绿色数据中心机房智能监控技术及应用

余长庚 著

Technology and Application of Intelligent Monitoring System for Green Data Center Computer Room

華中科技大學出版社
http://www.hustp.com

国家自然科学基金项目“绿色数据中心的热量管理关键问题研究”（61540055）
贺州学院博士科研启动基金项目“绿色数据中心的热量管理关键技术研究”（HZUBS201506）
资助出版

绿色数据中心机房智能监控技术及应用

Technology and Application of Intelligent Monitoring System for Green Data Center Computer Room

余长庚 著

华中科技大学出版社
http://www.hustp.com
中国·武汉

内 容 简 介

本书从数据中心机房监控系统架构入手，以研发支持多样性差异化设备快速接入、满足用户自定制监控需求、具有设备可信增强功能的智能机房监控系统为目标，重点开展数据中心机房监控系统的自定制技术、可信技术与评价方法研究及应用。主要内容包括智能绿色数据中心机房监控系统的内涵，基于大批量定制的绿色数据中心机房的自定制机理与方法，绿色数据中心机房的用户身份认证的可信技术方法等。介绍了绿色智能机房监控系统，在该绿色智能机房监控系统架构上实施用户自定制技术、可信增强技术模块功能，并测试各项技术及整个系统的应用效果。

本书可作为高等院校电子信息、通信、测控技术及仪器、物联网、信息安全、计算机等专业的博士生、硕士生和本科生的教科书，也可供相关工程技术人员参考。

图书在版编目(CIP)数据

绿色数据中心机房智能监控技术及应用/余长庚著. —武汉：华中科技大学出版社，2017.5
ISBN 978-7-5680-2692-5

Ⅰ.①绿… Ⅱ.①余… Ⅲ.①机房管理-安全监控系统 Ⅳ.①TP308

中国版本图书馆 CIP 数据核字(2017)第 068140 号

绿色数据中心机房智能监控技术及应用

Lüse Shuju Zhongxin Jifang Zhineng Jiankong Jishu ji Yingyong

余长庚 著

策划编辑：牧 心
责任编辑：苏克超
封面设计：饶 益
责任校对：马燕红
责任监印：周治超
出版发行：华中科技大学出版社(中国·武汉) 电话：(027)81321913
武汉市东湖新技术开发区华工科技园 邮编：430223
录 排：华中科技大学惠友文印中心
印 刷：湖北新华印务有限公司
开 本：710mm×1000mm 1/16
印 张：8 插页：1
字 数：145 千字
版 次：2017 年 5 月第 1 版第 1 次印刷
定 价：36.00 元

前　言

数据中心是我国实现经济转型升级的重要基础设施，它提供的巨大数据处理能力是国家战略资源，是实现智能制造、互联网＋、物联网、云计算、大数据等技术和应用的基础保障，同时因其巨大的能源消耗和对环境的影响，使绿色数据中心成为《中国制造 2025》中绿色制造中的重点领域。数据中心在我国未来一个时期内将持续快速发展，同时需进行有效管理以实现其低碳、绿色、可持续发展。绿色数据中心采用智能监控技术，不仅可提高质量与效益，而且可实现节能降耗，更重要的是它使生产更加安全，使环境更加舒适。因此，迫切需要通过专门的工作来寻求绿色数据中心机房监控的基础理论创新与应用。

本书从数据中心机房监控系统的自定制技术、监控系统的可信技术方法等方面，综述国内外研究进展，确定研究内容。第 1 章主要讲述智能绿色数据中心机房监控系统的内涵；第 2 章主要讲述基于大批量定制的绿色数据中心机房的自定制机理与方法；第 3 章主要讲述绿色数据中心机房的用户身份认证、完整性等可信技术方法；第 4 章主要讲述绿色数据中心机房智能监控技术应用，研制绿色智能机房监控系统，在该绿色智能机房监控系统架构上实施用户自定制技术、可信增强技术模块功能，并测试各项技术及整个系统的应用效果。

本书是作者长期从事数据中心机房监控系统，特别是数据中心机房监控系统自定制、可信性研究工作的方法和应用成果的总结，本书所研究的技术已应用到实际数据中心机房运行，这些实践工作对本书的形成具有十分重要的意义。

本书在撰写过程中，得到了华南理工大学刘桂雄教授的悉心指导和大力支持，在此表示诚挚的谢意！

本书的研究与出版工作得到了国家自然科学基金项目(61540055)、贺州学院博士科研启动基金项目(HZUBS201506)的资助，在此表示衷心的感谢！

由于作者水平有限，加之智能监控技术研究仍处于不断发展和变化之中，书中错误和不足之处在所难免，恳请专家、读者指正。

作　者

2017 年 3 月

目　录

第 1 章　智能绿色数据中心机房技术概述

随着信息技术的发展，大量数据集中已成为一种趋势，用户对数据交互的实时性要求，使得越来越多服务机构纷纷建立以数据集中为核心的数据中心机房，其建设市场需求逐年上升，现代机房特别是刀片服务器被普遍使用，其功率密度越来越高。[1-2]传统机房监控系统设计理念已不适合现代大规模数据中心机房现状[3]，机房运行费用所占比重大、使用效率低。在这种情况下，建立数据中心机房动力环境集中、主动、智能监控系统，保证机房设备安全可靠运行显得十分必要。

面临监控系统市场的巨大需求，市场上出现了参差不齐的监控产品，监控设备的异构性、用户需求的多样性，需要监控系统满足用户个性化定制的需求；监控系统在系统功能更强、使用更加灵活、性能更高的同时，面临着安全、服务质量保障等方面的挑战[4]，对监控系统完整性、可靠性保护和身份认证的实现和测评方法等，必须予以足够重视；随着数据中心规模不断扩大，电能消耗量急剧上升，需要研究满足设备、人员需求下的机房系统的环境、能效分析方法，为机房的绿色节能打下基础。

笔者以“绿色数据中心机房智能监控技术及应用”为题，从研发支持多样性差异化设备快速接入、满足用户自定制监控需求、具有设备可信增强功能的智能机房监控系统等方面，重点开展数据中心机房监控系统的自定制技术、可信技术与评价方法及应用研究。该研究对促进制造信息化、智能技术的发展，具有重要学术价值与实际意义。

1.1　智能绿色数据中心机房监控系统概述

为了更好地论述智能可信绿色数据中心机房监控系统国内外研究进展，有必要对数据中心机房监控系统的有关概念、通用要求、发展趋势等作简要阐述。

1.1.1　数据中心机房监控系统有关概念

数据中心机房是为单个或多个企业的数据处理、存储、通信设施等提供存放空间的一个或联网的一组区域[5-6]，机房设计既要考虑机房内设备的正常运行需要，又要考虑工作人员身心健康的需求。

数据中心机房监控系统(Datacenter Computer Room Monitoring System,DCRMS)主要是指对数据中心机房的动力设备、环境、安防参数进行集中监测与控制的系统,其目的是为机房内设备的正常运行创立条件,提高数据中心机房的科学管理水平。数据中心机房监控集成了传感技术、自动控制技术、网络技术、通信技术和计算机技术等。数据中心机房监控系统首先应用传感技术进行设备数据采集,同时应用自动控制技术对设备进行控制,然后应用网络技术进行系统组网,应用通信技术进行数据传输,应用计算机技术进行数据处理、存储及系统定制、维护,最终运用人机交互技术表现出来。其中,动力监测参数为:①发电机状态监测;②UPS(不间断电源)状态参数监测;③蓄电池状态参数监测;④市电供配电参数监测(包括市电电量参数开关状态);⑤PDU(电源分配单元)参数监测(包括机柜内电压、电流、温湿度)。环境监测参数为:①漏水存在监测与位置定位;②温湿度监测;③新风机开关状态监控;④精密空调监测(室内制冷、除湿、送风状况)。安防监测参数包括:①消防监测(火警状态);②安全门禁系统(关键门位的出入控制);③视频监测。

图 1-1 为数据中心机房监控系统 DCRMS 组成结构框图。[7]

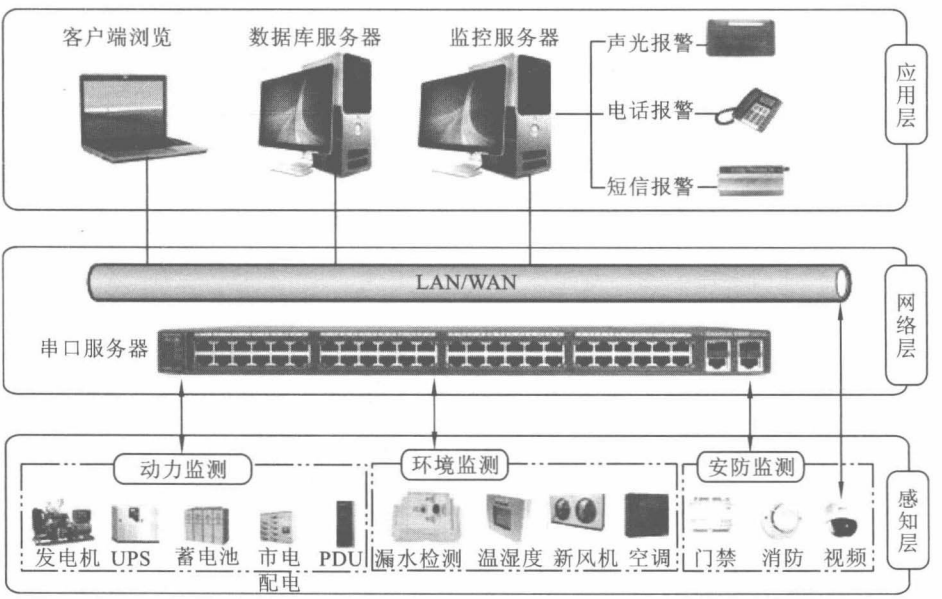

图 1-1 DCRMS 组成结构框图

监控平台由感知层、网络层和应用层等三部分组成。①感知层。由动力监测、环境监测、安防监测的各种智能传感器、I/O 控制模块等组成,直接连接各种被监

控设备，主要实现对机房动力、环境、安防状态和参数的智能感知识别、信息采集处理和自动控制。②网络层。由互联网/局域网、串口服务器等组成，实时将感知层采集到的监控数据转换成 TCP/IP 格式的数据上传给监控服务器，同时接收由监控服务器发出的控制命令并传输到现场设备。③应用层。主要由监控服务器、数据库服务器等构成，负责对机房动力、环境、安防进行集中监控管理，接收网络层传来的各种实时数据，显示监控画面，实现对数据的实时处理分析、存储、显示和输出等功能，处理所有的报警信息，记录报警事件，通过手机短信等输出报警内容，发送管理人员的控制命令等。[8-9]

1.1.2　智能绿色数据中心机房监控系统的通用要求

对于数据中心机房监控系统(DCRMS)，必须具有可靠性、实时性、安全性、可维护性和可扩展性等方面的通用要求。

可靠性(Reliability)是指 DCRMS 在规定时间内、规定条件下保持系统规定功能的能力，即保持正常运行的能力。[10-11] 监控系统要求具有极高的可靠性，否则会影响到监控系统的稳定性和数据的安全性。高可靠性要求监控系统的软硬件要合理，选用高可靠的工业级设备，保障系统 7×24 小时不间断运行，系统平均无故障时间要长；系统符合电磁兼容性和电气隔离性的设计要求，不会影响被监控设备的正常工作；监控设备具有良好的接地，抗干扰能力强；系统具有自诊断功能，对软硬件故障能够自动重启恢复。

实时性(Real Time)是指规定时间内监控系统的反应能力。[10] 实时性主要包括：遥控命令在监控系统中的传送时间；设备变化、状态变化信息在监控系统中的传送时间。如前端采集设备变化在监控系统中的传送时间应小于 2 秒，远程监控数据刷新时间小于 4 秒，短信、电话报警发出响应时间小于 30 秒。

安全性(Safety)是指确保监控系统正常运行，使它不会因为自然和人为因素而受到破坏。[10-11] DCRMS 应提供多种安全保护措施，例如，具备密码保护机制，对通信数据进行加密，系统具有多级权限管理，系统无人操作一定时间后可自动注销、锁定。能对异常情况进行分析、记录，对紧急情况予以报警。防止硬件单元更换、软件代码篡改和恶意程序注入。

可扩展性(Extensibility)是指监控系统能快速适应机房的监控环境多变性、监控设备异构性和用户需求多样性的需求。由于机房的监控容量以及监控设备的数量、厂家、协议等随时变化，监控系统能根据实际需要对机房环境与设备进行自定

制，在监控环境发生改变时只需要有针对地进行修改，不会影响整个监控系统的运行，满足用户监控智能化的要求。监控系统支持 RS232/485/422、TCP/IP、SNMP、OPC、DDE、MODBUS 等各种标准化协议和接口，可快速、方便地将各种监控对象集成到系统中。

可维护性(Maintainability)是指在规定条件下，按规定程序和手段实施维修时，设备或系统保持或恢复执行规定功能状态的能力。[12] 要保证平均故障修复时间尽可能短，且修复后运行状态和精度不受影响。

1.1.3 数据中心机房监控系统的发展动态

数据中心机房监控系统是伴随着数据中心机房的发展而发展的。20 世纪 80 年代末，我国开始大力发展通信行业，向国外一些厂商大规模地采购通信设备。但由于通信设备种类繁多，且设备的智能化自诊断程度不高，再加上世界各厂商通信设备生产也处于初级阶段，设备制造无统一的标准，这样一来就加大了后期的维护难度。如何对这些通信核心设备进行关键保障，快速发现故障、排除故障，成为一个新的课题。

第一代监控系统只是完成了集中监控功能，还未形成独立的监控系统，早期监控系统主要是对少量干节点运行信息进行简单监测，设备、环境参数信息是混合在传输设备中进行传送，监控系统只提供简单信息来反映设备运行情况。此监控方式下，机房维护人员只能知道少量设备信息，但不能准确确定设备故障位置。较少的采集点，使得在实际应用中无法判断设备故障原因。而且当发生故障时，往往供电也同时出现问题，无法依靠监控系统去排查故障，也就无法减轻现场维护人员的工作强度，保障力度非常有限。

经过近些年的发展，监控系统的规模、技术都取得很大进步。如第二代机房监控系统能监测动力和环境方面的模拟量、开关量，系统根据采集数据能对设备进行相应遥测、遥控和遥调，监控系统存储设备运行期间采集数据，运行维护人员通过采集数据来分析设备状况，如根据机房电池的充放电情况，可进一步分析电池的性能等。1992 年邮电部设计院和广州市电信局成立项目组，成功完成对广州长途枢纽楼开关电源设备的集中监控，为第二代监控系统奠定了坚实的基础，积累了宝贵的经验，基本实现了机房 24 小时无人值守。

随着计算机网络技术快速发展，机房监控系统由第二代客户机/服务器(C/S)结构向第三代浏览器/服务器(B/S)结构发展，现在监控体系管理方式更加先进，借

助全新的软件体系构建技术，将监控对象的监控设备在一套完整监控系统中进行监测与控制。[13] 最近几年，机房监控系统规模、数据逐渐增加，系统实时性、可靠性有了很大提高，技术更加成熟，相关技术规范也日益完善，产品走向市场的过程更加规范化。

目前国际上已有许多机房监控系统产品，如艾默生 PSMS 动力环境集中监控系统，适用于通信机房、通信局站内各种动力设备、空调设备及其环境实时监控、统一管理，开发基于 E1、IP、DDN、PSTN、ISDN、WAN 等组网方式，使用灵活；加拿大万联网络设备公司开发产品，采用 WEB 方式实现人机交互，支持 TCP/IP、SOCKET、XML 等多种标准网络协议和数据格式，可满足用户各种需求、方便进行二次开发。国内也有很多企业对极具发展前景的机房监控领域进行研究，如中兴力维公司的 E-Guard 监控网管软件采用模块化结构设计，以优化软件架构、高度可扩展性设计，实现动力和环境监控的基本功能和扩展功能。

随着科学技术的发展，机房对绿色、安全、多功能化的要求越来越高。未来机房监控朝着需求个性化、平台统一化、物联网技术融合化、监测参数多样化、能效监测分析与控制协调化方向发展。需求个性化将满足用户对监控系统设备异构性、需求多样性的要求；平台统一化下机房监控不再是单独的一个模块，它与网络监控、服务器监控、应用监控、业务监控整合起来，构成一个完整的企业 IT 管理系统；物联网技术融合化利用先进的计算机技术、控制技术和通信技术融合的物联网技术，对机房现场的环境数据进行实时高效的采集和处理，进行数据融合与挖掘；监测参数多样化实现从设备运行状态到机柜的微环境，再到机房整体环境的多层次监控、多参数监测，结合多层次阈值设置进行多层次预警；能效监测分析与控制协调化把能效监测分析与节能控制综合起来考虑，对机房的“测”和“控”进行协调，能效监控是绿色数据中心实现节能的前提和基础，使用户能够根据需求进行监控、整合、共享并匹配机房的电力资源。

1.2　智能绿色数据中心机房国内外研究进展

基于 DCRMS 的个性化要求，安全性与可靠性要求，以及能效监测分析与控制协调化发展要求，本书以研发支持异构监控设备快速接入、满足用户自定制监控需求、具有设备可信增强功能以及环境与能效分析的智能机房监控系统为目标，从 DCRMS 的自定制技术、监控系统可信性方法等方面讨论相关研究领域的国内外进展。

1.2.1 DCRMS的自定制技术

数据中心机房监控系统用户自定制是由于不同数据中心机房用户对监控系统界面有个性化要求，而且设备购置时间和厂家不同、各单位信息化程度不同，造成设备访问方式异构的需求。

数据中心机房监控系统用户自定制(Datacenter Computer Room Monitoring System Self-Customization，DCRMS-SC)技术，是指在使用DCRMS软件过程中，用户根据自身个性化要求，通过DCRMS软件平台即可自定制所需监控设备和个性化监控界面，独立完成个性化机房监控系统，在定制过程中不需依赖专业人员或开发人员重新修改代码或重新开发软件，满足DCRMS智能化要求。DCRMS-SC技术是数据中心机房监控系统发展的必然趋势。

多样性差异化设备接入集成技术是数据中心机房监控系统用户自定制DCRMS-SC技术的重要组成部分。由于监控对象设备数量大、种类多、品牌杂、型号多，或出于商业、技术考虑或历史原因，各个厂家采用的监控设备的功能、接口和协议都存在明显差异，使得整个机房监控系统搭建在一个异构平台上，加大监控系统开发的难度与复杂度。[14-15]基于设备接入技术不同，DCRMS有基于绑定驱动、基于组态技术、基于OPC技术等多样性差异化设备接入集成方式。

(1) 基于绑定驱动设备接入集成方式。基于绑定驱动监控系统软件架构如图1-2所示。DCRMS软件与监控设备连接方式是绑定驱动(Native Driver)，即针对特定硬件和目标设计专用驱动程序，驱动程序是动态链接库(Dynamic Link Library，DLL)连接动态数据交换(Dynamic Data Exchange，DDE)服务器的形式，例如专用于Modbus协议设备的监控系统等。[16]基于绑定驱动设备接入集成方式的驱动程序针对特定对象开发，当硬件设备升级、修改时，必须也要修改驱动程序，驱动开发重复性高、代价高、通用性差[17]，难以适应现代机房监控设备种类繁多的需要。

(2) 基于组态技术设备接入集成方式。组态(Configuration)是指通过配置计算机、软件使其自动执行特定操作。数据采集与监视控制SCADA的组态软件，基于强大的图形组态功能，以灵活多样的组态方式，为用户提供良好的开发界面和简捷的使用方法，主要用于工业自动控制系统的监控软件。[18]开发通用性机房集中监控软件(总体架构见图1-3)，应用工业控制组态技术，对现场设备通过高度抽象设备定义，提供灵活多样的控件、控件库，用户可根据实际需要对机房环境、设备进

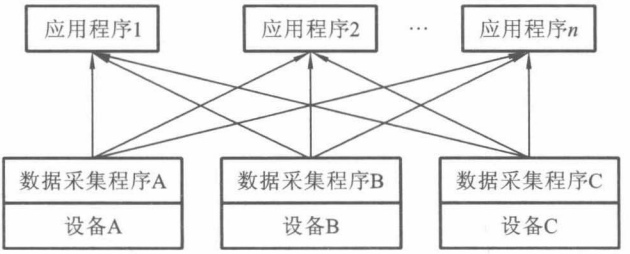

图 1-2　基于绑定驱动监控系统软件架构

行集中定制[19]。研究基于 MCGS 组态软件技术开发远程监控系统(见图 1-4),监控软件与设备接入在物理层完成,保证组态软件能够正确地与现场设备通信,使监控系统适应异构工业控制系统要求。现场设备与数据服务器通信,响应组态运行客户端请求。通过硬件组态,用户可以将现场设备与监控软件相连,监控软件自动加载相应的驱动程序动态链接库,可以按照正确通信协议获取设备数据。[20]

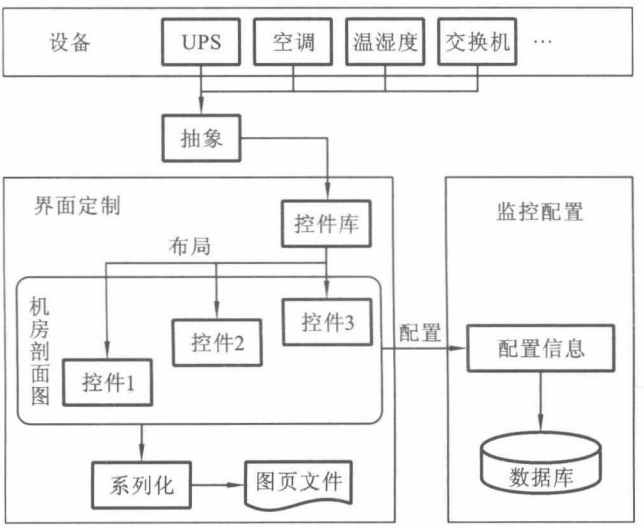

图 1-3　通用性机房集中监控系统架构

(3) 基于 OPC 技术的设备接入集成方式。为使传统机房监控系统可存取现场设备的数据信息,不同应用程序都需要编写专门的接口函数。由于监控设备种类繁多、产品不断升级,急需一种高效、可靠,具有可开发性、可互操作性的即插即用的设备驱动程序,OPC(OLE for Process Control,用于过程控制的对象链接和嵌入)标准应运而生。[21]OPC 标准是以微软公司的 OLE(Object Linking and Embedding,对

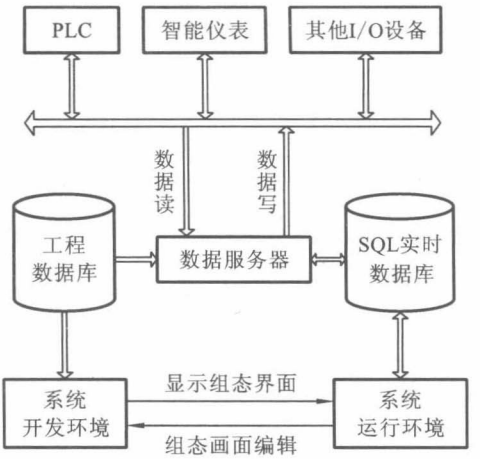

图 1-4　工业组态监控设备连接图

象链接和嵌入)、COM(Component Object Model,组件对象模型)、DCOM(Distributed Component Object Model,分布式部件对象模型)技术为基础,它的制定是通过提供一套标准的 OLE/COM 接口完成的。[22-24] OPC 采用客户/服务器模式,把开发访问接口任务放在设备厂家或第三方厂家,以 OPC 服务器形式向用户提供数据,解决了软、硬件厂商间的矛盾。

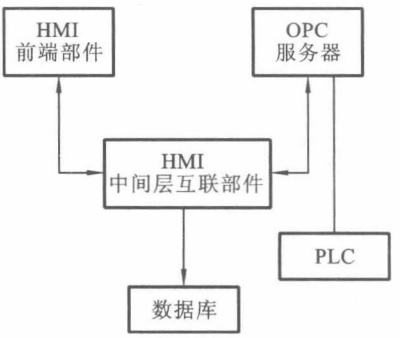

图 1-5　人机交互接口图

巴基斯坦的 M. Raafay Anwar 等(2004)基于 OPC 设计人机交互接口(HMI)(见图 1-5),包括 HMI 前端部件(提供工业化系统前端工业装置)、中间层互联部件、OPC 服务器(用来发送和接收不同参数和数值)和数据库(存储过程组件数据)等。[25] 新加坡国立大学 Jun Liu 等(2005)基于 OPC 设计实时过程监控系统(ONPS)(见图 1-6),包括平台模拟、信息数据库和高级过程监控应用三个模块,具有开放性、扩展性和设备即插即用功能。[26] 韩国的 Vu Van Tan 等(2007)研究基于 OPC 技术与 Internet 相结合的分布式远程监控系统(见图 1-7),基于 COM 的 OPC DA(OPC Data Access,OPC 数据访问服务器)规范和基于 XML 的 Web Service 技术的 OPC XML-DA,可在各种平台和 Internet 上实现数据通信。[27] 设计并实现串口设备 OPC 代理服务器(见图 1-8),设备驱动层采用 DLL、表文件方式为

设备提供驱动，OPC 服务器接口层向数据使用者提供标准 OPC 服务器接口，并向服务器读写数据，通过 OPC 代理服务器，对远程环境监控系统的各种不同监控设备进行统一管理。[28]

机房监控系统多样性差异化设备接入方法比较如表 1-1 所示。

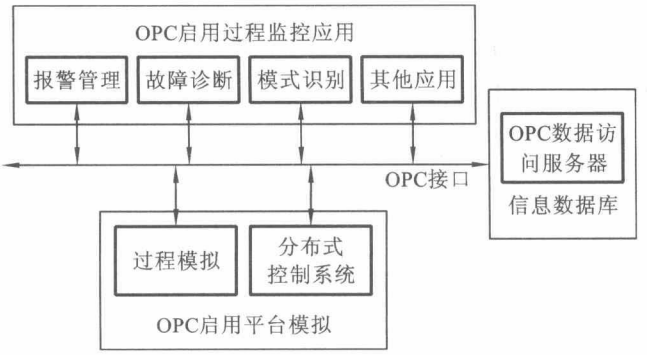

图 1-6　ONPS 系统结构图

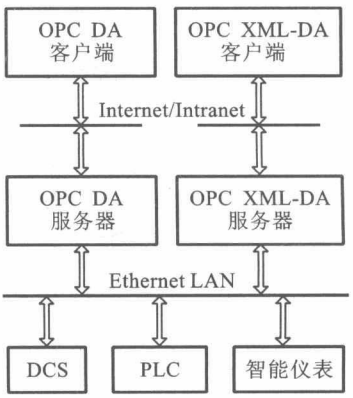

图 1-7　分布式远程监控架构

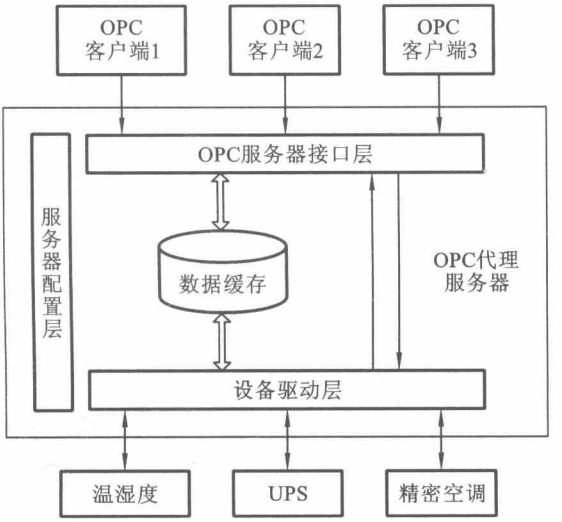

图 1-8　OPC 代理服务器整体设计

表 1-1　机房监控系统多样性差异化设备接入方法比较

接入方法	架　构	特　点
基于绑定驱动机房监控系统	针对特定硬件和目标设计专用驱动程序，采用 DLL 和 DDE 方式	针对特定对象开发，通用性差，重复开发

续表

接入方法	架　构	特　点
基于组态技术机房监控系统	采用 DLL 和 DDE 方式	架构简单，组态软件体系庞大，功能包多，价格昂贵，二次开发难度大
基于 OPC 技术机房监控系统	OPC	高效、可靠、开放、互操作性强

由表 1-1 可以看出：①针对监控系统与异构监控设备的连接要求，基于绑定驱动方式针对特定对象开发，驱动通用性差、开发工作重复性高；②现有组态软件体系结构庞大，价格昂贵，优于监测、弱于控制；③现有基于 OPC 技术的设备接入方式为数据读写提供统一的接口标准，但目前监控设备很少提供 OPC 服务接口，为适应不同监控环境，满足用户个性化需求，必须想办法将机房监控软件开发转为可重用构件大批量复用的问题。

1.2.2　监控系统可信性方法

DCRMS 可信度指 DCRMS 在监控过程中人们的预期与执行监测控制、运行维护等功能一致，产生可信监测数据结果的能力。传统数据中心机房安全技术包括物理安全、网络安全、数据安全等方面。但随着计算机和网络通信技术在监控系统领域应用，存在网络攻击、信息篡改、病毒木马等威胁，危及财产与国家政治经济安全，其结果直接影响系统可信度。[29]

图 1-9 为 DCRMS 可信度威胁因素及其相应可信技术图。感知层传感器设备存在硬件单元更换及固件篡改替换的威胁；应用层信息处理与计算平台软件面临代码修改、恶意程序注入威胁；平台数据面临标定参数篡改、监测数据截取更换的威胁；网络层传输网络方面存在非法操作、身份冒充威胁。

其中，硬件单元及固件、软件代码更换与篡改属于 DCRMS 平台完整性问题；网络的非法入侵及身份冒充行为影响平台内主体身份的可信度；监测平台数据截取、标定参数篡改影响平台数据的可信度。可从完整性验证方法、身份认证技术、数据保护方法等方面提高 DCMRS 平台的可信度。

（一）完整性验证方法

DCMRS 完整性验证是指通过对硬件、软件等模块在不同时期的不变特征值比较来判断模块是否已被更改。[30]若特征值一致，则 DCMRS 系统完整、安全；若不一致，则完整性发生了改变，通过分析改变部分，可判断受损的程度和范围。其

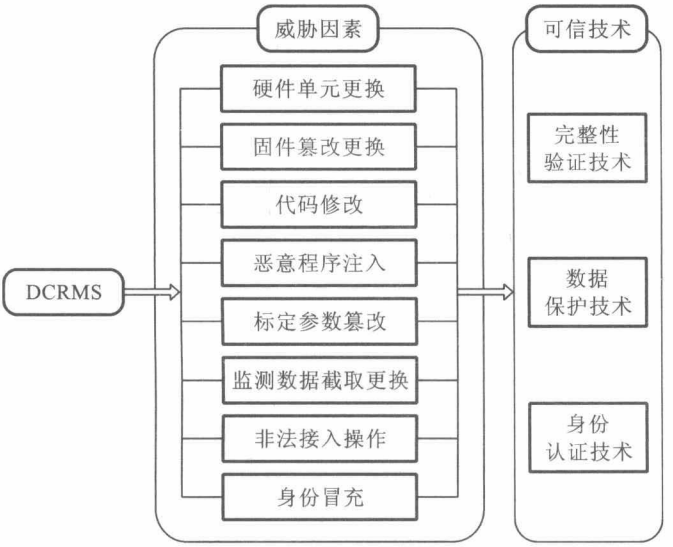

图 1-9　DCRMS 威胁因素及其相应可信技术

中，感知层设备保持完整是指监控设备的电子线路、硬件逻辑、固件代码等不变属性均未遭非授权更改，与预期状态、数值保持完全一致，监控设备完整性监控是指实时验证各不变属性实际状态值与预期值是否一致。由于电子线路、硬件逻辑状态难以直接读出并表示成数值形式，通常仅将设备标识码、模块防伪码、接口物理地址、保护锁状态、固件代码、标定参数等作为完整性监控用的不变属性。完整性验证原理为比较监控设备的不变属性值、监控服务器采集的数据等在不同时期的不变特征值，确定设备是否更换、数据是否更改。

图 1-10 为基于散列函数的数据完整性验证原理图。设监控设备不变属性集为 $FS=\{F_1,F_2,F_3,\cdots\}$，监控服务器采集的数据集为 $DS=\{D_1,D_2,D_3,\cdots\}$，监控系统完整性监控的不变属性 $MS=FS||DS$，在时刻 T 的实际不变属性为 MS_1。实际应用中都是先调用散列算法，将不变属性融合成一个完整参考值 $h(MS)$，在时刻 T，将待验证的不变属性状态融合成一个完整性验证值 $h(MS_1)$，通过比较散列函数的散列值 $h(MS)$ 和 $h(MS_1)$，来判断感知层的完整性状态。

针对散列函数，国内外学者进行了大量研究。Ron Rivest(1992)开发 MD5 算法，通过对原始数据进行填充及块处理，将任意长度原始数据映射为 128 位消息摘要。[31] 由于 MD5 算法安全性(单向性、碰撞性和雪崩效应)高，广泛应用于数据完整性验证及加密场合；美国国家标准与技术学会 NIST 和美国国家安全局 NSA (1995)以联邦信息处理标准(FIPS PUB 180)形式发布系列安全散列算法(Secure