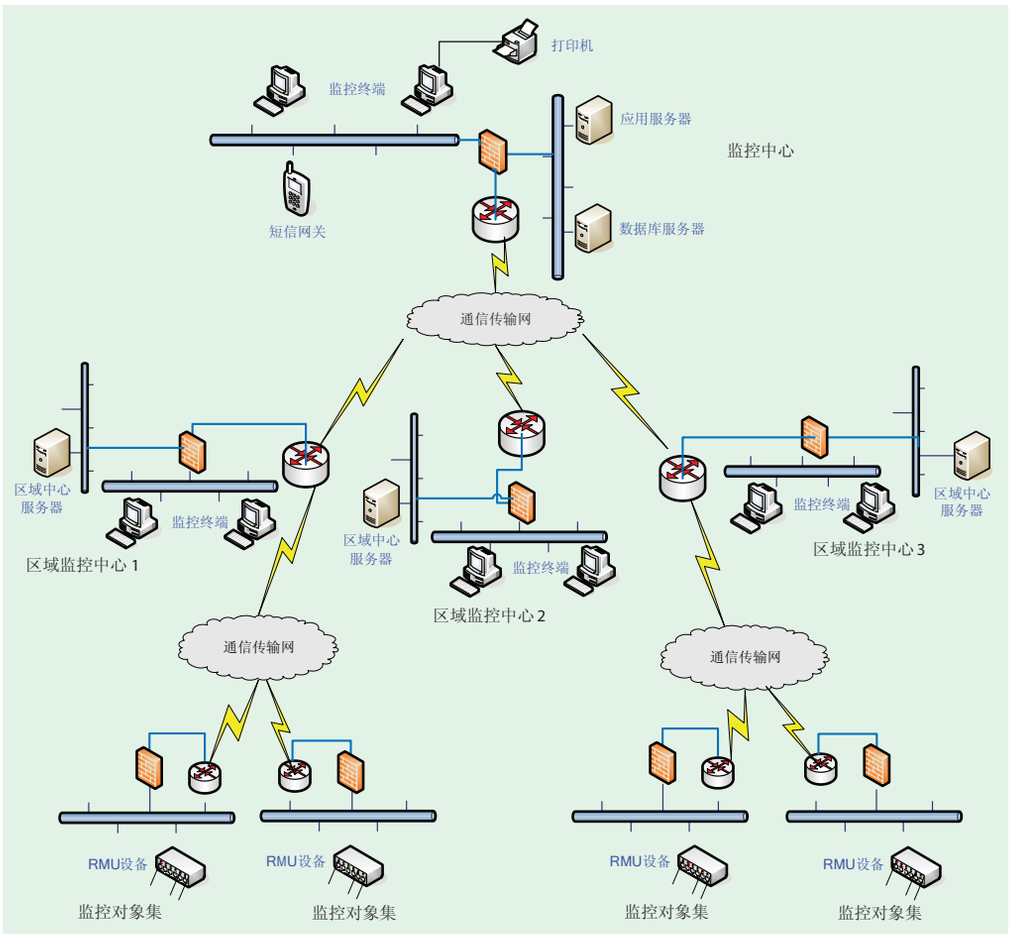

图3　平台网络结构图

2 关键技术

2.1 远程监控单元（RMU）设计与实现

远程监控单元作为平台最关键的设备，必须从功能需求与非功能需求两个角度进行设计与实现。

功能需求主要包括物理接口广泛全面，种类丰富扩展性强，具备数据预处理、格式化及存储功能，具备Web远程管理与控制功能。支持平台通信协议栈，完成数据采集，控制命令应答，告警数据上报等。

非功能需求主要包括产品可靠性、稳定性、免维护性及易扩展性等关注点，通过添加硬件监控狗，增加守护进程，合理优化产品架构，调优内核，加强质检与测试等技术与手段，保障非功能性需求得到满足与实现。

2.2 平台通信协议的设计与实现

鉴于物理安全内容丰富，体系众多，分类庞杂的事实，平台通信协议的设计与实现就显得十分重要与关键。平台采用非面向连接的UDP报文进行通信。报文包括：控制报文、数据报文、告警报文及协议内部报文等4类。通信协议支持错误处理机制，错误分级分类，保证容错容灾。通信协议采用CRC进行数据校验，采用BER编码进行二进制编码。平台通信协议栈，统一封装成API动态链接库供通信主体调用。

2.3 基于多线程的监控数据采集处理技术

为保证监控数据的实时性，平台采用多线程进行监控数据的并发采集。平台内每个监控进程在程序

（下转P27）